



ISSN 3044-6104

DEFENSE AND SECURITY CONFERENCE

Proceedings of the
Defense and Security Conference

Vol. 2, No. 1, pp. 1-360
24 April 2026, Zagreb, Croatia

www.sois-ft.hr



DR. FRANJO TUĐMAN
DEFENSE AND SECURITY
UNIVERSITY

Dr. Franjo Tuđman Defense and Security University
Institute for Security and Defense Studies
Zagreb, Croatia

Proceedings of the Defense and Security Conference

Vol. 2, No. 1, pp. 1-360

2026, Zagreb, Croatia

Published by:

Dr. Franjo Tuđman Defense and Security University, Zagreb, Croatia

For the Publisher:

Ivica Lučić, PhD, Rector of the Dr. Franjo Tuđman Defense and Security University, Zagreb, Croatia

Editors:

Dražen Smiljanić, PhD, Dr. Franjo Tuđman Defense and Security University, Zagreb, Croatia

Andrej Razumić, PhD, PhD, Dr. Franjo Tuđman Defense and Security University, Zagreb, Croatia

Dijana Gracin, PhD, PhD, Dr. Franjo Tuđman Defense and Security University, Zagreb, Croatia

Design:

Dražen Smiljanić, PhD, Dr. Franjo Tuđman Defense and Security University, Zagreb, Croatia

Marin Musa, dipl. graf. ing.

Print:

Croatian Defense Academy Dr. Franjo Tuđman, Zagreb, Croatia

ISSN 3044-6104

Conference proceedings are indexed in databases listed on the official web conference page: <https://www.sois-ft.hr/dsc/proceedings>

All papers included in these proceedings were written in English and subjected to an international, double-blind peer review process. Each paper was presented in English at the conference.

Program committee:

Asst. Prof. Janko Bekić, PhD, Dr Franjo Tuđman Defense and Security University, Zagreb, Croatia (Committee Chair)

Asst. Prof. Andrej Razumić, PhD, Dr Franjo Tuđman Defense and Security University, Zagreb, Croatia (Committee Co-Chair)

Asst. Prof. Daniel Pugar, PhD, Dr Franjo Tuđman Defense and Security University, Zagreb, Croatia (Committee Co-Chair)

Prof. Shlomo Shpiro, PhD, Bar Ilan University, Ramat Gan, Izrael

Prof. Iztok Podbregar, PhD, University of Maribor, Slovenia

Prof. Giray Sadik, PhD, Yildirim Beyazit University, Ankara, Turkey

Prof. Marco Lombardi, PhD, director of ITSTIME Research Center, Catholic University of Sacred Heart, Milano, Italy

Prof. Alexandra Gasztold, PhD, War Studies University, Warsaw, Poland

Prof. Giliam de Valk, University of Leiden, Netherlands

Prof. Iztok Prezelj, PhD, University of Ljubljana, Slovenia

Prof. Polona Šprajc, PhD, University of Maribor, Slovenia

Prof. John M. Nomikos, PhD, Research Institute for European and American Studies, Athens, Greece

Assoc. Prof. Thomas Wegener Friis, PhD, University of Southern Denmark, Denmark

Assoc. Prof. Maksym Kamenetskyi, PhD, Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

Assoc. Prof. COL Ian Mazal, PhD, Department of Military Robotics at the University of Defence in Brno, Czechia

Assoc. Prof. Dijana Gracin, PhD, Dr Franjo Tuđman Defense and Security University, Zagreb, Croatia

Anders Strindberg, PhD, Swedish Defence Research Agency-FOI, Sweden

Assoc. Prof. Igor Štambuk, PhD, Dr Franjo Tuđman Defense and Security University, Zagreb, Croatia

Domagoj Ćorić, MSc, Dr Franjo Tuđman Defense and Security University, Zagreb, Croatia

Arijana Marjanović, MSc, Dr Franjo Tuđman Defense and Security University, Zagreb, Croatia

Organizing committee:

Prof. Željko Dobrović, PhD, Dr Franjo Tuđman Defense and Security University, Zagreb, Croatia (Committee Chair)

Assist. Prof. Dražen Smiljanić, PhD, Dr Franjo Tuđman Defense and Security University, Zagreb, Croatia (Committee Co-Chair)

MG Gordana Garašić, Dr Franjo Tuđman Defense and Security University, Zagreb, Croatia (Committee Co-Chair)

Prof. Dragan Mišetić, PhD, Dr Franjo Tuđman Defense and Security University, Zagreb, Croatia

Martina Mak, Dr Franjo Tuđman Defense and Security University, Zagreb, Croatia

Iva Kišasondi Bašić, Dr Franjo Tuđman Defense and Security University, Zagreb, Croatia

Ante Batistić, Dr Franjo Tuđman Defense and Security University, Zagreb, Croatia

Domagoj Ćorić, MSc, Dr Franjo Tuđman Defense and Security University, Zagreb, Croatia

Lucija Pranjić, Dr Franjo Tuđman Defense and Security University, Zagreb, Croatia



© Dr. Franjo Tuđman Defense and Security University

Text © Authors & Dražen Smiljanić, 2026

This Conference Proceedings' book contains open-access articles distributed under the terms and conditions of the Creative Commons Attribution – Non-Commercial – Share Alike 4.0

International license (CC BY-NC-SA 4.0). This license allows you to share (copy and redistribute the material in any medium or format) and adapt (remix, transform, and build upon) the material. The licensor cannot revoke these freedoms as long as the license terms are followed. You must give appropriate credit, link to the license, and indicate if changes were made. You may do so reasonably, but not in any way that suggests the licensor endorses you or your use. The license does not allow the use of the material for commercial purposes. If you remix, transform, or build upon the material, you must distribute your contributions under the same license as the original.

<https://creativecommons.org/licenses/by-nc-sa/4.0/>

Contents

Foreword.....	4
----------------------	----------

Geopolitical and Strategic Dimensions of Contemporary Security	5
---	----------

Jurica Botić

THE EUROPEAN DEFENCE WHITE PAPER AND THE WESTERN BALKANS	6
--	---

Andreja Sršen

GEOPOLITICS OF CLIMATE CHANGE: THE EU'S PATH TOWARD A NEW GLOBAL SECURITY PARADIGM	25
---	----

Saša Đerić, Marijan Turkalj, Rafael Šubat, Branimir Bekavac

INTEGRATING DEFENCE AND SOCIETY: THE ROLE OF SPECIAL OPERATIONS FORCES IN NATIONAL RESILIENCE	40
--	----

Hybrid Threats, Information Operations, and Cognitive Security	61
---	-----------

Iva Kišasondi Bašić, Ivana Kovačević Bekić

CRISIS COMMUNICATION IN HYBRID THREAT ENVIRONMENTS: THE CROATIAN ARMED FORCES AND THE ZAGREB 2022 UAV INCIDENT	62
---	----

Marcin Składanowski

THE DRONE ATTACK ON POLAND (SEPTEMBER 2025) AND THE RUSSIAN DISINFORMATION CAMPAIGN: IMPLICATIONS FOR SOCIETAL RESILIENCE IN NATO STATES	83
--	----

Ines Grossi, Antonija Rimac Gelo

COGNITION IN WARFARE: CONCEPTUAL FRAMEWORK, CHALLENGES, AND IMPLICATIONS FOR NATIONAL SECURITY AND THE DEFENCE SYSTEM.....	102
---	-----

Arijana Marjanović

INSTITUTIONAL TRUST, MEDIA PRACTICES AND PERCEIVED RESILIENCE TO COGNITIVE MANIPULATION AMONG CROATIAN UNIVERSITY STUDENTS	121
---	-----

Dominik Dujić, Danijel Nekić, Tomislav Ivanjko THE ROLE OF UNMANNED AERIAL SYSTEMS (DRONES) IN CONDUCTING INFORMATION OPERATIONS: A CASE STUDY OF THE RUSSO-UKRAINIAN WAR SINCE 2022	150
Emerging and Disruptive Technologies and Warfare	174
Dinu Ștefan-Cosmin CYBER DEFENCE IN MODERN WARFARE	175
Zrinko Petener, Damir Stručić, Nikolina Mokricki AI AS A FORCE MULTIPLIER FOR FUTURE INTELLIGENCE OPERATIONS: FROM COLLECTION SUPERIORITY TO DECISION ADVANTAGE IN WAR.....	186
Ante Vučemilović ARTIFICIAL INTELLIGENCE AS A DISRUPTIVE TECHNOLOGY IN THE DESIGN OF NOVEL CHEMICAL AND BIOLOGICAL WEAPONS	213
Tomislav Sunko, Mihael Dedo, Lovro Strnad, Stipe Brnadić, Vilim Đura, Zoran Medvidović ASSESSMENT OF THE IMPACT OF UNMANNED AERIAL VEHICLES ON NAVAL SURFACE WARFARE	232
Applied Methodologies for Critical Infrastructure, Operational Systems, and Advanced Technologies	255
Alojzije Culej, Andrija Ljulj, Igor Štambuk METHODS AND APPLICATIONS OF MACHINE LEARNING FOR INTELLIGENT OBJECT DETECTION, CLASSIFICATION, AND TRACKING	256
Mario Muñoz Fernández, Nina Skorin-Kapov INITIAL DEPLOYMENT OPTIMIZATION OF TACTICAL MULTI-TECHNOLOGY TELECOMMUNICATIONS NETWORKS: A LITERATURE REVIEW	278
Josip Dorigatti CRITICAL INFRASTRUCTURE VULNERABILITY IN CRUISE SHIP OPERATIONS: STRUCTURAL PRESSURES AND RISK DIMENSIONS IN THE CENTRAL AND SOUTHERN PART OF THE EASTERN ADRIATIC	290

Ena Sarajlić, Maja Braović, Hrvoje Karna, Ljiljana Šerić, Damir Krstinić A MULTI-CRITERIA DECISION FRAMEWORK FOR ASSESSING ENVIRONMENTAL INFLUENCES ON WILDFIRE DETECTION	311
Jure Penga, Ena Sarajlić, Bruno Ševo, Željko Penga, Luka Mihanović NUMERICAL SIMULATION OF FUEL CELL INTEGRATION IN MILITARY AUV AS AN ALTERNATIVE TO BATTERY SYSTEMS.....	327
Željko Penga, Bruno Ševo, Jure Penga, Ena Sarajlić, Luka Mihanović AERODYNAMIC AND THERMAL CFD MODELING FOR PERFORMANCE ENHANCEMENT OF A PEM FUEL CELL POWER SYSTEM FOR UAVS.....	348

Foreword

We are pleased to introduce the Conference Proceedings as a follow-up to the Defence and Security Conference 2026, held in Zagreb, Croatia, on 23-24 April 2026, organised by the Dr Franjo Tuđman Defence and Security University. This second edition marks a significant milestone in fostering academic and professional exchange in defence and security studies.

This event brought together 60 esteemed authors and co-authors from six countries - Bulgaria, North Macedonia, Poland, Romania, Spain and the United States of America, - who contributed 29 scientific papers (out of which 18 is published in this issue of the *Proceedings*). The diversity of contributors and the scope of topics demonstrate a growing, shared commitment to advancing knowledge, policy, and practice in this critical domain. We are especially encouraged by the strong presence of young scientists, whose perspectives are essential in shaping the future of security and defence.

The Proceedings were structured around four thematic pillars:

- Geopolitical and Strategic Dimensions of Contemporary Security
- Hybrid Threats, Information Operations, and Cognitive Security
- Emerging and Disruptive Technologies and Warfare
- Applied Methodologies for Critical Infrastructure, Operational Systems, and Advanced Technologies

These proceedings collectively analyse current and emerging challenges, evaluate transformative forces, and propose informed strategies for enhancing future defence readiness. This broader categorisation ensures a more accurate representation of the content while continuing to highlight the value of interdisciplinary and international collaboration in addressing today's complex security environment.

We hope this publication informs, inspires, and encourages ongoing research, dialogue, collaboration, and innovation. We are optimistic that this marks the continuation of a lasting tradition of research excellence and meaningful exchange in the field of defence and security.

Editor

I

Geopolitical and Strategic Dimensions of Contemporary Security



www.sois-ft.hr

THE EUROPEAN DEFENCE WHITE PAPER AND THE WESTERN BALKANS

Jurica Botić

Dr. Franjo Tuđman Defense and Security University

E-mail: jurica.botic@sois-ft.hr

ORCID: <https://orcid.org/0000-0003-4774-4974>

Abstract

This article analyses the position of the Western Balkans within the *White Paper for European Defence – Readiness 2030* (European Union, 2025) in the context of EU acts related to common European security and defence policies. The region is framed not as a mere neighbourhood awaiting EU integration, but as a European “inner courtyard” and a geopolitical shatterbelt shaped by competing great power interests that challenge EU strategic cohesion. Integrating political geography with geopolitical realism, the study examines patterns of great power competition and balance-of-power strategies in the region. The analysis highlights the meaning of “like-minded” countries, indicating their closeness to common European policies.

The research contributes to the scholarly and policy debates on European security and defence by highlighting Western Balkan perspectives on these policies and their implications for EU enlargement. The methodology includes content and discourse analysis of the *White Paper*, focusing on the Western Balkans’ position between partnership and security vulnerability, with a comparative analysis of other recent EU documents; a secondary sources analysis of think-tank reports on the region’s alignment with European security and defence policies; and semi-structured interviews with three regional experts.

Content and discourse analysis show that Albania, Montenegro, and North Macedonia are considered “like-minded” countries, while others are not explicitly mentioned. Secondary sources indicate varying levels of alignment with EU policies. Interviews confirm various national positions on European security and defence, with alignment emerging as a key factor in EU enlargement dynamics. The research confirmed the first hypothesis: that the position of Western Balkan countries within European defence policy, as outlined in the *White Paper* (2025), is determined by their level of alignment with EU foreign and security policies. Consequently, the study also supports the second hypothesis, demonstrating that the nature of

these partnership relationships in European defence policies significantly influences EU enlargement dynamics in the Western Balkans.

Keywords: European Union, *White Paper for European Defence – Readiness 2030*, Western Balkans, Geopolitical realism, Shatterbelt theory, “Like-minded” countries, EU enlargement

INTRODUCTION

The White Paper for European Defence – Readiness 2030 (European Union, 2025) is the most recent European Union document on common European security and defence policies. Its topicality reflects not only the focus, strategies, and commitments of the European Union as a whole, but also the position and role of potential non-EU partners in such processes. The countries that the European Union recognises as part of the Western Balkans, given their geographical location, are of particular significance in assessing European defence capabilities. Namely, the Western Balkans countries are located in the literal spatial embrace of EU member states. Moreover, except for North Macedonia, which is geographically linked to the Aegean coast via Thessaloniki, the Western Balkan countries are oriented towards the Adriatic Sea, a Mediterranean gulf within the European Union. On the other hand, the Adriatic and Aegean Seas have long been part of Russia’s strategy of expanding its influence and access to the warm Mediterranean waters; consequently, the Balkans as a whole, and not just their western part, have traditionally been the focus of Russian geopolitical considerations (Cohen, 2003).

The Western Balkans must also be viewed in the broader context of global geopolitics - namely as a shatterbelt where the interests of the West, Russia, and, increasingly, China intersect. This region holds particular significance because it represents the inner courtyard of the European Union yet remains subject to various external influences, including Russian, Chinese, Turkish, and Arab interests. In the context of the war in Ukraine, this study primarily focuses on European defence policies directed against Russia and the position of Western Balkan countries within them. However, the analysis does not delve into the specific relations between the European Union, the United States, and NATO; instead, it focuses exclusively on European defence initiatives and the position of regional actors within them. It examines the level of military and defence cooperation between the European Union and Western Balkan countries to date, as well as the coordination of foreign policies between the two sides, as a basis for building trust and integrating this region into common European defence strategies.

In line with the above, the *White Paper* (European Union, 2025) is the central focus of this study, which aims to determine the position of the Western Balkans as a whole and of individual states in this most recent strategic act of European defence policy. Therefore, the first hypothesis is formulated: the position of the Western Balkan countries within European defence policy, as presented in the *White Paper* (European Union, 2025), is determined by the specific level of their alignment with EU foreign and security policies. Furthermore, based on the first hypothesis, the second posits that the nature of these partnership relationships in European

defence policies significantly affects the dynamics of European enlargement to the Western Balkans.

1. LITERATURE REVIEW

The American political geographer Cohen views the Balkans as part of a buffer zone between the sea powers and the Eurasian Heartland, suggesting that “the future may bring additional shatterbelts”, whereby “the most likely candidate is the new/old zone from the Baltic through Eastern Europe and the Balkans” (2003, p. 44). Tunjić (2004) also views the Balkans as part of the so-called “Europe-in-Between”, to which he attributes the characteristics of a shatterbelt for two key reasons: first, territorial fragmentation; and second, the conflictual nature of state borders. Recent reassessments of these theories since 2023 suggest that such classical concepts remain highly relevant in a post-globalised world, where the control of strategic “shatterbelts” is once again a primary objective of great-power competition (Topalidis et al., 2024). Gajić (2018, p. 24) concludes that “due to the force of historical events, the Balkan shatterbelt remained behind the ‘line of geopolitical conflict’ at the end of the 20th century, in the area where Atlanticism as a global geopolitical player achieved temporary relative supremacy”. At the same time, Proroković (2015, p. 167) believes that “the Atlanticist framework for cooperation in the Western Balkans is disastrous for Serbian interests”. Since the author is employed at the Serbian State Institute for International Politics and Economy, this attitude carries a more official tone.

The European Union also expects membership candidates to comply with its foreign policy. Cvetković (2022, p. 7) states that “in 2021, the EU issued 85 foreign policy declarations in total, asking the membership candidates to support the declarations. Serbia accepted with 52 declarations which is the rate of 61%”, and “the main reason is the issue of Kosovo and Metohija and the wish of Serbia to maintain good relationships with the countries which support its sovereignty [...] namely Russia (17), Belarus (4), China (3)”. This is why, Cvetković (2022, p. 7) points out, “in the report from 2021, the European Commission assessed that Serbia is moderately prepared in the area of the negotiating chapter 31 [...] mostly because of failing to harmonise with the EU foreign policy”.

In the preface to the Serbian edition of his book *Foundations of Geopolitics*, Dugin (2014, p. 6) points out that “the new world order has written off Serbia, as well as Russia”, and that “there is no place for them in the American-centric world, in the plans of unipolar globalism”. Consequently, Serbia is presented as a key country in the Balkans for Russia’s interests. The Balkans are traditionally a geostrategically vital region for Russia, and Dugin (2017) views the entire area from Russia to the Mediterranean, including the Balkans, as part of Greater Eastern Europe. This aligns with the broader neorealist observation that the international system has reverted to overt power politics, in which regional actors are increasingly pressured to choose sides within competing spheres of influence (Topalidis et al., 2024).

Apparently inspired by Dugin, Proroković, in an extremely anti-Western tone, calls for the breakup of NATO, arguing that “the Balkan issue has the capacity to help break down NATO” (2023, p. 203). The author accuses the West of destabilising the Balkans while considering Russia a stabilising factor, indeed a defender of international law. Proroković’s attitude towards the West is best outlined by the following statement: “NATO and the EU could not implement the planned de-Daytonization of B&H and force Serbia to accept the Albanian separatist creation; they could not even push through the looting of church property in Montenegro, and now they will mobilise all the Balkan nations for an exhausting ‘hybrid war’ against Russia!” (2023, p. 201). In terms of hybrid warfare, Russia’s influence in the Western Balkans has already manifested itself primarily through the use of Serbia as an entry point of Russian media into the region, and subsequently through support for pro-Serbian policies in Montenegro and Bosnia and Herzegovina, especially in the case of support for the political leadership of Republika Srpska (Ferreira da Cruz, 2021).

Abazi (2019, p. 169) highlights that “to most Albanians, Russia is the country that backed Milosevic yesterday and does not recognise Kosovo today”, thus “Albania fully aligned with EU foreign policy, including the imposition of EU-style economic sanctions on Russia”, and “pro-American sentiment in Albania is the highest in the region”. Davutoğlu (2014) indicates that US activities in the Balkans will rely on elements outside German and Slavic (i.e., Russian) influences, namely Albanians and Bosniaks. The author therefore concludes that Turkey can strengthen its position in the Balkans by coordinating with US activities in the region. Tanasković (2010) accuses Davutoğlu of being one of the main ideologues of neo-Ottomanism - that is, Turkey’s geopolitical orientation towards the restoration of influence in the former Ottoman Empire, where the Balkans are among the most strategically important regions for modern Turkey. Moreover, Turkey demonstrates significant soft power through cultural and institutional ties, often positioning itself as a regional balancer, especially in Bosnia and Herzegovina and Serbia (Vuksanović, 2023).

Furthermore, although the White Paper's narrative (European Union, 2025) primarily focuses on Russian actions, the influence of other non-European actors in the Balkans is by no means negligible. This multipolar competition reflects a shift in contemporary geopolitics, in which non-Western actors utilise alternative models of political and economic connectivity to challenge the European Union's normative supremacy (Topalidis et al., 2024). The Chinese presence, primarily through the Belt and Road Initiative and large-scale infrastructure investments, is fostering alternative models of political and economic connectivity that directly compete with the European ambitions of the countries in the region (Jaćimović et al., 2023). These diverse external influences, including the growing investments by the Gulf Cooperation Council (GCC) countries, create a complex geopolitical landscape that calls into question the prospect of full ‘like-mindedness’ and the purely strategic alignment of the Western Balkan countries' policies with the European Union (Saygin, 2025).

To address this, the paper employs a geopolitical realist framework that bridges the gap between International Relations (IR) and political geography. As argued by Wu (2017), classical geopolitics and the balance-of-power theory are inherently linked; geography defines the strategic environment in which states compete for influence. By synthesising Wu's insights with the 'shatterbelt' theory (Cohen, 2003; Steff, 2024), this study moves beyond a descriptive account. It adopts a critically engaged lens to examine how the structural and spatial realities of the Western Balkans - as a contested "rimland" - challenge the European Union's normative expectations. This theoretical foundation enables a robust analysis of how external actors navigate the region's fragmentation to establish their spheres of influence (Wu, 2017; Topalidis et al., 2024).

2. METHODOLOGY

The methods used in this study include an analysis of the content and discourse of the *White Paper for European Defence – Readiness 2030* (European Union, 2025). The analysis examines the position of the Western Balkan countries and the region as a whole in the *White Paper* (European Union, 2025) - specifically, how the European Union treats this area within this strategic document. At the same time, special attention is paid to the discourse that gives rise to closer or more distant partnership relations between the European Union and Western Balkan countries, namely, the possible treatment of this region or individual countries as a source of vulnerability to European security. In addition, a comparative analysis is applied between this document, the *Strategic Compass* (Council of the European Union, 2022), and the *Communication on EU Enlargement Policy* (European Commission, 2025), anticipating a correlation between partner relations in terms of security and the dynamics of the EU enlargement towards the Western Balkan countries.

Furthermore, the analysis of secondary sources (policy studies, think-tank reports) explores the achievements of the Western Balkan countries to date in harmonising with European security and defence policies, as well as their position in the European Union's enlargement perspectives for the region. Of particular importance are commentaries and reports on the most recent European Union documents, as they provide decision-makers with guidance from a highly analytical perspective. This opens up the possibility of their influence - especially in the case of think tanks founded by the European Union - on the dynamics of the European Union's cooperation with the Western Balkans, including enlargement policy.

Finally, semi-structured interviews were conducted with three carefully selected key informants from the Western Balkans, providing qualitative validation of the document analysis through purposive sampling. The experts were chosen to represent distinct geopolitical and security archetypes within the region. The first interviewee is a university professor from Bosnia and Herzegovina, an expert in geopolitics and security, representing a state facing complex internal constitutional and security challenges. The second is a university professor from Kosovo and an expert in political communication, representing a specific case of high

Euro-Atlantic orientation coupled with limited international recognition. The third interviewee is a Belgrade-based political analyst of Serbian ethnicity, originally from Montenegro, whose extensive professional experience in both Serbian and Montenegrin political landscapes allows for comparative insight into the divergent security paths of Montenegro (a NATO member and EU ‘like-minded’ partner) and Serbia (a militarily neutral country with strong non-EU ties).

Although the number of interviews is limited, they serve as a crucial qualitative corrective within a broader methodological triangulation. The goal was not statistical representativeness but rather to gain deep, professional insights into the strategic signals identified in the *White Paper* (European Union, 2025) and to assess how these are perceived by regional stakeholders. The questions were prepared in advance and related to: the position of the Western Balkan countries in the *White Paper* (European Union, 2025) and the conditionality of that position; the connection of that position with the policies and dynamics of the EU enlargement; and the perspectives for countries not explicitly mentioned in the document.

3. RESULTS (FINDINGS)

3.1. Content, Discourse, and Comparative Analysis

The Western Balkans are mentioned only once in the *White Paper* (European Union, 2025), in the context of Russia’s destabilising activities that may affect the situation in Europe. It states: “Russia is exploiting a network of systematic instability, including through close cooperation with other authoritarian powers. It is persistently fuelling tensions and instability in Europe’s neighbourhood, whether it is in the Western Balkans, Georgia, Moldova or Armenia and has a growing destabilising influence in Africa” (European Union, 2025, p. 5). It is clear from the content that the *White Paper* (European Union, 2025) recognises the Western Balkans as an area where tensions and instability persist and, as such, is exposed to (potential) Russia’s influence. It is also clear that, in terms of security, this statement places the Western Balkans alongside the former Soviet republics of Moldova, Georgia, and Armenia.

On the other hand, in the chapter of the *White Paper* (European Union, 2025) entitled *Enhanced security through partnership*, the Western Balkans is not mentioned explicitly; rather, certain countries from this region are cited as potential stabilisation and security factors and thus partners of the European Union. It states: “*The EU should continue mutually beneficial engagement and cooperation in the field of security and defence with all like-minded European, enlargement and neighbouring countries (including Albania, Iceland, Montenegro, the Republic of Moldova, North Macedonia and Switzerland) to promote peace, security and stability on our continent and beyond*” (European Union, 2025, p. 19). Here, there is an important difference compared to the previous explicit mention of the Western Balkans, primarily in that the countries which this document labels as “like-minded” countries are singled out. Being “like-minded” with the EU offers these countries the opportunity to transform their image from one of instability into one of stability, or to shift from being

beneficiaries to becoming creators of security policies. Finally, the fact that these countries are also NATO members makes them more reliable partners than the remaining non-members. In addition, the fact that some Western Balkan countries are not explicitly mentioned in this section should be understood as implying that these countries are considered “non-like-minded” or, at best, not completely “like-minded” due to internal instability and possible Russian or other destabilising influences. This perspective is crucial because distinguishing Western Balkan countries according to the criterion of being, as the document euphemistically puts it, more or less “like-minded” suggests that these countries are not necessarily approached collectively but individually, based on their distinguishing characteristics.

The reasons for the omission of Serbia, Kosovo, and Bosnia and Herzegovina from the list of “like-minded” countries can be found in the *Strategic Compass* (Council of the European Union, 2022, pp. 18-19), which states: “Security and stability throughout the Western Balkans is still not a given, also due to increasing foreign interferences, including information manipulation campaigns, as well as through potential spill over from the current deterioration of the European security situation. In this regard, it is of particular interest to support the sovereignty, unity and territorial integrity of Bosnia and Herzegovina, based on the principles of equality and non-discrimination of all citizens and constituent peoples as enshrined in the Bosnia and Herzegovina constitution, as well as the reform process on its European path and to take forward the EU-led Pristina-Belgrade dialogue.” The quote clearly identifies foreign influences as a European security challenge, a point also stated more generally in the *White Paper* (European Union, 2025). However, regarding the countries mentioned, the quote highlights the fundamental weaknesses and internal problems of Bosnia and Herzegovina, as well as Kosovo’s status as an obstacle to rapprochement between Serbia and Kosovo with the European Union.

In light of differences in their (geo)political Europeanness, the European Union not only sends messages to the Western Balkan countries about the dynamics of future enlargement as a geopolitical necessity amid the conflict in Ukraine, but also about the advantageous positions for some regional states in this enlargement. In the *2025 Communication on EU Enlargement Policy* (European Commission, 2025), Montenegro and Albania were noted as leading candidates for EU membership, while Ukraine and Moldova have made significant progress. At the same time, the *Communication* (European Commission, 2025, p. 30) warns that “Serbia should clearly manifest its geopolitical orientation towards the EU, including by starting to align with the EU’s restrictive measures taken in the context of Russia’s war of aggression against Ukraine”.

In the case of Bosnia and Herzegovina, the *Communication* (European Commission, 2025, p. 31) indicates that “in Bosnia and Herzegovina, the political crisis in the Republika Srpska entity and the ensuing end of the ruling coalition undermined progress towards EU accession”, but also that “Bosnia and Herzegovina’s continued full alignment with the EU’s common foreign and security policy testifies to its strategic choice”. Despite internal obstacles to intensifying

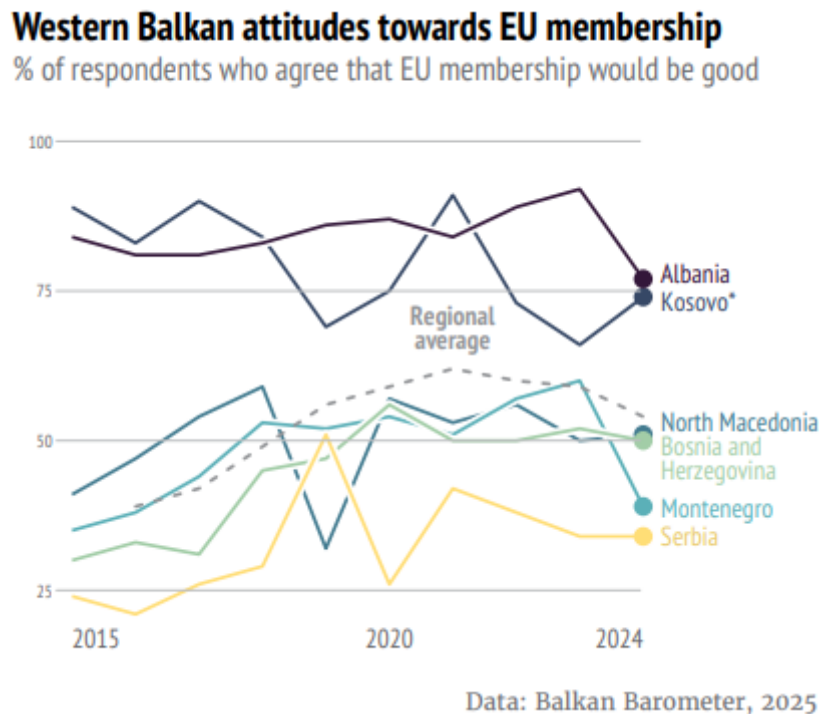
rapprochement with the European Union and even status differences compared to Serbia, the document clearly emphasises that Bosnia and Herzegovina is more “like-minded” with the EU, meaning that its foreign and security policy is more pro-European than Serbia’s.

3.2. Secondary Sources Analysis

The analytical review by Bojana Zorić (2025, p. 2) from the European Union Institute for Security Studies (EUISS) highlights significant differences in support for European integration across the Western Balkan countries (Figure 1). The highest level of support for EU accession is in Albania and Kosovo (both exceeding 70%), while the lowest is in Serbia (34%). In North Macedonia and Bosnia and Herzegovina, the figures stand slightly above 50%, while support for EU membership has dropped significantly in Montenegro, falling from 60% to 39%. The same institute, in an analysis by Kovalčíková, Salvi, and Zorić (2024), emphasises Russia Today's (RT) role in Russia’s propaganda activities in the Western Balkans. It notes that this media company already operates in the area through a regional centre in Belgrade, with the announced opening of a Serbian-language bureau in Banja Luka, in Bosnia and Herzegovina.

Figure 1

Western Balkan attitudes towards EU membership



Source: Zorić, 2025, p. 2

However, these aggregate national figures mask a profound internal “polarisation effect” (Barbarić et al., 2025) that is particularly evident in multi-ethnic societies where EU support is

fragmented along ethno-political lines. In Bosnia and Herzegovina, official data from the Directorate for European Integration (DEI, 2024) reveals a drastic gap, with support reaching 83.8% in the Federation of BiH compared to only 48.3% in the Republika Srpska. Similar internal fractures are observed in North Macedonia, where a strong pro-EU consensus among the Albanian community contrasts with growing scepticism and “identity fatigue” among the Macedonian majority (Damjanovski, 2023; Brie & Solcan, 2025). Likewise, in Kosovo, security perceptions and EU aspirations remain deeply divided between the Albanian majority and the Serbian community in the north (KCSS, 2023). This empirical fragmentation suggests that the *White Paper’s* (European Union, 2025) strategic narrative of like-minded partners fails to account for the complex, multi-layered reality of regional alignment.

The High Representative for Foreign Affairs and Security Policy, Kaja Kallas, stressed the necessity of enlargement if the EU wants to be a “stronger player on the world stage”, emphasising that “the enlargement of the Union by 2030 is very likely, with Montenegro and Albania earning the status of frontrunners for membership through their reform processes” (Klix.ba, 2025b). Bosnia and Herzegovina has the most reason to be disappointed, as it has not yet begun accession negotiations with the European Union. Local media in Bosnia and Herzegovina have expressed dissatisfaction, calling Brussels’ enlargement policy paradoxical, since “unlike Kyiv, which is at war and faces destruction every day, Bosnia and Herzegovina is not even close to opening accession negotiations three decades after the war” (Klix.ba, 2025a).

Zweers and Kelečević (2025, p. 16) from Clingendael, the Netherlands Institute of International Relations, in their geopolitical analysis of the Western Balkans, provide guidelines and recommendations to the European Union and its member states regarding Russia’s influence in the region, stating: “*The EU could adopt a firmer stance against Russian interference in the Balkans. It could make it clear to Serbia and Republika Srpska that continued non-alignment with the EU’s foreign policy is unacceptable, and link this to the withholding of EU financial support. The EU could further assist other WB countries in shielding them from Russian malign instruments, for example, in the disinformation and cyber domains*”.

A realistic assessment of the strength of Russia’s influence is given by Vulović (2023, p. 2), stating that “Moscow cannot offer a significant economic or political alternative to the EU in the region, thus it primarily works to obstruct the further integration of the Western Balkan (WB) states into the EU just as it aims to halt NATO expansion”. Vulović further warns that through “economic ties, China has gained foreign and security policy relevance in the Balkans”, emphasising “China’s arms trade with the region and its role in Serbia’s surveillance infrastructure”.

Vulović (2023, p. 4) argues that “Serbia is the only WB country that buys arms from Russia and China”, while all six countries in the region “import many arms from the EU: Albania, for example, imports them from Italy, Germany and France; Montenegro from Austria; North

Macedonia from Ireland; and Serbia from Germany and France”. According to a report by the Friedrich Ebert Stiftung (2025), in addition to American and Turkish suppliers, the Western Balkan countries favour European suppliers of weapons and equipment. At the same time, there are around 200 companies producing defence goods in the region, with Serbia and Bosnia and Herzegovina accounting for the largest share of production and exports.

Albania, Bosnia and Herzegovina, North Macedonia, and Serbia are already involved in EU police and military operations worldwide (Cvetković, 2022; Ferreira da Cruz, 2021). Moreover, the report by the Hellenic Foundation for European and Foreign Policy (2025) indicates that the potential of the regional partnership with Western Balkan countries to realise the collective advantage envisaged by the White Paper (European Union, 2025) is much greater than has been realised to date. The report notes that the Western Balkan countries, except Bosnia and Herzegovina, have already exceeded NATO’s defence investment target of 2% of GDP, and that all countries, including Serbia, which maintains relations with Russia, are providing various forms of aid to Ukraine.

The Friedrich Ebert Stiftung report (2025, p. 5) emphasises that Western Balkan countries have strong potential across four of the ten specific priority tracks of the industrial and capability push. “First, Europe’s objective to produce at least 2 million large-calibre artillery rounds annually underscores the need to mobilise every credible source of capacity; regional plants that already mass-produce 155mm shells and compatible Soviet-calibre ammunition can help close the gap. Second, artillery systems themselves - where several Western Balkan manufacturers have proven designs and agile production lines - offer scope for cooperative investment and licensing to increase output quickly. Third, drones and counter-drone systems: while high-end combat Unmanned Aircraft Systems (UAS) will remain the province of larger Original Equipment Manufacturers (OEMs), the region is well-placed to scale affordable Intelligence, Surveillance, and Reconnaissance (ISR) and loitering munitions – areas where rapid iteration and cost control matter. Fourth, mobility and logistics: building a resilient southern supply artery to Ukraine through Balkan corridors would diversify risk, relieve pressure on hubs further north, and demonstrate European responsibility for sustainment.”

3.3. Semi-structured interviews

When asked how to assess the position of the Western Balkan countries in the *White Paper* (European Union, 2025) and the basis for this position, the interviewees unanimously point out that the Western Balkans occupy only a peripheral position in the document. There are certain differences in perspective. The university professor from Bosnia and Herzegovina points to the treatment of the Western Balkans as a “vulnerable periphery of the European security architecture” in the document, which is conditioned by the destabilising influence of non-EU factors in the region, primarily Russia. The interviewee from Kosovo also claims that the Western Balkans in the document are “seen as a weak link or as an opportunity by the Russians to initiate any destabilising campaign in Europe”, but this expert goes a step further and directly

names Serbia as a country whose political and defence priorities deviate from those of other regional states in terms of alignment with European policies. The political analyst operating in both Serbia and Montenegro most clearly identifies Montenegro and Albania as the countries closest to full EU membership, whose status, as defined by the *White Paper* (European Union, 2025), can be easily upgraded to full membership. However, this interviewee neither acknowledges nor mentions that some countries in the region are non-compliant with European foreign policies, which could pose a security challenge.

The answers to the question of whether the position of the Western Balkan countries in the *White Paper* (European Union, 2025) corresponds with the policies and dynamics of EU enlargement differ in content and nuance but still retain the basic idea that the treatment of the region's countries in this document reflects their proximity to or distance from EU membership. The Kosovo university professor claims that "the EU has to remove the red tape (which is identified as a problem in this document anyway) and continue the integration of the remaining Western Balkan countries before the scepticism reaches the point of no return". The interviewee from Bosnia and Herzegovina states that the document "recognises the Western Balkans as an area of importance for European security through the prism of threats coming from outside, which is in line with the position that the region is geostrategically important for the EU", but that "unlike Ukraine, which is explicitly mentioned in the document along with plans for integration into the European defence market, the Western Balkan countries appear implicitly only through the security lens". Therefore, the expert claims that "this inconsistency somewhat reflects the reality of the dynamics of enlargement because the EU rhetorically supports the future membership of the Western Balkans, but operationally it still treats these countries as external partners". Nevertheless, the political analyst operating in both Serbia and Montenegro emphasises that the document "makes it completely clear that there are countries in the Western Balkans that can be counted on in the short term and that there are those whose membership, and subsequent compliance with EU policies, is a long process".

The question of what alternative scenarios, if any, respondents foresee for the Western Balkan countries that are not explicitly mentioned in the *White Paper* (European Union, 2025) yields diverse responses. The expert from Kosovo does not see "any alternative for the Western Balkans besides the one related to the EU and NATO" but emphasises that "there is an imminent need for the EU to take a firm stance towards any Western Balkan country which does not share the same views on security". The interviewee explains that "those countries have the right to do so and should be ready for any consequences that come with that decision", because "playing both sides is rather dangerous for the whole Western Balkans". The professor from Bosnia and Herzegovina foresees three scenarios: first, "integration into the Western bloc, which would be the most positive outcome"; second, a "continuation of balancing and the status quo" in which "the EU would continue to hesitate with full membership, and the Western Balkan countries would try to balance between East and West, without a clear classification"; and third, "the least favourable for the region is the scenario of geopolitical fragmentation", that is, a "division into spheres of influence due to the failure of European integration". The

expert claims that “if the EU postpones or abandons the serious integration of the Balkans, the power vacuum on the southeastern wing of Europe will be filled by rivals such as Russia and China”. The expert operating in both Serbia and Montenegro points even more explicitly to alternative scenarios, emphasising China’s significant presence in the region, Russia’s traditional interest in influencing the area, and the US’s promotion of its own policy in the region independently of the EU. At the same time, the interviewee points out the problem of “the absence of institutional authorities in the EU itself and strategic thinking about how the Western Balkans should be integrated into European flows”.

4. DISCUSSION

The position of the Western Balkans in the *White Paper* (European Union, 2025) is not clearly defined, as it ranges narratively from a de facto risk zone exposed to Russian influence on selectively singled-out partners - namely, countries that share more common positions with the European Union than others. When it comes to the Western Balkans as a zone of (potential) instability, and especially when the aforementioned Caucasus countries are added, this area fits the traditional perspective of both the Balkans and the Caucasus as shatterbelts - zones of discontinuity and conflict.

However, the *White Paper*’s narrative (European Union, 2025) reveals a selective geopolitical focus, primarily addressing challenges associated with Russian influence. While the war in Ukraine conditions this prioritisation, such a targeted approach raises questions about its long-term comprehensiveness. While the collective term “Western Balkans” appears only once in the *White Paper* (European Union, 2025), the region’s strategic treatment is addressed through the brief, selective inclusion of individual states. However, the rarity of these mentions, coupled with the document’s heavy focus on the war in Ukraine, points to a notable lack of a comprehensive strategic focus for the region as a whole. This suggests that the EU’s current security priorities are reactive, focusing only on those specific countries that demonstrate immediate policy alignment. Consequently, the Western Balkans are not approached as a holistic geopolitical unit, but rather through a fragmented lens that prioritises like-minded partners while leaving the complex challenges of non-aligned states and other non-EU influences insufficiently addressed. By focusing almost exclusively on these specific dynamics, the EU adopts a reactive posture that may overlook other non-EU actors whose presence also shapes the broader European security landscape. This suggests that the document reflects a crisis-driven response rather than a fully integrated, proactive strategy for diverse geopolitical challenges.

This strategic fragmentation is further evidenced by the document’s marginalisation of non-European actors whose influence is structurally embedded in the region’s daily political and economic life. As established in the literature review, the 'economic statecraft' of China and the institutionalised “soft power” of Turkey and the Gulf States (Vuksanović, 2023; Saygı, 2025) offer alternative models of connectivity that often compete with the EU’s normative

requirements. By failing to address these actors, the *White Paper* (European Union, 2025) risks oversimplifying the Western Balkans as a narrow EU–Russia geopolitical contest, overlooking the complex reality in which regional states balance among diverse global power centres.

Western Balkan countries that align with the European Union’s foreign policy are termed “like-minded”. This treatment reflects not only the different approaches to membership in the European Union, but also, more importantly, each country’s individual strategic determination. It is important to emphasise that the categorisation of countries as like-minded is a terminological construct of the *White Paper* (European Union, 2025) itself, rather than an analytical framework set by this research. This classification relies primarily on a state’s formal adherence to EU foreign policy statements, which may represent a strategic limitation of the document. By focusing on high-level policy alignment, the *White Paper’s* (European Union, 2025) discourse tends to bypass more complex internal dynamics - such as ethnic divisions or socio-religious tensions - that strongly impact regional stability. The absence of a granular focus on internal fragmentation is directly challenged by empirical evidence of a deep “polarisation effect” (Barbarić et al., 2025) within the region. For instance, the 35% gap in EU support between the two entities in Bosnia and Herzegovina (DEI, 2024), alongside the ethno-political dilemmas surrounding integration in North Macedonia (Abazi Imeri, 2025), suggests that “like-mindedness” is often a fragile top-down construct rather than a reflection of a unified domestic consensus. While this research acknowledges these internal complexities as significant, its primary focus remains on the strategic signals and partnership criteria as defined within the official EU defence narrative. Countries that are more susceptible to the influence of other international actors, or that are themselves influential, are not considered like-minded and are therefore not highlighted as partners in the *White Paper* (European Union, 2025). Since it is a document that primarily focuses on European defence readiness, it is expected that the text assigns the position of implicit partner to countries whose pro-European - or rather pro-Western - geopolitical orientation is unquestionable.

When each Western Balkan country is considered individually, the selection of Albania, North Macedonia, and Montenegro suggests that NATO membership is a key criterion for being considered “like-minded.” In the case of the omitted countries, their pro-Westernism - if we translate “like-minded” in this way - is no means at the same level. Namely, Serbia has moved furthest from the three remaining Western Balkan countries that are not mentioned as “like-minded”, but the European defence document does not indicate the existence of a level of partner trust. Assuming the document’s initial statement about Russia’s influence in the Balkans omits “like-minded” countries, it can be inferred that “not like-minded” countries are those exposed to Russia’s influence. Although this is not stated explicitly, among such countries, we can look directly at Serbia and, indirectly, at Bosnia and Herzegovina through the influence of Serbia and Russia on the Republika Srpska. The absence of Kosovo from the list of (potential) partner countries of the European Union reflects the ambivalent policy of the member states, since not all EU countries have yet recognised Kosovo.

In addition, it is important to note that the different treatment that the *White Paper* (European Union, 2025) provides to the Western Balkan countries corresponds to the Croatia's precedent of an individual approach and transitioning out of the problematic region, i.e. rewarding success by accepting it into full membership of the European Union without the obligation to wait for candidates who are lagging in the integration processes.

The way in which the interviewed experts from the Western Balkans evaluate the position of the countries of the region in the *White Paper* (European Union, 2025), as well as the future of the region in terms of European integration and alternative scenarios, is to a certain extent conditioned by the perspectives of the countries they come from. Although their answers point to uncertainty about the dynamics of EU enlargement in the region, both individually and collectively, experts still differ in their interpretations of the reasons for this situation. Namely, among experts from Bosnia and Herzegovina and Kosovo, one can sense a fear of destabilising external factors and the need for a clear geopolitical positioning of each country in the region individually, but with a certain dose of criticism towards Brussels' slowness and hesitation in providing the countries of the region with firm guarantees for imminent enlargement. On the other hand, the expert operating in both Serbia and Montenegro does not see alternative scenarios for the region as a catastrophe, emphasising that the European Union itself is responsible for such scenarios due to its lack of readiness for rapid enlargement. All this indicates that integrating the region "as a package" is not even possible, both because of the different levels of readiness among individual countries and because of differences in their relations with external factors and their interests in the region.

CONCLUSION

The *White Paper for European Defence – Readiness 2030* (European Union, 2025) does not prioritise the Western Balkans as a central issue of European security, but it undoubtedly underscores the region's importance in the broader reflection on European security policies. However, even in this passing reference to the Western Balkans, it is possible to draw certain conclusions about the region's perspectives towards the European Union, especially by correlating the statements in this document with other recent EU strategic initiatives. The content and discourse analysis of the *White Paper* (European Union, 2025), the comparative analysis of related acts, and the arguments provided by the interviewed regional experts, undoubtedly confirm the first hypothesis: the position of the Western Balkan countries within the European defence policy, as presented in this document, directly reflects the specific level of their alignment with the European Union's foreign policy.

Furthermore, the highlighted need for unambiguous alignment with common European foreign and security policy priorities, as a prerequisite for developing trust and partnership relations, necessarily implies distancing from external factors that the European Union recognises as destabilising, primarily Russia. An analysis of the *White Paper* (European Union, 2025), other strategic documents, and think-tank reports clearly indicates that the pursuit of alternative

geopolitical ties by individual Western Balkan countries, such as Serbia, with Russia (and China) reduces trust and partner reliability in joint security actions. This also confirms the second hypothesis: namely, that the nature of the partnership relationship in European defence policies - as a reflection of policy alignment - exerts a significant impact on the dynamics and pace of EU enlargement to the Western Balkan countries.

REFERENCES

- Abazi, E. (2019). Albania: New geopolitics and shifting linkages. In F. Bieber & N. Tzifakis (Eds.), *The Western Balkans in the world: Linkages and relations with non-Western countries* (pp. 164-183). Routledge. <https://doi.org/10.4324/9780429243349-9>
- Barbarić, D., Bošnjak, A.-M., & Galić, D. (2025). The mainstream effect and the polarization effect in Bosnia and Herzegovina: Public opinion on the European Union. *Hum: časopis Filozofskog fakulteta Sveučilišta u Mostaru*, 20(33), 98-120. <https://doi.org/10.47960/2303-7431.20.33.2025.98>
- Brie, M., & Solcan, A. (2025). The identity challenges of the European integration process of North Macedonia. *Analele Universității din Oradea, Seria Relații Internaționale și Studii Europene*, 17, 7-28. <https://doi.org/10.58603/YDYL4023>
- Cohen, S. B. (2003). *Geopolitics of the World System*. Rowman & Littlefield Publishers.
- Council of the European Union. (2022, March 21). *A strategic compass for security and defence – for a European Union that protects its citizens, values and interests and contributes to international peace and security*. https://www.eeas.europa.eu/sites/default/files/documents/strategic_compass_en3_web.pdf
- Cvetković, N. (2022). Common security and defence policy of the European Union and readiness of the Republic of Serbia for integration. *Vojno delo*, 74(5), 1-14. <https://doi.org/10.5937/vojdelo2205001C>
- Damjanovski, I. (2023). *Analysis of public opinion on North Macedonia's accession to the European Union (2014-2023)*. Konrad Adenauer Foundation & Institute for Democracy "Societas Civilis" – Skopje (IDSCS). <https://idscs.org.mk/wp-content/uploads/2023/12/B5-Public-Opinion-Analysis-Paper-No.-27-2023-WEB.pdf>
- Davutoğlu, A. (2014). *Strategijska dubina: Međunarodni položaj Turske*. Službeni glasnik.
- Direkcija za europske integracije (DEI). (2024). *Istraživanje javnog mnijenja: Stavovi građana o članstvu u Europskoj uniji i procesu integracija*. Vijeće ministara Bosne i Hercegovine. <https://www.dei.gov.ba/bs/clanstvo-bih-u-eu-podrzava-712-posto-gradana>
- Dugin, A. (2014). *Osnovi geopolitike: Knjiga 1: Geopolitička budućnost Rusije*. Ekopres.
- Dugin, A. (2017). *Geopolitika multipolarnog svijeta*. Zadruga Eneagram.
- European Commission. (2025, November 4). *2025 Communication on EU Enlargement Policy*. https://enlargement.ec.europa.eu/document/download/eb69a890-40d6-4696-801e-612d51709fdd_en?filename=2025%20Communication%20on%20EU%20Enlargement%20Policy.pdf

- European Union. (2025, March 19). *White Paper for European Defence – Readiness 2030*.
https://commission.europa.eu/document/download/e6d5db69-e0ab-4bec-9dc0-3867b4373019_en?filename=White%20paper%20for%20European%20defence%20%E2%80%93%20Readiness%202030.pdf
- Ferreira da Cruz, M. (2021). The European Union and the creation of the new security periphery: the case of the Western Balkans. *Debater a Europa*, 25, 75-98.
https://doi.org/10.14195/1647-6336_25_4
- Friedrich Ebert Stiftung (2025, September). *Strategic partners at Europe's edge: Harnessing the Western Balkans for EU defence readiness* [Policy brief]. Dialog Southeast Europe.
<https://library.fes.de/pdf-files/bueros/sarajevo/22364.pdf>
- Gajić, A. S. (2018). Aktualna geopolitička pozicija Srbije: između atlantizma, evroazijstva i kineskog uticaja. *Politika nacionalne bezbednosti*, 15(2), 13-29.
<https://doi.org/10.22182/pnb.1522018.1>
- Hasanaj, E. (2023). What are the changes in the trust of citizens of Kosovo and Serbia in European integration? In Sh. Isufi (Ed.), *Youth Perspectives on Western Balkans Security: WBSB 2023 Essay Selection* (pp. 19–24). Kosovar Centre for Security Studies (KCSS).
https://qkss.org/images/uploads/files/Youth_Perspectives_on_Western_Balkans_Security_-_WBSB_2023_Essay_Selection.pdf
- Imeri, A. A. (2025). Reducing political polarization as a prerequisite for EU accession: The case of North Macedonia. *Academic Journal of Business, Administration, Law and Social Sciences*, 11(2), 102–115. <https://doi.org/10.2478/ajbals-2025-0022>
- Jaćimović, D., Deichmann, J. I., & Tianping, K. (2023). The Western Balkans and Geopolitics: Leveraging the European Union and China. *Journal of Balkan and Near Eastern Studies*, 25(4), 626–643. <https://doi.org/10.1080/19448953.2023.2167164>
- Klix.ba. (2025a, November 4). *Briselski paradoks: Ukrajina bi za pet godina mogla ući u EU iako je u ratu, dok za BiH ni pregovori nisu na vidiku*.
<https://www.klix.ba/vijesti/svijet/briselski-paradoks-ukrajina-bi-za-pet-godina-mogla-uci-u-eu-iako-je-u-ratu-dok-za-bih-ni-pregovori-nisu-na-vidiku/251104156>
- Klix.ba. (2025b, November 4). *Kallas: EU bi mogla primiti nove članice do 2030. godine, Crna Gora i Albanija otišle najdalje s reformama*.
<https://www.klix.ba/vijesti/svijet/kallas-eu-bi-mogla-primiti-nove-clanice-do-2030-godine-crna-gora-i-albanija-otisle-najdalje-s-reformama/251104203>
- Kovalčiková, N., Salvi, A. & Zorić, B. (2024, November). *Countering cyber-enabled hybrid interference in the Western Balkans: A scenario-based approach* (Special Report). European Union Institute for Security Studies.
<https://www.iss.europa.eu/sites/default/files/2024-12/2024-02%20BZ%20FIMI%20in%20WB.pdf>

- Krstinovska, A. & Marrone, A. (2025, March 10). *Europe's Overlooked Allies: Why the Western Balkans Matter for EU Defence Readiness* (think nea – New Narratives of EU Integration). Hellenic Foundation for European and Foreign Policy (ELIAMEP). https://osfwb.org/wp-content/uploads/2025/10/think-nea-defense-report-FINAL_compressed.pdf
- Proroković, D. (2015). *Geopolitika Srbije*. Službeni glasnik.
- Proroković, D. (2023). NATO in the Balkans: Consequences and Perspectives. In D. Proroković & E. Entina (Eds.), *Eurasian Security After NATO* (pp. 183-205). Institute of International Politics and Economics; Institute of Europe of the Russian Academy of Sciences. https://doi.org/10.18485/iipe_easnato.2023.ch9
- Saygın, E. (2025). Comparative Analysis of Foreign Direct Investment Strategies in Western Balkan Countries. *Eskişehir Osmangazi Üniversitesi Sosyal Bilimler Dergisi*, 26(2), 534-557. <https://doi.org/10.17494/ogusbd.1674006>
- Steff, R. (2024). Theoretical framework: Geopolitical realism and great power competition. In *New Zealand's geopolitics and the US-China competition* (pp. 21–55). Palgrave Macmillan. https://doi.org/10.1007/978-981-96-0282-7_2
- Tanasković, D. (2010). *Neoosmanizam: Povratak Turske na Balkan*. Službeni glasnik & Službeni glasnik Republike Srpske.
- Topalidis, G. T., Kartalis, N. N., Velentzas, J. R., & Sidiropoulou, C. G. (2024). New developments in geopolitics: A reassessment of theories after 2023. *Social Sciences*, 13(2), Article 109. <https://doi.org/10.3390/socsci13020109>
- Tunjić, F. (2004). *Vmesna Evropa: Konfliktnost državnih teritorialnih meja*. Univerza na Primorskem.
- Vuksanovic, V. (2023). So Similar, Yet So Different: Russia and Turkey in the Western Balkans – The Case of Serbia. *Uluslararası İlişkiler Dergisi*, 20(79), 105-122. <https://doi.org/10.33458/uidergisi.1300342>
- Vulović, M. (2023). *Western Balkan Foreign and Security Ties with External Actors: An arena of geostrategic rivalry for the EU or a local power struggle?* (SWP Comment, 8/2023). Stiftung Wissenschaft und Politik (SWP). <https://doi.org/10.18449/2023C08>
- Wu, Z. (2018). Classical geopolitics, realism and the balance of power theory. *Journal of Strategic Studies*, 41(6), 786–823. <https://doi.org/10.1080/01402390.2017.1379398>
- Zorić, B. (2025, June). *EU enlargement and integration: Voices of support and scepticism* (Brief No. 12). European Union Institute for Security Studies. https://www.iss.europa.eu/sites/default/files/2025-06/Brief_2025-12_Enlargement%20and%20scepticism.pdf

Zweers, W., Kelečević, I. (2025, August). *Geopolitically mapping the Western Balkans: A tale of merchants, missionaries and miracles* (Clingendael Policy Brief). The Clingendael Institute. <https://www.clingendael.org/sites/default/files/2025-08/geopolitically-mapping-the-western-balkans.pdf>

GEOPOLITICS OF CLIMATE CHANGE: THE EU'S PATH TOWARD A NEW GLOBAL SECURITY PARADIGM¹

Andreja Sršen

University of Zagreb

Faculty of Croatian Studies

E-mail: asrsen@fhs.hr

ORCID: <https://orcid.org/0000-0003-1667-4651>

Abstract

Climate change is increasingly recognised as one of the main drivers of global insecurity, as it affects migration patterns, resource scarcity, and geopolitical stability. Sociologist Ulrich Beck argues that climate change transforms geopolitics by creating a globally interdependent risk society, where environmental threats transcend national borders and require coordinated international responses (Beck, 1992; 2009). It is widely expected that global warming will increase the risk of conflict both within and between nations, worsen food insecurity, disrupt international trade systems, and lead to large-scale migration. Recent dynamics have led to significant changes across various aspects of the European Union's foreign policy, which is increasingly defined by "climate security." These new dynamics have led to significant changes across several dimensions of the European Union's foreign policy, which is increasingly framed in terms of "climate security." In this context, the European Union has begun integrating climate issues into its security and defence policies to anticipate and mitigate climate-related threats. The article also highlights the United Nations Climate Change Conference (COP), which serves as a platform to align EU priorities with global governance, strengthen multilateral cooperation, and increase resilience in climate-vulnerable areas. By linking sociological insights with geopolitical and security frameworks, this article demonstrates that effective climate security strategies require attention not only to environmental factors and geopolitical shifts but also to social risk perceptions and institutional capacities.

Keywords: geopolitics of climate change; environmental threats; European Union; sociology; risk society.

¹ This paper was created as part of the institutional research project "*Climate Change and Security Risks*" (CLISEC), funded by Source 581 – Recovery and Resilience Mechanism (Next Generation EU).

1. INTRODUCTION

The development of the concept of environmental security has become particularly prominent in the context of climate change. Climate change has gradually become a global environmental threat paradigm because it transcends national borders, has long-term consequences, and affects almost all sectors of society.

In this sense, climate change is a classic example of a "threat multiplier," as it amplifies existing social, economic, and political instabilities. The 1963 agreement among the United States, the Soviet Union, and Great Britain that prohibited atmospheric nuclear testing was the first significant international environmental accord. (Ó Tuathail, Dalby, & Routledge, 2007, p. 199). In this historical context, the development of the contemporary international climate negotiation process should be viewed within the frameworks of international organisations, integrations, and alliances such as the United Nations, the European Union, and NATO. These not only align the political and security priorities of their members but also shape a global climate-security strategy, promote multilateral cooperation, facilitate the transfer of technologies and resources, and enable coordinated adaptation and mitigation of climate risks across regions worldwide.

This process integrates ecological challenges into diplomatic, security, and economic decisions, making climate change an integral part of international policy and global stability strategy. The United Nations Framework Convention on Climate Change (UNFCCC) plays a crucial role, serving as a global multilateral instrument for coordinating climate policies. Annual Conferences of the Parties (COP) under the UNFCCC are forums where member states negotiate to reduce greenhouse gas emissions, address climate adaptation, provide financial and technological support to developing countries, and monitor the implementation of international climate agreements. Conferences of the Parties COPs serve as key platforms for global cooperation, aligning national strategies with international objectives, strengthening multilateral initiatives, and developing climate security policies in line with states' geopolitical and economic interests.

A particularly important moment was the 2015 United Nations Climate Change Conference in Paris, which included climate protection plans that each UNFCCC member state was obligated to fulfil. During COP2015, a decision was made to limit global warming to below 2 degrees Celsius in the medium term. Through this agreement, states committed to limiting global temperature rise and strengthening adaptation to climate risks, formally integrating climate change into global governance and broader security and development strategies.

2. METHODOLOGY

This study examines how three theoretical approaches - the risk society theory, climate policy, and securitisation theory - contribute to understanding climate change as a contemporary

security challenge. The analytical basis of the paper relies on the theoretical contributions of Ulrich Beck (1992), whose risk society theory emphasizes the global nature of modern risks; Anthony Giddens (2009), who examines climate change through the lens of climate policy and social risk governance; and Barry Buzan and colleagues (1998), whose securitization concept explains the process by which issues such as climate change frames as security problems in political discourse. Together, these theoretical approaches form an integrated analytical framework for understanding climate change as a complex global security risk.

The methodological framework also relies on Ulrich Beck's risk society theory, viewing climate change as a globally produced risk that transcends national borders and traditional governance patterns. Following this approach, Bulkeley (2001) analyses the scientific implications of climate risks, emphasising their political and institutional dimensions. The study combines theoretical analysis of the concept of risk with qualitative analysis of relevant documents and public policies to examine how climate risk constructs are interpreted and integrated into security and development strategies.

3. CLIMATE CHANGE AND ADAPTATION POLICY

Understanding climate security as a means of shaping a new global order underscores its growing role in geopolitical decisions and international initiatives. In this context, COP conferences, or the annual meetings of the states parties to the United Nations Framework Convention on Climate Change, must be considered, where negotiations on global climate policies and obligations take place.

Ian Bailey (2010) points out that climate change creates new political geographies of power. Bailey shows that negotiations at the Copenhagen conference (COP15) revealed a shift in global decision-making, in which informal coalitions of major powers and regional blocs supplemented traditional multilateral negotiation patterns. He emphasises that the Copenhagen climate negotiations revealed the emergence of new political geographies of climate policy, in which states, international organisations, and other actors shape climate governance at different levels.

Similarly, Peter Christoff (2010) notes that the COP15 negotiations revealed significant geopolitical differences among major powers, especially between the United States and China, which significantly affected the conference outcome. The conference has simultaneously drawn criticism for the lack of a legally binding agreement. However, it has also received positive reviews for including all the world's largest greenhouse gas emitters in a joint negotiation process.

Negotiations continued after COP15, culminating in the adoption of the Paris Agreement in 2015, which incorporated many elements agreed upon in Copenhagen. According to the authors Jolene McGee and Jens Steffek (2016), COP15 marked an important turning point in

global climate change governance, paving the way for the model of voluntary national commitments, which was later institutionalised in the Paris Agreement.

Within this discourse, climate policy becomes a space in which power relations between states and between the global North and South are redefined. Bailey emphasises that the Copenhagen conference marked the rise of "new political geographies of climate change," where climate negotiations evolved into a platform for political and geopolitical competition among states (Bailey, 2010, p. 128). This observation aligns with Anthony Giddens' (2009) thesis on the necessity of strategic climate risk management. In this context, climate initiatives - such as participation in COP processes and the promotion of green technologies - become crucial tools for long-term political and economic strategy.

Table 1

Climate Change Conferences (COP) - Key Outcomes and Policy Implications

Year	COP Conference	Key Outcome / Agreement	Geopolitical and Policy Implications	Reference
1995	COP1 (Berlin)	Berlin Mandate – beginning of negotiations on binding emission targets.	Start of formal international climate negotiation process.	UNFCCC (1995). Decision 1/CP.1 – The Berlin Mandate.
1997	COP3 (Kyoto)	Kyoto Protocol adopted – first legally binding emission reduction targets for developed countries.	Establishment of global climate governance and emission trading mechanisms.	UNFCCC (1997) Kyoto Protocol.
2009	COP15 (Copenhagen)	Copenhagen Accord – recognition of the 2°C global temperature target.	Shift toward voluntary national commitments and climate diplomacy.	UNFCCC (2009) Copenhagen Accord.
2015	COP21 (Paris)	Paris Agreement – commitment to limit warming to well below 2°C and pursue 1.5°C.	New global climate governance framework based on nationally determined contributions (NDCs)	UNFCCC (2015). Paris Agreement.
2021	COP26 (Glasgow)	Glasgow Climate Pact – strengthening emission targets and reducing coal use.	Increased global pressure for decarbonisation and climate finance.	UNFCCC (2021). Glasgow Climate Pact.
2022	COP27 (Sharm el-Sheikh)	Establishment of Loss and Damage Fund for vulnerable countries.	Recognition of climate justice and financial responsibility of developed states.	UNFCCC (2022). Sharm el-Sheikh Climate Change Conference – Conference outcomes.

2023	COP28 (Dubai)	First Global Stocktake under the Paris Agreement.	Greater focus on energy transition and reducing fossil fuel dependence.	UNFCCC, 2023. Outcomes of the COP28 UN Climate Change Conference.
2024	COP29 (Baku)	Negotiations on a new global climate finance goal.	Strengthening financial mechanisms for global climate transition.	UNFCCC, 2024 UN Climate Change Conference Baku – COP29.
2025	COP30 (Belém)	Adaptation Roadmap with 59 adaptation indicators and a two-year guidance programme.	Lack of binding financial commitments from developed countries and fossil fuels were not mentioned at all in the final decisions.	UNFCCC, 2025 UN Climate Change Conference – COP30, Belém, Brazil.

Table 1. presents key United Nations climate change conferences (COPs) held from 1995 to 2025, focusing on the main agreements and goals of each conference and their wider geopolitical implications in the context of the development of global climate governance. These conferences play a key role in shaping international climate policies by serving as the main institutional framework for negotiations, harmonising national interests, and developing new models of multilateral cooperation to address climate change.

The United States officially withdrew from the Paris Agreement in January 2025, missing COP30 in Belém, Brazil. However, the conference was labelled as "COP implementation." Its outcomes generated mixed reactions due to the lack of binding fossil fuel targets, the removal of fossil fuels from the official decision, the absence of binding financial commitments from developed countries, and the fact that new national plans still do not put the world on track to limit warming to 1.5 °C.

Klein and Schäfer (2025) note that countries at COP30 should have strengthened legislation, administrative procedures, and implementation mechanisms to ensure effective climate policy in the short and long term. Recent climate litigation redefines the legal framework for COP30, clearly indicating state responsibilities in mitigation, adaptation, loss and damage, and climate finance.

The geopolitical implications of COP30 include deepening polarisation between developed and developing countries, exacerbated by the U.S. absence, rising tensions over trade measures, and the conflict between national sovereignty over energy resources and collective climate goals. According to the Wuppertal Institute (Obergassel et al., 2025, p. 27), COP30 did not achieve significant progress in reducing fossil fuel use, as profit-driven countries - including OPEC states, Russia, China, and India - largely blocked concrete measures. Current decisions

and actions are deemed insufficient to limit global warming to 1.5 °C or 2 °C, with fossil fuels omitted from final decisions despite the urgency of implementing existing climate agreements. Considering all relevant COP30 facts and implications, climate security serves not only as a risk-protection mechanism but also as a tool for shaping a new global order.

The United Nations is increasingly acknowledging climate change as a security issue. The United Nations Security Council (2025) has repeatedly discussed the link between climate change and conflict, particularly in unstable and vulnerable states. These discussions demonstrate how climate disruptions can affect political stability, resource availability, and migration flows. These discussions are also evident in the strategic documents utilized by the European Union. The EU integrates the connection between climate change and conflict into its security and strategic framework through official documents, including the European Green Deal (European Commission, 2019), EU Global Strategy (EEAS, 2016), Strategic Compass (Council of the EU, 2022), and Joint Communication on Climate-Security Linkages (European Commission & HR/VP, 2023), defining climate change as a threat multiplier and integral to security planning.

These documents can be reviewed through:

- Security framework - The EU recognises that climate change increases risks of conflict, migration, energy insecurity, and instability in nearby or global regions, analysing threats and planning responses through defence, crisis, and humanitarian strategies (Dalby, 2009; Beeson & Firth, 2016). Transatlantic relations are particularly relevant, as NATO affirmed in its 2021 Brussels Summit Communiqué and 2022 Strategic Concept that it will become the leading international organisation in understanding and adapting to the impacts of climate change on security (García Rico, 2022, p. 5). Considering that NATO Allies and EU member states uphold similar democratic values and principles, it is essential to examine this alliance through a security lens. Within this framework, both entities face interconnected risks and threats that affect their collective safety and stability. By recognising these shared challenges, we can better understand the importance of cooperation in addressing security concerns that impact both NATO and the European Union. Since NATO Allies and EU member states share common values, this alliance should also be understood within a security framework where shared risks and threats exist.
- Strategic framework - Climate goals, such as reducing greenhouse gas emissions and energy transition, are integrated into the EU's long-term strategic autonomy and foreign policy plans. Climate security thus becomes part of geopolitical decisions and international initiatives, including participation in COP processes and global promotion of green technologies (UNFCCC, 2023; Giddens, 2009).
- Prevention and resilience policy - The EU uses climate resilience data and projects to plan and strengthen institutional capacities in at-risk regions, linking environmental and security dimensions into a unified framework (European Union & UNEP, 2025). In its strategic documents, the European Union identifies climate change as a key threat to long-term

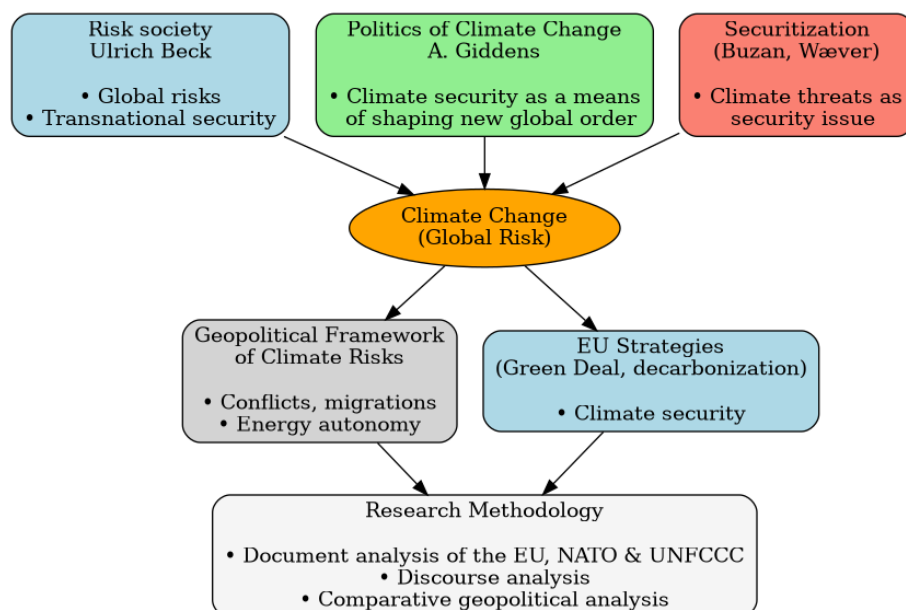
stability. Within the European Green Deal, the climate transition is viewed not only as an environmental issue but also as a geopolitical and security transformation, particularly in terms of energy independence, reducing reliance on fossil fuels, and enhancing societal resilience. In this broader context, environmental security is a concept that links environmental protection, climate policy, and international security. Climate change is thus no longer seen solely as an ecological problem but as a structural challenge to the global order, confirming the historical trajectory that began in the 1960s - from social movement and political agenda, through the security conceptual expansion of the 1990s, to today's integrated approach where climate change is part of global security, economic, and development strategies.

3.1. Theoretical Approaches and the EU's Climate Security Strategy

This section analyses and applies the theoretical concepts of Ulrich Beck (1992; 2009), Anthony Giddens (1990; 2009), and Buzan & Ole Wæver, whose frameworks enable a multi-level understanding of climate change as a security and geopolitical issue. Beck's "risk society" theory provides a basis for interpreting climate change as a produced, global, and transnational risk transcending national borders. Giddens contributes to understanding the political dimension of climate change, particularly in relation to climate security and strategic global governance. Buzan and Wæver's securitisation theory explains how climate change becomes constructed as a security threat through political discourse and institutional practices. Together, these authors integrate sociological, political, and security perspectives in analysing climate change within a contemporary geopolitical framework (Figure 1).

Figure 1

Integrated theoretical-methodological framework for studying climate change as a global security risk



The central position, "Climate Change (Global Risk)," emphasises that, within these theoretical concepts, climate change is addressed through multilateral cooperation, especially via international platforms such as COP conferences and strategic documents, linking climate risks to foreign policy priorities and positioning climate geopolitics as a new global influence.

3.2. Risk Society and Climate Change

Ulrich Beck's "risk society" concept provides a foundation for understanding climate change as a produced, global risk arising from modernisation processes and industrial development. Unlike traditional threats, which are territorially limited, climate change now has a transnational dimension, creating a new global security structure. Risks are no longer exclusively natural but are socially constructed and distributed, with consequences that unevenly affect different regions and social groups. Social risk perceptions are crucial in shaping political decisions, as interpretation and communication of risk directly influence public policy and institutional responses (Beck, 1992; 2009).

Beck introduces the "risk society" concept, in which global risks such as climate change require transnational coordination. He emphasises that industrial production generates new forms of insecurity, ranging from ecological disasters to economic and political instability. Climate change transforms societal risk perception, prompting states to develop resilience institutions and integrated environmental and security policies. Dalby (2009) adds that climate change generates global insecurity, including migration, food disruptions, and geopolitical tensions, confirming Beck's analysis of transnational risk.

Regional approaches to climate change also exist, highlighting that the issue is not merely a matter of nation-states competing for power and prestige. Anthony Giddens summarised his understanding of climate action in the context of the Kyoto Protocol (UNFCCC, 1997), arguing that it is not multilateralism in action but a series of regional initiatives of varying scope (Giddens, 2009, p. 211). Following emphasis on regional actions and strategic planning, energy security becomes a key element in understanding climate and geopolitical risks.

According to the Energy Institute (2024), global proven economically recoverable fossil fuel reserves - including coal, oil, and natural gas - amount to approximately 42,508.6 EJ. Coal constitutes 60.0 %, oil 24.1 %, and natural gas 15.9 % of reserves. Annual production is 514.4 EJ, with oil 36.7 %, coal 34.8 %, and natural gas 28.4 %. The reserves-to-production ratio (R/P) indicates an estimated lifespan of 82.6 years for total fossil fuels, 54.1 years for oil, 46.3 years for natural gas, and 142.3 years for coal. These data show that after World War II, coal was largely replaced by oil and gas, with many coal reserves remaining unused. In the context of the net-zero by 2050 goal, the fate of fossil fuels - including whether they will follow coal's path or be fully phased out - depends on the policies implemented to achieve it. Ediger (2025) emphasises that the transition to sustainable energy must be just, including fossil-fuel–

producing countries, so that no one is excluded from emission reductions and energy transformation.

Although these reserve and production values suggest that physical depletion of fossil fuels does not pose an immediate short-term threat to global energy system stability, the geopolitical and climate dimension of resource availability reflects a more complex context, in which strategic management of energy resources and transition to sustainable energy become key elements of international security and climate adaptation policies.

3.3. Anthony Giddens' Political Climate Governance Theory

The geographical concentration of oil and gas continues to define global power dynamics, trade, and security. Relying on a few suppliers exposes importers to risk during crises, wars, or sanctions. While LNG market growth and new supply routes change some geopolitical aspects, the underlying strategic reliance on fossil fuels persists.

Giddens (2009) emphasises that the consequences of climate change are long-term and potentially catastrophic. He notes that political systems often react only when threats become immediately visible. Accordingly, the energy transition is not a result of market logic driven by resource depletion. Instead, it is a matter of political governance, regulation, and strategic planning. The long lifespan of fossil fuels means that the decision to phase them out will be political. Giddens advocates a strong role for the state and international cooperation in managing climate risks. Today, energy policy becomes an instrument for shaping a new global order, intertwining security, sustainability, and technological competitiveness.

Within the broader sociological discourse on climate change, Giddens conceptualises the challenge of climate governance through what he famously describes as the “Giddens paradox.” According to this argument, societies tend to delay meaningful action against climate change because its most severe consequences are perceived as distant and abstract. Furthermore, political systems are generally oriented toward short-term interests and electoral cycles. As a result, effective climate policy often emerges only when environmental risks become sufficiently visible and politically urgent (Giddens, 2009). Thus, this paradox highlights a structural mismatch between the temporal nature of climate risks and the decision-making logic of modern democratic systems.

From a sociological perspective, Giddens (2009; 1990) also links climate change to broader processes of modernity, globalisation, and institutional reflexivity. In advanced modern societies, scientific knowledge increasingly shapes political decision-making, yet it simultaneously produces uncertainty and public contestation. As a result, climate change becomes a paradigmatic example of a “manufactured risk,” generated by industrial development and technological progress (Giddens, 1990). Addressing such risks requires new forms of governance that combine state authority and international cooperation, as well as

participation from non-state actors, including corporations, scientific institutions, and civil society. Consequently, climate governance becomes embedded within global political structures and reflects broader transformations in how modern societies manage uncertainty and environmental threats.

3.4. Securitisation of Climate Threats (Buzan & Wæver)

The way climate change is framed as a security issue, demanding urgent and extraordinary measures, is often explained by the concept of securitisation (Buzan, Wæver, & de Wilde, 1998). In this perspective, climate change is not treated solely as an environmental challenge but also as a threat to political stability, economic systems, and human security. The securitisation of climate change reflects the growing perception that environmental threats are closely linked to migration pressures, energy transitions, and regional stability (Kantemnidis & Botetzagias, 2023).

This conceptual framework enables European Union institutions to incorporate climate risks into broader strategic planning, including defence, foreign policy, and crisis management. Through this process, climate-related risks become integrated into institutional responses, enabling the mobilisation of resources and the international legitimisation of climate adaptation and climate security policies (Brzoska & Fröhlich, 2015).

According to securitisation theory, an issue becomes a matter of "security" when a political actor - such as a state, an international organisation, or the European Union - presents a particular problem as an existential threat that requires immediate and exceptional measures. Within this framework, the climate crisis can be interpreted as a threat to human life, critical infrastructure, state stability, or regional security. Political actors frequently employ a language of urgency and threat to justify such extraordinary responses. In the context of climate change, narratives of "global ecosystem collapse," "catastrophic flooding," and "European energy security" function as discursive mechanisms of securitisation.

However, Buzan and his colleagues emphasise that securitisation is not complete unless a relevant audience, such as policymakers, institutions, or the broader public, accepts these claims. In the case of climate change, public perception and political actors must recognise climate risks as sufficiently serious to justify interventionist measures, including climate governance policies, crisis preparedness strategies, and security-oriented institutional responses.

The relocation of climate change from the domain of environmental policy into the sphere of security governance has significant implications. Framing climate change as a security challenge recognises it as a potential driver of conflict, migration flows, and geopolitical instability, thereby legitimising strategic and institutional responses at national and international levels (Buzan, Wæver, & de Wilde, 1998; Dalby, 2009).

Such an analytical perspective enables a broader understanding of climate change not only as an ecological phenomenon but also as a structural factor influencing the evolution of European Union security policy. Numerous scholars argue that climate change operates as a threat multiplier, intensifying existing vulnerabilities through population displacement, resource scarcity, and regional instability (Barnett, 2003; Homer-Dixon, 1999).

Within the European Union, the recognition of climate change as a security issue has led to the gradual incorporation of climate-related risks into formal security frameworks and policy instruments. Climate threats are therefore no longer perceived solely as environmental concerns but increasingly as factors capable of destabilising regions, influencing migration dynamics, and threatening the EU's strategic interests.

Consequently, European institutions - including the European External Action Service - have begun integrating climate risk assessments, adaptation strategies, and crisis management mechanisms into foreign policy and security strategies (EEAS, 2020; EEAS, 2021; Missiroli, 2010). This process can be described as the institutional normalisation of climate security, whereby climate risks become a routine component of security planning rather than an exceptional policy concern.

Through this process of securitisation, environmental challenges are incorporated into a broader strategic framework that connects climate policy with security governance. In practice, the European Union increasingly treats climate change not only as an environmental problem but also as a structural driver of instability, geopolitical competition, and potential conflict.

4. CONCLUSION

Climate change is becoming an increasingly significant factor in shaping contemporary global security. By intensifying existing political, economic, and social pressures, climate change creates new geopolitical risks. In particular, climate-related disruptions may trigger conflicts, increase migration pressures, and exacerbate resource scarcity, especially in regions already characterised by limited access to water, food, and energy (Buzan, Wæver, & de Wilde, 1998; Brzoska & Fröhlich, 2015).

In response to these challenges, climate change is progressively redefining global security priorities. States and international organisations - including the European Union - are increasingly incorporating climate risks into their crisis management, defence, and foreign policy strategies (EEAS, 2021; Missiroli, 2010).

Geopolitical theories provide important analytical insights into these developments. From a classical geopolitical perspective, geographical and environmental factors - including climate conditions and access to natural resources - shape the strategic opportunities of states and

intensify competition for key territories (Kaplan, 2012). In contrast, critical and constructivist approaches emphasise that climate risks are not purely material phenomena but are also socially constructed through political discourse and institutional practices. In this context, perceptions of climate threats play a crucial role in shaping policy responses, resource allocation, and international cooperation (Dodds & Ingram, 2009).

Within this analytical framework, climate change can be understood as a threat multiplier, reinforcing geopolitical tensions and compelling international actors to redefine their security strategies through a combination of diplomatic, economic, and defence instruments (Wæver, 1995; Buzan et al., 1998).

The integration of sociological and security perspectives provides a comprehensive framework for understanding climate change as a global risk with profound political, social, and geopolitical implications. Beck's theory of the risk society (1992; 2009), Giddens' conceptualisation of political governance and climate policy (1990; 2009), and the securitisation theory developed by Buzan and Wæver (1998) together form an interdisciplinary approach to analysing climate threats and the evolution of EU climate security strategies.

Within this context, multilateral platforms such as the Conferences of the Parties (COP) play a crucial role in shaping global climate governance. Through its participation in COP negotiations, the European Union contributes to the formulation of global climate objectives, promotes innovation in green technologies, and strengthens international cooperation on energy security and climate adaptation (EEAS, 2021; European Commission, 2019; European Union, 2023).

Looking ahead, the geopolitics of energy transition will increasingly revolve around access to strategic minerals such as cobalt, lithium, and graphite, which are essential for renewable energy technologies and energy storage systems. As a result, climate security is evolving into a strategic geopolitical resource. By combining sociological and security perspectives, it becomes possible to understand how climate risks transform environmental and societal challenges into geopolitical and strategic priorities. In this sense, climate change should be understood not merely as an environmental phenomenon but as a central driver of the transformation of international relations and global security strategies, particularly within the European Union and the evolving global order.

REFERENCES

- Bailey, I. (2010). Copenhagen and the new political geographies of climate change. *Political Geography*, 29(3), 127–129. <https://doi.org/10.1016/j.polgeo.2010.02.008>
- Barnett, J. (2003). Security and climate change. *Global Environmental Change*, 13(1), 7–17. [https://doi.org/10.1016/S0959-3780\(02\)00045-1](https://doi.org/10.1016/S0959-3780(02)00045-1)
- Beck, U. (1992). *Risk society: Towards a new modernity*. London, UK: Sage.
- Beck, U. (2009). *World at risk*. Cambridge, UK: Polity Press.
- Beeson, M., & Firth, S. (2016). *Environmental security in East Asia*. Abingdon, UK: Routledge.
- Brzoska, M., & Fröhlich, C. (2015). Climate change, migration and violent conflict: Vulnerabilities, pathways and adaptation strategies. *Migration and Development*, 4(2), 281–305. <https://doi.org/10.1080/21632324.2014.928060>
- Bulkeley, H. (2001). Governing climate change: The politics of risk society? *Transactions of the Institute of British Geographers*, 26(4), 430–447. <https://doi.org/10.1111/1475-5661.00028>
- Buzan, B., Wæver, O., & de Wilde, J. (1998). *Security: A new framework for analysis*. Boulder, CO: Lynne Rienner.
- Christoff, P. (2010). Cold climate in Copenhagen: China and the United States at COP15. *Environmental Politics*, 19(4), 637–656. <https://doi.org/10.1080/09644016.2010.489718>
- Consilium. (2025). Council conclusions on climate diplomacy. *European Council*. <https://www.consilium.europa.eu/en/documents-publications/>
- Council of the European Union. (2022). *Strategic Compass for Security and Defence*. Brussels, BE: Council of the EU. https://www.consilium.europa.eu/media/54784/strategic-compass_en.pdf
- Dalby, S. (2009). *Security and environmental change*. Cambridge, UK: Polity Press.
- Ediger, V. Ş. (2025). Leaving no one behind: Just energy transition of fossil fuel-producing countries. *Frontiers in Political Science*, 7, 1536594. <https://doi.org/10.3389/fpos.2025.1536594>
- EEAS – European External Action Service. (2016). *Climate change and international security*. Brussels, BE: EEAS. <https://www.eeas.europa.eu/climate-change-and-security>
- EEAS – European External Action Service. (2020). *Climate-related security risks: EU approach*. Brussels, BE: EEAS. <https://www.eeas.europa.eu/climate-security>
- EEAS – European External Action Service. (2021). *Climate diplomacy: EU strategic framework*. Brussels, BE: EEAS. <https://www.eeas.europa.eu/climate-diplomacy>

- Energy Institute. (2024). *Global energy outlook 2024*. London, UK: Energy Institute.
<https://www.energyinst.org/global-outlook>
- EU UNEP. European Union & United Nations Environment Programme. (2025). Climate Change, Environment, Peace & Security Partnership (Phase II). https://global-threats.europa.eu/our-projects/eu-unep-climate-change-and-security-partnership-phase-ii_en
- European Commission. (2019). *The European Green Deal*. Brussels, BE: European Commission. https://ec.europa.eu/commission/presscorner/detail/en/ip_19_6692
- European Commission. (2025). *EU positions at COP30*. Brussels, BE: European Commission. <https://ec.europa.eu/cop30>
- European Commission & HR/VP. (2023). *Joint communication on climate and security*. Brussels, BE: European Commission. <https://ec.europa.eu/joint-communication-climate-security>
- European Union. (2023). *EU climate policy framework*. Brussels, BE: European Union. <https://europa.eu/climate-policy>
- García Rico, L. (2022). NATO and Climate Change: A Climatized Perspective on Security (Research Paper 01/2022).
- Giddens, A. (1990). *The consequences of modernity*. Cambridge, UK: Polity Press.
- Giddens, A. (2009). *The politics of climate change*. Cambridge, UK: Polity Press.
- Homer-Dixon, T. (1999). *Environment, scarcity, and violence*. Princeton, NJ: Princeton University Press.
- Kaplan, R. D. (2012). *The Revenge of Geography: What the Map Tells Us About Coming Conflicts and the Battle Against Fate*. Random House.
- Klein, F. M., & Schäfer, L. (2025, September). From courtrooms to COP30: How 2025 climate cases can raise global climate ambition. *Germanwatch*.
<https://www.germanwatch.org/en/93278>
- Missiroli, A. (2010). *Climate change and EU foreign policy*. Paris, FR: European Union Institute for Security Studies. <https://www.iss.europa.eu/content/climate-change-eu-foreign-policy>
- Obergassel, W., Arens, C., Beuermann, C., Brandemann, V., Elsner, C., Höhne, C., Kreibich, N., Schell, J., Schulze Steinen, M., & Ott, H. E. (2025). *The bitter (COP of) truth – Belém 2025 climate conference not up to the challenge (COP30 Report)*. Wuppertal Institut für Klima, Umwelt, Energie gGmbH.
https://wupperinst.org/fa/redaktion/downloads/publications/COP30-Report_en.pdf
- UNFCCC. United Nations Framework Convention on Climate Change. (1995). *Decision 1/CP.1: The Berlin Mandate*. <https://unfccc.int/resource/docs/cop1/07a01.htm>

- UNFCCC. United Nations Framework Convention on Climate Change. (1997). *Kyoto Protocol to the United Nations Framework Convention on Climate Change*. <https://unfccc.int/resource/docs/convkp/kpeng.pdf>
- UNFCCC. United Nations Framework Convention on Climate Change. (2009). *Copenhagen Accord*. <https://unfccc.int/resource/docs/2009/cop15/eng/107.pdf>
- UNFCCC. United Nations Framework Convention on Climate Change. (2023). *COP28 official outcomes*. Bonn, DE: UNFCCC. <https://unfccc.int/cop28>
- United Nations Security Council (2025). 10035th meeting - TIPS: Climate and security – environmental impact of armed conflict and climate-driven security risks. <https://main.un.org/securitycouncil/en/events/10035th-meeting-tips-climate-and-security-environmental-impact-armed-conflict-and-climate>
- Wæver, O. (1995). Securitization and desecuritization. In R. Lipschutz (Ed.), *On security* (pp. 46–86). New York, NY: Columbia University Press.

INTEGRATING DEFENCE AND SOCIETY: THE ROLE OF SPECIAL OPERATIONS FORCES IN NATIONAL RESILIENCE

Saša Đerić¹, Marijan Turkalj², Rafael Šubat³, Branimir Bekavac^{4*}

¹Croatian Armed Forces

E-mail: dericsasa@gmail.com

ORCID: <https://orcid.org/0009-0001-2126-2961>

² Croatian Armed Forces

E-mail: marijan.turkalj@gmail.com

ORCID: <https://orcid.org/0009-0000-1747-5705>

³ Croatian Armed Forces

E-mail: subatrafael@gmail.com

ORCID: <https://orcid.org/0000-0001-6475-0888>

⁴ Croatian Armed Forces

E-mail: bbekavac@xbe.33mail.com

ORCID: <https://orcid.org/0009-0005-3639-1941>

Abstract

In the current unstable, volatile international system, hybrid threats to nations include cyberattacks, disinformation, sabotage, subversion, criminal and terrorist activities, underscored by an increasing threat of conventional force. In addition, looming climate change and future pandemics broaden the spectrum of security challenges, while defence resources remain comparatively low.

* Disclaimer: The following text is based on a review of the academic and professional literature on the topic, completed with analysis of available open-source material and discussion with practitioners and scholars during academic conferences. No content of this paper is based on classified material, the authors' professional experience, nor does it contain any sensitive information. The views expressed in this paper are those of the authors. They do not reflect the policy and should not be seen as an official position of any institution or government that the authors otherwise may represent or may be affiliated with.

To counter these, NATO emphasises resilience, defined as the ability to prepare for, withstand, and recover quickly from crises while maintaining the Alliance's functions. Central to this is civil preparedness, which ensures continuity of governance, essential services, and civilian support for military operations, as well as the resilience of critical infrastructure. This implies a role for the armed forces in building resilience, potentially allowing special operations forces (SOF) to play a pivotal role.

The first part of the paper will define resilience and distinguish it from related concepts, after which the authors will provide historical examples of SOF's use in building national resilience. The case studies will focus on the experiences of Croatian SOF during the Homeland War, and the activities of the USA and other NATO states' SOF in the Baltic states and Ukraine.

While this role of SOF is thus anything but new, the authors will highlight potential challenges, including doctrinal, conceptual and legislative discrepancies in a local context, as well as the necessity to adapt plans and concepts from a legacy mindset to one of competition in the age of AI, big data, and remote warfare.

Ultimately, this paper aims to present SOF's potential to serve as a bridge between institutions and concepts by breaking out of an outdated box. The authors hope to identify clear recommendations on leveraging SOF's unique strengths to help contribute to national resilience in the current era.

Keywords: Resilience; Civil Preparedness; Hybrid Threats; Special Operations Forces

INTRODUCTION

In the current global landscape, threats are pervasive and continue to expand in both scope and complexity. Ranging from propaganda, disinformation and cyberattacks at the non-kinetic end of the spectrum, through terrorism and insurgency, to open high-intensity warfare, epitomised by war in Ukraine. The perception of the threat is also further intensified by a resurgence in nuclear sabre-rattling. Beyond anthropogenic threats, the increasing frequency and severity of floods, wildfires, and storms associated with global warming place considerable strain on already overstretched state capacities, at a time when the societal and economic consequences of the COVID-19 pandemic have yet to abate fully.

When confronted with hybrid threats that target multiple sectors of society, the public sector – namely governments – which on average comprise approximately 2% of the national population, lacks the capacity to respond effectively (Pierini, 2023, p. 360). To mobilise the untapped 98% of the population, primarily the private and civic sectors, and to transform defence from a whole-of-government into a whole-of-society endeavour, NATO Special Operations Headquarters (NSHQ), later renamed as Allied Special Operations Command (SOFCOM), developed the Comprehensive Defence Concept (NATO Special Operations

Headquarters, 2020a). Within this framework, resilience constitutes the first line of defence, and its development is conceived as a whole-of-government effort. This article examines how Special Operations Forces (SOF), an integral component of the military establishment, can strengthen national resilience.

This study examines the role of Special Operations Forces in strengthening national resilience, with methodology and research design outlined in the following section.

1. METHODOLOGY

1.1. Research aims and objectives

The article aims to substantiate the hypothesis that Special Operations Forces (SOF) are a valuable tool for strengthening national resilience and to explore opportunities for doing so. The value of SOF in building resistance networks has already been explored through the Resistance Operating Concept (Fiala, 2019). In contrast, the role of SOF in building resilience, a prerequisite for resistance, remains under-researched. This article could provide insights into why some nations never formalise their resistance plans, given the inherent political risks. Not formalising a resistance plan puts even greater emphasis on building and strengthening resilience as a first line of defence. In this context, SOF can leverage their unique capabilities to enhance a whole-of-government and whole-of-society effort to respond to current and future threats.

1.2. Research design

This article adopts a case study methodology to examine the role of SOF in building national resilience, with particular emphasis on Croatia, Ukraine, the Baltic states, and Georgia. The case study seeks to answer the question:

"How can Special Operations Forces (SOF) contribute to building and strengthening national resilience?"

The study follows a structured progression, starting with theoretical definition and delineation, through past and present application, and possible future, and is organised as follows:

1.2.1. Theoretical foundation

To enhance the reader's understanding, the first part of the methodology establishes a theoretical framework that defines and delineates the following concepts: Total Defence, Comprehensive Defence, Resilience, and *Resistance*. This part also examines how resilience contributes to a state's overall defence and deterrence capacity, and why some states adopt a Comprehensive Defence concept while others do not.

1.2.2. Case study approach

A case study methodology is employed to illustrate the practical applications of SOF in building resilience and to explore how their roles vary across different strategic and institutional contexts. The selection of Croatia, Ukraine, the Baltic states, and Georgia is purposeful, reflecting variation in the threat environment, the level of NATO integration, and the maturity of resilience and resistance frameworks. This variation allows for a structured comparison of how SOF contribute to resilience under conditions ranging from active conflict to peacetime preparation.

Each case is examined through a common analytical lens, focusing on the functional roles SOF performs, their level of integration within broader governmental and societal structures, and the type of contribution they make to resilience, whether in preparation, crisis response, or sustainment. This enables the identification of recurring patterns and context-specific differences.

The case studies include:

Croatia: SOF supporting the protection of the nation's critical infrastructure and building resistance-to-occupation capacities, illustrating key tenets of possible SOF roles in a historical context.

Ukraine: SOF as an interagency integrator, innovator and cross-sectoral liaison. The only recent battle-proven effort is highly instructive for the other endeavours.

Baltic states: SOF as a whole-of-society trainer, interoperability enabler, and external support provider. A case study encompassing states with some of the most developed resilience and resistance capabilities, especially given their size.

Georgia: SOF leading efforts toward a whole-of-government approach to resilience and resistance, albeit under significant political and institutional constraints and with limited external support.

1.2.3. Strategic recommendations

Based on insights from theoretical analysis and case studies, the paper offers strategic recommendations for employing SOF to build and strengthen national resilience. Rather than prescribing resistance to states unwilling to employ a comprehensive defence framework, the paper distils how SOF can still be employed to build national resilience, thereby enhancing the state's capacity to defend itself and facilitating a flexible, broad response to threats.

The article ultimately aims to stimulate Croatian academic discussion on the incorporation of resistance plans into the state's defence, particularly in light of the November 2025 reintroduction of conscription (Hrvatski Sabor, 2025). It also aims to illustrate the importance and benefits of fostering resilience and to outline how SOF can contribute to building national resilience as part of the broader whole-of-government endeavour.

2. DEFINING RESILIENCE

The concept of *Comprehensive Defence* – a whole-of-society approach to national security – has its roots in Total Defence strategies adopted by non-aligned states during the Cold War. These approaches emphasised military preparedness within a whole-of-government framework, acknowledging the power imbalance with the Soviet Union (Berzina, 2020). Lacking the capacity to match Soviet military strength, these states adopted deterrence-by-denial strategies: conscripting both military and civilian populations, organising pre-conflict resistance, and, metaphorically, rendering themselves an "indigestible hedgehog" to raise the cost of invasion. A notable by-product of this extensive civil defence network and broad civic integration was a high level of societal resilience (Fiala, 2020, p. 171).

The Swiss model of *Total Defence* during World War II served as a template for the later Cold War *Total Defence* model (Fiala, 2020, p. 171), in which Special Operations Forces served as a stay-behind guerrilla capability in Soviet-occupied areas. Though never employed and sidelined by the fall of the Soviet Union and the advent of the Global War on Terror (GWOT), *Total Defence* resurfaced in response to Russia's hybrid warfare campaign in Crimea and eastern Ukraine.

Hybrid threats, which are multi-domain, ambiguous, and target all sectors of society, exceed the capacity of traditional security sectors, which typically comprise only 2% of a state's population. Thus, effective defence requires mobilising the remaining 98% – namely, the private and civic sectors – transforming defence into a truly whole-of-society effort (Pierini, 2023, p. 360). In this context, NATO Allied Special Operations Command (SOFCOM) (then still called NSHQ) developed the *Comprehensive Defence Handbook* in two volumes (NATO Special Operations Headquarters, 2020a, 2020b), which also outlines concepts of resilience and resistance.

A cornerstone of this strategy is the *Resistance Operating Concept* (ROC), which defines resistance as:

"A nation's organised, whole-of-society effort, encompassing the full range of activities from non-violent to violent, led by a legally established government (potentially exiled/displaced or shadow) to re-establish independence and autonomy within its sovereign territory that has been wholly or partially occupied by a foreign power" (Fiala, 2020, p. XV)

This distinguishes resistance from insurgency: the former is a legitimate government-led, whole-of-society effort to restore national sovereignty, while the latter is typically led by non-legitimate actors and motivated by other political grievances (Fiala, 2020, p. XV). Recognising its deterrent value and influenced by geographic proximity to Russia and/or historical

precedents, countries such as Switzerland, Finland, Sweden, Poland, Estonia, Latvia, Lithuania and Ukraine have institutionalised resistance strategies.

Nevertheless, organising resistance carries inherent political risks. It may be interpreted as either a tacit admission of the state's inability to defend its territory or an inadvertent empowerment of revolutionary actors. Consequently, many states avoid formal resistance frameworks (Burrell & Collison, 2025, p. 40), though they may still invest in resilience – a foundational element of effective resistance (Fiala, 2020, p. 7).

Resilience is defined as: "*The will and ability to withstand external pressures and influences and/or recover from the effects of those pressures or influences.*" (Fiala, 2020, p. XV)

According to Fiala (2020, p. 187), national resilience is shaped by several factors: a sense of national identity, as that is usually amongst the most influential factors affecting the willingness to defend the country (Murauskaite, 2024, p. 5); psychological preparation; vulnerability recognition and reduction; preparation and planning for crisis; interoperability with external supporters; and planning for resistance. As former NATO Secretary General Jens Stoltenberg observed, a strong military is essential, but it cannot be strong if society is weak (Pierini, 2023, p. 356).

This link between civilian preparedness and national defence is codified in Article 3 of the North Atlantic Treaty (1949), which commits member states to develop their capacity to resist armed attack through continuous and effective self-help and mutual aid. The increasing interdependence of civilian and military infrastructure – especially evident during disaster response operations – underscores the need for coordinated, cross-sectoral approaches to contemporary threats, including cyberattacks, disinformation campaigns, hybrid warfare, armed incursions, and natural disasters (NATO Special Operations Headquarters, 2020a, p. 18). The importance of this was further underscored by the 2025 NATO Summit in The Hague, although no substantive discussion on resilience took place (Wright, 2025). Allies committed to hitting 5% of states' GDP for defence spending, of which 3.5% will be on core defence requirements, while 1.5% will go to protecting critical infrastructure, defending networks, ensuring civil preparedness and resilience, enhancing innovation, and strengthening defence industrial base, i.e. strengthening national resilience (NATO, 2025).

Governments, therefore, must ensure inter-agency coordination, which has historically been problematic (Stringer, 2022, p. 67), educate and empower citizens to contribute to national security, and foster private- and civic-sector awareness and engagement (NATO Special Operations Headquarters, 2020a, pp. 16–17). This is achieved through training, education, and integration, all of which involve SOF. This also positively influences overall resilience, which, in turn, enhances deterrence (Fiala, 2020, p. 7).

3. CASE STUDIES OF EMPLOYING SOF IN BUILDING NATIONAL RESILIENCE

The Resistance Operating Concept defines resilience as a foundational condition enabling a nation to resist aggression and restore sovereignty following external coercion or occupation (Fiala et al., 2020, pp. 17-19). Resistance, in turn, is understood as a whole-of-society effort conducted under legitimate state authority, encompassing both violent and non-violent actions (Fiala et al., 2020, p. 23). This conceptual distinction is central to understanding the cases selected below. As Pettersson and Ilis-Alm (2022, pp. 77-80) argue, resilience forms the foundation upon which resistance is built; without institutional continuity, societal cohesion, and adaptive capacity, organised resistance cannot be sustained. In this sense, resilience is not a passive condition but an actively cultivated capability. Fedorchak (2024, pp. 18-21) further develops this argument by introducing the concept of resilient fighting power, emphasising that modern conflict favours states capable of integrating military operations with political legitimacy, social mobilisation, and institutional learning.

The case studies below were selected for their relevance in the extant European security environment.

3.1. Croatia

The dissolution of the Socialist Federal Republic of Yugoslavia and the Croatian War for Independence, locally known as the Homeland War, provide a fascinating and understudied case study of societal resilience and resistance. Yugoslavia, one of the founders of the non-aligned movement during the Cold War, was a heavily militarised society that espoused a total defence variant (Marijan, 2008, pp. 25-34). Through mandatory secondary school classes on total defence and societal protection (*općenarodna obrana i društvena samozaštita*, colloquially *ONO i DSZ*), as well as through mandatory conscription of men for service in the Yugoslav People's Army (*Jugoslavenska narodna armija* – JNA), the country might have been a textbook example of designed resilience and planned resistance – had it not disintegrated from within. Unable to override the perpetual internal crisis of competing national programs, the system had sown the seeds of its own destruction.

Though extremely poorly armed in 1991, the nascent armed formations of newly independent Croatia (police forces growing into National Guard, and then into the Armed Forces) could thus rely on a nationally cohesive society with clear crisis roles, infrastructure, and a very large pool of militarily trained men. Among the more numerous conventional formations, various special operations or special-purpose units were soon established, generally as independent battalions under direct command of the Ministry of Defence or the General Staff of the Armed

Forces.¹ These units were often based on command or training cadre with foreign experience, often combat veterans from the French Foreign Legion.

Among the first tasks they were given was to help protect critical infrastructure. At the time, the JNA was losing the Battle for the Barracks but remained present throughout Croatia, including the capital, as did various elements of the Yugoslav intelligence and security services. Information superiority was key to cohering and maintaining national morale, conveying the reality of the aggression against Croatia, and countering the opposing side's narrative.

Croatian Radiotelevision (*Hrvatska radiotelevizija* – HRT) was receiving regular telephone and written threats, as well as small arms fire incidents. It had been guarded by the National Guard (*Zbor narodne garde* – ZNG) until they were dispatched to the deteriorating front lines (Šulj, 2023, pp. 37–38). To overcome initial scepticism about their assessment and to demonstrate the compound's vulnerability, Croatian SOF organised an unannounced simulated small-group raid. They took over the Information Program studios within minutes and completely paralysed the institution. As a result of this demonstration, the Frankopan battalion was tasked with revising security for HRT headquarters. Indicative in this episode was the perceived need to force external elements of a young national security system into action. The event spurred a more serious approach to security for critical infrastructure: surrounding terrain was cleared, air defence and heavy machine guns were deployed, mines were planted, and additional guard positions were established at entrances. The stabilised security of HRT was then handed to other units (Šulj, 2023, pp. 38–41).

Providing essential services, including protection, potable water, transportation, and information, is one of the main governmental functions in any crisis. As crises escalate, especially given a hybrid-war context underwritten by open warfare in Europe, security services' capacities may be saturated relatively quickly under a multi-pronged assault. Although the Croatian security and defence system of 2026 differs greatly from that which existed at the beginning of the Homeland War, Croatian SOF retains an institutional memory of its role in protecting critical infrastructure, including through red teaming, as well as in providing military assistance to interagency and intersectoral partners.

To effectively employ SOF in comprehensive defence, two main principles should be adhered to: it should be employed early in competition and crisis, and it may be employed "*primarily*

¹ These included the Zrinski, Frankopan, Ban Jelačić, Alpha, Kralj Tomislav, Matija Vlačić, Ferdo Sučić battalions, as well as a Company of Tactical Snipers. Other special purpose units during the war included the General Staff Diversionary Unit (*Diverzantski odred Glavnog stožera* – DOGS), General Staff Reconnaissance-Diversionary Company (*Izvidničko-diverzantska satnija Glavnog stožera HV-a* IDS GSHV), the 1st Croatian Guards Corps (*1. Hrvatski gardijski zdrug*), and 352nd Naval Diver-Saboteur Battalion (*352. Roniteljsko-diverzantska bojna HRM*) (Čanić, 2023, p. 12). The naming conventions and name changes add another layer of complexity to chronicling, as do the disparate ideas of what SOF really is. A comprehensive history of special operations in the Homeland War and assessment of their effectiveness is yet to be written.

where other military or civilian assets are unable to singularly create desired effects "(NATO Special Operations Headquarters, 2020a). Croatian SOF was employed early in its existence for a non-traditional, resilience-building task, demonstrating that using SOF to protect critical infrastructure is neither heretical nor novel.

Other tasks assigned to multiple Croatian SOF units, related to building resilience during the Homeland War, were centred on military assistance, a traditional SOF mission. For example, the first Croatian SOF unit ever established was immediately tasked with building resistance to the occupation. From June 1991, the unit participated in establishing, organising, and training the Vukovar National Guard battalion. Simultaneously, they conducted patrols and reconnaissance of the area (Lucić, 2011, pp. 22–23).

A comprehensive history of the Croatian SOF units' contributions to resistance and resilience in the 1990s remains to be fully researched and offers a venue for future academic endeavour. These initial findings, however, support the indication of a key SOF role in building national resilience at a pivotal moment of a defensive context.

3.2. Ukraine

Russia's full-scale invasion of Ukraine represents arguably the most consequential test of national resilience in Europe since the end of the Cold War. Beyond conventional military performance, the conflict has demonstrated that national survival increasingly depends on the ability to integrate military power, state institutions, civil society, and international support into a coherent system of resistance. In this context, Ukraine offers a uniquely instructive case for analysing how resilience functions in practice under conditions of sustained, high-intensity warfare.

The Ukrainian experience confirms that resilience is not merely a supporting element of defence but a decisive factor shaping the outcome of conflict. As Fedorchak (2024, pp. 18-21, 27-28) argues, Ukraine's ability to endure and adapt cannot be explained solely by force size or external assistance, but rather by the development of what she terms resilient fighting power, understood as the capacity to sustain, regenerate, and effectively employ military power under prolonged pressure. This represents the capacity of a state to integrate military effectiveness, institutional adaptability, societal mobilisation, and external support into a coherent and enduring defence system. Within this framework, SOF have emerged as a critical enabler of national resilience. Rather than functioning solely as tactical units, Ukrainian SOF have acted as institutional integrators, interagency coordinators, and international liaisons, translating strategic intent into operational resilience. The term "Ukrainian SOF" is used here in a broad sense, encompassing units from multiple departments, ministries, and agencies with varied tasks and remits (Stringer & Vivdych, 2025), reflecting a post-Soviet evolution not entirely unlike the Croatian post-Yugoslav experience. This role closely reflects the principles

articulated in the Resistance Operating Concept (Fiala et al., 2020, p. 17) and identifies resilience as a prerequisite for successful resistance (Fiala et al., 2020, p. 25).

Ukraine's experience strongly supports this assessment. Following 2014, and especially after 2022, Ukraine progressively developed the institutional and societal foundations necessary to sustain long-term resistance (Shelest, 2022, pp. 1-2), while specialised and small-unit forces, including elements of the SOF, played an important enabling role in sustaining operational resilience and battlefield momentum (Watling & Reynolds, 2023, pp. 13-14, 21).

One of the most significant dimensions of Ukraine's resilience has been the protection and maintenance of critical infrastructure amid constant attacks. While legal responsibility for infrastructure protection remained with civilian authorities, SOF played an enabling role in supporting risk assessment, contingency planning, and interagency coordination within national resistance planning frameworks (Fiala, 2020, pp. 3, 8-10).

SOF facilitated communication between military planners, government institutions, and private infrastructure operators, particularly in the energy, transport, and communications sectors. This coordination proved essential in mitigating the effects of Russian strikes and ensuring continuity of essential services. The protection of critical functions and services is also recognised in NATO doctrine as a key element of resilience, particularly the ability to sustain governance and essential systems under pressure (Fiala et al., 2020, pp. 25-26). Ukraine's experience confirms this assessment. As Fedorchak (2024, pp. 18-21, 27-28) notes, resilient fighting power depends not on preventing disruption entirely, but on sustaining functionality and recovery under persistent pressure, an area in which SOF played a decisive facilitating role (Fiala, 2020, pp. 73-75, 77, 80-81).

A defining feature of Ukraine's resilience has been the central role of training and education in building adaptive capacity across both military and civilian domains. Ukrainian SOF were instrumental in developing not only tactical competence but also leadership, decentralised decision-making, and crisis-management capabilities. This approach reflects the ROC's emphasis on preparing societies for conflict through education, planning, and coordination among governmental and non-governmental actors (Fiala et al., 2020, pp. 27-29). Hedenskog (2023, pp. 2-3, 5-6) highlights that Ukraine's ability to mobilise local authorities, volunteers, and civil institutions significantly compensated for material disadvantages during the early phases of the war. A particularly innovative aspect of Ukraine's approach was the use of the Remote Advise and Assist Cell (RAAC) model, which enabled continuous advisory support from partner nations without physical deployment. This model allowed Ukraine to benefit from allied expertise while reducing the risk of escalation and preserving operational autonomy (Meredith, 2024). Fedorchak (2024, pp. 18-21, 27-28) identifies adaptive learning as one of Ukraine's key advantages, noting that resilience emerged through continuous feedback between combat experience, institutional reform, and external support. SOF played a key role in

facilitating this learning process by emphasising mission command, flexibility, and rapid adaptation (Watling & Reynolds, 2023, pp. 13-15; Spulak, 2007, pp. 11-16).

A defining characteristic of Ukrainian SOF employment has been its role as an interagency integrator. As outlined in the United States' SOF Interagency Reference Guide, SOF are uniquely positioned to operate across institutional boundaries, linking military, governmental, and civilian actors (JSOU, 2020, pp. 2-8). In Ukraine, this role manifested in close coordination between SOF, intelligence agencies, territorial defence forces, civil authorities, and international partners. SOF served as connective tissue within a fragmented security environment, ensuring the coherence of effort and the continuity of decision-making. At the international level, this integrative function was institutionalised through cooperation with Combined Joint Special Operations Task Force-10 (CJSOTF-10) (Meredith, 2024). This structure enabled sustained liaison with NATO partners, synchronisation of training and advisory efforts, and coordination of external support while preserving Ukrainian operational autonomy. SOF also played a key role in engaging private-sector actors involved in logistics, communications, medical support, and technological innovation. These civil-military-commercial partnerships proved essential for rapid adaptation and sustained operational effectiveness, highlighting the evolving nature of resilience in contemporary conflict.

The Ukrainian experience demonstrates that SOF serve as catalysts for innovation under conditions of strategic pressure. Faced with material constraints and constant operational threats, Ukrainian SOF adopted decentralised command structures, rapid experimentation cycles, and flexible logistics models. These innovations included the integration of commercial technologies, adaptive use of unmanned systems, and decentralised sustainment solutions. Such approaches reduced vulnerability to disruption and enhanced operational resilience. As Jones and Love (2022, pp. 22-26, 30-31) argue, modern resilience and resistance are fundamentally adaptive processes in which success depends on a state's ability to learn, adjust, and respond more effectively than its adversary to changing conditions. SOF, by virtue of their organisational culture and mission command philosophy, are uniquely suited to drive such adaptation.

The Ukrainian case also demonstrates that resilience itself constitutes a form of deterrence. By maintaining societal cohesion, operational continuity, and adaptive capacity, Ukraine significantly reduced the strategic effectiveness of Russian coercion. SOF contributed to this effect by sustaining resistance networks, facilitating international assistance, and reinforcing public confidence in state institutions.

The Ukrainian case suggests that SOF are central to the construction of national resilience in modern conflict. Their value lies not primarily in kinetic action, but in their capacity to integrate institutions, enable cooperation, foster innovation, and sustain societal cohesion under extreme pressure. By functioning simultaneously as interagency coordinators, international liaisons, trainers, and innovation enablers, Ukrainian SOF embodied the principles articulated in

NATO's Resistance Operating Concept. Their experience demonstrates that resilience is not a by-product of defence planning but a foundational element of national security. For NATO and partner nations, the Ukrainian case underscores a critical lesson: investing in SOF as integrative and adaptive actors is essential for building resilient societies capable of withstanding contemporary hybrid threats.

3.3. Baltic states

The security environment of the Baltic states has been profoundly shaped by the evolving threat posed by the Russian Federation, which manifests not only through conventional military capabilities but also through hybrid activities, information operations, and sustained political pressure. In response to this security environment, Estonia, Latvia, and Lithuania have adopted a comprehensive approach to defence that goes beyond traditional military concepts and places resilience and societal preparedness at the centre of national security planning (Flanagan et al., 2019, pp. 1-2, 6; Saxi, Sundelius, & Swaney, 2020, pp. 2-5).

This strategic shift is grounded in the understanding that modern conflicts are increasingly waged below the threshold of open warfare. The Resistance Operating Concept (ROC) reflects this reality by emphasising that resistance and resilience must be developed in advance of conflict and embedded across military, governmental, and societal structures (Fiala, 2020, pp. 1-2). Rather than relying solely on conventional deterrence, the ROC framework emphasises the importance of preparing societies to absorb shocks, remain functional, and resist coercion, even under conditions of occupation or sustained pressure.

Within this framework, US SOF play a central role. Their contribution extends well beyond tactical military training and encompasses the development of institutional capacity, interagency coordination, and civil-military integration. According to the U.S. Special Operations Command, SOF are uniquely suited to operate in complex environments where political, military, and societal dimensions intersect, enabling them to act as integrators between national institutions, security forces, and civilian actors (U.S. Special Operations Command, 2020, pp. 1-3).

Following Russia's annexation of Crimea in 2014, US SOF engagement in the Baltic region intensified significantly. As documented by Piotr Szymański (2021), this engagement focused on strengthening national special operations forces, enhancing interoperability with NATO allies, and improving readiness for hybrid and irregular conflict scenarios. These activities were not limited to operational training; they also included doctrinal development, command-and-control integration, and the establishment of enduring professional networks between U.S. and Baltic personnel.

A defining feature of the Baltic approach to security is the integration of military defence with broader societal resilience. Latvia's concept of comprehensive state defence exemplifies this

model by formally incorporating government institutions, local authorities, the private sector, and citizens into a unified security framework (Ministry of Defence of the Republic of Latvia, n.d.). This approach reflects the understanding that national defence cannot be sustained by the armed forces alone but depends on society as a whole's ability to function during crises.

The development of national special operations forces occupies a particularly important place within this framework. As Jauniskis (2012, pp. 1-2, 11-12) argues, small states lack the strategic depth and mass required for conventional deterrence and must therefore rely on highly capable, adaptable, and interoperable forces. US SOF have played a crucial role in assisting the Baltic states in building such forces, supporting doctrinal development, professional education, and establishing operational standards aligned with NATO practices.

Joint exercises represent another critical pillar of this cooperation. These exercises serve not only to enhance tactical proficiency but also to build trust, improve interoperability, and ensure mutual familiarity among allied forces. From a strategic perspective, they function as an important element of deterrence by signalling preparedness and resolve while simultaneously reducing uncertainty in crisis situations. The International Centre for Defence and Security (2023) highlights the growing importance of societal resilience and whole-of-society preparedness in the Baltic region, which together shape contemporary approaches to deterrence.

Beyond the military domain, the Baltic model emphasises civilian resilience and the continuity of essential services. This dimension is particularly evident in efforts to strengthen energy security and infrastructure resilience. The study on societal resilience to energy outages highlights how disruptions to critical infrastructure can have cascading effects on national security, economic stability, and public confidence, underscoring the need to integrate civilian preparedness into defence planning (Kramens, 2025, pp. 5-7, 20-22). Although not a military document, this analysis reinforces the broader logic of total defence by demonstrating how societal resilience directly supports deterrence and crisis endurance.

The Lithuanian model of total defence further illustrates this integrated approach. As analysed by Stringer and Noyes (2025), Lithuania has developed a system that actively involves citizens, volunteer organisations, and civil institutions in national defence planning. The Lithuanian total defence model seeks to strengthen deterrence by ensuring that any act of aggression would encounter not only military resistance but also broad societal involvement capable of sustaining long-term resistance (Stringer & Noyes, 2025).

In this context, US SOF serve as a critical enabling actor. Their long-term engagement supports the development of resilient defence ecosystems in which military capability, institutional preparedness, and societal cohesion reinforce one another. The Baltic experience demonstrates that contemporary deterrence is no longer defined solely by military superiority but increasingly by a state's ability to withstand pressure, adapt to disruption, and mobilise society

in defence of national sovereignty. Through their advisory role, training activities, and integration into national defence planning, US SOF directly contribute to this broader form of deterrence, making them an essential component of the Baltic security architecture.

3.4. Georgia

Georgia, with its 4.9 million citizens and 69,700 sq km ('Country Factsheet', n.d.), is comparable in size to Croatia. It borders Russia to the north, Russia-controlled Black Sea to the west, and Türkiye, Armenia, and Azerbaijan to its south. It has no geopolitical allies in its neighbourhood, and although Georgia aspires to join the EU, the nearest EU member state lies across the Black Sea. (Lavrelashvili, 2018, p. 192). After the Bucharest NATO Summit in 2008, Russia invaded Georgia to prevent it from joining NATO or the EU.

Teona Lavrelashvili (2018) in her article from 2018 suggested that promoting resilience in Georgia (as well as Moldova and Ukraine) "requires more proactive and effective policies, but also more political commitment and smart resource allocation. The EU should design policies tailored to the specific needs of each of the three countries, with security being the common main concern" (Lavrelashvili, 2018, p. 194).

In 2020, Brian Petit directed a U.S. Special Operations Command Europe (SOCEUR) sponsored National Resistance Course (NRC) in Tbilisi (Petit, 2025, p. 110). The course introduced Georgian Special Operations Forces (GSOF) to whole-of-society resistance. Petit (2025) acknowledges that GSOF quickly became the national leader in spreading the new concept. Guided by its Ministry of Defence, Georgia developed a national resistance concept that has not yet been codified into law (Petit, 2025, pp. 110–111). There are three main reasons the concept has not been elevated to a law. Firstly, it could be considered by some as provocative and openly anti-Russian. Secondly, it would disrupt the balance of Georgian relationships with Russia and the West. Finally, there is no sufficient political will to implement whole-of-society resilience and resistance measures, especially since the Russian invasion of Ukraine in 2022 (Petit, 2025, pp. 111–112).

While the GSOF effort is noteworthy, it is a bottom-up approach that has not been able to involve the whole of government, let alone the whole of society. SOF can be the leader in resilience-building efforts, but a comprehensive assessment and plan should come from the governmental level. Therefore, it would be most effective to have a national resilience strategy document that all other resilience plans should align with.

The Tbilisi-based think tank, the Georgian Institute of Politics, identified four "dimensions" for building resilience in its 2022 policy paper. First, the institutional/legal dimension pertains to "*streamlining of strategic documents and legislation, as well as improved public governance and inter-agency coordination*". Second, the societal dimension involves extending responsibility for resilience-building across all societal groups, ensuring a whole-of-society

effort and increasing social trust and psychological resilience. Third, the political dimension addresses low political trust, polarisation, radicalisation, and poor governance practices. Fourth, the public-private dimension refers to the extension of ownership of resilience-building from the public to the private sector (Kakachia et al., 2022, p. 3).

Kapanadze (2022, as cited in Kakachia et al., 2022, p. 9) argues that Georgia has poor overall civil-military preparedness for major disruptions. It has no warning or shelter systems in place. He further emphasises that it lacks properly organised and effective territorial defence units. In conclusion, Georgia needs a holistic approach to resilience, with the primary objective of protecting and preserving society's vital functions during crises or major armed attacks (Kakachia et al., 2022, p. 10). The Georgian example confirms that SOF is not a panacea but remains a powerful tool for resilience and resistance.

5. STRATEGIC RECOMMENDATIONS

The Republic of Croatia is in many ways disadvantaged by its territorial shape and lack of strategic depth. In addition, Croatia's declining population trend has not yet recovered from the initial dip caused by the casualties and displacement of the Homeland War in the 1990s, and has only been worsened by the freedom of movement afforded by EU membership (Državni zavod za statistiku, 2025a). While the economy has since improved (Državni zavod za statistiku, 2025b), it is still heavily reliant on tourism for revenue. A sense of national identity, however, remains high, and societal cohesion in the face of hardship can almost certainly be relied on, even if a large body of militarily trained men cannot.

Given the case studies presented and the deeply unfavourable strategic environment in which Croatia finds itself, a focus on deterrence is critical to maintaining national security. Deterrence by overmatch of arms, however, is hard to achieve after decades of neglect and declining troop levels. Fostering societal resilience and a whole-of-society approach to defence is therefore key to deterring potential adversaries.

Steps in that direction seem to have been made: through the establishment of the Homeland Security System framework (Croatian Parliament, 2017, p. 23), through the return of compulsory military service to Croatia after 17 years of hiatus (Hrvatski Sabor, 2025), and through other efforts to bring up to date the critical national defence documents. The authors of this article believe that a national Resistance and Resilience Plan would be a prudent addition to these strategic documents.

Furthermore, to avoid the appearance of "silos of excellence", a far stronger political mandate should be given to habitual and deep interagency cooperation. The versatility of SOF in this role, as shown by the case studies, could provide outsized benefits.

In these rapidly changing (volatile, uncertain, complex, and ambiguous) operational environments enabled by the proliferation of space, AI, drone, and cyber technologies, SOF could play an even greater role. In 2022, then-US Army Special Operations Command commanding officer Lt. Gen. Jonathan Braga announced a construct he termed the *SOF-Space-Cyber Triad*. He noted that an "*increasingly complex strategic landscape requires innovative approaches that fuse and integrate all our expertise to maximise our collective impact*" (Braga, 2022, pp. 1–2). This level of ambition is not easily attainable for small states, but through true interagency integration and by leveraging its innovative, unconventional mindset, SOF can create real opportunities for collective capability growth.

Potential strategic obstacles to this vision include a lack of political will, low interagency initiative, and a ponderous national security apparatus. With NATO's pillars shaken, and with European security no longer as assured as it appeared only a few years ago, these obstacles will have to be overcome if Croatia wishes to maintain deterrence both independently and as a responsible ally.

On the operational side, obstacles include an underutilised interagency process, whose training must include precisely delineated responsibilities for both exercising command and control and remedying detected weaknesses. Legal authorities are reasonably well delineated, but responsibilities and capabilities are spread across ministries, departments, and agencies, with limited apparent coordination. The authors' view is that SOF can serve well in the "cracks" between agencies, supporting a clear mandate to build resilience.

Once given this mandate and mission, SOF must be allowed the latitude to experiment, coordinate, innovate and communicate across the interagency and intersectoral processes, with strategic oversight. It is worth emphasising that the core mission of SOF is to provide tactical actions with operational and strategic effect. It is also worth restating that this must be part of a comprehensive government-level policy, rather than relying on a bottom-up approach.

CONCLUSION

Contemporary conflicts demonstrate that national resilience depends on states' ability to sustain functionality, adapt, and coordinate across military, civilian, and societal spheres under persistent pressure. The analysis of the selected cases presented in this paper shows that Special Operations Forces contribute to national resilience through several recurring mechanisms. They act as interagency integrators, linking military, civilian, and private-sector actors and enabling coordinated responses to complex threats. They serve as capacity builders, providing training, education, and advisory support that enhance both institutional and societal preparedness. They also contribute to the protection and maintenance of critical infrastructure, particularly where civilian capabilities are insufficient, and function as enablers of adaptation and innovation by facilitating rapid learning and the integration of new technologies and

operational approaches. In addition, SOF act as bridges to external support, enhancing interoperability and facilitating the effective use of allied assistance.

Taken together, these roles enable SOF to translate strategic intent into practical resilience by strengthening coordination, preparedness, and continuity across sectors. Their organisational culture of mission command, flexibility, and rapid adaptation further allows them to operate across land, maritime, air, cyber, space, and information environments, effectively serving as connective tissue within a multi-domain approach to national defence.

When supported by clear political direction and institutional frameworks, SOF can bridge gaps between military and civilian actors and help build the adaptive, whole-of-society resilience required for credible deterrence and sustained resistance in contemporary security environments.

REFERENCES

- Berzina, I. (2020). From "Total" to "Comprehensive" national defence: the development of the concept in Europe. *Journal on Baltic Security*, 6 (2), 1-9.
- Braga, J. (2022, April 27). Statement of Lieutenant General Jonathan Braga Commanding General United States Army Special Operations Command (USASOC) Before The Senate Armed Services Committee Emerging Threats and Capabilities Sub-Committee. *United States Army Special Operations Command*. [https://www.armed-services.senate.gov/imo/media/doc/2022%20USASOC%20Posture%20-%20LTG%20Braga%20-%20SASC-ETC%20\(27%20April\)%20\(Final\).pdf](https://www.armed-services.senate.gov/imo/media/doc/2022%20USASOC%20Posture%20-%20LTG%20Braga%20-%20SASC-ETC%20(27%20April)%20(Final).pdf)
- Burrell, R. S. & Collison, J. (2025). Measuring Resiliency and Resistance in Burrell, R. S. (Ed.), *Resilience and Resistance: Interdisciplinary Lessons in Competition, Deterrence, and Irregular Warfare* (pp. 35-51). JSOU Report 25-16. MacDill Air Force Base. FL: The JSOU Press.
- Country Factsheet. (n.d.). In *The World Factbook*. Central Intelligence Agency. Retrieved 4 January 2026, from <https://www.cia.gov/the-world-factbook/countries/georgia/factsheets/>
- Croatian Parliament. (2017). *National Security Strategy of the Republic of Croatia*. Croatian Parliament, NN 73/2017. https://www.morh.hr/wp-content/uploads/2018/04/strategy_18012018.pdf
- Čanić, D. (2023). Osnove ustroja i povjesnica suvremenih vojnih postrojbi. In T. Šulj, (Ed.), *Bojna Frankopan: Prvi hrvatski komandosi* (pp. 11-16). Udruga Bojna Frankopan: Hrvatski memorijalno-dokumentacijski centar Domovinskog rata.
- Državni zavod za statistiku. (2025a). *Hrvatska u brojkama*. <https://web.dzs.hr/hub25/stanovnistvo.html>
- Državni zavod za statistiku. (2025b). *NR-2025-2-2 Godišnji bruto domaći proizvod za razdoblje 1995. – 2024*. <https://podaci.dzs.hr/2025/hr/97201>
- Fedorchak, V. (2024). *The Russia–Ukraine war: Towards resilient fighting power*. Routledge. <https://doi.org/10.4324/9781003351641>
- Fiala, O. C. (2020). *Resistance operating concept (ROC)*. MacDill Air Force Base. FL: The JSOU Press.
- Flanagan, S. J., Osburg, J., Binnendijk, A., Kepe, M., & Radin, A. (2019). *Deterring Russian aggression in the Baltic states through resilience and resistance*. RAND Corporation.
- Hedenskog, J. (2023). *Explaining Ukrainian resilience*. Stockholm Centre for Eastern European Studies. <https://sceus.se/en/publications/explaining-ukrainian-resilience/>
- Hrvatski Sabor. (2025). *Zakon o izmjenama i dopunama Zakona o obrani*. https://narodne-novine.nn.hr/clanci/sluzbeni/2025_11_136_2011.html

- International Centre for Defence and Security. (2023). *Europe's war and the Baltic lesson: Building resilience when the front is everywhere*. <https://icds.ee/en/europes-war-and-the-baltic-lesson-building-resilience-when-the-front-is-everywhere>
- Jauniskis, D. (2012). *Collective defense of the Baltic states: A SOF beginning*. U.S. Army War College. <https://apps.dtic.mil/sti/tr/pdf/ADA561675.pdf>
- Joint Special Operations University. (2020). *SOF interagency reference guide* (4th ed.). MacDill Air Force Base, FL: The JSOU Press.
- Jones, D., & Love, J. B. (2022). Resilience and resistance 2.0: Initial lessons of Ukraine and implications for deterrence. *Security: Theory and Practice*, 3(1), 19–35. <https://doi.org/10.48269/2451-0718-btip-2022-3-001>
- Kakachia, K., Lebanidze, B., & Kandelaki, S. (2022). *National resilience strategy for Georgia: Lessons from NATO, EU and beyond* (Policy Paper No. 33). Georgian Institute of Politics. <https://gip.ge/wp-content/uploads/2022/12/Policy-Paper-33.pdf>
- Kramens, J. (2025). *Enhancing societal resilience in the Baltic states to energy outages*. NATO Energy Security Centre of Excellence.
- Lavrelashvili, T. (2018). Resilience-building in Georgia, Moldova and Ukraine: Towards a tailored regional approach from the EU. *European View*, 17(2), 189–196. <https://doi.org/10.1177/1781685818805680>
- Lucić, J. (Ed.). (2011). *I. Hrvatski gardijski Zdrug*. Ministarstvo obrane republike Hrvatske.
- Marijan, D. (2008). *Slom Titove Armije: Jugoslavenska narodna armija i raspad Jugoslavije 1987.-1992*. Zagreb: Golden Marketing - Tehnička Knjiga / Hrvatski institut za povijest.
- Meredith, S. B. (2024). *The key to Ukrainian victory is partnering, not Ukrainifying*. Irregular Warfare Initiative. <https://irregularwarfare.org/articles/the-key-to-ukrainian-victory-is-partnering-not-ukrainifying/>
- Ministry of Defence of the Republic of Latvia. (n.d.). *Comprehensive state defence: Building resilience*. <https://www.mod.gov.lv/en/nozares-politika/comprehensive-state-defence/building-resilience>
- Murauskaite, E. E. (2024). *Civilian Resilience and Resistance: Integrating Cross-disciplinary Perspectives with a Focus on Ukraine*. ICONS Project. Asymmetric Threats Analysis Center, the University of Maryland.
- NATO (1949). *The North Atlantic Treaty*. Washington D.C. <https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/1949/04/04/the-north-atlantic-treaty>
- NATO (2025). *2025 NATO Summit in The Hague*. <https://www.nato.int/en/news-and-events/events/2025/6/overview---2025-nato-summit-in-the-hague>
- NATO Special Operations Headquarters. (2020a). *Comprehensive Defence Handbook Vol I*. SHAPE.

- NATO Special Operations Headquarters. (2020b). *Comprehensive Defence Handbook Vol II*. SHAPE.
- Petit, B. (2025). Building resistance in Georgia. In R. S. Burrell (Ed.), *Resilience and resistance: Interdisciplinary lessons in competition, deterrence, and irregular warfare* (pp. 107–116). The Joint Special Operations University Press.
<https://jsou.edu/Press/PublicationDashboard/284>
- Pettersson, U., & Ilis-Alm, H. (2022). Resistance operations: Challenges and opportunities for special operations forces. *Journal on Baltic Security*, 8(1), 76–93.
https://doi.org/10.57767/jobs_2022_0009
- Pierini, G. (2023). Allied security strategies: NATO special operations as a case study. In R. S. Burrell (Ed.), *Resilience and resistance: Interdisciplinary lessons in competition, deterrence, and irregular warfare* (JSOU Report 25-16, pp. 355–367). The JSOU Press.
- Shelest, H. (2022). *Defend. Resist. Repeat: Ukraine's lessons for European defence*. ECFR.
<https://ecfr.eu/wp-content/uploads/2022/11/Defend.-Resist.-Repeat-Ukraines-lessons-for-European-defence.pdf>
- Spulak, R. G., Jr. (2007). *A theory of special operations*. Joint Special Operations University Press.
- Stringer, K. D. (2022). Special Operations Forces (SOF): The Integrators for Total Defense and Resistance. *Journal on Baltic Security*, 8(1), 65-75.
https://doi.org/10.57767/jobs_2022_0001
- Stringer, K. D., & Noyes, A. (2025, November 6). What Lithuania can teach America about resilience: Lithuania's total defense resilience model. *Small Wars Journal*.
<https://smallwarsjournal.com/2025/11/06/lithuania-total-defense-resilience-model/>
- Stringer, K.D., & Vivdych, T. (2025). A Primer on Ukrainian Special Forces: Beyond Joint. *Joint Force Quarterly*, 119, 54-63.
- Szymański, P. (2021, July 14). More U.S. special operations forces for the Baltic states. *Ośrodek Studiów Wschodnich*. <https://www.osw.waw.pl/en/publikacje/analyses/2021-07-14/more-us-special-operations-forces-baltic-states>
- Šulj, T. (2023). *Bojna Frankopan: Prvi hrvatski komandosi*. Udruga Bojna Frankopan: Hrvatski memorijalno-dokumentacijski centar Domovinskog rata.
- U.S. Special Operations Command. (2020). *Special Operations Forces interagency reference guide (4th ed.)*. The JSOU Press, MacDill AFB, Florida <https://apps.dtic.mil/sti/citations/AD1131128>
- Watling, J., & Reynolds, N. (2023). Stormbreak: Fighting through Russian defences in Ukraine's 2023 offensive. *Royal United Services Institute (RUSI)*.
<https://www.rusi.org/explore-our-research/publications/special-resources/stormbreak-fighting-through-russian-defences-ukraines-2023-offensive>

Wright, K. A. M. (2025, October 14). Realising Societal Resilience for a Whole of Society Approach to Defence. *Royal United Services Institute (RUSI)*.
<https://www.rusi.org/explore-our-research/publications/commentary/realising-societal-resilience-whole-society-approach-defence>

II

Hybrid Threats, Information Operations, and Cognitive Security



www.sois-ft.hr

CRISIS COMMUNICATION IN HYBRID THREAT ENVIRONMENTS: THE CROATIAN ARMED FORCES AND THE ZAGREB 2022 UAV INCIDENT

Iva Kišasondi Bašić¹, Ivana Kovačević Bekić²

¹Dr. Franjo Tuđman Defense and Security University

E-mail: ikbasic@unin.hr

ORCID: <https://orcid.org/0009-0009-9996-3213>

²MORH, Zapovjedništvo za kibernetički prostor

E-mail: ivkobekic@unin.hr ili ivana.kovacevic.bekic@morh.hr

ORCID: <https://orcid.org/0009-0006-3831-8016>

Abstract

This paper examines crisis communication practices of the Croatian Armed Forces following the crash of an unmanned aerial vehicle in Zagreb in March 2022, situating the event within a broader context of disinformation dynamics and hybrid-threat environments. Drawing on Situational Crisis Communication Theory (SCCT), the study analyses how institutional actors communicated during a low-responsibility but high-uncertainty security incident.

Using a qualitative case study approach, the research combines media content analysis, discourse analysis of official statements, and a review of secondary sources to assess message coherence, communication strategies, and media framing. Particular attention is given to the interactions among professional military communication, political messaging, and media narratives, and to their influence on public perception.

The findings reveal that although professional actors largely adhered to SCCT principles by providing cautious, evidence-based communication, the overall response was undermined by inconsistencies among institutional actors, a lack of coordinated messaging, and the absence of a unified spokesperson. These shortcomings contributed to narrative fragmentation, increased uncertainty, and reduced communicative effectiveness, particularly within a hybrid information environment characterised by rapid information flows and heightened susceptibility to disinformation.

The study highlights the importance of strategic alignment, institutional coherence, and proactive communication planning in military crisis contexts. It contributes to the literature by offering an empirically grounded analysis of defence-sector communication in a real-world incident and by conceptualising defence institutions as a single communicative actor from the perspective of public perception, thereby advancing understanding of crisis communication under hybrid-threat conditions.

Keywords: crisis communication; public relations; Croatian Armed Forces

INTRODUCTION

The growing prevalence of disinformation and hybrid threats has significantly increased the importance of strategic communication and public relations within contemporary security environments. Rapid technological development and the expansion of digital media ecosystems have transformed the conditions under which organisations operate, requiring more adaptive, coordinated, and strategically planned communication responses, particularly in situations characterised by uncertainty and heightened public sensitivity.

Within this context, it is essential to distinguish between public relations and strategic communication. While public relations traditionally focuses on managing relationships between an organisation and its publics, strategic communication is a broader, more integrated approach that encompasses the planning, coordination, and alignment of communication activities to achieve defined institutional objectives. Originating largely in military practice under the concept of “StratCom,” strategic communication has evolved into a critical organisational function, particularly in security and defence settings, where it directly influences public perception, credibility, and legitimacy.

This paper examines crisis communication in the context of the crash of an unmanned aerial vehicle in Zagreb, focusing on the Croatian Armed Forces' response. The study analyses institutional communication practices through the lens of public relations and strategic communication, with particular attention to message coherence, coordination among actors, and the interaction between institutional messaging and media narratives. In doing so, the Croatian Armed Forces are conceptualised as a unified communicative actor - comprising the Ministry of Defence, the Armed Forces, and the Minister of Defence - reflecting how public perception constructs institutional responsibility.

The study adopts a qualitative case study approach to explore how crisis communication unfolds in a complex information environment shaped by disinformation dynamics and hybrid threats. By integrating media analysis, institutional discourse, and theoretical insights from crisis communication scholarship, the research seeks to identify key communication patterns, inconsistencies, and their implications for public understanding of the event.

This paper contributes to the literature by offering an empirically grounded analysis of crisis communication within the Croatian defence sector in the context of a real-world, unanticipated incident. It advances theoretical understanding by demonstrating how institutional actors are perceived as a single communicative entity and how this perception influences expectations of message coherence and accountability. More broadly, the study provides insights relevant to improving communication preparedness and strategic alignment in military and security organisations operating in hybrid information environments.

1. METHODOLOGY

This study employs a qualitative approach, which is particularly well-suited to analysing complex communication processes in security-sensitive and crisis-related contexts. Given that the paper focuses on understanding institutional responses, media framing, and the construction of public perception regarding the unmanned aerial vehicle incident in Zagreb, a qualitative approach enables a deeper interpretation of meanings, communication patterns, and interactions among the various actors involved.

The methodological framework is designed as a case study in which the crash of the unmanned aerial vehicle in Zagreb is examined as a distinct security and communication event, enabling analysis of crisis communication within the Republic of Croatia's defence and security system. This approach is particularly appropriate because it permits a detailed examination of a specific event within its political, media, institutional, and social context.

The study relies on three mutually complementary methods: content analysis, discourse analysis, and the analysis of secondary sources. By combining these methods, the research seeks to provide comprehensive insight into how the incident was communicatively constructed, interpreted, and presented to the public.

The first method consists of a qualitative content analysis of media coverage. The analysed corpus includes more than 50 media articles and reports published between 10 and 20 March 2022, that is, in the immediate aftermath of the incident, when the initial narratives and public interpretations of the event were being formed. The corpus includes materials from major Croatian media outlets: Jutarnji list, Index.hr, HRT (Croatian Radio and Television), and Večernji list, which reported extensively on the incident during the observed period and played an important role in shaping public discourse. The analysis focused on thematic emphases, reporting tone, dominant interpretive frames, and patterns of media framing.

The second method involves the discourse analysis of official statements made by key state and security actors. In this segment, 15 official statements and public addresses were analysed, including those by the President of the Republic of Croatia, Zoran Milanović; the Prime Minister of the Republic of Croatia, Andrej Plenković; representatives of the Croatian Armed Forces; and relevant statements and reactions from NATO. The discourse analysis focused on

how these actors constructed the meaning of the incident, interpreted the level of threat, communicated the issue of responsibility, and attempted to shape public understanding of the event. Special attention was given to the distinction between professional and political communication registers, as well as to the degree of coherence or contradiction among the communicated messages.

The third segment of the research includes secondary sources, namely expert analyses, specialist reports, and relevant NATO documents related to the incident. The role of secondary sources was both contextual and interpretive: they enabled the theoretical and security-related positioning of the case and contributed to understanding the broader framework of hybrid threats, disinformation, and crisis communication in the military and security environment.

In addition to these sources, the study incorporated publicly available Twitter/X data to identify dominant patterns of public reaction in the digital sphere. These data were used as indicative evidence of public interpretations, emotional reactions, irony, political polarisation, and attitudes toward institutional messages. Although the analysis of social media content was not conducted as a separate quantitative study, it served as a valuable supplementary source for understanding the online circulation of the crisis narrative.

The data were collected from publicly available archives and sources, and the analysis was conducted with particular emphasis on themes, tones, and framing patterns. In the analytical process, the material was classified according to dominant communication patterns, substantive emphases, and modes of presenting the incident, and the findings from media content, official statements, and secondary sources were then compared. Such a procedure enabled an interpretive comparison of different levels of communication and the identification of points of convergence, divergence, and communicative gaps.

The study aims to determine how different actors shaped the incident's communicative framework and how that framework influenced public perceptions of security threats. In this regard, the study seeks to demonstrate how, in crisis situations - particularly those marked by security-related uncertainty and potential hybrid activity - institutional messages, media reporting, and digital reactions become intertwined in constructing public meaning around the event.

Given the nature of the research, certain limitations must also be acknowledged. As a qualitative case study, the findings cannot be directly generalised to all crisis situations within the military and security system. Nevertheless, this approach provides an in-depth understanding of a specific event and enables the identification of communication patterns and institutional weaknesses that may serve as a relevant analytical basis for future research and for the development of communication protocols in similar circumstances.

2. THEORETICAL FRAMEWORK AND KEY CONCEPT

The theoretical framework of this paper is based on the principles of the Situational Crisis Communication Theory. Situational Crisis Communication Theory emphasises, among other things, that organisations facing a crisis have the ability to choose a strategy, that is, an approach to crisis communication (Coombs, 2007, p. 164). It is precisely these choices that account for differences in effectiveness.

Furthermore, it is important to emphasise the connection between this paper and systems theory, given the relevance of systems theory for public relations, as it provides a clear insight into the functioning of organisations and the relationships within them, as well as their relationships with the external environment, under conditions of change and adaptation to change.

The key concepts related to the subject matter of this paper that require definition are information (notification), disinformation (counterintelligence), hybrid threats and hybrid operations, public relations, strategic communication, crisis, crisis communication, cognition, the cognitive aspect of communication, and social cognition. The need for particular emphasis on these fundamental concepts arises from their frequent use without critical reflection.

The number of definitions describing the concepts of information and notification is extremely large. Information is studied from various perspectives and is accordingly defined. In essence, every piece of information represents a set of data with attributed meaning. *The Lexicon of Intelligence Terminology* (Part 1), authored by Miroslav Tuđman, Gordan Akrap, and Vedran Matošić, defines information (notification, intelligence data) as “a general term for all types of unevaluated materials regardless of the type of source and degree of reliability, which can be processed and used in the production of intelligence reports. From a data protection perspective, a notification refers to any information that can be communicated, or any documentary material, regardless of its physical form or characteristics, that is owned by the government, produced in or for the government, or under government control. ‘Control’ refers to the authority of government institutions to prescribe access to the information they create or that is in their possession” (Tuđman, Akrap, & Matošić, 2021, pp. 168–169).

Information, when viewed in the context of practical application in public relations and strategic communication, can be understood as a working tool, a resource, or material. However, the value of information depends on how it is used.

When considering disinformation or counterintelligence, we primarily think of something consciously and intentionally created and disseminated through a medium with a clearly defined purpose, thereby revealing the very essence of disinformation. In the broader social context, the field of inaccurate information is saturated with perspectives on fake news,

misinformation, malicious information, lies, conspiracies, and related phenomena, many of which lack scientific precision and conceptual grounding.

However, in the context of public relations, it is also necessary to address disinformation. Regardless of which definition of disinformation is applied, for public relations, it represents something that must be corrected, “cleansed,” and returned to circulation in an accurate form. At the same time, it represents a situation in which it is necessary to repair the damage caused by disinformation itself, whether by halting the spread of false information, restoring a damaged image, or otherwise.

In addition, the concept of unplanned, high-impact incidents requiring strategically coherent and institutionally coordinated communication has been extensively articulated in crisis management scholarship. Pearson and Clair define a crisis as “*a low-probability, high-impact event characterised by ambiguity regarding cause, effect, and resolution*”, underscoring the heightened communicative and organisational uncertainty that accompanies such incidents and the consequent need for robust information-management mechanisms (Pearson & Clair, 1998).

Within the military environment, these challenges become even more pronounced. Rawlinson’s assessment of U.S. Army crisis communication highlights that unexpected incidents - particularly those occurring in volatile information environments - demand pre-established, coherent communication protocols to preserve credibility, ensure message alignment across institutional actors, and maintain operational stability (Rawlinson, 2018).

Consequently, communication in contemporary security settings assumes a strategic and operational role: it becomes not merely a channel for conveying information but a core capability essential to mitigating uncertainty, safeguarding institutional legitimacy, and supporting national security objectives.

3. HYBRID THREATS AND HYBRID OPERATIONS

Although the concepts of hybrid threats and hybrid operations have been extensively discussed in recent years, a considerable degree of conceptual ambiguity, oversimplification, and misinterpretation persists in both academic and policy discourse. Hybrid threats should not be understood as isolated phenomena, but rather as integral components of broader hybrid operations; the two are conceptually interconnected and analytically inseparable.

Hybrid operations encompass a wide spectrum of coordinated activities aimed at achieving informational superiority and shaping the target environment in accordance with strategic objectives. Within this framework, hybrid threats represent specific manifestations of such operations, characterised by targeted, organised actions directed at selected audiences to exploit vulnerabilities and influence cognitive, social, and political processes (Akrap, 2019, p. 40).

However, it is important to emphasise that the incident analysed in this paper - the crash of the unmanned aerial vehicle in Zagreb - cannot be unequivocally classified as a hybrid operation. There is no conclusive evidence that the event itself constituted a deliberate hybrid action.

In contemporary public discourse, the concept of hybrid threats is frequently applied in an overly broad and imprecise manner. This tendency largely stems from limited public understanding of the term itself, which traditionally refers to the coordinated use of multiple, mutually reinforcing instruments of power by state or non-state actors. As a result, routine political disagreements, socio-economic fluctuations, or even ordinary informational noise are increasingly mischaracterised as deliberate hybrid operations. Such mislabeling obscures the concept's analytical boundaries and diminishes its explanatory value. A notable example is the growing perception that the mere presence or civilian use of drones inherently signals a hybrid threat, even when no strategic intent or coordinated hostile activity is evident. When examined using rigorous scientific methods, many alleged hybrid activities show no evidence of strategic intent or coordinated hostile action. Instead, they often emerge as spontaneous social dynamics or consequences of structural complexities within modern information ecosystems. Overgeneralization in this domain risks generating unnecessary alarm and fostering a climate of suspicion. It may also divert attention from genuinely coordinated and empirically verifiable hybrid campaigns. Scholarly analyses consistently emphasise the importance of distinguishing between correlation and intentional manipulation. Moreover, the inflation of the term “hybrid threat” contributes to conceptual ambiguity within security studies. This ambiguity complicates policy formulation and leads to inefficient allocation of resources. A more disciplined and evidence-driven approach is therefore essential for maintaining conceptual clarity. Ultimately, scientifically grounded assessments demonstrate that not every disruptive or ambiguous event should be interpreted as part of a hybrid strategy, despite prevailing public perceptions to the contrary.

Nevertheless, the analytical relevance of the hybrid threat framework lies in the informational and communicative environment within which the incident occurred. The event unfolded during an ongoing armed conflict in Ukraine and within a highly dynamic information space characterised by heightened sensitivity to security risks, rapid information flows, and increased vulnerability to disinformation, speculation, and competing narratives.

In this context, the concept of hybrid threats is not employed to categorise the incident itself, but rather to interpret the communication dynamics that emerged in its aftermath. The lack of consistent institutional messaging, combined with intensive media coverage and digitally mediated public reactions, contributed to an environment marked by uncertainty and narrative fragmentation - conditions that closely align with those identified in hybrid threat environments.

This perspective can be further integrated with the assumptions of Situational Crisis Communication Theory (SCCT). While SCCT primarily focuses on the relationship between

crisis type, attribution of responsibility, and appropriate communication strategies (Coombs, 2007), its effectiveness depends on the organisation's ability to maintain message coherence and credibility. In hybrid information environments, however, these conditions are significantly more difficult to achieve.

Specifically, environments characterised by disinformation, rapid narrative shifts, and competing interpretations can amplify reputational risk, even in crises with low responsibility attribution, as in the case analysed in this study. Although SCCT would categorise this incident as a low-responsibility crisis, the presence of hybrid-like informational conditions increases the likelihood of misinterpretation, politicisation, and erosion of trust.

Accordingly, the hybrid threat framework complements SCCT by providing a broader contextual layer that explains why standard crisis communication strategies may face limitations in practice. It highlights that beyond selecting an appropriate response strategy, organisations must also manage the informational environment in which their messages circulate, including countering uncertainty, mitigating disinformation, and ensuring internal alignment in communication.

In this sense, the analysis of the Croatian Armed Forces' communication response cannot be fully understood without considering both the strategic prescriptions of SCCT and the structural constraints imposed by a hybridised information environment.

3.1. Public relations

The concept of public relations cannot be excluded from the topic of the cognitive aspect of organisational crisis communication, as public relations represents the connecting element - that is, the binding tissue that holds together the cognitive aspect, the mode of communication, the organisation, and the messages, that is, the information being transmitted. Although there are views suggesting that public relations as a function is not of major importance because they "merely transmit" information, such perspectives should be disregarded as they do not correspond to the actual function of public relations. The functional distribution within an organisation, as well as the positioning of functions within a hierarchy of importance, are not the subject of this paper.

Public relations have attracted substantial scholarly attention, with extensive research, theories, and definitions. From a practitioner's perspective, public relations is a complex yet highly effective mode of communication between an organisation and its publics. At the same time, they serve as the voice of the managerial or ownership structure and as a source of feedback. According to Zoran Tomić, public relations is the process of communication between an organisation and its internal and external publics, to achieve mutual understanding, build social responsibility, and realise shared interests (Tomić, 2008, p. 50). The complexity of public

relations was most comprehensively defined by Božo Skoko, who states that public relations constitute a skill through which, by drawing on the disciplines of communication studies, psychology, and sociology, influence is exerted on the creation and strengthening of a positive reputation and image of a company (institution, individual, or state) in the public sphere, and quality relationships are maintained with all segments of the public, for the purpose of achieving one's own success, mutual understanding and cooperation, as well as preventing or neutralizing unfavourable publicity (Skoko, 2004, p. 77).

3.2. Strategic Communication

Strategic communication and public relations are not synonymous; rather, strategic communication should be viewed as a specialised extension of public relations. The term *strategic communication* emerged at the beginning of this millennium as a designation for a combination of elements, that is, aggregated elements of organisational communication. The term itself became established primarily through military usage, especially as the abbreviation "StratCom".

According to Skoko, strategic communication encompasses various forms of planned and purposeful communication, which have clearly defined objectives and messages, identified target publics, and the strategies and tactics employed to reach them; it usually includes public relations, marketing, political communication, public diplomacy, and other related disciplines (Skoko, 2021, p. 491). Strategic communication is not an evolution of public relations, but rather a distinct direction - a functional upgrade for organisations (and actors) that possess both the mandate and the necessity to plan, shape, and direct communication toward their publics.

3.3. Crisis and Crisis Communication

Defining the concept of crisis is relatively straightforward, given the rich theoretical foundation. Numerous authors have defined the concept of crisis from different perspectives (e.g., Coombs, 2012; Jugo, 2017; Novak, 2001), identifying common elements: the event's unpleasant or negative nature, its unpredictability, and its limited duration. The authors also agree that a crisis is an event that requires attention and must be addressed in a planned and systematic manner. The source of a crisis, that is, its foundation, may originate from various domains - from natural disasters, business and financial crises, and various harmful events, to deaths, material and emotional losses, loss of reputation, and so forth. Depending on an individual's or organisation's perception and cognition, a crisis may be any negative or unpleasant event.

A crisis, it can be concluded quite simply, is by its defining characteristics equivalent to change. Accordingly, the fields of crisis communication and crisis management share features with change management. The field of crisis communication falls within the broader area of communication in special situations. Regarding the concept of crisis, various authors have also

defined it. Although Smiljana Leinert Novosel, in her book *Communication Compass* (2015), does not explicitly define crisis communication as communication in special situations, she places establishing relationships at the core of such communication as one of its essential features. Furthermore, Leinert Novosel emphasises that establishing relationships is important in both long-term and ad hoc communication. Crisis communication is interwoven with both types of relationships, regardless of the crisis. Taking the previous facts into account, the effectiveness of crisis communication will depend on the success of established relationships with all publics, since the degree of public cooperation in a crisis will depend on those relationships. Crisis communication and crisis management are not synonymous, as crisis management is a set of (most often planned) activities that occur during a crisis - starting when it becomes imminent, continuing throughout the crisis, and extending into the period after it. Crisis communication serves as an umbrella activity, accompanying other crisis-related activities and coordinating the creation and dissemination of information to the public.

3.4. Cognition, Social Cognition and the Cognitive Aspect of Communication

Jacques-Philippe Leyens and Benoit Dardenne, writing on the fundamental concepts and approaches in the field of social cognition and adopting an information-processing perspective, define cognition, following Neisser (Neisser, 1976, p. 1), as the activity of knowing - that is, the acquisition, organisation, and use of knowledge (Hewstone & Stroebe, 2011). Furthermore, Leyens and Dardenne link cognition to the mechanisms that produce such forms of knowledge, including perception, memory, speech, mental elaboration, and similar processes.

From a cognitive perspective, the human being is not merely a passive recipient of information from the environment but an active subject who collects, processes, and constructs personal interpretations based on that information. When examining how individuals form their own constructs, it is necessary to refer to the scientific contributions in the field of social cognition theory, such as those by Arcuri, Beauvois, Fiske, Taylor, Ostrom, Devine, and Hamilton when discussing the formation of individual constructs, as well as Leyens, Yzerbyt, Schladron, Oakes, Haslam, and Turner when discussing shared beliefs and the behaviour of group or organizational members, among others.

Social cognition and communication studies share a common concept related to the construction of knowledge: *thinking* in social cognition and a lens or angle of perception in communication studies. The conclusion is identical for both fields: there are no completely identical opinions about a particular person, concept, or object, nor are there completely identical perspectives on a given person, concept, or phenomenon. Through the prism of the shared elements of social cognition and communication studies, processes such as categorisation, schema formation, stereotyping, and the formation of shared values, opinions, or ideas can be observed. The connection between social cognition and communication is logically explainable as a consequence of living in society and engaging in mutual communication, yet it is also of fundamental importance for scholarly analysis.

3.5. Strategies and Techniques of Public Relations in Crisis Conditions

The functions of public relations and strategic communication constitute parts of a single organisational system. Their response to an organisation being in crisis is crucial. If both functions are adequately prepared for such situations, the pressure on the organisation will be reduced, and it will be better able to cope with the newly emerged circumstances.

The function of public relations aims to build and maintain positive relationships between the organisation and its publics, and to preserve the organisation's image. Crisis events directly challenge this objective by influencing public perceptions of the organisation, its image and reputation, and the level of public trust in it.

A proactive approach and strategic planning strengthen the public relations function and ensure an effective response under such conditions. The necessity of a rapid response in a crisis requires prior planning and the preparation of functions for swift action. A particularly important segment comprises the ethical principles that guide public relations and strategic communication. In crisis communication and crisis response, it is essential to uphold high ethical standards when confronted with unethical practices. Through analytical approaches and early-detection methods, it is possible to anticipate trends in the spread of disinformation (counterintelligence) and hybrid threats, as well as in public sentiment and attitudes relevant to the organisation. In conclusion, before a crisis, a wide range of strategies, techniques, and methods is available to strengthen organisational functions and prepare for a rapid and effective response. The priorities of organisations that genuinely strive for business stability and the preservation of reputation should, in addition to establishing crisis-management functions, include investments in developing awareness of the digital environment, ethical communication, and proactive strategies.

4. THE CASE OF THE UNMANNED AERIAL VEHICLE INCIDENT IN ZAGREB – AN ANALYSIS OF CRISIS COMMUNICATION PRACTICES IN THE CROATIAN ARMED FORCES

The unmanned aerial vehicle Tupolev Tu-141 (Strizh) crashed in Zagreb on 10 March 2022 at 23:01 Central European Time. It crashed in the Horvati (Jarun) neighbourhood, near the Stjepan Radić Student Dormitory. The crash formed a crater measuring 5.05 meters in diameter and 4.5 meters deep. The aircraft entered Croatian airspace at 22:55, travelling at 700 km/h and at an altitude of 1,300 meters after crossing Romanian and Hungarian airspace (Index.hr). The impact was recorded seismologically at 23:01:49. Material damage occurred, but there were no human casualties. The Tupolev Tu-141 is a Russian reconnaissance drone.

The incident occurred during an intense phase of the Russian invasion of Ukraine, amid the still ongoing COVID-19 pandemic and post-pandemic adjustments, and two years after a series

of earthquakes that had already unsettled the Croatian public, causing shock and a new form of public anxiety. Although there were no casualties, the event raised questions about the defence capabilities of the Croatian Armed Forces and NATO, crisis-communication protocols, and media management in emergency situations.

The analysis is based on theories of crisis communication (Coombs, 2007; Fearn-Banks, 2011), the mediatization of security (Cottle, 2008), and models of discursive construction of threat (Wæver, 1995). The analysis relies on the Situational Crisis Communication Theory (SCCT; Coombs, 2007) to assess institutional responses, media framing theory (Entman, 1993) to examine the representation of the event, and the concept of mediated security (Cottle, 2008). These frameworks enable an examination of how inconsistent messages from state actors and media sensationalism influenced public perceptions of threat.

5. ANALYSIS OF CRISIS COMMUNICATION IN THE CASE OF THE UNMANNED AERIAL VEHICLE INCIDENT IN ZAGREB

The crash of the unmanned military aerial vehicle Tu-141 in Zagreb on 10 March 2022 represented an unintended but highly risky security crisis with potentially serious consequences. The incident occurred in the context of the war in Ukraine, which further intensified the perception of threat and heightened public sensitivity. According to Situational Crisis Communication Theory (SCCT), this constitutes a crisis with low responsibility attribution, given that the Republic of Croatia was not the direct cause of the event but remains responsible for managing its consequences and communicating about it.

From the moment of the accident on 10 March 2022, the City of Zagreb, the Ministry of Defence, and other actors responsible for citizens' security were confronted with a newly emerged crisis characterised by high uncertainty, numerous open questions, and limited verified information. Although large organisations and state institutions typically develop crisis scenarios and communication protocols in advance, based on publicly available data, it remains unclear whether a unified crisis communication strategy existed in this case or whether institutional actors operated independently.

5.1. SCCT-Based Analysis of Institutional Communication

Table A.1 (in the Annex) presents a chronological overview of public statements made by political and professional actors and serves as the primary empirical basis for analysing communication strategies in this case. When interpreted through the lens of SCCT, the data reveal inconsistent application of communication strategies and insufficient alignment of messages among institutional actors.

In the initial phase of the crisis (10–11 March), a clear distinction can be observed between professional and political communication. Colonel Vlado Kovačević, as a representative of the

Ministry of Defence, communicated cautiously, procedurally, and without speculation, emphasising the ongoing investigation and the absence of final conclusions. Such an approach is consistent with SCCT's adjusting information strategy, as it aims to reduce uncertainty without increasing fear or speculation.

Similarly, early communication from local authorities, particularly the Mayor of Zagreb, emphasised the absence of casualties and the safety of citizens. This reflects elements of instructive information, as it provides reassurance and prioritises public well-being. However, as shown in Table A.1, a shift occurs in the subsequent phase (12–15 March), during which political actors increasingly introduced messages diverging from SCCT recommendations. Statements referring to the possible presence of an explosive device - communicated before definitive confirmation - represent risk-amplifying communication, which contradicts the SCCT principle of reducing uncertainty in low-responsibility crises.

Furthermore, statements by the Prime Minister framing the incident as a “serious security threat” and criticising the surveillance system indicate the introduction of elements associated with rebuild and attack strategies, which are typically more appropriate in crises with higher levels of organisational responsibility. Their application in this context contributed to the politicisation of the incident and a shift from a technical-security issue to a broader political narrative.

5.2. Lack of Message Coherence and Communication Vacuum

One of the key communication problems was the lack of a unified message. This claim is directly supported by the data in Table A.1, which shows inconsistencies among statements issued by different institutional actors.

Professional communication, primarily from the Ministry of Defence and Military Police, remained cautious and evidence-based. In contrast, political actors introduced interpretative and evaluative elements that were not always aligned with verified information. Statements regarding the possible presence of an explosive device were later questioned by international actors and media analyses, illustrating a clear example of contradictory messaging. From an SCCT perspective, such inconsistencies undermine the effectiveness of both instruction and strategy adjustment by preventing the public from forming a stable, coherent understanding of the situation. Instead of reducing uncertainty, communication amplified it.

Particularly significant was the absence of public statements from intelligence services (SOA and VSOA). While this absence is consistent with protecting classified information, in the context of crisis communication it contributed to a communication vacuum. As a result, the public sphere became dominated by political actors, while professional security analysis remained indirect and largely absent. This dynamic supports the conclusion that institutional

silence also constitutes a form of communication, but not necessarily one that enhances clarity or public trust.

5.3. Media Framing and Communicative Consequences

During the first hours following the incident, the media employed sensationalist frames, such as references to a “Russian threat” or a “mysterious aircraft,” before shifting toward political interpretations and accusations. International media marginalised the event, whereas Croatian media emphasised NATO’s role, the aircraft’s origin, and potential systemic failures.

In the absence of a coherent institutional narrative, media outlets assumed a more active role in shaping the event’s interpretation. From an SCCT perspective, this indicates a failure to maintain control over the crisis narrative. When institutions do not consistently provide instructive and adjusting information, media actors fill the interpretative gap, often prioritising conflict and speculation.

The analysis also indicates a high level of sensationalism in headlines and a lack of verified information in the early stages of reporting, which further contributed to uncertainty and narrative fragmentation.

5.4. Public Discourse and Digital Communication

Social media, particularly Twitter/X, was characterised by two dominant patterns: memification and irony, often directed at NATO’s perceived failure, and polarisation between competing geopolitical narratives. The Mayor of Zagreb frequently appeared as a stabilising communicator, emphasising the absence of casualties.

These reactions demonstrate how digital platforms amplify emotional responses while simultaneously enabling participatory reinterpretation of crisis events. In the absence of a stable and unified institutional narrative, users actively construct alternative interpretations, contributing to the fragmentation of meaning.

5.5. Synthesis: SCCT and Hybrid Information Environment

Communication in this case can be assessed as partially effective but structurally uncoordinated. While professional actors adhered to the principles of crisis communication - particularly accuracy, caution, and gradual information disclosure - political communication introduced additional layers of interpretation that contributed to inconsistency.

From an SCCT perspective, the simultaneous use of adjusting, diminishing, and rebuilding strategies, as evidenced in Table A.1, resulted in a hybrid and internally inconsistent

communication approach. This inconsistency generated communicative confusion, prolonged uncertainty, and hindered the establishment of a clear and authoritative narrative.

These dynamics are further intensified by the characteristics of a hybrid information environment, in which rapid information flows, media competition, and digital participation amplify even minor inconsistencies in messaging. Consequently, the absence of a unified communication strategy, clearly defined spokesperson roles, and consistent reliance on verified information prevented the crisis from reaching communicative closure and weakened the overall effectiveness of the institutional response.

6. DISCUSSION

The crash of the Tupolev Tu-141 unmanned aerial vehicle demonstrated the importance of communicative coherence in crisis situations. The incident involving the Tupolev Tu-141 unmanned aerial vehicle underscored the critical importance of maintaining communicative coherence, strategic messaging alignment, and information-management discipline within the broader framework of crisis-communication protocols. Instead of a single authoritative spokesperson, competing interpretations - military, political, and media-based - emerged, making it difficult to maintain informational credibility. In a broader context, the case illustrates how the media field in post-transitional societies serves as an arena for contesting interpretations of reality.

Inconsistencies in institutional messaging eroded credibility, underscoring SCCT's recommendation for a unified spokesperson (Coombs, 2007). Media framing intensified emotional perceptions and fostered participatory discourse on digital platforms, raising questions about digital crises in a post-pandemic context.

CONCLUSION

This study examined crisis communication in the case of the crash of the Tupolev Tu-141 unmanned aerial vehicle in Zagreb on 10 March 2022, situating the incident within a broader security environment characterised by disinformation dynamics and hybrid-threat conditions. Drawing on Situational Crisis Communication Theory (SCCT), the analysis identified the event as a low-responsibility crisis accompanied by significant reputational and communicative risks.

The findings reveal a clear divergence between professional and political communication. Professional actors, particularly representatives of the Ministry of Defence, adhered to SCCT principles by providing cautious, procedural, and evidence-based communication to reduce uncertainty. In contrast, political communication introduced interpretative and evaluative elements that contributed to inconsistency, narrative fragmentation, and a shift from a technical-security issue to a politicised discourse. The absence of visible communication from

intelligence institutions further contributed to a communicative vacuum, enabling media speculation and competing interpretations.

The analysis demonstrates that, although elements of effective crisis communication were present, the overall response was undermined by insufficient coordination, the lack of a unified spokesperson, and the absence of clearly defined communication roles. As a result, the crisis failed to achieve communicative closure, and public understanding remained fragmented. These dynamics were further intensified by the characteristics of a hybrid media environment, in which rapid information flows, sensationalist framing, and digitally mediated public discourse amplify even minor inconsistencies in institutional messaging.

The study contributes to the literature by providing an empirically grounded analysis of crisis communication in a military context and by conceptualising defence institutions as a single communicative actor from the perspective of public perception. This approach highlights the importance of message coherence, institutional alignment, and legitimacy management in shaping crisis outcomes.

From a practical perspective, the findings underscore the need to develop integrated strategic communication frameworks within defence systems. Such frameworks should include unified spokesperson structures, clearly defined communication protocols, alignment with SCCT principles, and mechanisms for managing communication in hybrid information environments. Strengthening these capacities is essential for ensuring timely, consistent, and credible communication in future security crises.

REFERENCES

- Akrap, G. (2019). Suvremeni sigurnosni izazovi i zaštita kritičnih infrastruktura. *Strategos*, 3(2), 37–49.
- Bajarūnas, E. (2020). *Addressing hybrid threats: Priorities for the EU in 2020 and beyond*. Wilfried Martens Centre for European Studies.
- Boin, A., 't Hart, P., & McConnell, A. (2010). *The Politics of Crisis Management*. Cambridge University Press. <https://doi.org/10.1017/9781316339756>
- Coombs, W. T. (2007). Protecting organization reputations during a crisis: The development and application of situational crisis communication theory. *Corporate Reputation Review*, 10(3), 163–176.
- Coombs, W. T. (2012). Crisis communication and its allied fields. In W. T. Coombs & S. J. Holladay (Eds.), *The handbook of crisis communication* (pp. 54–64). Wiley-Blackwell.
- Coombs, W. T. (2020). *Situational Crisis Communication Theory: Influences, Provenance, Evolution, and Prospects*. In F. Frandsen & W. Johansen (Eds.), *Crisis Communication* (pp. 121–140). De Gruyter Mouton. <https://doi.org/10.1515/9783110554236-005>
- Cottle, S. (2008). Reporting mass murder as a problem of belonging: British TV coverage of the Biafran famine. *Journalism*, 9(5), 523–542. <https://doi.org/10.1177/1464884908094162>
- Cao, K., Glaiser, S., Pena, A., et al. (2021, May 20). Countering cognitive warfare: Awareness and resilience. *NATO Review*. <https://www.scribd.com/document/838634646/NATO-Review-Countering-cognitive-warfare-awareness-and-resilience-2021>
- Entman, R. M. (1993). Framing: Toward clarification of a fractured paradigm. *Journal of Communication*, 43(4), 51–58.
- Dnevnik.hr. (2022, March 12). *Iz olupine letjelice izvučena crna kutija: "Dio fragmenata letjelice ukazuje da je nosila eksploziv"*. <https://dnevnik.hr/vijesti/hrvatska/brigadir-vlado-kovacevic-potvrdio-da-je-izvucena-crna-kutija-drona-u-zagrebu---699681.html>
- Dnevnik.hr. (2022, March 11). Brigadir Kovačević: "Ovako nešto još nisam doživio. Glavni događaj bi se trebao dogoditi u subotu". *Dnevnik.hr*. <https://dnevnik.hr/vijesti/hrvatska/brigadir-vlado-kovacevic-o-padu-drona-u-zagrebu---699591.html>
- European Commission. (2018). *Tackling online disinformation: A European approach* (COM/2018/236 final). https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=51804
- Ferenčić, D. (2022, 15. ožujka). *NATO Secretary General says drone crash in Zagreb was not an attack*. Glas Hrvatske – HRT. <https://glashrvatske.hrt.hr/en/politics/nato-secretary-general-says-drone-crash-in-zagreb-was-not-an-attack-6115713>
- Hewstone, M., & Stroebe, W. (Eds.). (2011). *Socijalna psihologija: Priručnik*. Naklada Slap.

- HINA. (2022, March 15). Drone which crashed in Zagreb was unarmed, Stoltenberg says. Hina.hr. <https://www.hina.hr/news/10937003>
- HRT. (2022, March 12). *Kovačević: Iz olupine letjelice izvučena crna kutija*. HRT Vijesti. <https://vijesti.hrt.hr/hrvatska/kovacevic-izvukli-smo-crnu-kutiju-trebala-bi-dati-podatke-o-letu-i-radu-raketnog-motora-6050850>
- Index.hr. (2022, March 11). Stručnjak: U Zagrebu se srušila bespilotna letjelica Tu-141. <https://www.index.hr/vijesti/clanak/strucnjak-u-zagrebu-se-srusila-bespilotna-letjelica-tu141-doletjela-je-iz-ukrajine/2346383.aspx>
- Index.hr. (2024, March 10). Prije dvije godine se srušio dron u Zagrebu, ni danas ne znamo što se točno dogodilo. <https://www.index.hr/vijesti/clanak/prije-dvije-godine-se-srusio-dron-u-zagrebu-ni-danas-ne-znamo-sto-se-tocno-dogodilo/2545943.aspx>
- Jugo, D. (2017). *Menadžment kriznog komuniciranja*. Školska knjiga.
- Leinert Novosel, S. (2015). *Komunikacijski kompas*. Plejada.
- Novak, B. (2001). *Krizno komuniciranje i upravljanje opasnostima*. Binoza Press.
- Nölleke, D., Scheu, A. M., & Birkner, T. (2020/2021). *The Other Side of Mediatization: Expanding the Concept to Defensive Strategies*. *Communication Theory*, 31(4), 737–757. <https://doi.org/10.1093/ct/qtaa011>
- Skoko, B. (2004). *Hrvatska – identitet, imidž, promocija*. Školska knjiga.
- Skoko, B. (2021). *Strateško komuniciranje država: Javna diplomacija, brendiranje država i nacija, međunarodni odnosi s javnošću*. Synopsis.
- Sun Tzu. (2010). *Umijeće ratovanja*. Zagrebačka naklada.
- Suchman, M. C. (1995). *Managing Legitimacy: Strategic and Institutional Approaches*. *Academy of Management Review*, 20(3), 571–610. <https://doi.org/10.5465/AMR.1995.9508080331>
- Tomić, Z. (2008). *Odnosi s javnošću: Teorija i praksa*. Synopsis.
- Pearson, C. M., & Clair, J. A. (1998). *Reframing Crisis Management*. *Academy of Management Review*, 23(1), 59–76. <https://doi.org/10.5465/AMR.1998.192960>
- Petranović, D. (2022, March 14). Komunikacijski kaos: “Bolje ne govoriti ništa nego ostavljati dojam kao da vrh države nema pojma otkud dron u centru glavnog grada”. *Tportal.hr*. https://www.tportal.hr/vijesti/clanak/dron-u-zagrebu-komunikacijska-analiza-jerko-troglic-foto-20220314?meta_refresh=1
- Rawlinson, J. S. (2018). *The Hot Seat: Assessing Military Crisis Communication*. U.S. Army War College.
- Reilly, P., & Salojärvi, V. (2022). *(De)constructing societal threats during times of deep mediatization*. *The Communication Review*, 25(3–4), 147–151. <https://doi.org/10.1080/10714421.2022.2139056>

- Telegram.hr. (2022, March 11). Skandalozna reakcija NATO saveza na pad drona u Zagrebu - pratili smo putanju objekta. *Telegram.hr*. <https://www.telegram.hr/politika-kriminal/skandalozna-reakcija-nato-saveza-na-pad-drona-u-zagrebu-pratili-smo-putanju-objekta/>
- Tuđman, M., Akrap, G., & Matošić, V. (2021). Leksikon izvještajnog nazivlja (1. dio). *National Security and the Future*, 22(1–2), 143–184. <https://hrcak.srce.hr/262828>
- Šurina, M. (2025, March 10). *Tri su godine prošle od pada drona u Zagrebu*. Tportal.hr. <https://www.tportal.hr/vijesti/clanak/tri-su-godine-prosle-od-pada-drona-u-zagrebu-sto-sve-ne-znamo-foto-20250310>
- Večernji list. (2022, March 11). NATO-u je trebalo šest sati da sroči prvu reakciju. <https://www.vecernji.hr/vijesti/nato-integrirana-obrana-pratila-je-putanju-leta-objekta-koji-se-srusio-u-zagrebu-1570081>

Annex A

Table A.1.

Chronological Overview of Media Statements by Political and Professional Actors Following the Incident

Date	Time	Institution/ Actor	Media	Summary of Statement	Communication Role in the Crisis	SCCT category
10 th March 2022	23:00	-	-	Crash of an unmanned aerial vehicle in Zagreb, Jarun, no human casualties	onset of the crisis situation	Crisis event
11 th March 2022	night/ morning	Ministry of Defence / Ministry of the Interior	news agencies	Securing the crash site, no official conclusions	crisis site management	
11 th March 2022	morning	Tomislav Tomašević mayor of the City of Zagreb	Media statement	Emphasis on the absence of injuries, focus on citizens' safety	Calming, local communication	Instructing & Adjusting Information
11 th March 2022	evening	Colonel, OF-5 Vlado Kovačević, Head of the Independent Sector for Military Police Affairs, Ministry of Defence	HRT Daily News – guest appearance	Investigation ongoing, no conclusions at this stage, extraction of the main part of the drone, possible traces of explosives	Professional, cautious, process-oriented communication	Diminish strategy

11th March 2022	during the day	Mario Banožić, Minister of Defence	media	outlines flight trajectory, investigation ongoing	operational-informative communication	Bolstering + Diminish
12th March 2022	during the day	Colonel, OF-5 Vlado Kovačević, Head of the Independent Sector for Military Police Affairs, Ministry of Defence	HRT	unknown owner and mission of the drone, rejection of speculation, presence of an explosive device	information control, reduction of disinformation	Adjusting information
12th March 2022	during the day	Military Police, Ministry of Defence	media	Some fragments indicate the possibility of an explosive device	technical communication	Risk-prone messaging
13th - 15th March 2022		Andrej Plenković, Prime Minister of the Republic of Croatia	Press conference	Incident represents a serious security threat; criticism of the surveillance system	Political crisis management	Rebuild / Attack the system
March 2022		Jens Stoltenberg NATO Secretary General	International media		International calming communication	Diminish strategy
2023		Mario Banožić, Minister of Defence			Postponement of final interpretation	Post-crisis reframing

THE DRONE ATTACK ON POLAND (SEPTEMBER 2025) AND THE RUSSIAN DISINFORMATION CAMPAIGN: IMPLICATIONS FOR SOCIETAL RESILIENCE IN NATO STATES

Marcin Składanowski

Department of Political Systems and International Communication,

The John Paul II Catholic University of Lublin, Poland

E-mail: marcin.skladanowski@kul.pl

ORCID: <https://orcid.org/0000-0003-1437-8904>

Abstract

This article examines the Russian disinformation campaign that accompanied the repeated violation of Polish airspace by Russian drones on the night of 9–10 September 2025. Its main goal is to determine how coordinated disinformation campaigns accompanying hostile actions threaten societal resilience in NATO member states. The article combines qualitative content analysis of reports and monitoring data published by Polish information security institutions with an analysis of Russian strategic documents on national and information security. The study asks how the disinformation campaign was structured, which narratives dominated it, and how these narratives may weaken the social strength of NATO member states. The findings show that the Russian disinformation campaign was exceptional in its speed and narrative coherence, successfully attributing responsibility to Ukraine, questioning NATO's credibility, and undermining confidence in Polish state institutions. There is a shift in dissemination tactics, with narratives increasingly reproduced by real users and domestic political actors rather than automated bot networks. Disinformation accompanying hostile actions has the potential to amplify uncertainty, polarisation, and distrust, and weaken confidence in national and allied security structures. The conclusion outlines policy implications, especially the need for faster strategic communication, tighter coordination between military and information responses, and stronger resilience measures in the social media environment.

Keywords: information security; Russian aggression; Russian security policy; Russian drones; Russia and NATO

INTRODUCTION

On the night of 9–10 September 2025, Polish airspace was repeatedly violated by Russian drones. Although similar incidents had occurred previously, they generally involved the incursion of individual drones or missiles into Polish airspace (e.g., Polska Agencja Prasowa, 2024). These earlier incidents were typically attributed to navigation errors or technical malfunctions or were assessed as posing no genuine threat. Such explanations were also communicated to the Polish public by the General Staff of the Polish Armed Forces and the Ministry of National Defence (Polska Zbrojna, 2024). In contrast, the September 2025 violations indicate a deliberate provocation by the Russian Federation against Poland and NATO. The timing of the incursion also appears non-coincidental, as it occurred immediately before the commencement of the joint Russian-Belarusian military exercises ‘Zapad-2025’, which simulated offensive operations by Russia and Belarus against Poland and the North Atlantic Alliance.

This article focuses on a dimension of Russia’s aggressive actions that is particularly significant for the societal resilience of NATO member states. In the Polish media space, the drone incursions were accompanied by a rapid and highly aggressive pro-Russian disinformation and propaganda campaign. This campaign pursued three clearly identifiable objectives: undermining public trust in Polish state authorities, questioning the defence capabilities of the North Atlantic Alliance, and fomenting hostility towards Ukraine. Similar pro-Russian disinformation and propaganda activities have been conducted with considerable intensity in the Polish-language online environment, primarily on social media, since 2022, that is, since the onset of Russia’s full-scale aggression against Ukraine. However, the disinformation campaign linked to the drone incursions was exceptional in its intensity, scale, and the simultaneous deployment of all three of the aforementioned narratives, in line with Russia’s broader political objectives.

Research approach

The article examines a distinctive case in which a kinetic provocation was synchronised with a targeted information operation. The September 2025 drone incident represents a significant evolution in Russian cognitive aggression. Particular attention should be paid to its timing (preceding Zapad-2025) and the use of real people to disseminate disinformation rather than bot networks. By isolating this specific event, the article draws attention to the methods through which cognitive warfare exploits immediate crisis environments to degrade societal resilience from within. To investigate these dynamics, this study employs a qualitative content analysis. The empirical material comprises datasets, social media monitoring outputs, and specialist assessments collected by three Polish institutions specialising in information security: the ResFutura analytical team, the NASK Disinformation Analysis Centre, and the Polish Institute of International Affairs (PISM). The dominant thematic narratives were identified within the

collected social media data and subsequently compared against the objectives outlined in official Russian strategic documents on national and information security.

To address the identified deficiencies in understanding how synchronised kinetic and informational provocations operate, this study is guided by the following primary research question: How do disinformation campaigns accompanying hostile actions threaten societal resilience in NATO member states?

The article is structured into five parts. The first provides contextual background and draws on Russian strategic documents to identify the principal objectives of Russia's aggressive actions in the information space, particularly online. The second outlines how pro-Russian disinformation and propaganda are conceptualised in this study and identifies the core content characteristics of such communication in the Polish media environment. The third examines the course and substance of pro-Russian information activities associated with the incursion of Russian drones into Polish airspace in September 2025. The fourth analyses the consequences of these activities within the contemporary Polish social and political context. The fifth offers recommendations concerning the implications of Russia's aggressive information activities for the societal resilience of NATO member states.

Key concepts and ideas

To properly interpret the phenomena discussed in the article, four key concepts must be taken into account:

1. *Cognitive warfare* is the main conceptual framework in this study. It refers to the strategic weaponisation of public opinion, where the psyche becomes the battlefield. The objective is not simply to change what people think, but to manipulate how they think and act, integrating cyber, information, psychological, and social domains to degrade societal resilience (Du Cluzel, 2020, p. 25).
2. *Psychological Operations (PSYOPS)*, also known as *Military Information Support Operations (MISO)*, denote the specific, planned operational activities intended to convey selected information and indicators to foreign audiences. Their goal is to influence the emotions, motives, objective reasoning, and ultimately the behaviour of foreign governments, organisations, groups, and individuals (Joint Chiefs of Staff, 2010). The specific tools used for these operations are propaganda and disinformation.
3. *Propaganda* is a systematic dissemination of biased, selective, or misleading information intended to promote a specific political cause, ideology, or narrative. It is not always entirely false, but it is inherently manipulative (Jowett & O'Donnell, 2018, p. 7).
4. *Disinformation* is understood as false, inaccurate, or manipulated information deliberately created, presented, and disseminated with the explicit intent to deceive and cause public harm (Wardle & Derakhshan, 2017, p. 20).

To explain how disinformation campaigns accompanying hostile actions affect societal resilience, this study adopts a causal framework in which disinformation contributes to the rapid emergence of dominant narratives in the information space. These narratives shape public perceptions of events, which in turn influence levels of trust in state institutions and allied actors. As trust declines, societal resilience, understood as the capacity of a society to maintain cohesion and confidence in security structures during a crisis, is correspondingly weakened.

1. THE AGGRESSIVE NATURE OF RUSSIAN INFORMATION POLICY

Contemporary Russia pursues an increasingly aggressive foreign and security policy despite its declared commitment to creating a just international order, particularly based on respect for state sovereignty (e.g., Russian Federation, 2021, p. 95; Russian Federation, 2023, pp. 18–19). Russian aggression is most visibly directed against Ukraine. However, a defining characteristic of Russia's security and foreign policy is the conduct of a broad spectrum of destructive and destabilising activities against other states that remain below the threshold of open armed conflict (Jones, 2025). In particular, aggressive actions directed against NATO member states can be interpreted, in light of statements by Defence Minister Andrey Belousov, as preparations for a future full-scale armed conflict that the Russian authorities anticipate may occur within the next decade (Kremlin, 2025).

A key component of these activities conducted below the threshold of armed conflict is cognitive aggression, sometimes described as cognitive warfare (Bugayova & Stepanenko, 2025). This form of aggression manifests itself in attempts to exert destructive and destabilising influence on the societies of states regarded as potential adversaries in a future war. Such influence is informational, psychological, and emotional. Its objective is to weaken targeted states by fuelling social unrest, intensifying anti-government sentiment, undermining trust in state institutions and armed forces, and fostering the perception that information disseminated by official media is unreliable or deliberately misleading (Polegkyi, 2023, p. 92).

Disinformation activities related to the intrusion of Russian drones into Polish airspace in September 2025 should be understood as an element of this broader pattern of aggressive Russian policy. For this reason, before analysing these activities and their consequences, it is necessary to outline the theoretical foundations of Russian information aggression, as articulated primarily in Russian strategic documents. Recent strategic documents emphasise identifying media content not controlled by the state as a fundamental threat to Russia's national security. Consequently, before the 2022 aggression against Ukraine, the last partially independent media outlets in Russia were shut down, and systematic efforts were undertaken to isolate the Russian segment of the Internet. At present, Russian mass media cannot be regarded as a means of disseminating information. Since the end of 2021, they have functioned exclusively as instruments of state information policy, serving both to maintain domestic control and to advance the objectives of Russian foreign and security policy internationally (Składanowski et al., 2025).

1.1. Perceived Information Threats in Russian Strategic Doctrine

Russian strategic documents conceptualise the information space primarily as a domain of threat, with the West accused of conducting hostile information activities against Russia and other states. In Russian security literature, it is common to attribute anti-Russian and destructive information operations to Western actors, especially the United States. As Dobren'kov and Agapov (2011) argue, the directives of the US National Security Council explicitly tasked American institutions and subdivisions with destroying Russia through information warfare. This persistent anti-Western narrative has remained a dominant feature of Russian strategic documents published during Vladimir Putin's rule.

According to the 2014 Military Doctrine, information and communication technologies in the contemporary world are increasingly used for military and political purposes that violate international law, undermine state sovereignty, political independence, and territorial integrity, and threaten international peace and security (Security Council of the Russian Federation, 2014, article 12m). In modern armed conflicts, information measures are extensively employed to exploit the potential for popular protest (Security Council of the Russian Federation, 2014, article 15b). Information activities are intended to influence the adversary across its entire territory and simultaneously within the global information space (Security Council of the Russian Federation, 2014, article 15v).

Similarly, the Foreign Policy Concept of the Russian Federation asserts that an increasing number of states use information tools to pursue geopolitical interests, thereby posing a threat to regional and global security (Russian Federation, 2016a, p. 8; Russian Federation, 2023, p. 8). Instruments of so-called 'soft power' are also portrayed as inherently aggressive (Russian Federation, 2016a, p. 9). The portrayal of Russia and like-minded states as victims of Western information aggression is used in the Military Doctrine to justify measures aimed at enhancing information warfare capabilities (Security Council of the Russian Federation. 2014, articles 46v and g), including international cooperation to counter military threats arising from the extensive use of information and communication technologies for military and political purposes (Security Council of the Russian Federation. 2014, article 55ye). The 2021 National Security Strategy and the 2023 Foreign Policy Concept further assert that the information space has become a new domain of warfare (Russian Federation, 2021, p. 17) and that Russia is threatened by information originating abroad (Russian Federation, 2021, pp. 44–52; Russian Federation, 2023, p. 48).

According to the Military Doctrine, external information that influences the population, particularly young people, aimed at undermining historical, spiritual, and patriotic traditions related to the defence of the homeland constitutes a serious threat (Security Council of the Russian Federation, 2014, article 13v). Foreign information influence is also framed as a direct threat to Russia's sovereignty, independence, and territorial integrity (Security Council of the Russian Federation, 2014, article 21). The emphasis on territorial integrity intensified in

strategic documents issued after 2014, following the refusal of most states to recognise Russia's illegal occupation and annexation of Crimea and Sevastopol, as well as other actions aimed at questioning the inviolability of Ukraine's borders (Russian Federation, 2016b, articles 2d, 15, 16, 22, 23a). External sources of information accessible to Russian citizens are also portrayed as a threat to Russia's cultural sovereignty (Russian Federation, 2021, p. 82). Other strategic documents explicitly identify the United States and its allies as the sources of information aggression against Russia (Russian Federation, 2016a, p. 61; Russian Federation, 2021, p. 12). The 2016 Information Security Doctrine further warns of a 'growing risk that information technologies will be used to infringe upon the sovereignty, territorial integrity, or political and social stability of the Russian Federation' (Russian Federation, 2016b, p. 16).

1.2. Strategic Responses to Information Threats

Russian strategic documents not only assert that the West is conducting aggressive information activities against Russia but also, purportedly in response, outline how information tools may be employed to achieve the objectives of Russian foreign and security policy.

Firstly, Russia declares its intention to ensure national and international information security and to counter threats to national, economic, and social security posed by information and communication technologies. Given the authorities' determination to restrict information accessible to citizens via the Internet, strategic documents call for enhanced state control over this channel, citing it as a potential source of external threat (Russian Federation, 2017, pp. 16–17). Such measures are intended to 'strengthen Russia's sovereignty' in the information space (Russian Federation, 2021, p. 56). In particular, state actions aim to counter the use of foreign information sources for military and political purposes directed against the interests of Russia and its allies, or, more broadly, to counter external information influence perceived as threatening global peace, security, and stability. Within this framework, Russia's information policy also seeks the 'fair' governance of the global Internet (Russian Federation, 2016a, p. 28).

Secondly, Russian media are institutionally integrated with the state within the information sphere. Media outlets controlled by the authorities are expected to strengthen their global position to reach broad international audiences with the Russian perspective on international affairs (Russian Federation, 2016a, article 3k). Their task is to disseminate information reflecting Russia's position on key international issues (Russian Federation, 2016a, p. 46) and, above all, to exert effective influence on public opinion abroad. Particular emphasis is placed on Russian-language media (Russian Federation, 2016a, p. 47; Russian Federation, 2021, p. 57), which is directly linked to efforts to influence Russian-speaking populations in neighbouring states.

These elements of Russian information security policy provide important interpretative frameworks for analysing Russian media coverage related to the intrusion of Russian drones

into Polish airspace in September 2025. In Putin's Russia, the role of the media differs fundamentally from that in democratic societies. According to the 2016 Information Security Doctrine, Russian media constitute components of the national information security system (Russian Federation, 2016b, p. 33). As a result, media professionals are jointly responsible for implementing the objectives of state security policy in the information domain. The primary function of Russian media, therefore, is not to provide reliable information but to transmit messages aligned with state policy objectives. Consequently, media output is closely integrated with the authorities' political goals and does not necessarily reflect empirical reality. The reproduction and dissemination of such content thus constitute the propagation of official Russian narratives or narratives serving the objectives of Russian information warfare.

In this context, it is also essential to consider how information warfare objectives are conceptualised in Russian scholarly literature. As Dobren'kov and Agapov (2011, p. 132) argue, 'every major information strategy is aimed at undermining historical and national roots [...] The strategy of information warfare is a strategy of long-term lies, falsifications and disinformation.' Viren (2018, pp. 138–149) further emphasises that information warfare is particularly effective in the online environment due to factors such as broad audience access, rapid dissemination of disinformation, limited content verification, the ability to circumvent standards applied to traditional media, anonymity, and reduced legal accountability. This Russian understanding of information warfare must be taken into account when analysing attempts to influence Western societies through information operations.

2. PRO-RUSSIAN MEDIA COVERAGE IN POLAND

Russian disinformation and propaganda activities (namely those originating in the Russian Federation) related to the intrusion of Russian drones into Polish airspace in September 2025 were subsequently reproduced within the Polish media environment, primarily on social media platforms. This communication can be described as 'pro-Russian'. Given that it was disseminated by Polish actors, including Polish citizens, it is necessary to clarify what is meant here by the pro-Russian character of this media coverage.

In most cases, such content does not imply that its authors or disseminators openly support Russia, endorse Russia's war against Ukraine, or advocate political demands against Poland or other NATO member states. Admittedly, there are individuals and groups within Polish political circles who are openly pro-Russian or accused of acting on behalf of Russian interests (Marek, 2023; Polskie Radio, 2025). However, political actors who explicitly and directly support Russia remain marginal within the Polish political landscape, and their social influence is negligible (Jagiellonia, 2015). This marginalisation stems largely from the fact that Polish society widely perceives Russia and its aggressive actions towards other states as one of the principal threats to Poland's sovereignty and national security. Moreover, a significant proportion of Polish respondents consider Russian military aggression likely (Waluszko, 2026).

In this article, the term ‘pro-Russian narrative’ is understood in a different and more indirect sense. It refers to the dissemination of specific interpretations of the causes, objectives, and conduct of Russia’s war against Ukraine, as well as assessments of the European Union’s internal and external policies, Poland’s military capabilities, and the defence potential of the North Atlantic Alliance. These interpretations align with Russian political objectives and replicate Russian state propaganda, while simultaneously avoiding explicit identification with Russian interests.

Within the Polish media space, such narratives typically manifest themselves in the following forms (Wóycicki et al., 2017; Olchowski, 2022):

1. Anti-Ukrainian rhetoric: presenting Ukraine’s actions or policies as having provoked Russia’s decision to wage war; exaggerating or instrumentalising tensions between Poles and Ukrainians living and working in Poland.
2. Anti-European narratives: emphasising alleged internal weaknesses of the European Union; foregrounding ideological and worldview conflicts; portraying European political elites as pro-immigration, left-wing, and hostile to traditional Christian values.
3. Questioning Poland’s military potential: criticising the direction of the reconstruction and modernisation of the Polish Armed Forces; highlighting organisational, logistical, and technical shortcomings; stressing the financial burden of military investment; and asserting that the Polish military would be ineffective in the event of a Russian attack.
4. Criticism of NATO’s defence capabilities: highlighting the Alliance’s alleged unpreparedness to defend member-state territories; pointing to the absence of a coherent defence strategy; and emphasising internal divisions resulting from divergent policies pursued by the United States and European NATO members.

In general, such pro-Russian narratives, like political stereotypes more broadly, are based on selectively interpreted, manipulated, or exaggerated facts. Crucially, however, they tend to obscure their primary objective: the erosion of public trust in the Polish state, the European Union, and NATO as the political and military frameworks responsible for Poland’s security. The reproduction of these narratives, closely aligned with Russian disinformation, occurred in Polish social media with unprecedented intensity during the Russian drone incursions into Polish airspace in September 2025 and can therefore be analytically classified as pro-Russian.

3. STRUCTURE AND DYNAMICS OF THE DISINFORMATION CAMPAIGN

The course, content, and consequences of the Russian and pro-Russian disinformation campaign have been analysed by numerous Polish institutions. This study draws in particular on the findings of the Res Futura analytical team, the NASK Disinformation Analysis Centre (Research and Academic Computer Network – National Research Institute), and the Polish Institute of International Affairs (PISM).

3.1. Operational Development of the Disinformation Campaign

On the night of 9–10 September 2025, the Polish Air Force, in cooperation with NATO allies, neutralised several Russian drones that had entered Polish airspace. According to Prime Minister Donald Tusk, the first violation of Polish airspace by Russian drones occurred at 22:30 on Tuesday, 9 September (Polska Agencja Prasowa, 2025b). In total, 21 Russian drones entered Polish territory, crossing the border from the direction of Ukraine and Belarus. The Armed Forces Operational Command stated in an official communiqué published online that an “*unprecedented violation of Polish airspace by drones*” had taken place and that “*this act of aggression posed a real threat to the safety of our citizens*” (Polska Agencja Prasowa, 2025a). Although the coordinated disinformation campaign related to the drone intrusions intensified between 9:00 and 10:00 on 10 September 2025, evidence of prior coordination between the Russian act of aggression and the accompanying information operation is evident. As analysts from the Polish Institute of International Affairs noted, even before the drones entered Polish airspace, social media accounts known for disseminating Russian disinformation began posting claims that the incident was a Ukrainian provocation aimed at drawing Poland into a war with Russia (Bryjka & Wójtowicz, 2025).

The disinformation campaign was initially launched by Russian state-controlled media outlets (Polska Agencja Prasowa, 2025c), including Komsomolskaya Pravda, RIA Novosti, and Gazeta.ru. Around 10:00, the so-called Russian Z-bloggers on Telegram joined the campaign. Shortly thereafter, the Russian embassy in Poland became directly involved. Andrey Ordash, Chargé d’Affaires of the Russian Embassy in Warsaw, stated that the drones had entered Polish airspace from Ukrainian territory, thereby implying that the drones were either of Ukrainian origin or that Ukraine bore responsibility for the incursion. This claim was partially false, as Polish authorities subsequently established that some of the Russian drones had entered Polish airspace from Belarusian territory. Around midday, Belarusian sources joined the disinformation effort, disseminating claims that Belarus had allegedly warned Poland about drones flying in from Ukraine (Menkiszak & Chawryło, 2025). From 10:00 onwards, Russian disinformation narratives were also reproduced by Polish actors, primarily via social media platforms. Certain Polish politicians further amplified elements of the Russian propaganda message.

3.2. Dominant Narratives in the Disinformation Campaign

As noted in the analysis conducted by the Res Futura research group, “*the attack by Russian drones on Polish territory was immediately used as a catalyst for an organised information and psychological operation (PSYOPS). The objective of this operation was to shape public sentiment by escalating emotions, polarising public opinion, and systematically undermining trust in state institutions and NATO allied structures. Analysis of Polish social media content indicates a high saturation of repetitive narratives characteristic of coordinated action rather than spontaneous public reactions*” (Res Futura, 2025b).

Within the disinformation campaign related to the intrusion of Russian drones, initiated by Russian sources and subsequently reproduced by Polish internet users, three of the four principal categories of pro-Russian media narratives in Poland identified above were clearly observable:

Anti-Ukrainian narrative. A widespread claim on social media asserted that Ukraine was dragging Poland into a war with Russia and that Polish assistance to Ukraine, including military support, increased the risk of war for Poland. Echoing Russian narratives, it also became common to allege that Ukraine was deliberately provoking a future conflict between Russia and Poland by sending its own drones into Polish territory disguised as Russian drones, or by taking actions intended to ensure that Russian drones entered Polish airspace and thereby provoked a NATO military response.

Narrative questioning NATO's military capabilities. Social media content frequently emphasised the alleged lack of a clear response from the United States to the drone incursions, which was interpreted as evidence that Washington would be unwilling to defend Poland in the event of an armed conflict. In some cases, the absence of an explicit statement from Donald Trump or his administration was framed as proof of an ally's 'betrayal' of Poland.

Narrative questioning Poland's military potential. Pro-Russian media coverage also highlighted the perceived ineffectiveness of Poland's public warning system, as evidenced by the absence of text-message alerts from the Government Security Centre (RCB). In addition, claims circulated regarding the alleged inability of the Polish Armed Forces to counter drone attacks effectively. In particular, it was argued that Poland lacked the capacity to repel a large-scale drone assault comparable to those observed in Ukraine.

In the days following the incident, Polish government representatives and military authorities presented counterarguments demonstrating that much of the pro-Russian media content circulating in Poland was based on disinformation and manipulation. From the perspective of the threat posed by pro-Russian disinformation in the online environment, however, it is significant that the response of state authorities and the armed forces was delayed. As a result, during the critical initial hours following the incursion, especially on social media platforms, pro-Russian narratives clearly dominated the information space.

4. CONSEQUENCES

Russian disinformation, subsequently reproduced by pro-Russian actors within the Polish segment of the Internet, primarily on social media platforms, had observable and immediate effects in the days following the incursion of Russian drones into Polish airspace. At the same time, the more consequential issue concerns the potential long-term implications of the

sustained presence of pro-Russian narratives in Polish social media, particularly from the perspective of Poland's national security.

4.1. Initial effects of the disinformation campaign

Analyses of Polish social media platforms indicate that more than 60 per cent of comments concerning the drone incident contained pro-Russian narratives. According to the Res Futura research group (ResFutura, 2025a) and the NASK Disinformation Analysis Centre (Gov.pl 2025), approximately 40 per cent of comments in the Polish online space reproduced the Russian narrative portraying the incident as a Ukrainian provocation, while only 34 per cent explicitly attributed responsibility for the attack to Russia. An examination of early online reactions reveals that a greater proportion of users blamed Ukraine (38 per cent) than Russia (34 per cent) for the drone incursions. These responses reflected a decline in public trust in NATO and Polish state authorities, accompanied by growing fears of an armed conflict with Russia. The spread of narratives attributing responsibility to Ukraine corresponds to a measurable decline in trust in allied actors, which constitutes a key dimension of societal resilience.

The dominant narrative present in the comments was the claim that the drone intrusion constituted a 'Ukrainian provocation' (32 per cent). Other recurring narratives included the assertion that 'Russia is testing NATO' (28 per cent); the view that the incident demonstrated the incompetence of the Polish government (18 per cent); accusations that the drone intrusions were being exploited to intensify anti-Russian and pro-Ukrainian propaganda in the Polish media (12 per cent); and claims that NATO would not defend Poland in the event of an armed conflict (10 per cent). These dynamics illustrate how the rapid dominance of disinformation narratives shapes public perceptions and directly erodes trust, thereby weakening societal resilience in the immediate aftermath of a crisis.

4.2. Possible long-term effects of pro-Russian disinformation

In assessing the possible long-term consequences of pro-Russian disinformation, it is essential to highlight a frequently overlooked but deeply concerning trend evident in online reactions to the drone incident.

The primary channels disseminating pro-Russian disinformation were not automated bot networks, but real individuals who voluntarily reproduced Russian narratives. This case suggests an evolution of cognitive warfare, where effectiveness depends less on automation and more on the internalisation of narratives within target societies. In this context, disinformation is no longer imposed exclusively from external sources but resonates within segments of society, thereby increasing its effectiveness and durability.

Pro-Russian content is predominantly promoted by anti-Ukrainian and anti-government users and channels, as well as by political circles associated with the Konfederacja political movement. Notably, leaders and prominent representatives of this far-right, anti-European formation were particularly active in disseminating pro-Russian narratives, including content questioning Poland's and NATO's defence capabilities (Brzozowski, 2025; Grochal, 2025; Skórko, 2025). This development is especially troubling given the possibility that Konfederacja may join a governing coalition after the 2027 parliamentary elections. More broadly, the presence and dissemination of pro-Russian messaging in the Polish online space reflect the views of a distinct and potentially growing segment of Polish society that has been effectively influenced by Russian propaganda.

An analysis of the disinformation campaign surrounding the September 2025 drone incident, viewed against the backdrop of Poland's current political context, suggests three potential long-term effects:

First, such narratives may further exacerbate negative attitudes among Poles towards Ukraine and Ukrainians. A deterioration in public perceptions has been observed since 2022 (Gazeta Prawna, 2025), particularly regarding the Ukrainian state and its functioning. This includes persistent narratives concerning corruption in Ukraine and allegations regarding the misuse of weapons and ammunition supplied by Western states, including Poland. These perceptions also extend to attitudes towards the substantial Ukrainian population residing in Poland, consisting primarily of economic migrants and, to a lesser extent, war refugees. Negative sentiment is expressed through claims regarding difficulties in adapting to Polish social norms and values, the alleged prevalence of crime among Ukrainians, and the perceived financial burden imposed by social benefits allocated to Ukrainian residents. The political movement Konfederacja (Andrysiak & Sowa, 2025), some of whose current and former leaders have expressed overtly pro-Russian views (Mierzyńska, 2026), has played an active role in shaping a negative image of Ukraine and Ukrainians, particularly through social media channels.

Second, the dominance of pro-Russian narratives in social media may contribute to the further strengthening of extreme right-wing, anti-European, and anti-Ukrainian political forces in Poland. Although the rise of the far right has been evident for several years, the principal concern is that these groups promote positions fundamentally at odds with Poland's national security interests, notably continued European integration and sustained support for Ukraine in its defence against Russian aggression.

Third, pro-Russian disinformation may undermine the authority and public legitimacy of the Polish Armed Forces. Opinion polls indicate that the military in Poland traditionally enjoys high levels of public trust (Ceglarz, 2025). This trust is of particular importance given that, since the onset of Russia's full-scale aggression against Ukraine, successive Polish governments, irrespective of political orientation, have pursued an ambitious programme of military expansion and modernisation. Defence expenditure in the 2026 state budget amounted

to 4.8 per cent of GDP (Defence24, 2025). At the beginning of 2026, the size of the Polish Armed Forces (comprising professional soldiers, voluntary basic military service personnel, and members of the Territorial Defence Forces) stood at approximately 216,000. The planned target force size by 2039 is 500,000 personnel, including 300,000 in active service and 200,000 in reserve (Ciślak, 2026). Against this backdrop, pro-Russian narratives circulating within the Polish online space increasingly target the military itself. These narratives criticise armaments modernisation programmes, training systems, personnel expansion, and, more broadly, question the combat effectiveness of the Polish Armed Forces, including their capacity to defend national territory.

It can therefore be concluded that the sustained presence of pro-Russian narratives within the Polish media environment, particularly on social media, may, in the long term, seriously weaken Poland's defence potential. This process is likely to be driven by the erosion of public trust in state efforts to strengthen the armed forces, the spread of beliefs that Poland is incapable of defending itself, doubts regarding the reliability of NATO commitments, and the intensification of social tensions through the instrumentalisation of conflicts involving Ukrainians living and working in Poland.

RECOMMENDATIONS AND CONCLUSIONS

One of the principal objectives of Russian propaganda and disinformation is to weaken the North Atlantic Alliance, which Russian strategic documents identify as the primary threat to Russia's security (Russian Federation, 2021, p. 35). The very existence of the Alliance, together with the prospect of its further enlargement, runs counter to Russia's neo-imperial and revisionist policy in Central and Eastern Europe. Moreover, the principles underpinning social life in Western societies, most notably dominant liberal values, are portrayed by Russian authorities as a threat to the stability of Russian society (Russian Federation, 2021, p. 19; Russian Federation, 2023, p. 59). In the context of escalating tensions between Russia and democratic Western states, and in light of publicly articulated Russian plans for a potential armed confrontation with NATO, Russian information policy is therefore aimed not only at isolating Russian society from external information flows, but also at exerting a destructive and destabilising influence on Western societies.

It would be naïve to assume that Russian propaganda is disseminated exclusively through bots and troll farms. Although the primary sources of disinformation designed to disrupt political and social life in NATO member states are often located in Russia, this content is frequently reproduced by social media users and, at times, by Western politicians who may fail to recognise both its origin and its strategic purpose.

Analysis of Russian and pro-Russian disinformation campaigns surrounding the drone intrusions into Polish airspace in September 2025 demonstrates that maintaining and

strengthening societal resilience in NATO member states requires complex, coordinated, and multifaceted responses.

National security strategies should explicitly recognise disinformation, particularly from Russia, as a fundamental threat to societal resilience. Such strategies should provide comprehensive, coordinated measures to counter this threat, integrating political, legal, informational, and security instruments.

One essential, though not sufficient, measure is to limit the reach of Russian cognitive aggression by controlling the penetration of Russian disinformation into NATO countries' information spaces and preventing sabotage aimed at undermining public trust in state institutions, particularly those responsible for ensuring security. This also encompasses strictly military measures, such as the effective neutralisation of Russian or unidentified drones that violate NATO airspace. Such incursions not only disrupt transport and pose risks to human life and critical infrastructure, but – crucially from an informational perspective – may also be exploited to reinforce Russian and pro-Russian narratives portraying state authorities as incapable of guaranteeing citizens' security.

In the domain of information security, including efforts to counter Russian cognitive aggression, it is imperative to enhance public awareness within Western societies. In particular, it is necessary to emphasise that Russian media do not function as mass media in the Western sense and do not aim to provide objective or independent information. Rather, they serve as instruments of state information policy, including information warfare and disinformation operations.

The information policies of NATO member states, both at the national level and within the framework of joint allied activities, must therefore incorporate the systematic planning and execution of measures designed to counter Russian disinformation. In the context of Russia's cognitive warfare strategy, it should be assumed that any hostile or sabotage-related action undertaken by Russia will be accompanied by immediate and coordinated disinformation efforts. These activities are intended, first, to obscure or relativise Russia's responsibility and, second, to exploit such incidents to destabilise social and political life in the affected states. Consequently, information responses and disinformation countermeasures should be closely coordinated with other security-related activities, including military operations, and should be implemented as rapidly as possible following any hostile action.

Finally, when designing information activities and counter-disinformation strategies, it is essential to account for the declining influence of traditional mass media. While the inclusion of counter-disinformation content in school-based media literacy or defence education programmes remains important, active engagement in the media sphere is also required. Social media platforms, in particular, should increasingly become key arenas for such efforts. In this context, the visible and credible presence of representatives of the armed forces and other state

institutions responsible for national security within these platforms is both necessary and desirable.

More broadly, the findings indicate a shift in cognitive warfare towards the internalisation of disinformation within target societies, where the reproduction of narratives by domestic actors becomes a key mechanism of influence.

Disinformation campaigns accompanying hostile actions weaken societal resilience by exploiting crises to spread narratives that weaken trust in institutions, alliances, and security structures. By simultaneously deploying kinetic provocations and informational warfare, these operations may succeed in increasing social divisions and undermining public confidence in the state's ability to provide security.

REFERENCES

- Andrysiak, A., & Sowa, B. (2025, April 20). Tak nakręcają niechęć do Ukraińców. Poseł Konfederacji napisał: „ukraiński western”. I się zaczęło. *TOK FM*.
<https://www.tokfm.pl/polska/tokfm-7-103085-31860649-nastroje-antyukrainskie-rosnachodza-osilki-i-rzekomo-pilnuja>
- Bryjka, F., & Wójtowicz, A. (2025). *Rosyjska dezinformacja w sprawie ataku dronów na Polskę*. Polski Instytut Spraw Międzynarodowych.
<https://www.pism.pl/publikacje/rosyjska-dezinformacja-w-sprawie-ataku-dronow-na-polske>
- Brzozowski, A. (2025, September 12). Prorosyjska prawica w oparach absurdu. Przekonuje: „Atak dronów na Polskę, to prowokacja gangu Tuska i Sikorskiego”. *Wyborcza.pl*.
<https://wroclaw.wyborcza.pl/wroclaw/7,35771,32247095,prorosyjska-prawica-w-oparach-absurdu-przekonuje-atak.html>
- Bugayova, N., & Stepanenko, K. (2025). *A Primer on Russian Cognitive Warfare*. Institute for the Study of War. https://understandingwar.org/wp-content/uploads/2025/08/ISW20CW20Russian20Cognitive20Warfare2C20June20302C20202520PDF20FINAL_0.pdf
- Ceglarz, J. (2025, September 17). Oto zaufanie Polaków do armii. Rzadko jesteśmy tak jednomyślni. *Business Insider*. <https://businessinsider.com.pl/wiadomosci/oto-zaufanie-polakow-do-armii-rzadko-jestesmy-tak-jednomyslني-sondaz/cyew17n>
- Ciślak, J. (2026, January 21). Jak rośnie armia. Wiemy, ilu żołnierzy ma Wojsko Polskie. *Defence24*. <https://defence24.pl/sily-zbrojne/jak-rosnie-armia-wiemy-ilu-zolnierzy-ma-wojsko-polskie-analiza>
- Defence24 (2025, December 5). *Budżet uchwalony, prawie 5 proc. PKB na obronność*.
<https://defence24.pl/polityka-obronna/budzet-uchwalony-prawie-5-proc-pkb-na-obronnosc>.
- Dobrenkov, V. I., & Agapov, P. V. (2011). *Voina i bezopasnost' Rossii v XXI veke* [War and security of Russia in the 21st century]. Akademicheskiy proekt.
- Du Cluzel, F. (2020). *Cognitive Warfare*. <https://natoassociation.ca/tag/cognitive-warfare/>.
- Gazeta Prawna. (2025, November 5). *Coraz więcej negatywnych opinii o Ukraińcach w sieci. Część oparta na dezinformacji*.
<https://www.gazetaprawna.pl/wiadomosci/kraj/artykuly/10575325,coraz-wiecej-negatywnych-opinii-o-ukraincach-w-sieci.html>
- Gov.pl. (2025, September 15). *Najnowsze narracje dezinformacyjne w polskiej infosferze związane z dronami*. <https://www.gov.pl/web/baza-wiedzy/najnowsze-narracje-dezinformacyjne-w-polskiej-infosferze-zwiazane-z-dronami>

- Grochal, R. (2025, November 22). Co po dywersji stało się z rozumem Konfederacji? To nie trzyma się logiki. *Newsweek.pl*. <https://www.newsweek.pl/opinie/konfederacja-powielaproorosyjska-propagande-po-dywersji-na-kolei/1wvw5te>
- Jagiellonia (2015, April 15). Środowiska prorosyjskie w Polsce. *Jagiellonia.org*. <https://jagiellonia.org/srodowiska-prorosyjskie-w-polsce/>
- Joint Chiefs of Staff. (2010, June 15). *Psychological Operations* (Joint Publication 3-13.2). U.S. Department of Defense. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_13_2.pdf
- Jones, S.G. (2025, March 18). *Russia's Shadow War Against the West*. Center for Strategic & International Studies. <https://www.csis.org/analysis/russias-shadow-war-against-west>
- Jowett, G. S., & O'Donnell, V. (2018). *Propaganda & Persuasion*. SAGE Publications. <https://csmeyns.github.io/propaganda-everyday/pdf/odonnell-jowett-2018-what-is-propaganda.pdf>
- Kremlin.ru. (2025, December 16). Rasshirennoye zasedaniye kollegii Minoborony. *Kremlin.ru*. <http://kremlin.ru/events/president/news/78801>
- Marek, M. (2023, July 20). *Bieżąca aktywność środowisk prorosyjskich i rosyjskich ośrodków dezinformacyjnych w Polsce – druga połowa lipca 2023*. Centrum Badań nad Współczesnym Środowiskiem Bezpieczeństwa. <https://infowarfare.pl/2023/07/20/rosja-dezinfo-w-pl-druga-polowa-lipca/>
- Menkiszak, M., & Chawryło, K. (2025, September 10). *Oslabić, podzielić i odstraszyć: cele rosyjskiej prowokacji wobec Polski*. Ośrodek Studiów Wschodnich. <https://www.osw.waw.pl/pl/publikacje/analizy/2025-09-10/oslabic-podzielic-i-odstraszyc-cele-rosyjskiej-prowokacji-wobec>
- Mierzyńska, A. (2026, January 26). Oni stoją za Braunem. Zobacz, kto legitymizuje sympatyków Putina i siewców teorii spiskowych. *OKO.press*. <https://oko.press/za-braunem-legitymizuja-sympatykow-putina-i-siewcow-teorii-spiskowych>
- Olchowski, J. (2022, June 30). *Rosyjska propaganda uderza w relacje polsko-ukraińskie*. Instytut Europy Środkowej. <https://ies.lublin.pl/wp-content/uploads/2022/06/ies-komentarze-646-158-2022.pdf>
- Polska Agencja Prasowa. (2024, 26 August). Co przekracza polską przestrzeń powietrzną? Wtargnięcia rosyjskich obiektów od początku wojny. *Polska Agencja Prasowa*. <https://www.pap.pl/aktualnosci/co-przekracza-polska-przestrzen-powietrzna-wtargniecia-rosyjskich-obiektow-od-poczatku>
- Polska Agencja Prasowa. (2025a, September 10). „Akt agresji, który stworzył realne zagrożenie dla obywateli”. Komunikat wojska. *Polska Agencja Prasowa*. <https://www.pap.pl/aktualnosci/akt-agresji-ktory-stworzyl-realne-zagrozenie-dla-obywateli-komunikat-wojska>

- Polska Agencja Prasowa. (2025b, September 10). Premier Tusk w Sejmie o naruszeniu przestrzeni powietrznej. Podał liczby. *Polska Agencja Prasowa*.
<https://www.pap.pl/aktualnosci/premier-naruszenia-polskiej-przestrzeni-trwaly-cala-noc>
- Polska Agencja Prasowa. (2025c, September 10). Rosyjskie media i tzw. blogerzy wojenni dezinformują ws. dronów nad Polską. *Polska Agencja Prasowa*. .
<https://www.pap.pl/aktualnosci/rosja-media-i-tzw-blogerzy-wojenni-dezinformuja-w-sprawie-dronow-nad-polska>
- Polegkyi, O. (2023). Russian disinformation and propaganda before and after the invasion of Ukraine. *Rocznik Instytutu Europy Środkowo-Wschodniej*, 21(1), 91–107.
<https://doi.org/10.36874/RIESW.2023.1.6>
- Polska Zbrojna. (2024, March 2024). Wojsko informuje o rosyjskiej rakiecie nad Polską. *Polska Zbrojna*. <https://polska-zbrojna.pl/home/articleshow/41419>
- Polskie Radio. (2025). April 16). Lista 25 nazwisk pod lupą służb. Według służb to oni sieją rosyjską propagandę. *Polska Zbrojna*,
<https://www.polskieradio.pl/399/7977/artykul/3511408,lista-25-nazwisk-pod-lupa-sluzb-wedlug-sluzb-to-oni-sieja-rosyjska-propagande>
- Res Futura. (2025a, September 15). *Drony w Polsce*. <https://resfutura.pl/150925-2/>
- Res Futura. (2025b, September 10). *Raport specjalny*. <https://resfutura.pl/polska100925/>
- Russian Federation. (2016a, November 30). *Kontseptsiiia vneshnei politiki Rossiiskoi Federatsii* [Foreign policy concept of the Russian Federation].
<http://www.kremlin.ru/acts/bank/41451>
- Russian Federation. (2016b, December 5). *Doktrina informatsionnoi bezopasnosti Rossiiskoi Federatsii* [Information security doctrine of the Russian Federation].
<http://kremlin.ru/acts/bank/41460>
- Russian Federation. (2017, May 9). *Strategiia razvitiia informatsionnogo obshchestva v Rossiiskoi Federatsii na 2017–2030 gody* [Strategy for the development of the information society in the Russian Federation for 2017–2030].
<https://kremlin.ru/acts/bank/41919>
- Russian Federation. (2021, July 2). *Strategiia natsional'noi bezopasnosti Rossiiskoi Federatsii* [National security strategy of the Russian Federation].
<http://www.kremlin.ru/acts/bank/47046/page/1>
- Russian Federation. (2023, March 31). *Kontseptsiiia vneshnei politiki Rossiiskoi Federatsii* [Foreign policy concept of the Russian Federation].
<http://kremlin.ru/events/president/news/70811>
- Security Council of the Russian Federation. (2014, December 25). *Voennaia doktrina Rossiiskoi Federatsii* [Military doctrine of the Russian Federation].
<http://www.scrf.gov.ru/security/military/document129/>

- Składanowski, M., Smuniewski, C., & Łukasik-Turecka, A. (2025). The Media's Role in Preparing Russian Society for War with the West: Constructing an Image of Enemies and Allies in the Cases of Latvia, Poland, and Serbia (2014–2022). *Journalism and Media*, 6(2), 79. <https://doi.org/10.3390/journalmedia6020079>
- Skórko, O. (2025). September 10). Burza po wypowiedzi Mentzena. „Konfederacja zdaje się przygotowywać do złożenia hołdu na Kremlu”. *Dziennik.pl*. <https://wiadomosci.dziennik.pl/polityka/artykuly/9884179,burza-po-wypowiedzi-mentzena-konfederacja-zdaje-sie-przygotowywac-do.html>
- Waluszko, F. (2026, January 8). Nowy sondaż IPSOS: Spytały Polaków, czy boją się ataku ze strony Rosji. *Business Insider Polska*. <https://businessinsider.com.pl/polityka/nowy-sondaz-ipsos-spytali-polakow-czy-boja-sie-ataku-ze-strony-rosji/eb0vt66>
- Wardle, C., & Derakhshan, H. (2017). *Information Disorder: Toward an interdisciplinary framework for research and policymaking*. Council of Europe. <https://edoc.coe.int/en/media/7495-information-disorder-toward-an-interdisciplinary-framework-for-research-and-policy-making.html>
- Viren, G. V. (2018). *Tret'ia mirovaia... informatsionnaia. Informatsionnye voyny v mediaprostranstve* [The Third World... informational: Information wars in the media space]. Zvonitsa-MG.
- Wóycicki, K., Kowalska, M., & Lelonek, A. (2017). *Rosyjska wojna dezinformacyjna przeciwko Polsce* [Russian disinformation war against Poland] (Raport). Fundacja im. Kazimierza Pułaskiego. <https://pulaski.pl/wp-content/uploads/2015/02/RAPORT-Rosyjska-wojna-dezinformacyjna-przeciwko-Polsce.pdf>

COGNITION IN WARFARE: CONCEPTUAL FRAMEWORK, CHALLENGES, AND IMPLICATIONS FOR NATIONAL SECURITY AND THE DEFENCE SYSTEM

Ines Grossi¹, Antonija Rimac Gelo²

¹ PhD candidate at the Doctoral School of the J. J. Strossmayer University of Osijek,
E-mail: ines.benkovic@gmail.com

² Croatian Parliament
E-mail: antonija.gelo@gmail.com

Abstract

The paper examines cognition in contemporary warfare by analysing the relationship between the proposed cognitive domain, the cognitive dimension as used in NATO documents, and the emerging concept of cognitive warfare. NATO strategic frameworks recognise the cognitive space as a decisive arena in which perception, understanding, motivation, and the will to act are shaped among both military and civilian actors. It is within this realm that operations are conducted to influence how individuals and societies make decisions, interpret information, and respond to crises. Drawing on the literature on cognitive warfare, information operations, and multidomain warfare, the paper first presents the theoretical foundations of the cognitive domain. It then examines key challenges, including the term's conceptual inconsistency, the ethical and legal dilemmas it raises, and the risks of militarising the human and social sciences.

In the final section, the paper analyses the implications for the defence system, including the development of cognitive skills and resilience among members of the armed forces, the strengthening of societal resilience to disinformation, and opportunities for cross-sectoral cooperation among the military, academia, and civil society. The paper thus offers a conceptual framework for the critical evaluation of the cognitive domain and reflection on its role in the future development of Croatia's defence system. Ultimately, it argues that, regardless of formal categorisation, the cognitive domain constitutes an indispensable dimension of contemporary

warfare and requires an integrated approach that brings together psychology, communication sciences, military doctrine, and emerging technologies.

Keywords: cognitive domain, cognitive warfare, information environment, resilience, NATO doctrine

INTRODUCTION

Changes in the security environment in the 21st century, marked by accelerated technological development, global interconnectedness, and the growing role of information, have led to a gradual re-examination of traditional concepts of warfare. Alongside classical domains - land, sea, and air - and newer ones such as space and cyber, the concept of the cognitive domain is increasingly appearing in strategic and doctrinal discussions. This term denotes the space in which the perceptions, understandings, motivations, and willingness to act of individuals and societies are shaped, and thus their ability to make decisions under conditions of crisis, conflict, or war. Although it is often described as the “sixth domain of warfare,” its status, content, and boundaries remain the subject of intensive theoretical and practical debate. While the term “cognitive domain” frequently appears in academic and conceptual discussions, NATO’s formal doctrinal framework primarily treats “cognitive” as a dimension of the information environment rather than as a separate operational domain. In this paper, the term “cognitive dimension” is used in accordance with NATO terminology. In contrast, references to the cognitive domain are retained when addressing analytical or conceptual proposals that treat it as a potential sixth domain of warfare. This article, therefore, distinguishes between the notion of a so-called *cognitive domain* as a proposed “sixth domain of warfare”, the *cognitive dimension* as it appears in NATO doctrinal documents, and *cognitive warfare* as a set of strategies and practices targeting perception and decision-making.

In contemporary conflicts, kinetic dominance and technological superiority are no longer sufficient to achieve political and military objectives. An increasingly decisive role is played by the ability to shape perception, interpret information, and act, not only among adversaries but also within one’s own society. Information campaigns, disinformation, psychological operations, and strategic communication are therefore directed at human perception of reality and interpretation of events, thereby making the cognitive domain a common analytical framework for understanding these activities. The problem with the so-called cognitive domain lies not in its relevance but in its unclear theoretical and normative status. Despite the term’s increasing use, the cognitive domain has not yet been fully consolidated, either theoretically or doctrinally. Strategic documents and conceptual debates reveal terminological inconsistencies and overlaps with existing concepts, such as information and psychological operations, as well as hybrid warfare. In addition, the idea of the cognitive domain raises a range of ethical and legal questions, particularly regarding the limits of legitimate military action and the risk of the militarisation of the humanities and social sciences. It is precisely this indeterminacy that makes the concept simultaneously analytically stimulating and normatively problematic.

Building on the foregoing, this paper aims to critically analyse the cognitive domain as a proposed “sixth domain of warfare” and to examine its actual status within contemporary strategic and doctrinal frameworks. The paper primarily focuses on the theoretical and conceptual foundations of the cognitive domain in the context of multidomain warfare and subsequently analyses how this concept is presented and operationalised in relevant NATO documents. Particular attention is devoted to conceptual, ethical, and legal challenges arising from efforts to treat human perception and decision-making processes as a space of military activity. In the final part of the paper, the implications of the cognitive domain for the Republic of Croatia's defence system are examined in the context of existing national security and defence documents and NATO allies' obligations. In doing so, the paper seeks to offer a balanced, critically grounded conceptual framework that enables understanding of the cognitive dimension and the proposed cognitive domain not only as a military challenge but also as a broader societal phenomenon.

1. METHODOLOGY

The central research method is content analysis of strategic, conceptual, and doctrinal documents, with particular emphasis on NATO documents. The analysed literature includes key NATO strategic and doctrinal documents, encompassing conceptual frameworks, allied doctrines, and innovation and experimental concepts related to cognitive warfare. The analysis focuses on how the concept of the cognitive domain is defined, used, and normatively positioned, and on identifying terminological differences and conceptual overlaps with existing concepts such as information and psychological operations, hybrid warfare, and strategic communication. In addition to content analysis, the paper applies a comparative method, particularly in a section that compares classical domains of warfare with the proposed cognitive domain and examines their relationship to the object of action, the spatial dimension, and the measurability of effects. This method enables a systematic highlighting of the specificities of the cognitive domain and its conceptual differentiation from established domains of contemporary warfare. Based on the identified concepts, terminological patterns, and normative emphases, the implications of the cognitive domain for the Republic of Croatia's defence system are considered.

The central research question of the paper is: Can the proposed cognitive domain be justifiably considered a distinct domain of warfare, or is it more appropriate to view it as an overarching conceptual framework that integrates the psychological, informational, and social dimensions of contemporary conflicts? The selected methodology provides comprehensive insight into the cognitive domain of warfare as a multidimensional phenomenon, while maintaining critical distance from its conceptual and normative use in contemporary security discourses. The research is limited to publicly available documents and conceptual debates, without access to classified doctrinal or operational materials, which necessarily affects the level of operational concretisation of the conclusions.

2. THEORETICAL AND CONCEPTUAL FRAMEWORK OF THE COGNITIVE DIMENSION OF WARFARE

To provide clearer insight into the specific characteristics of the cognitive domain relative to the classical domains of warfare, the following section presents a comparative overview of key features. In this context, it is important to distinguish the concept of the cognitive domain from that of cognitive warfare: while the latter refers to a set of strategies, tactics, and means of action, the cognitive domain denotes an analytical space in which these effects are realised. In line with NATO usage, this paper nevertheless treats the *cognitive* primarily as a dimension of the information environment, while using the term "*cognitive domain*" only in analytical models that explicitly frame it as a potential sixth domain of warfare. Authors Deppe and Schaal define cognitive warfare as a tactic that combines "traditional and new technologies as well as measures above and below the threshold of war in order to achieve cognitive effects on the adversary's population and on its political and military leaders" (Deppe & Schaal, 2024: 2). Such an approach points to expansion of the battlefield beyond physical and information-communication frameworks into the space of human perception, interpretation, and judgment. In this context, Claverieu and Cluzel emphasize that "*cognitive warfare represents an unconventional form of conflict that employs cyber tools to alter the opponent's cognitive processes, exploit mental biases or reflexive thinking, and generate distortions in perception, influence decision-making, and hinder action—with negative consequences at both the individual and collective levels*" (Claverieu & Cluzel, 2022, p. 4). Cited definitions are further complemented by a technological perspective that views cognitive warfare as the result of an increasingly pronounced convergence of advanced systems and human factors. Thus, Masakowski and Blatny define cognitive warfare (CogWar) as the "convergence of a broad spectrum of advanced technologies combined with human factors and systems, including artificial intelligence (AI), machine learning (ML), information and communication technologies (ICT), neuroscience, biotechnology, and human enhancement" (Masakowski & Blatny, 2023, p. 19). The common denominator of these approaches is an understanding of cognitive action as a deliberate, systematic influence on how individuals and collectives perceive reality, interpret information, and make decisions. In this way, the cognitive domain is clearly positioned as an interdisciplinary and hybrid area of activity, in which the boundaries between technological, psychological, and social spaces are blurred. Such an understanding is not entirely new; it builds on earlier strategic reflections on the shift in the centre of gravity of contemporary conflicts. As early as 2009, Akrap warned that "*the new centre of gravity of strategic action in the 21st century is becoming the mind of the individual, group, and community; individual and group cognitive processes aimed at shaping their opinions, attitudes, conclusions, and decisions, in order to influence their actions and a perception of reality that is not based on truth and facts*" (Akrap, 2009, p. 126). In this sense, cognitive warfare can be understood as a logical continuation of the evolution of warfare, in which the decisive struggle is increasingly conducted in the space of perception, meaning, and the interpretation of reality. Thus, "*cognitive warfare aims to undermine trust (public trust in electoral processes, trust in institutions, allies, politicians...).* Consequently, the individual

becomes a weapon, and the objective is not to attack what individuals think, but the way they think” (Cluzel, 2020, p. 8). NATO has declared five operational domains so far: land, maritime, air, cyber and space (North Atlantic Treaty Organisation [NATO], 2019; North Atlantic Treaty Organisation Allied Command Transformation [NATO ACT], 2023). The land domain encompasses the space of direct physical interaction and territorial control. The maritime domain concerns power projection, the protection of lines of communication, and strategic mobility. The air domain enables rapid action, precision strikes, and surveillance. The space domain encompasses communication, intelligence collection, navigation, and positioning. The cyber domain is a global domain composed of interconnected communication and information systems, networks, and their data (NATO, 2020). What the aforementioned domains have in common is that they are defined through relatively clearly delineated spaces of action and technically measurable effects, which enables their stable doctrinal operationalisation. While these domains are traditionally defined primarily in terms of physical or virtual spaces of action, the cognitive domain introduces a qualitatively different focus on perception, interpretation, and decision-making. Comparing the classical domains of warfare with the cognitive domain clarifies the specific features of this concept, particularly regarding the object of action, dominant actors, and the measurability of effects. For these reasons, comparing classical domains of warfare with the cognitive domain is a useful analytical tool for understanding its conceptual distinctiveness.

Table 1

Comparison of Classical Domains of Warfare and the Cognitive Domain

Domain of Warfare	Object of Action	Spatial Dimension	Dominant Actors	Measurability of Effects
Land	Territory and forces	Physical	Armed forces	High
Maritime	Maritime space	Physical	Naval forces	High
Air	Airspace	Physical	Air forces	High
Space	Orbital systems	Physical (extra-atmospheric)	State and commercial actors	Medium
Cyber	Information systems	Virtual/informational	State and non-state actors	Medium
Cognitive	Perception, interpretation, and decision-making	Psychosocial	Individuals, societies, institutions	Low/indirect

Note. Table created by the authors based on an analysis of NATO literature.

Table 1 provides an overview of fundamental differences between classical domains of warfare and the cognitive domain, clearly illustrating why the cognitive domain is difficult to integrate into the established domain framework. Classical domains - land, maritime, and air - are characterised by clearly defined physical spaces of action, a relatively homogeneous set of dominant actors, and a high level of measurable effects, which enable their stable doctrinal and operational application. A similar assessment applies to the space and cyber domains, although these already exhibit a certain degree of complexity through the involvement of commercial and non-state actors, as well as a reduced yet still recognisable ability to assess effects. In contrast, the cognitive domain differs fundamentally in the object of action, which is not material but encompasses perception, interpretation, and decision-making. Accordingly, the spatial dimension of action shifts from a physical or virtual framework to a psychosocial space with no clear boundaries and no stable reference points. As a consequence, the measurability of effects in the cognitive domain remains low and largely indirect, since changes in attitudes, beliefs, or the will to act can be observed only over the long term and often cannot be unambiguously and independently linked to a specific action.

This comparison clearly demonstrates that the cognitive domain can hardly be viewed, normatively or doctrinally, as a domain of warfare in the classical sense, comparable to land, sea, or air. Instead, it emerges as an analytical framework that encompasses the human and societal dimensions of conflict and transcends strictly military and operational categories. In this context, Akrap's assertion is particularly illustrative that "*the cognitive domain has become the primary battlefield, the information domain secondary, and the physical domain only tertiary*" (Akrap, 2009, p. 111). Building on this understanding, the cognitive domain cannot be interpreted merely as another operational domain of warfare, but rather as a conceptual framework encompassing the psychological, social, and communicative dimensions of contemporary conflicts and fundamentally redefining how power, influence, and security are exercised today. This interpretation is further reinforced by Miller, who warns that cognitive warfare, despite its strategic importance and growing presence in contemporary conflicts, cannot yet be considered war in the full sense of the term, but rather a form of conflict below the threshold of war, which often unfolds under peacetime conditions and overlaps with covert political operations. According to Miller, the key characteristics of cognitive warfare are not territorial conquest or kinetic force, but influence over perception, decision-making, and social cohesion, with issues of attribution, responsibility, and the legitimacy of influence being particularly pronounced (Miller, 2023, pp. 2–10).

3. THE COGNITIVE DIMENSION OF WARFARE IN NATO DOCUMENTS

Although in formal NATO doctrines the cognitive is generally described as a dimension of the information environment, alongside physical and virtual dimensions, more recent conceptual documents and innovation initiatives increasingly refer to the cognitive domain as a space for targeted effects, particularly in the context of "cognitive warfare" and "attacks against the cognitive domain" (North Atlantic Treaty Organization & UK Ministry of Defence, 2023;

Bernal et al., 2023). In this regard, it is important to distinguish between formal doctrinal publications (the AJP series and core strategic documents) and conceptual and innovation initiatives that lack binding doctrinal status. Within NATO's normative–doctrinal framework, the cognitive dimension is not included among the classical operational domains (land, maritime, air, space, cyber), but it is increasingly affirmed in strategic, conceptual, and doctrinal documents. To illustrate how the cognitive dimension is conceptualised and operationalised within NATO, the following section provides an overview of key documents that explicitly or implicitly address it. The analysis compares terminology, contexts of use, and the normative status of the cognitive dimension across different levels of NATO's doctrinal and strategic documents.

Table 2

Development and Status of the Cognitive Domain in NATO Documents

Document	Year	Terminology	Context of Use	Status of the Cognitive Domain
NATO Warfighting Capstone Concept (NATO ACT, 2021).	2021	Cognitive superiority; cognitive understanding/dimension	Multi-Domain Warfare, Warfare Development Imperatives	Cognitive dimension, Dimension and objective of superiority, Not formally defined as a domain
NATO ACT – Cognitive Warfare (Claverie & du Cluzel, 2022; Claverie et al., 2022; Cluzel, 2020; Bernal et al., 2023)	2020-2022	Cognitive warfare; cognitive domain; cognitive attacks	Innovation and experimental framework, Warfare Development Agenda	Concept under development, lower-level concept subordinate to the NWCC, outside the AJP framework
NATO Strategic Concept 2022 (NATO, 2022a)	2022	Resilience; information environment; hybrid threats (implicit cognition)	Societal and institutional resilience, hybrid activity	Cognitive dimension is implicitly recognised, not as a separate domain
AJP-01 Allied Joint Doctrine (NATO, 2022b)	2022	Behaviour-centric approach; cognitive dimension	Foundational Allied doctrine, focus on behaviour and effects	Cognitive as a dimension of effects and behaviour, not as a domain

AJP-10 Allied Joint Doctrine for Strategic Communications (UK Ministry of Defence, 2023a)	2023	Cognitive dimension; effects in the cognitive dimension; narratives; perceptions, attitudes, and behaviours of target audiences	Strategic communications as a framework for coordinating and integrating the communication activities of different instruments of power toward target audiences	The cognitive dimension is explicitly recognised as a space for desired effects on perceptions, attitudes, and behaviour, but is not formalised as a separate operational domain.
AJP-10.1 Allied Joint Doctrine for Information Operations (UK Ministry of Defence, 2023b)	2023	Information environment; perceptions; attitudes; behaviours; target audiences	Information operations, targeted shaping of perceptions and behaviours	The cognitive dimension is practically treated as a key component of the information environment.
AJP-10.3 Allied Joint Doctrine for Military Public Affairs (UK Ministry of Defence, 2024)	2024	Public perception; credibility; trust; target audiences	Military public affairs, informing the public and the media in order to preserve the trust and legitimacy of defence and allied activities	The cognitive dimension is implicitly present through an emphasis on perception, trust, and legitimacy, but not as a formally designated domain.

Note. Table created by the authors based on an analysis of NATO literature.

Table 2 shows that NATO consistently recognises the cognitive dimension as an important space of effects and competition, but does not codify it as a separate operational domain on par with the classical physical and cyber domains. In the NATO Warfighting Capstone Concept (NATO ACT, 2021), cognitive is primarily articulated through the notion of “cognitive superiority” and linked to understanding and shaping the operational environment in the context of multi-domain warfare, underscoring its role as an integrative dimension rather than an independent battlefield. Such positioning of the cognitive in the NWCC confirms that it is a dimension that permeates multi-domain operations, rather than an autonomous space of warfare.

The concept of cognitive warfare developed by NATO ACT through the Innovation Hub (Claverie & du Cluzel, 2022; Claverie et al., 2022; Cluzel, 2020; Bernal et al., 2023) goes a step further by addressing the cognitive domain and cognitive attacks, yet it remains an innovative, experimental concept subordinate to top-level strategic documents and outside the formal doctrinal hierarchy. However, these concepts are developed outside the formal doctrinal hierarchy and therefore do not have a binding character for Allied armed forces. The 2022 NATO Strategic Concept does not explicitly name the cognitive dimension but instead

elaborates on it through an emphasis on resilience, the information sphere, and hybrid threats, thereby implicitly recognising the cognitive space as a key area of contemporary competition without introducing a separate “cognitive domain.” Allied doctrinal documents, including AJP 01, AJP 3.10, AJP 10, AJP 10.1, and AJP 10.3 (NATO, 2022b; NATO, 2015; NATO, 2023a; NATO, 2023b; UK Ministry of Defence, 2024) explicitly place the cognitive within the “cognitive dimension,” alongside the physical and the virtual/information dimension, and link it to the perceptions, beliefs, and behaviour of target audiences, while operational domains remain limited to land, sea, air, space, and cyberspace. Overall, the table indicates that, within NATO’s framework, the cognitive dimension is primarily understood as an analytical and conceptual tool for understanding and directing activities in other domains. Rather than becoming a formally defined domain of warfare, it appears in doctrine and concepts as an overarching framework encompassing the psychological, social, and communicative aspects of contemporary conflicts. It serves to articulate targeted effects on the attitudes, will, and behaviour of adversaries, allies, and the broader public. Alongside the strengthening of material and technical defence capabilities, NATO is gradually developing complex mechanisms of action in the cognitive domain. Particular attention is devoted to countering disinformation, enhancing member states’ resilience to information threats, and deliberately shaping narratives to ensure the legitimacy and effectiveness of Allied activities. Within this approach, the importance of cooperation with civilian institutions, the education system, and the private technology sector is emphasised, while joint exercises and operational activities increasingly integrate cognitive methods systematically across all levels and dimensions of military activity (Masakowski & Blatny, 2023, p. 25).

Although NATO has been intensively developing the concept of “cognitive warfare” for several years through ACT initiatives, the Innovation Hub, and the work of the NATO Science & Technology Organization - including the technical report *Mitigating and Responding to Cognitive Warfare* (Masakowski & Blatny, 2023) - a comprehensive overarching concept of cognitive warfare has not yet been formalized as an official doctrinal document comparable to the NATO Warfighting Capstone Concept or the Allied doctrines of the AJP series.

4. CONCEPTUAL, ETHICAL, AND LEGAL CHALLENGES

The development of the cognitive domain as a new dimension of contemporary conflict raises a range of conceptual ambiguities and profound ethical and legal questions that extend beyond traditional frameworks in security and military studies. These challenges do not relate solely to operational effectiveness, but also encompass fundamental issues of legitimacy, responsibility, and the limits of permissible action in contemporary security practices. Gerasimov’s depiction of modern warfare, in which “*methods of warfare (...) include extensive use of political, economic, informational, humanitarian, and other non-military measures,*” with the local population actively encouraged as “*a significant element of power,*” clearly points to a shift of the centre of gravity of conflict from the physical to the cognitive and social space (Gerasimov, 2013, p. 5). Although Gerasimov’s text is not a doctrinal document in the

Western sense, his analysis reflects broader trends in which the boundary between military and non-military action is increasingly shifting towards the cognitive and social sphere. In this context, information and psychological operations, hybrid warfare, and the cognitive domain constitute interconnected, yet analytically distinct concepts. The following table illustrates their interrelationships and positions the cognitive domain as an overarching framework within which these instruments and strategies operate.

Table 3

Relationship Between the Cognitive Domain and Related Concepts

Concept	Primary Objective	Level of Action	Relationship to the Cognitive Domain
Information operations	Influence on information, information environment, and perception	Operational/strategic	Instrumental component of activity within the cognitive domain
Psychological operations	Influence on attitudes and behaviour of target audiences	Tactical/operational	Operational tool within the cognitive domain
Hybrid warfare	Combined political, military, and informational pressure	Strategic	Broader framework that includes the cognitive dimension
Cognitive domain	Shaping processes of perception and decision-making	Strategic and societal	Meta-concept encompassing these instruments and frameworks

Note. Table created by the authors based on an analysis of NATO literature.

Table 3 analyses the relationship between the cognitive domain and related, often intertwined concepts of contemporary warfare, and clearly demonstrates the hierarchical and functional differences among them. In doing so, it eliminates the frequent terminological confusion in which the cognitive domain is erroneously equated with information or psychological operations, or reduced to a set of individual tools with predefined objectives and partially measurable effects. In the table, information operations are presented as a concept whose primary objective is to influence information and perception, and that operates predominantly at the operational level. The importance of information as a means of shaping perception is emphasised by Miroslav Tuđman, who notes that “information has become a weapon that directly affects collective consciousness, and the media have become an invisible battlefield” (Tuđman, 2009, p. 26). Such an understanding confirms the role of information operations as an instrument for shaping how reality is perceived and interpreted, but it does not encompass

the broader context of decision-making processes. For this reason, it is analytically more appropriate to treat the cognitive not as an ontologically separate operational domain comparable to land, maritime, air, space, or cyber domains, but rather as a cross-cutting dimension that permeates and integrates activities across existing domains.

Their relationship to the cognitive domain can therefore be defined as instrumental, since information operations are one means of action within the cognitive space, but they do not, in themselves, encompass the entirety of meaning-making and decision-making processes, nor the ability to measure the effects of such actions on the target population. Psychological operations are further narrowed to directly influence the attitudes and behaviour of target audiences, most often at the tactical or operational level. In this sense, they appear as a concrete, clearly directed, and time-limited operational tool whose purpose is to elicit a specific response, which is why they address only one segment of the cognitive domain and cannot be equated with it.

Hybrid warfare is positioned in the table as a broader strategic framework within which political, military, informational, and other forms of pressure are combined. Its strategic level of action points to a long-term and coordinated use of various instruments of power, among which the cognitive dimension plays a significant, but not exclusive, role; therefore, the cognitive domain cannot be considered synonymous with hybrid warfare, but rather as one of its key, yet not self-sufficient, elements. The cognitive domain, as presented in the table, occupies the highest, meta-conceptual level. Its primary objective is to shape decision-making processes, and its scope of action extends to both strategic and societal spheres.

Unlike other concepts, it does not denote a specific set of operations or instruments but rather an analytical framework that encompasses how meanings, perceptions, and decisions are formed in contemporary conflicts. The cognitive domain is therefore more appropriately understood as an overarching concept that integrates and contextualises informational, psychological, and hybrid approaches, rather than as yet another operational category. Such an understanding allows for more precise theoretical differentiation of concepts and helps avoid their simplified or normatively problematic use in strategic and doctrinal debates.

Although Table 3 shows that the cognitive domain can be analytically distinguished from information and psychological operations, as well as from hybrid warfare, this conceptual positioning raises a range of additional questions and dilemmas. These are precisely the issues addressed by the key challenges of the cognitive domain, presented in Table 4, which encompass conceptual, ethical, legal, and societal levels of its understanding and potential operationalisation.

Table 4*Key Challenges of the Cognitive Domain*

Type of Challenge	Description	Potential Implications
Conceptual	Unclear definition and boundaries of the concept	Doctrinal confusion
Ethical	Influence on autonomy and free will	Erosion of trust
Legal	Limits of legitimate military action	Normative ambiguity
Societal	Militarisation of the social sciences	Long-term societal risks

Note. Table created by the authors based on an analysis of NATO literature

Table 4 summarises key challenges associated with the conceptualisation and application of the cognitive domain. Such an overview indicates that the cognitive domain cannot be viewed solely as an operational or strategic challenge, but rather as a phenomenon with far-reaching theoretical, normative, and societal implications. Challenges related to the cognitive domain thus go beyond a narrowly defined military-technical framework and affect the fundamental normative and social structures of contemporary societies, while the consequences and ultimate effects are often difficult to define in advance, monitor, and ultimately measure.

Conceptual challenges arise primarily from the cognitive domain's unclear definition and indeterminate boundaries. Since there is no generally accepted theoretical foundation, the term is used inconsistently across documents and analyses, leading to doctrinal confusion. Such inconsistency complicates its coherent incorporation into strategic planning and opens the door to arbitrary interpretations, particularly within military and security discourse.

Ethical challenges concern the influence on individual autonomy and free will. This dimension is particularly emphasised by Miller, who analyses cognitive warfare from an applied ethics perspective and notes that systematic efforts to shape modes of thinking and judgment can seriously undermine individual autonomy and the legitimacy of democratic decision-making (Miller, 2023). As Kulaš Mirosavljević et al. (2025) point out, referring to Vukasović (1993), ethical norms play a key role in the functioning of society because they guide behaviour, contribute to the preservation of social order, protect fundamental values, support the common good, enable the building of trust, and participate in shaping the identities of individuals and communities.

They are not immutable, but change under the influence of cultural, economic, social, and technological processes; consequently, new communication technologies often prompt the questioning of existing ethical frameworks and require their adaptation or redefinition (Kulaš Mirosavljević et al., 2025, p. 51). Actions directed at perception, attitudes, and decision-making processes inevitably engage fundamental ethical categories, as the boundary between legitimate influence and manipulation is often difficult to clearly delineate and, consequently, difficult, often impossible, to control and, if necessary, sanction. A potential implication of such actions is the erosion of trust, both within society and in the relationship between citizens and institutions, which, in the long term, may undermine social cohesion, democratic processes, and the security and freedom of individuals and specific targeted social groups.

This raises a fundamental democratic dilemma: where is the boundary between legitimate strategic communication and impermissible manipulation of cognitive autonomy? Without clear normative safeguards, activities conducted in the cognitive dimension risk undermining precisely those democratic values they are intended to protect. Legal challenges concern the limits of legitimate military action. The cognitive domain problematizes existing normative frameworks, as traditional warfare and international law are based on physical spaces and clearly defined actors. When military activity expands into the psychosocial space, normative ambiguity arises regarding permissible means, targets, and levels of action, particularly in relation to civilian populations and peacetime conditions. Societal challenges include the risk of the gradual militarisation of the social sciences and humanities. The inclusion of psychology, communication studies, and sociology within military concepts may lead to the instrumentalisation of scientific knowledge for security purposes, thereby opening the door to long-term societal risks, including the loss of scientific autonomy and changes in its social role. This further underscores the need for a cautious, interdisciplinary, and critical approach to developing this concept, especially in the context of its potential institutionalisation within defence systems, where uncritical application could produce long-term negative normative and societal consequences.

5. IMPLICATIONS OF THE COGNITIVE DOMAIN FOR THE DEFENCE SYSTEM OF THE REPUBLIC OF CROATIA

The cognitive domain is directly linked to societal resilience against disinformation, manipulation, and polarising narratives, particularly in the context of contemporary hybrid threats. As emphasised by the NATO Innovation Hub, “understanding the brain is one of the key challenges of the future” (Cluzel, 2020, p. 12). In this regard, the Croatian defence system cannot operate in isolation, but only as part of a broader national security system in which the media, the education system, and civil society institutions play a significant role.

The Defence Strategy of the Republic of Croatia, as a fundamental national strategic planning document, aligns with NATO and European Union security guidelines and recognises the complexity and multidimensionality of contemporary security challenges, including hybrid

threats that manifest in non-material spheres of security. This points to the need for institutional resilience and the integration of diverse capabilities to address them (Hrvatski Sabor, 2025). For small, highly interconnected states such as the Republic of Croatia, whose information environment is strongly influenced by external actors and transnational media flows, the cognitive dimension is a particularly sensitive area of vulnerability. The asymmetry of informational power and the speed of digital dissemination may amplify societal divisions and increase exposure to externally driven influence operations. Strengthening strategic communications, cooperating with national institutions responsible for cyber and information security, and participating in international initiatives to enhance societal resilience to cognitive threats are necessary elements of the national response. In this regard, recent security analyses emphasise that effective countermeasures cannot rely solely on technological or institutional instruments, but must also include the systematic development of digital literacy, inclusive social policies, and structured forms of intergroup dialogue as mechanisms for strengthening societal resilience to cognitive manipulation (Marjanović & Smiljanić, 2025)

The cognitive dimension of contemporary conflicts concerns not only specialised units or information-psychological capabilities but also affects the way armed forces conceptualise the operational environment, communicate with the public, and cooperate with civilian institutions. In this sense, the cognitive dimension becomes an issue of (military) organisational culture, educational programs, and doctrinal socialisation within the armed forces, rather than exclusively a matter of specialised capabilities or individual branches. In itself, this points to an evident need to systematically develop cognitive skills and resilience among members of the Armed Forces of the Republic of Croatia. As emphasised by The Geneva Centre for Security Policy (GCSP), effective defence of cognitive security rests on a comprehensive approach that links the development of societal awareness and resilience, systematic education for critical and information-literate thinking, responsible and transparent technological solutions, and clear political and regulatory frameworks for the protection of individual mental autonomy (GCSP, 2025).

This does not imply only classical psychological preparation, but also the development of critical thinking skills, the ability to recognise disinformation, an understanding of the information environment, and awareness of one's own cognitive biases and vulnerabilities. Furthermore, the implications of the cognitive domain point to the need for clear ethical and legal frameworks of action. Croatia, as a member of NATO and the European Union, is already bound to respect international humanitarian law and human rights standards, but the specifics of cognitive activities, aimed at the perceptions and decisions of individuals and groups, require further elaboration. It is necessary to consider how doctrinal concepts of cognitive action can be aligned with the domestic constitutional order, the protection of privacy, freedom of expression, and individual integrity, to avoid the normatively problematic militarisation of cognitive and social processes. Accordingly, the cognitive domain offers opportunities and responsibilities for enhancing cooperation among the military system, the academic community, and civil society.

Since key insights into perception, decision-making, communication, and social processes derive from psychology, sociology, communication studies, law, and other humanities and social science disciplines, the defence system of the Republic of Croatia can benefit from partnerships with universities, research institutes, and relevant non-governmental organisations, with a clear distinction between scientific research and operational application. Such cooperation should be grounded in clear ethical standards and transparency to reduce the risk of the instrumentalisation of science and to preserve the societal legitimacy of defence policies. Finally, reflection on the cognitive domain also encourages a systematic reassessment of Croatian strategic documents. The inclusion of the cognitive dimension in strategic concepts, doctrinal manuals, and training plans does not necessarily imply the adoption of the rhetoric of a “sixth domain of warfare,” but rather an acknowledgement of the fact that key outcomes of security challenges are increasingly recognised and decided in the realm of perception, trust, and social cohesion. Integrating a cognitive perspective into national security and defence policies is, therefore, a necessary step in adapting to the contemporary security environment. *“In essence, the concept of cognitive warfare should enhance understanding of emerging cognitive threats within NATO, protect cognitive resilience by defining possible effects, and shape a comprehensive strategy for mitigating the consequences of adversarial cognitive warfare through measures such as education, cooperation, protection, and action in the cognitive domain”* (Deppe & Schaal, 2024, p. 4).

CONCLUSION

In contemporary debates, the cognitive domain of warfare is often presented as a “sixth domain” that complements the classical physical and the newer virtual spaces of action. An analysis of relevant literature and NATO documents, however, shows that its status is conceptually and normatively far more complex. Rather than a stably codified operational domain, it is a conceptual framework encompassing perception, interpretation, and decision-making as key processes in contemporary conflicts, and overlapping with informational, psychological, and hybrid forms of activity. Within NATO, the cognitive dimension is recognised as a decisive space of effects through concepts such as “cognitive superiority” and “cognitive dimension.” However, it remains primarily designated as a dimension and an objective of superiority, rather than as a formally defined domain of warfare whose desired effects can be fully clearly defined, monitored, and precisely measured. Documents such as the NATO Warfighting Capstone Concept, NATO Allied Command Transformation’s concepts of cognitive warfare, and Allied Joint Publications on information operations and strategic communications demonstrate that the cognitive domain is affirmed as an analytical tool for linking physical, cyber, and informational activities, rather than as an independent battlefield comparable to land, sea, or air, thereby confirming its integrative rather than operational-domain character.

Contemporary Alliance practice shows that the cognitive dimension is not developing as a separate battlefield, but rather as an integrative level of activity that permeates all domains of warfare and links military, informational, and societal instruments of power. At the same time, the conceptual ambition to encompass the human mind and social processes as a space for military action poses several serious challenges. Inconsistent definitions and boundaries of the concept lead to doctrinal confusion and the risk of overlap with existing categories, while ethical and legal dilemmas arise from questions about the limits of legitimate influence on the autonomy and decision-making freedom of individuals and communities. Societal risks related to the militarisation of the humanities and social sciences further reinforce the need for a critical approach in order to prevent the reduction of scholarly knowledge about human beings and society to mere instruments of security policy. In this context, the cognitive domain requires particular normative restraint, as any systematic action directed at perception and decision-making inevitably touches upon fundamental ethical and democratic values, while sanctioning of impermissible activities of influence and action is made difficult, or even impossible. For the defence system of the Republic of Croatia, the cognitive domain is therefore not primarily a technical or organisational issue, but rather an impetus for deeper reflection on the relationship between security, society, and science.

The development of cognitive skills and resilience among members of the Armed Forces, the strengthening of societal resilience to disinformation, the establishment of clear ethical and legal frameworks, and the building of partnerships with the academic community and civil society represent key directions for responsibly operationalising this concept. Ultimately, whether the cognitive domain is formally accepted as a separate operational domain or remains a conceptual framework, it is clear that it is an unavoidable dimension of contemporary warfare. The analysis in this paper indicates that codifying the cognitive domain as a separate operational domain of warfare is not justified; rather, it is more appropriate to view it as a dimension permeating all domains and integrating psychological, informational, and societal aspects of contemporary conflicts. This distinction is not merely terminological, but conceptual and normative: how the cognitive is framed directly shapes doctrinal development, strategic planning, and the ethical boundaries of contemporary military practice.

Conflicts of the 21st century are waged as much within information systems and physical space as within the minds of individuals and collectives. Recognising this fact and thoughtfully incorporating it into national security and defence policies is a fundamental prerequisite for adapting to the challenges of the future security environment. Future research should complement this conceptual analysis with empirical insights into how relevant institutions in the Republic of Croatia and within NATO perceive cognitive threats and how they operationalise cognitive resilience in their doctrinal and educational practices.

REFERENCES

- Akrap, G. (2009). Informacijske strategije i oblikovanje javnoga znanja. *National Security and the Future*, 10 (2), 77-151. <https://hrcak.srce.hr/80639>
- Bernal, A., Carter, C., Singh, I., Cao, K., & Madreperla, O. (2023). *Cognitive warfare*. NATO Innovation Hub. <https://innovationhub-act.org/wp-content/uploads/2023/12/Cognitive-Warfare.pdf>
- Claverie, B., & du Cluzel, F. (2022). Cognitive warfare: The advent of the concept of “cognitics” in the field of warfare. In B. Claverie, B. Prébot, N. Buchler, & F. du Cluzel (Eds.), *Cognitive warfare: The future of cognitive dominance*. NATO Science and Technology Organization. <https://hal.archives-ouvertes.fr/hal-03635889/document>
- Claverie, B., Prébot, B., Buchler, N., & Du Cluzel, F. (Eds.). (2022). *Cognitive Warfare Symposium – ENSC – March 2022 Publication (Symposium proceedings)*. NATO Innovation Hub & École Nationale Supérieure de Cognitique. <https://innovationhub-act.org/wp-content/uploads/2023/12/Cognitive-Warfare-Symposium-ENSC-March-2022-Publication.pdf>
- Cluzel, F. du (2020). *Cognitive Warfare*. NATO ACT Innovation Hub. https://innovationhub-act.org/wp-content/uploads/2023/12/20210122_CW-Final.pdf
- Deppe C., & Schaal G.S. (2024). Cognitive warfare: a conceptual analysis of the NATO ACT cognitive warfare exploratory concept, *Frontiers in Big Data*. <https://www.frontiersin.org/articles/10.3389/fdata.2024.1452129/full>
- GCSP. (2025). *Enhancing cognitive security and societal resilience to counter cognitive warfare* (Policy paper). Geneva Centre for Security Policy. <https://www.gcsp.ch/publications/enhancing-cognitive-security-and-societal-resilience-counter-cognitive-warfare>
- Gerasimov, V. (2013). The value of science is in the foresight: New challenges demand rethinking the forms and methods of carrying out combat operations. *Military Review*, 93(1), 23–29. https://www.armyupress.army.mil/portals/7/military-review/archives/english/militaryreview_20160228_art008.pdf
- Hrvatski Sabor (2025). Strategija obrane Republike Hrvatske [National Defence Strategy of the Republic of Croatia]. Narodne novine NN 104/2025. https://narodnenovine.nn.hr/clanci/sluzbeni/2025_07_104_1433.html
- Kulaš Miroslavljević, A., Matić, N. & Martić, B. (2025). Etičnost na društvenim mrežama. *Festung*, 1 (1), 48-55. <https://hrcak.srce.hr/334232>
- Masakowski, Y. R., & Blatny, J. M. (Eds.). (2023). *Mitigating and responding to cognitive warfare (STO-TR-HFM-ET-356)*. NATO Science & Technology Organization. <https://www.sto.nato.int/document/mitigating-and-responding-to-cognitive-warfare/>

- Marjanović, A., & Smiljanić, D. (2025). Cognitive warfare – The human mind as the new battlefield. *Proceedings of the Defence and Security Conference*, 1(1), 84–114.
- Miller, S. (2023). Cognitive warfare: An ethical analysis. *Ethics and Information Technology*, 25, Article 46. <https://doi.org/10.1007/s10676-023-09717-7>
- North Atlantic Treaty Organization Allied Command Transformation. (2021). *NATO Warfighting Capstone Concept*. Norfolk, VA: HQ SACT. <https://www.act.nato.int/our-work/nato-warfighting-capstone-concept/>
- North Atlantic Treaty Organization Allied Command Transformation. (2023). *Multi-Domain Operations*. <https://www.act.nato.int/activities/multi-domain-operations/>
- North Atlantic Treaty Organization. (2015). *Allied Joint Doctrine for Information Operations* (AJP-3.10). NATO Standardization Office. <https://info.publicintelligence.net/NATO-IO.pdf>
- North Atlantic Treaty Organization. (2019). *London Declaration*. North Atlantic Treaty Organization. <https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2019/12/04/london-declaration>
- North Atlantic Treaty Organization. (2020). *Allied Joint Doctrine for Cyberspace Operations* (AJP-3.20). NATO Standardization Office. https://assets.publishing.service.gov.uk/media/5f086ec4d3bf7f2bef137675/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf
- North Atlantic Treaty Organization. (2022a). *NATO 2022 Strategic Concept*. Madrid: North Atlantic Treaty Organization. <https://www.nato.int/en/about-us/official-texts-and-resources/strategic-concepts/nato-2022-strategic-concept>
- North Atlantic Treaty Organization. (2022b) *AJP-01, Allied Joint Doctrine*. NATO Standardization Office. [https://www.coemed.org/files/stanags/01_AJP/AJP-01_EDF_V1_E_\(1\)_2437.pdf](https://www.coemed.org/files/stanags/01_AJP/AJP-01_EDF_V1_E_(1)_2437.pdf)
- Tuđman, M. (2009). Informacijske operacije i mediji ili kako osigurati informacijsku superiornost. *National Security and the Future*, 10(3-4), 25-45. <https://hrcak.srce.hr/80565>
- UK Ministry of Defence. (2023a). *AJP-10, Allied joint doctrine for strategic communications* (Edition A, Version 1, UK Change 1). NATO Standardization Office. <https://www.gov.uk/government/publications/allied-joint-doctrine-for-strategic-communications-ajp-10>
- UK Ministry of Defence. (2023b). *Allied Joint Publication-10.1: Allied joint doctrine for information operations*. NATO Standardization Office. https://assets.publishing.service.gov.uk/media/650c03bf52e73c000d9425bb/AJP_10_1_Inf_Ops_UK_web.pdf

UK Ministry of Defence. (2024). *Allied Joint Publication-10.3. Allied Joint Doctrine for Military Public Affairs*. The United Kingdom Ministry of Defence.
https://assets.publishing.service.gov.uk/media/670900d830536cb92748303e/AJP_10_3_Military_Public_Affairs.pdf

Vukasović, A. (1993). *Etika – moral – osobnost*. Školska knjiga.

INSTITUTIONAL TRUST, MEDIA PRACTICES AND PERCEIVED RESILIENCE TO COGNITIVE MANIPULATION AMONG CROATIAN UNIVERSITY STUDENTS

Arijana Marjanović

Dr. Franjo Tuđman Defense and Security University

E-mail: arijana.marjanovic@sois-ft.hr

Abstract

In the context of contemporary security challenges, cognitive warfare is becoming an increasingly significant form of conflict, with the human mind as the new battlefield. The aim of this paper is to explore the social factors that shape societal resilience to cognitive manipulation and the possibilities for building “societal resilience” by strengthening trust and media literacy. The paper adopts a sociological perspective, viewing resilience as a social process rather than merely an individual ability to recognise disinformation. The theoretical section connects the concepts of social cohesion and institutional trust, emphasising their role in collective resistance to manipulation.

The empirical part of the study is based on a survey conducted among students at the Catholic University of Croatia (N = 64). A quota sampling method was used. The data were collected through an online survey, which relied on voluntary participation. The questionnaire examines levels of trust in institutions and the media, information habits, self-assessed resilience to manipulation, and perceived social support within the community. Descriptive analyses are expected to show levels of institutional trust, information-verification habits, and *self-assessed* resilience to cognitive manipulation. In addition, the research explores how participants perceive open communication and education within the community as key mechanisms for strengthening individual and collective “societal resilience.”

Keywords: cognitive warfare; societal resilience; institutional trust; media literacy; misinformation; students; Croatia

INTRODUCTION

In recent years, the information environment has become increasingly complex, shaped by rapid technological development, the expansion of digital media, and the growing volume of available content. Individuals are exposed to a constant flow of information, much of which is difficult to verify and often presented in ways that influence perception, emotions, and decision-making. Within this context, the concept of cognitive manipulation, and more broadly cognitive warfare, has gained increasing attention in both academic and public discourse. Unlike traditional forms of influence, cognitive manipulation does not rely on physical force but rather on subtle strategies that shape how people think, interpret information, and form beliefs. These processes are often difficult to detect, as they operate through everyday media consumption and social interaction. As a result, the ability of individuals and communities to recognise and respond to such influences has become an important area of research.

One of the key concepts in this context is resilience. Rather than being understood solely as an individual psychological trait, resilience is increasingly viewed as a multidimensional process that includes cognitive, social, and structural components. It involves not only the ability to critically evaluate information but also the capacity to engage with others, exchange perspectives, and maintain trust within a community. In this study, resilience is conceptualised as a multidimensional construct encompassing psychological (self-assessed), behavioural (verification-based), and social (community-based) components.

Students represent a particularly relevant group for studying these processes. On the one hand, they are highly exposed to digital media and diverse sources of information. On the other hand, they are expected to develop critical thinking skills and independent judgment. This combination makes them both potentially vulnerable to manipulation and capable of developing resistance to it. The subject of this research is resilience among students at the Catholic University of Croatia. Students represent a population particularly exposed to cognitive manipulation due to intensive media use and the ongoing development of critical evaluation skills. At the same time, they constitute a socially important group whose capacity to evaluate information contributes to broader societal stability.

At the same time, the broader societal context plays an important role. In Croatia, levels of institutional trust are relatively low, which may influence how individuals perceive information sources and evaluate their credibility. This creates a specific environment in which trust, scepticism, and information practices interact in complex ways.

This study aims to examine students' self-perceived resilience to cognitive manipulation within the context of institutional trust, media evaluation, and community cohesion. In addition, the study explores how these factors are related to patterns of information verification and the role of social interaction in shaping collective resilience. By combining theoretical insights with empirical data, this research seeks to contribute to a better understanding of how resilience to

cognitive manipulation is formed and sustained within a contemporary information environment. Rather than testing causal relationships, this study adopts an exploratory approach to identify patterns that can inform and refine a theoretical model of resilience to cognitive manipulation.

1. THEORETICAL FRAMEWORK

1.1. Cognitive Warfare

There is still no single, universal definition of cognitive warfare that adequately describes this concept. Marjanović and Smiljanić (2025, pp. 86–87) derived a definition of cognitive warfare based on the works of various scholars and experts in the field:

It describes cognitive warfare as the deliberate use of psychological, informational, and technological tactics to manipulate the cognitive processes of individuals, groups, and societies, such as perception, emotions, beliefs, and decision-making. Targeting the human mind seeks to weaken, influence, or destabilise the intended audience by undermining trust, cohesion, and autonomy, often without relying on physical force. (Marjanović & Smiljanić, 2025, pp. 86-87)

In this study, a conceptual distinction is made between cognitive warfare and cognitive manipulation. Cognitive warfare is understood as a broader strategic and doctrinal framework that encompasses organised, long-term efforts to influence the cognitive domain of target populations. In contrast, cognitive manipulation refers to specific practices, techniques, and communicative acts through which such influence is operationalised at the micro-level. In other words, cognitive warfare represents the strategic level, while cognitive manipulation represents the operational level of influence.

Such warfare encompasses various dimensions, including information, psychological, and hybrid warfare. However, cognitive warfare is a distinct category, as it is not waged solely through information nor does it influence only emotions; rather, it influences cognition and thinking as a whole. Many individuals are unaware that cognitive manipulation is being conducted against them, and this is precisely the objective of cognitive warfare. Rarely does an individual realise that their system of thinking is being shaped from the outside, which is why it is essential to build individual and societal resilience, as discussed in the following chapter. The aim of such warfare is “targeting the human mind seeks to weaken, influence, or destabilise the intended audience by undermining trust, cohesion, and autonomy, often without relying on physical force” (Marjanović & Smiljanić, 2025, p. 87).

Specific social groups are particularly targeted by the mechanisms of cognitive warfare, such as youth, older adults, politically polarised groups, marginalised communities, and others. One group identified as especially vulnerable to cognitive manipulation is young people and students. Their vulnerability lies in their high exposure to social networks and media and their

constant contact with an overwhelming amount of information. Due to their age, they do not yet possess sufficiently developed critical-thinking skills and tend to have a short attention span (Marjanović & Smiljanić, 2025, p. 90). Young people are known for consuming information through images and headlines, and only rarely actually reading entire articles, which often do not align with the headlines, which tend to be far more dramatic than the real situation. A group that belongs to the young population, is entering the higher education system, and is expected to demonstrate a higher level of critical thinking, is undoubtedly students. In this case, the students of the Catholic University of Croatia are the population examined in this study.

1.2. Societal Resilience

In the simplest terms, social resilience is a community's ability to adapt to crises while maintaining functionality. In this context, it is important to begin by defining the term of resilience. The concept has evolved over time: initially, it referred to the ability of natural systems to persist despite change; later, to how natural and social systems adapt to environmental changes; and eventually to how society can fundamentally transform and adapt to global challenges (Keck et al., 2013, p. 6). Resilience factors can be individual, social, and societal. Individual factors include psychological characteristics that help individuals cope with challenges (such as optimism and self-efficacy); social factors refer to resources in a person's immediate environment, provided by other people or the community (such as support from family and friends); societal factors include broader social conditions and resources provided by the state or community that affect people's well-being (such as community security and public resources) (Shafer et al., 2024, p. 2). Cutter et al. (2008) define social resilience as "the ability of a social system to respond to and recover from disasters," noting that it "encompasses those inherent conditions that allow the system to absorb impacts and cope with an event, as well as post-event adaptive processes that facilitate the ability of the social system to reorganise, change, and learn in response to a threat" (Keck et al., 2013, p. 9).

Resilience as an outcome can be defined as "the maintenance or fast recovery of mental health during or after stressor exposure. Within this framework, so-called resilience factors protect individuals from the potentially negative effects of stressors and increase the likelihood of resilient responses" (Shafer et al., 2024, pp. 1–2). In more recent approaches, social resilience also refers to social relations of power, politics, and participation, where resilience is not only about survival, but also about the ability to actively shape change under conditions of uncertainty (Keck et al., 2013, p. 8). Social support is essential for social resilience. According to Schafer et al. (2024, pp. 2–3), social support can be: perceived (it is important how support is experienced), received (support that is actually obtained), provided (offering support to others can increase one's own sense of resilience), and structural (referring to the size and quality of social networks and the number of people an individual has around them). Most findings indicate that perceived social support is associated with small but favourable effects on mental responses during social challenges and crises. However, some contexts limit this

effect, such as a pandemic, which restricts social contact and thereby reduces the benefits of social support (Shafer et al., 2024, pp. 14–15).

Keck et al. (2013) divide resilience into three categories: resilience as persistability, resilience as adaptability, and resilience as transformability. Resilience as persistability refers to the ability of a system to endure and maintain its core functions and relationships regardless of the changes occurring; resilience as adaptability refers to the ability of a system to absorb changes and reorganise while still preserving its fundamental function and identity; and resilience as transformability refers to the ability of a system to fundamentally change when existing systems become unsustainable (Keck et al., 2013, pp. 6–8).

Pelling and High (2005), Traerup (2012) and Keck et al. (2012) constitute a second group of studies that emphasise the substance of social relations and the key roles of trust, reciprocity, and mutual support (Keck et al., 2013, p. 11). It is emphasised that institutions play a key role in shaping social resilience, as they determine the mechanisms for accessing resources that enable society to cope with crises. This means that resilience does not depend solely on the physical availability of resources, but also on institutional and historically conditioned power relations (Keck et al., 2013, p. 12).

1.3. Trust in Institutions

Trust in institutions is one of the foundations of social stability. It refers to an individual's belief in the reliability of general societal actors, such as the government, police, or public organisations (van Zoonen et al., 2024, p. 2). On social media, such institutions play an important role in distributing information and shaping public knowledge, and, due to their authority and social power, the public often attributes credibility to them. According to the authors, this makes institutional trust fundamental for communication and information management in contemporary society. Paradoxically, excessive trust in social media institutions may increase the likelihood of sharing unverified information (van Zoonen et al., 2024, p. 2). Individuals who have “blind trust” in institutions and a high level of confidence in their own ability to recognise disinformation are simultaneously less motivated to verify sources. This leads to faster dissemination of unverified content and the creation of “echo chambers” (van Zoonen et al., 2024). At the same time, a lack of trust in institutions fosters feelings of frustration, dissatisfaction, and isolation.

In the context of Croatia, the situation with institutional trust is very specific. Namely, trust in institutions is extremely low, even the lowest in the EU. According to the 2024 Eurobarometer, only about 30% of citizens trust the government and parliament, while trust in the judiciary and political parties is only 26%. On the other hand, the military (74%) and the police (69%) are rated significantly higher than the general public (European Commission, 2024). However, almost all respondents (94%) believe that corruption in the country is widespread, which further contributes to a decline in citizens' trust and cooperation with state initiatives (European

Commission, 2022). Although it is encouraging that there is trust in the military and the police, these institutions are not crucial for implementing key laws and initiatives. They are also not key actors in disseminating information or providing statements to the media. The low level of trust in key and legislative institutions is a significant problem, especially for resilience.

Therefore, young students constitute the specific group examined in this research, precisely because they live in Croatia, where a strong atmosphere of distrust prevails. It is important to research how this environment affects them and whether they demonstrate resilience within their student community or are instead influenced by feelings of hopelessness and mistrust. It should also be researched whether this general distrust leads them to verify information more frequently.

1.4. Conceptual model

This study assumes that resilience to cognitive manipulation does not emerge from a single psychological trait but from a sequence of interconnected social-cognitive processes. Based on previous research on institutional trust, media literacy, and social resilience, a multi-level mechanism can be conceptualised linking macro-level perceptions to collective outcomes.

Institutional trust as the starting condition

Institutional trust shapes how individuals approach information environments. When trust in public institutions is high, individuals tend to rely on institutional authority as a cognitive shortcut when evaluating information. Conversely, low institutional trust reduces reliance on authority and encourages independent judgment but may simultaneously increase generalised suspicion toward the entire informational system. Therefore, institutional trust does not directly determine susceptibility to manipulation; rather, it influences the criteria individuals use to evaluate information credibility.

In contexts of moderate or low trust, individuals are more likely to shift from authority-based acceptance to source-comparison strategies. However, excessive distrust may lead to systemic scepticism, in which all sources are perceived as potentially manipulative.

Media evaluation as an interpretative filter

Institutional trust shapes media evaluation, meaning the perceived credibility of traditional media, social media platforms, and official communication channels. Individuals who rely strongly on institutional authority often treat established media outlets as inherently credible. In contrast, individuals with lower institutional trust apply more conditional credibility judgments and differentiate between sources, formats, and communicative intent.

Media evaluation functions as a cognitive filter: information is not accepted or rejected directly, but first categorised as trustworthy, suspicious, or manipulatively framed. This filtering process determines whether the individual engages in further cognitive effort. Thus, institutional trust

influences how critically media messages are interpreted, not whether information is consumed.

Verification behaviour as an active coping mechanism

Media evaluation then affects verification behaviour. When information is perceived as uncertain or potentially manipulative, individuals are more likely to engage in fact-checking, cross-referencing sources, or delaying judgment. Verification behaviour, therefore, represents the transition from passive exposure to active cognitive defence.

Importantly, verification behaviour depends not solely on knowledge but also on perceived necessity. People verify information primarily when they believe the information environment requires vigilance. A context of moderate distrust combined with perceived personal responsibility, therefore, produces the highest verification activity, whereas both blind trust and complete cynicism reduce verification motivation.

Verification behaviour represents the operational level of resilience, the point at which abstract attitudes become concrete actions.

Perceived individual resilience

Repeated verification practices contribute to perceived individual (psychological) resilience, defined as an individual's belief in their capacity to resist manipulation and make rational judgements under informational pressure. This perception emerges through behavioural experience rather than through abstract knowledge alone. However, perceived resilience may differ from actual resistance. Individuals who regularly evaluate and verify information develop confidence in their judgment abilities, even though cognitive biases may still operate. Therefore, perceived resilience functions as a psychological outcome of verification behaviour rather than as its prerequisite.

From individual to social (community) resilience

Finally, individual resilience contributes to social (community) resilience through social interaction. When individuals discuss information, warn others about inaccuracies, and tolerate disagreement, resilience becomes a collective property rather than a purely personal one.

Community resilience emerges when three conditions are present:

1. willingness to share and discuss information,
2. mutual trust among members,
3. shared norms of verification and responsibility.

In this model, resilience shifts from vertical dependence on institutional authority toward horizontal reinforcement through peer communication. The community becomes a distributed

verification network in which manipulation is countered through dialogue rather than solely through institutional correction.

Analytical implication

The proposed mechanism can therefore be summarised as a sequential relationship:

Institutional trust → media evaluation → verification behaviour → perceived individual resilience → community resilience

Institutional trust operates as a contextual condition, media evaluation as a cognitive filter, verification behaviour as a defensive practice, perceived resilience as a psychological outcome, and community resilience as a social outcome.

This framework allows the empirical analysis to move beyond measuring attitudes in isolation and instead to examine resilience as a process linking societal structure, cognition, and collective interaction.

1.5. Research hypotheses

Based on the proposed sequential model of resilience formation, this study assumes that resistance to cognitive manipulation emerges through a chain of cognitive and social processes rather than a single factor. Each stage of the mechanism can therefore be expressed as a testable empirical relationship.

H1 - Institutional trust and media evaluation

Institutional trust influences how individuals evaluate the credibility of information sources. Individuals with higher trust in institutions are more likely to evaluate traditional and official media as credible, whereas lower trust is associated with greater scepticism toward institutional communication channels.

H1: Institutional trust is expected to shape how individuals perceive the credibility of traditional and official media sources.

H2 - Media evaluation and verification behaviour

When individuals perceive media content as uncertain or potentially biased, they are more likely to engage in verification practices such as cross-checking and delaying judgment. Thus, lower perceived media credibility should increase active information checking.

H2: Lower perceived media credibility is expected to encourage more frequent information verification practices.

H3 - Verification behaviour and perceived individual resilience

Repeated engagement in verification practices strengthens confidence in one's ability to resist manipulation. Individuals who actively verify information should therefore report greater self-assessed cognitive and emotional resilience.

H3: Engagement in information verification is expected to contribute to higher levels of self-assessed individual resilience to manipulation.

H4 - Individual resilience and community resilience

Resilience becomes collective when individuals interact, discuss, and correct misinformation within their social environment. Individuals who perceive themselves as resistant are more likely to participate in communicative correction and cooperative sense-making.

H4: Higher levels of self-assessed individual resilience are expected to be reflected in stronger perceptions of community resilience and cohesion.

H5 - Integrated resilience mechanism

If resilience is a process rather than an isolated trait, then the combined pathway should be observable: institutional trust should indirectly shape community resilience through media evaluation, verification behaviour, and individual resilience.

H5: Institutional trust is expected to play a role in shaping community resilience through a sequence of processes involving media evaluation, verification behaviour, and individual resilience.

In addition to hypothesis testing, the study explores how students perceive credibility of information sources, their own emotional and cognitive resistance to misinformation, and the role of community cohesion in strengthening resilience.

2. METHODOLOGY

2.1 Research Design

The research was conducted using a quantitative, cross-sectional survey design with an exploratory focus. The study aimed to examine how institutional trust, media evaluation, and verification behaviour relate to students' perceived individual (psychological) resilience to cognitive manipulation. Given the nature of the topic, an exploratory approach was used to examine patterns between key variables rather than to establish causal effects.

2.2 Sample

The study was conducted with a convenience sample of students from the Catholic University of Croatia. A total of 64 respondents participated in the research. Data collection took place in January 2026.

The questionnaire was distributed via email through the university's student services and, additionally, shared via snowball sampling through WhatsApp groups. Participation was voluntary and anonymous, and respondents provided informed consent before completing the questionnaire.

2.3 Instrument

Data were collected using a self-developed questionnaire designed specifically for this research. The instrument was constructed based on insights from existing literature on cognitive manipulation, media literacy, and social resilience.

The questionnaire included several sections addressing institutional trust, perceptions of media credibility, information verification behaviour, and self-assessed emotional and cognitive resilience. In addition, a perception test was included to examine respondents' ability to recognise inaccurate or misleading information. The final part of the questionnaire consisted of an open-ended question that allowed respondents to express their views on how resilience to cognitive manipulation could be strengthened. Responses were measured using Likert-type scales ranging from "strongly disagree" to "strongly agree," as well as perception-based scales from "completely inaccurate" to "completely accurate."

2.4 Variables

The study focused on several key variables. Institutional trust refers to respondents' confidence in official sources and public institutions. Media evaluation captures perceptions of credibility of both traditional and social media. Verification behaviour refers to the extent to which respondents check and cross-reference information before accepting it as true.

Perceived individual resilience reflects respondents' self-assessed ability to recognise and resist manipulation, while community resilience refers to perceptions of trust, communication, and cohesion within their social environment. These variables were operationalised through grouped questionnaire items and analysed both individually and in relation to one another.

2.5 Data Analysis

The collected data were analysed using descriptive statistical methods, with a focus on identifying patterns in responses. Although correlational analysis (e.g., Pearson or Spearman correlation) was initially considered in line with the theoretical model, it was not conducted due to the relatively small sample size, which limits the reliability of such statistical procedures. All data were processed using Microsoft Excel. Given the exploratory nature of the study, the results are interpreted as indicative patterns within the observed sample rather than statistically generalisable findings.

2.6 Ethical Considerations

The study was conducted in accordance with ethical standards in the social sciences. Participation was entirely voluntary, and respondents were informed about the purpose of the research before completing the questionnaire.

Informed consent was obtained from all participants prior to participation. The survey was anonymous, and no personal or identifying data were collected at any stage of the research process. All data were used exclusively for research purposes and handled to ensure respondents' confidentiality and privacy.

3. RESULTS

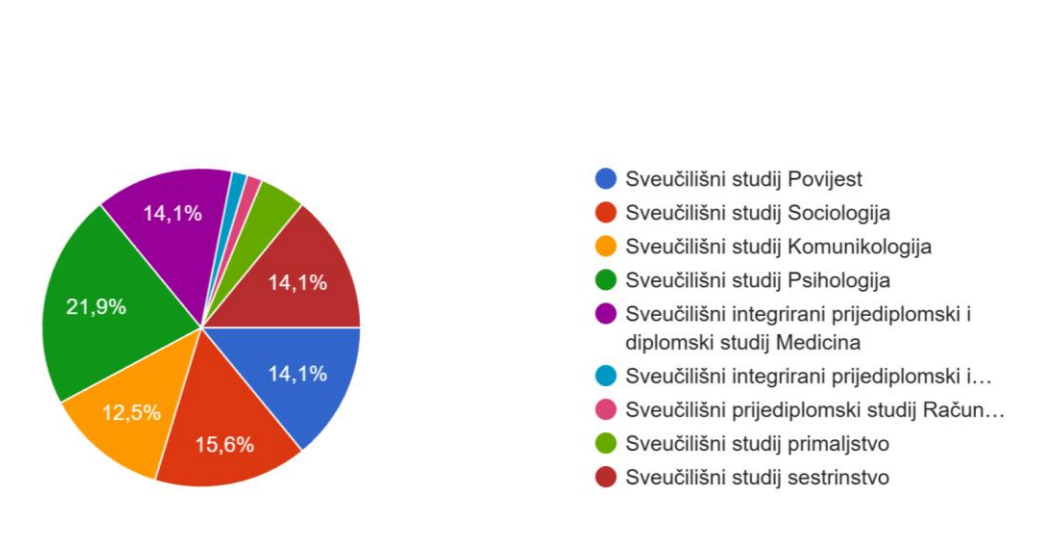
3.1 Sample Characteristics

The sample consisted of 81.3% female and 18.8% male participants. Regarding age, the majority of respondents were between 18 and 27 years old (78.2%), while 21.8% were between 30 and 59 years old, reflecting the study's inclusion of doctoral students.

In terms of field of study, participants were relatively evenly distributed across different study programmes. The largest proportion of respondents was enrolled in psychology (21.9%), while the smallest proportions were in newly established programmes with fewer enrolled students: law, midwifery, and computing for social applications (Figure 1). Other respondents were from the fields of history, sociology, communicology, medicine and nursing programmes.

Figure 1

Field of study



A similar distribution was observed for years of study, with participants relatively evenly represented across academic years, and no single year stood out significantly in proportion. A

slightly higher percentage of respondents were in the fifth year of study (23.4%), while the third year had the lowest representation (7.8%), with all other years falling between these values.

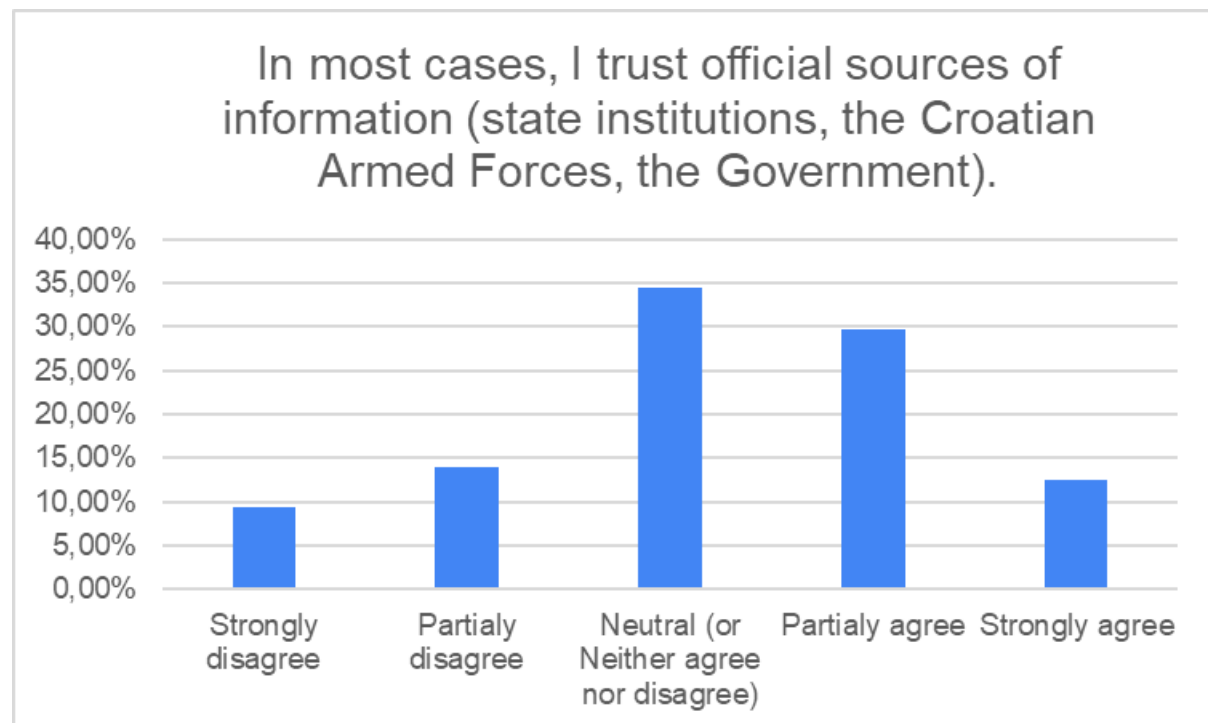
3.2 Institutional Trust and Media Practices

This section included eight variables measured on a five-point Likert scale ranging from 1 = strongly disagree to 5 = strongly agree. The first statement read: *“In most cases, I trust official sources of information (state institutions, public television, Government).”* The largest proportion of respondents (approximately 35%) selected the neutral option, indicating neither clear trust nor pronounced distrust (Figure 2). The distribution does not point to strong polarisation.

Nevertheless, moderate levels of trust outweigh distrust: approximately 42% of respondents agree, compared with 23% who disagree. This neutral-to-moderately positive pattern is broadly consistent with findings from the European Values Study (EVS) in Croatia, which show considerable variation in trust across institutions, with the government typically receiving lower levels of trust than the armed forces. Although EVS data are derived from a nationally representative sample, the overall pattern of moderate institutional trust observed in this student sample appears similar.

Figure 2

Trust in official sources of information

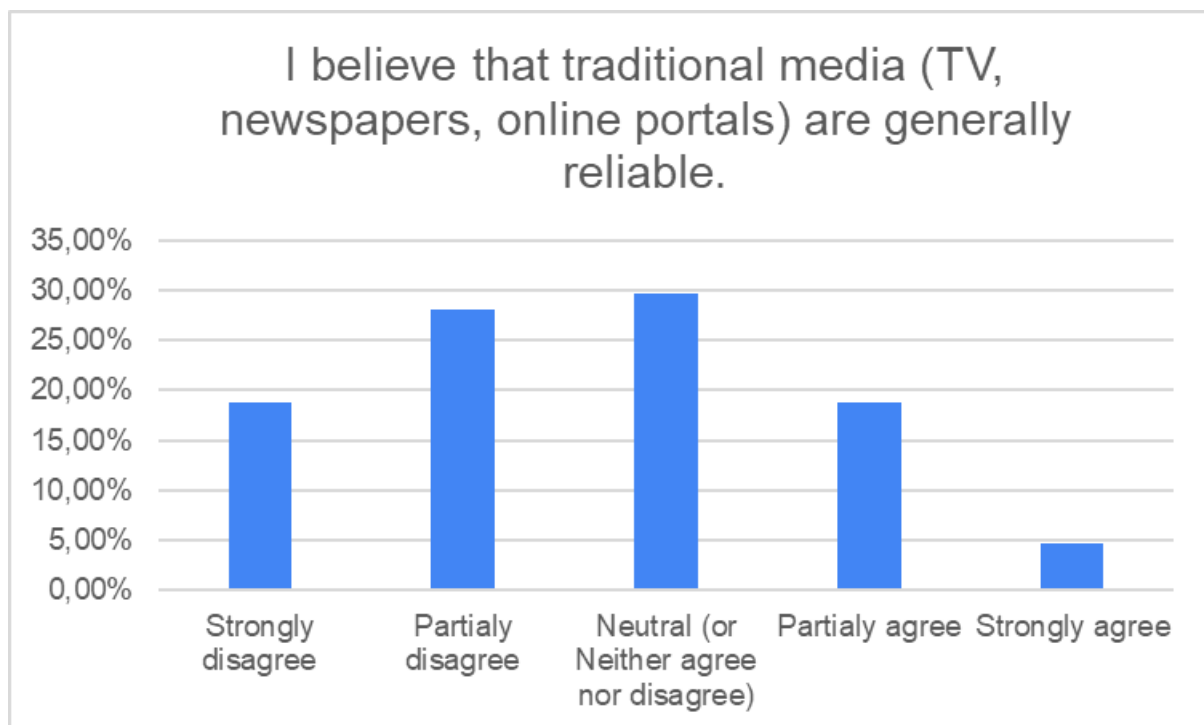


The second statement read: *“I believe that traditional media (television, newspapers, online news portals) are generally reliable.”*

Previous findings from the European Values Study (EVS) indicate relatively low levels of trust in the media, and the present results appear to reflect a similar pattern. Scepticism toward traditional media prevails in this sample, with approximately 47% of respondents disagreeing, compared with only 24% agreeing (Figure 3).

Figure 3

Trust in traditional media’s reliability



The third statement read: *“I treat news from social media with caution and attempt to verify it.”*

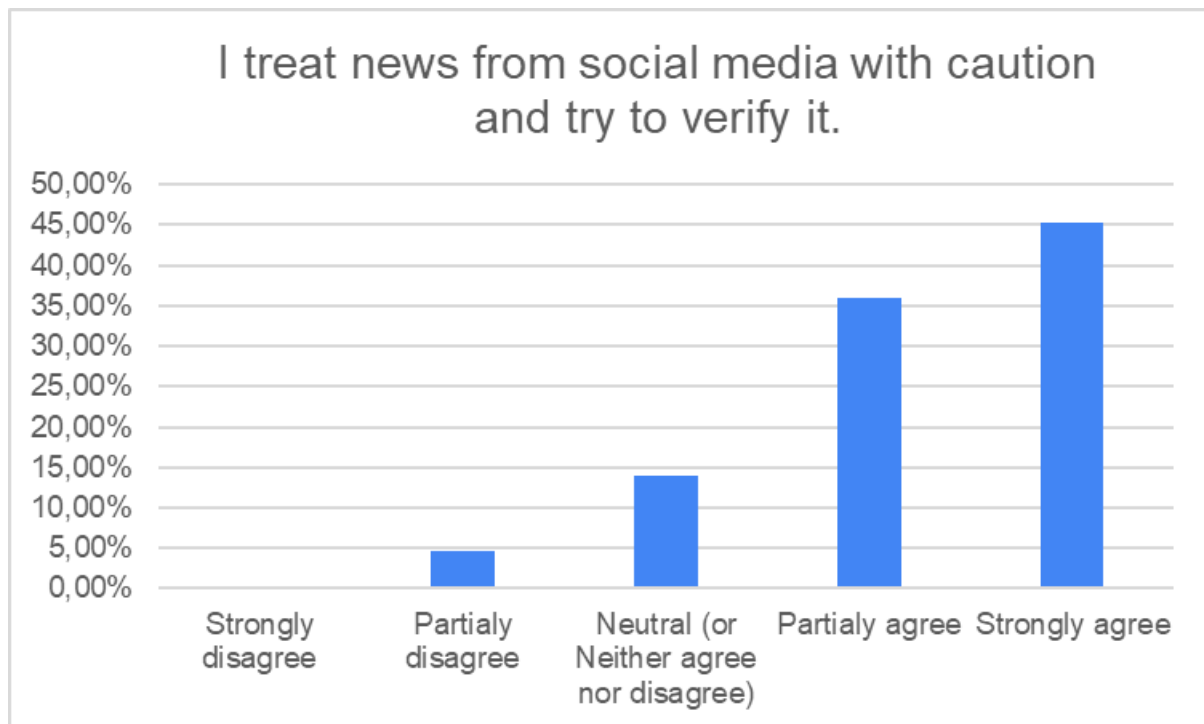
A majority of respondents (81%) reported treating information obtained through social media with caution and seeking to verify it. This finding may indicate relatively developed information-verification practices within the sample. Therefore, a high level of self-assessed resilience and reported information verification does not necessarily guarantee that individuals consistently verify information in practice; however, within the scope of this study, the primary focus is on how respondents perceive and evaluate their own resilience (Figure 4).

The combination of lower trust in traditional media and high levels of information verification suggests that respondents’ attitudes may reflect critical engagement with information sources

rather than generalised distrust. It is important to emphasise that these findings reflect respondents' opinions and self-perceptions.

Figure 4

Treating news from social media with caution



The fourth statement read: *"If a news item provokes a strong emotional reaction, I usually pause and verify the facts."*

The distribution of responses follows a pattern similar to that observed in the previous variable, with a clear majority indicating agreement. This finding suggests that respondents tend to adopt a reflective approach when confronted with emotionally charged content, pausing to verify information rather than reacting impulsively. Such a pattern may indicate a relatively high level of critical information processing within the sample.

The fifth statement read: *"In my community (class, unit, group), people openly discuss different opinions."*

More than half of the respondents (57%) agreed with this statement, while about 15% disagreed. These results suggest that the majority perceive their immediate social environment as communicatively open and pluralistic. Respondents appear to experience their communities as spaces where differing viewpoints can be expressed and discussed.

The sixth statement read: *"When I notice inaccurate news, I try to warn others."*

A similar response trend was observed for this variable, with a majority indicating agreement. This suggests that respondents are inclined not only to evaluate information individually but also to engage in corrective communication by informing others of inaccuracies.

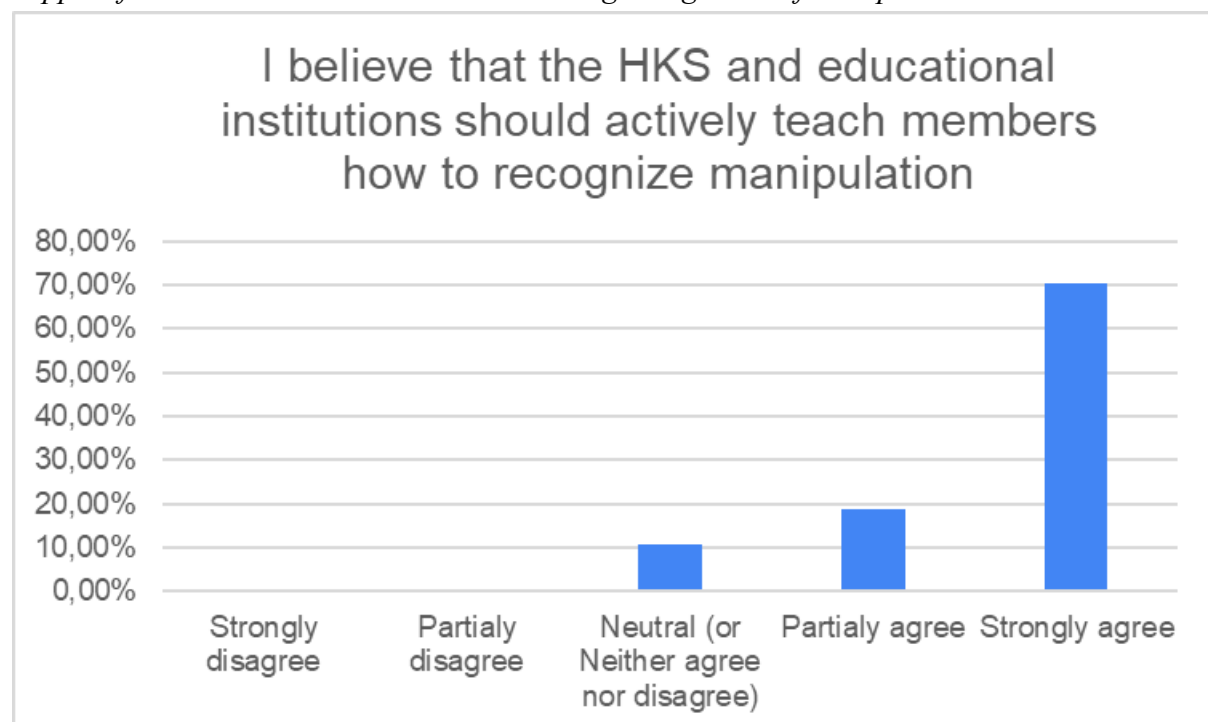
The seventh statement read: *“I know people with whom I can discuss news from different sources, even when we disagree.”*

A notably high level of communicative connectedness was observed, with 79% of respondents indicating that they have individuals with whom they can discuss news even in situations of disagreement. Also, some research argues that the general public tends to hold more centrist views, while political actors and media outlets often emphasise divisions and ideological differences (Marjanović & Smiljanić, 2025, p. 94, drawing on Duffy et al., 2019). From this perspective, online articles and headlines may amplify the perception of polarisation beyond what is experienced in everyday interpersonal interactions. The present findings, indicating a high willingness to engage in cross-opinion discussions, appear consistent with this interpretation.

The final statement in this category read: *“I believe that the Catholic University of Croatia and other educational institutions should actively teach members how to recognize manipulation.”*

Figure 5

Support for educational institutions in teaching recognition of manipulation



A strong majority of respondents (89%) agreed with this statement, with no participants disagreeing. This finding reflects a strong normative consensus regarding the importance of institutional involvement in fostering cognitive resilience. Furthermore, respondents appear to

conceptualise resilience not solely as an individual responsibility but as a collective, structurally supported process requiring organised educational intervention (Figure 5).

Overall, the empirical findings suggest that resilience in this student sample is not grounded in unconditional trust but rather in a combination of moderate institutional trust, critical media engagement, strong interpersonal discussion networks, and support for institutional educational interventions.

3.3 Perception Test and Cognitive Evaluation

The next category refers to information assessment, or a perception test. It examines attitudes toward statements whose truthfulness is often the subject of public debate. The first statement was: *“5G technology has been proven to cause the spread of the COVID-19 virus.”*

According to the results, 87.5% of respondents disagree with this claim, no respondents agree, and the remaining participants are neutral. The findings indicate that a large majority of respondents recognise this statement as false (misinformation). This pattern suggests a relatively high level of resilience among respondents to this particular piece of disinformation. The second statement was: *“Politicians control most of the information we receive through the media.”*

A total of 48% of respondents agree with this statement, 33% are neutral, and 18% disagree. Unlike the previous claim about 5G technology, there is no clear consensus here. Although the largest single group is neutral, overall, nearly half of the respondents (around 48%) partially or fully agree that politicians control most media information. This indicates a certain level of distrust toward media and political structures, as well as a perception of political influence over the information space. Such findings may serve as an important indicator of broader media and institutional scepticism among respondents.

The third statement was: *“Airplane trails (‘chemtrails’) are used to control the population.”*

The majority of respondents reject this theory, considering it a conspiracy theory. However, 10.9% agree that this claim is true, indicating that a small but notable proportion of respondents are receptive to this type of misinformation.

The fourth statement was: *“Social media platforms deliberately hide certain information in order to influence public opinion.”*

A total of 73% of respondents agree with this statement, indicating a strong belief that social media actively and intentionally manages information to shape public opinion. There is a strong perception of manipulation within digital platforms, and these findings point to significant distrust toward algorithms and social media platforms.

The fifth statement reads: *“Historical facts are often deliberately shaped by powerful groups in order to direct public understanding.”*

Overall, 65% of respondents partially or fully agree with this claim. This indicates a strong belief that powerful groups actively shape historical narratives to influence public understanding.

The results reveal an interesting paradox: on the one hand, the majority of respondents clearly reject classic conspiracy theories such as 5G or “chemtrails,” indicating a certain level of resilience to these claims. On the other hand, there is a certain level of distrust toward social media and traditional media, precisely the actors that most frequently debunk such theories. Respondents consistently demonstrate a strong inclination toward broader narratives of manipulation by elites, the media, and digital platforms, suggesting a high level of systemic distrust rather than simple susceptibility to individual pieces of misinformation.

The next category examines the following statements:

- “If a news item comes from a well-known media outlet, it does not need to be additionally verified.”
- “If a news item has been shared many times on social media, it is probably true.
- “Photographs or videos on the internet always represent real events as they actually happened.”
- “If the person sharing the news is a soldier or an official, there is no need to verify the accuracy of the information.
- “In Croatia, all information transmitted through official channels is always credible
- “Most disinformation is designed to provoke emotional reactions in the audience.”
- “Only educated people can recognise manipulation in the media.”

The results in this category indicate a relatively high level of critical thinking among respondents, but also a pronounced degree of systemic distrust. A significant majority reject the claim that news does not need further verification if it comes from a well-known media outlet, goes viral on social media, or is shared by an official figure. This suggests a developed awareness of the need to verify information regardless of source, authority, or popularity. Respondents also strongly reject the idea that photographs and videos always faithfully represent real events, demonstrating an understanding of how visual content can be manipulated. At the same time, there is clear distrust toward official channels and institutions. Taken together with previous findings, this suggests that respondents are not inclined to accept information uncritically, yet they exhibit a high level of general, systemic scepticism toward the informational and institutional systems. In other words, respondents perceive themselves

as resistant to individual pieces of misinformation and to formal authority, while simultaneously expressing substantial systemic distrust toward institutions and media. This represents a complex but highly important finding for understanding how they perceive information.

In addition, a significant majority (75%) agree that most disinformation is designed to provoke emotional reactions in the audience. The final statement in this category reads: “*Only educated people can recognize manipulation in the media.*” The results show that around 26% of respondents completely disagree, and an additional 33% partially disagree, meaning that nearly 60% reject the idea that recognising manipulation is reserved exclusively for educated individuals. About 26% are neutral, while approximately 14% partially or fully agree with the statement. These findings indicate that most respondents believe the ability to recognise media manipulation is not solely linked to formal education but also depends on other factors, such as experience, awareness, and critical thinking. At the same time, the presence of a smaller group who agree suggests a perception that education still plays an important, though not exclusive, role in developing media literacy.

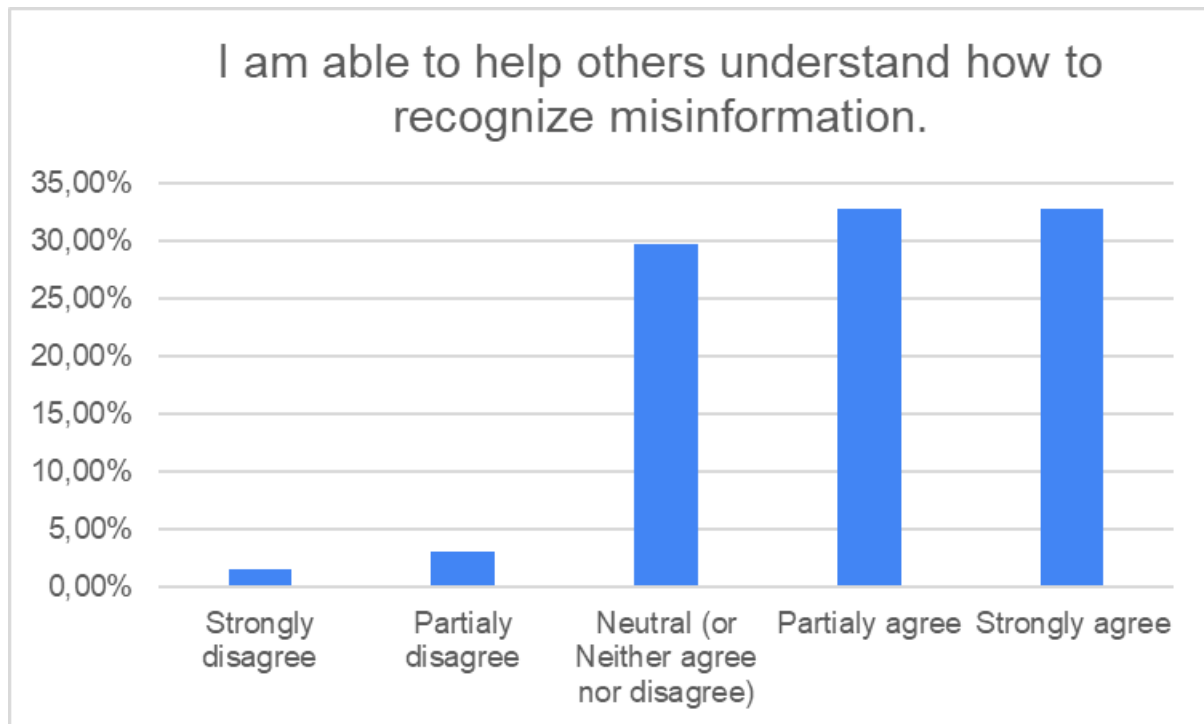
The next category focuses on the self-assessment of emotional and cognitive resilience. The results in this group indicate a relatively high level of self-perceived emotional regulation and awareness of one’s own cognitive processes. A large majority of respondents (84%) state that they try to remain calm and rational when hearing disturbing news. As many as 90.6% are aware that emotions can influence their assessment of the truthfulness of information. Furthermore, 67.1% believe they can recognise when someone is attempting to manipulate the audience emotionally. However, a higher proportion of neutral responses in this item may suggest some uncertainty in their self-evaluation. In addition, 73.4% of respondents report verifying facts before forming an opinion during discussions with others, and 85.9% believe that open discussion of diverse viewpoints contributes to community resilience. Overall, these findings suggest that respondents perceive themselves as rational, self-aware, and responsible participants in the information environment, placing strong value on dialogue and critical thinking.

3.4 Self-assessed Resilience

The majority of respondents (65.6%) believe they can help others recognise disinformation, indicating confidence in their own knowledge. Nearly 30% are undecided, while the remaining respondents disagree, meaning they do not feel sufficiently confident in their ability to identify disinformation (Figure 6).

Figure 6

Ability to help others understand how to recognise misinformation



Almost half of respondents (48.4%) are willing to respond publicly when they encounter inaccurate or manipulative information, while 34.4% are unsure whether they would. The remaining 17.2% would not be willing to react publicly. Furthermore, 87.5% believe that verifying information sources is one of the main ways to avoid manipulation; however, it remains unclear how many individuals consistently do so in practice. Once again, 65.6% of respondents consider themselves able to easily recognise disinformation. As discussed in the theoretical framework, individuals who exhibit high confidence in their own ability to recognise disinformation are often less motivated to verify sources, which can contribute to the rapid spread of unverified content and the formation of echo chambers (van Zoonen et al., 2024).

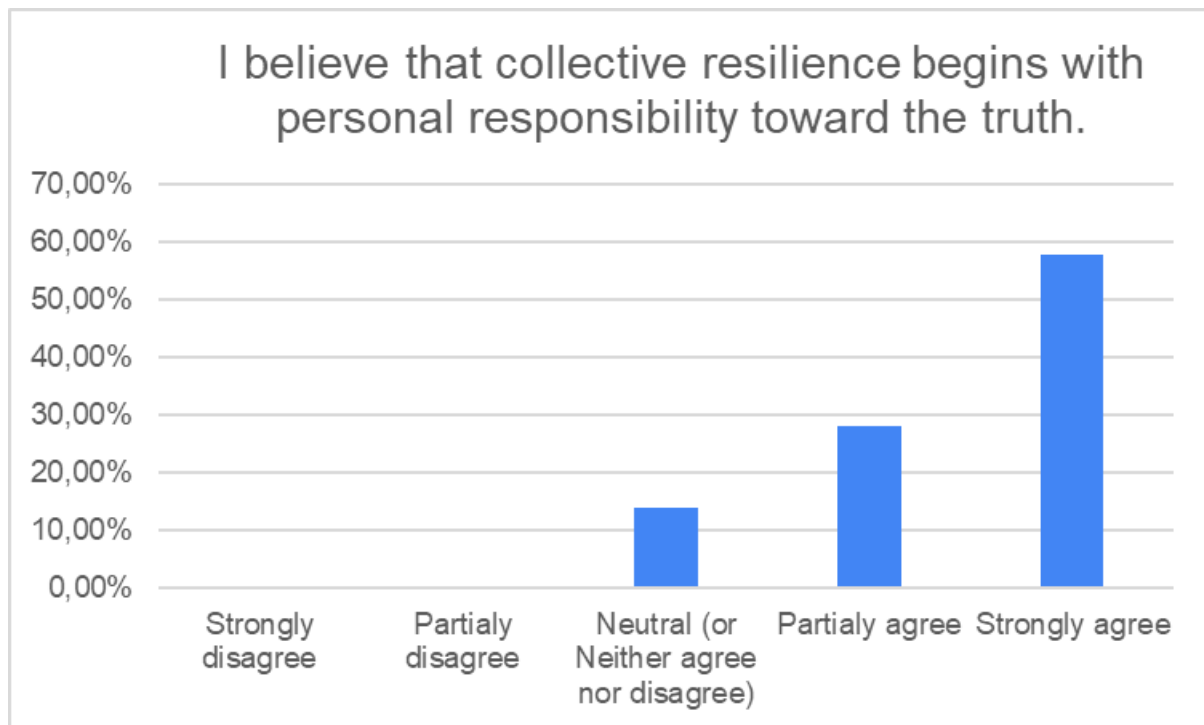
As many as 85.94% of respondents believe that collective resilience begins with personal responsibility for the truth, while none disagreed with this statement (0% disagree). A total of 57.81% strongly agree, 28.13% partially agree, and 14.06% remain neutral. (Figure 7). Additionally, 81.2% believe that trust among community members helps them recognise manipulation together. In other words, respondents see both personal responsibility and collective cohesion as essential components of resilience.

Accordingly, 67% believe their community is willing to help others in times of crisis, while 11% disagree. Nearly 59.4% of respondents believe that communities with higher levels of mutual trust are more resistant to manipulation, and as many as 84.4% agree that dialogue

between educational institutions and civil society is important for information security. In conclusion, 92.1% of respondents agree that a collective sense of responsibility reduces the spread of fake news.

Figure 7

Perception of personal responsibility as the basis of collective resilience



Open-ended question: In your opinion, what would most increase community resilience to cognitive manipulation and information threats?

In this research, community resilience refers to the ability of members of a group or organisation to collectively recognise, prevent, and mitigate the impact of manipulative information while maintaining mutual trust and social cohesion.

The majority of responses emphasise the need for education and continuous learning; media, digital, and algorithmic literacy; the development of critical thinking skills; the introduction of workshops and structured programs within the education system; and education for all age groups. This indicates that respondents view education as the primary mechanism for long-term resilience.

Another very prominent group of responses highlights personal responsibility for truth, source verification, caution with emotionally charged information, reflection before sharing content, and morality, values, and commitment to truth. Here, resilience is perceived as both an ethical

and cognitive issue, rather than merely a technical one. Concepts such as values, morality, and cohesion are mentioned frequently.

Furthermore, many responses emphasise the importance of dialogue, open discussion, mutual trust, freedom of expression, and healthy community cohesion. This aligns with the quantitative findings from the earlier section of the questionnaire, which identified cognitive responsibility and trust as important factors in resilience.

A segment of responses expresses scepticism toward official fact-checkers, fear of political or ideological bias, distrust of state structures, and doubt that “official truth” necessarily represents the actual truth. This pattern is also confirmed in the closed-ended questions, where respondents reject classic conspiracy theories (such as 5G and chemtrails), yet simultaneously demonstrate a high level of systemic distrust. From their perspective, the solution cannot be exclusively institutional; it must also include transparency and public accountability.

A smaller portion of respondents mentions stricter laws, media control, sanctions for spreading false information, and public labelling of disinformation. Finally, several responses address reducing time spent on social media and other online environments, personal withdrawal, strengthening faith and virtues, enhancing economic and military power, and the need for charismatic leadership. Although these responses are less frequent, they indicate that some participants perceive resilience within a broader cultural, security, or spiritual framework.

3.5 Community Cohesion

Most respondents perceive their community as open in communication. 57% report that different opinions are openly discussed within their group, while 79% indicate that they have people with whom they can discuss news, even when they disagree.

Respondents also actively react to inaccurate information, with the majority reporting that they warn others when they notice incorrect news. The collective dimension of resilience was rated highly. A total of 85.9% believe that collective resilience begins with personal responsibility toward truth, while 81.2% consider mutual trust essential for recognising manipulation.

Additionally, 67% of respondents believe that their community would help others in a crisis. A large majority (84.4%) emphasise the importance of dialogue between educational institutions and society, and 92.1% believe that collective responsibility reduces the spread of disinformation.

3.6 Open-ended Responses

Responses to the open-ended question were grouped into several thematic categories. The most frequently mentioned theme was education and the development of media literacy, including

workshops, critical thinking training, and continuous learning. A second group of responses focused on personal responsibility and information verification, including exercising caution when sharing content and verifying sources.

A third theme emphasised dialogue, mutual trust, and open discussion within the community. Some respondents expressed distrust toward official fact-checking institutions and highlighted the need for greater transparency. Less frequently mentioned were regulatory measures, reduced social media use, and broader cultural or spiritual factors.

Table 1
Summary of Key Findings

Category	Key Findings
Sample	Predominantly female; majority aged 18–27; diverse programmes
Trust and Media	Moderate institutional trust; low trust in traditional media
Verification	High self-reported verification of social media information
Critical Awareness	Clear rejection of misinformation; awareness of manipulation
Systemic Distrust	Strong scepticism toward media, platforms, and institutions
Self-assessed Resilience	High perceived ability to recognise manipulation
Community	Strong dialogue, mutual trust, and corrective behaviour
Open-ended	Emphasis on education, responsibility, and need for guidance

4. DISCUSSION – EXPLORATORY INTERPRETATION OF FINDINGS

4.1. Institutional Trust and Media Evaluation (H1–H2)

Consistent with previous research (Katsitadze et al., 2025; DeAngelis, 2024), respondents most commonly reported spending 3–4 hours per day on social media (45.3%), followed by 1–2 hours (32.8%). When it comes to reading news or consuming informational content, the majority of participants (51.6%) reported spending less than 1 hour per day, while nearly half (46.9%) reported spending between 1 and 2 hours per day.

The findings indicate a moderate level of institutional trust accompanied by limited polarisation. Although trust in official sources was low, respondents did not outright reject institutional information. At the same time, trust in traditional media and digital platforms was notably lower, and many respondents perceived those powerful actors shape information flows. On the one hand, such scepticism may indicate the presence of critical distance and elements of media literacy. On the other hand, lower levels of trust in traditional media could potentially increase vulnerability to alternative or unverified sources of information.

The findings suggest a pattern consistent with the expectations outlined in H1. Institutional trust exists, but it does not serve as a primary basis for accepting information. Instead, respondents appear to apply conditional credibility judgments, evaluating information across sources rather than relying solely on authority. The absence of unconditional trust suggests a shift from authority-based acceptance toward evaluative filtering of information.

The observed patterns are consistent with the assumption that lower perceived media credibility is associated with increased verification behaviours. Lower perceived credibility of media sources corresponds with increased verification behaviour. A large proportion of respondents reported verifying social media information and rejecting credibility cues such as institutional authority, popularity, or source familiarity. Thus, reduced trust did not produce passivity but rather encouraged active evaluation practices.

Overall, the results suggest that moderate distrust may function as a cognitive activation mechanism rather than a vulnerability factor, encouraging information checking rather than uncritical acceptance.

This pattern may indicate that institutional trust is conditional and context-dependent, potentially varying across topics or situations.

4.2. Verification Behaviour and Perceived Resilience (H3)

The study found high levels of reported verification behaviour and self-assessed resistance to manipulation. A majority of respondents (81%) reported treating information obtained through social media with caution and seeking to verify it, which may indicate relatively developed information-verification practices within the sample.

In addition, respondents reported checking emotionally provocative content, recognising manipulative techniques, and rejecting widely known misinformation claims. Such a pattern aligns with the conceptualisation of behavioural resilience as an active, reflective process of evaluating information rather than the passive acceptance or rejection of sources.

The observed patterns are consistent with the assumption that verification behaviour contributes to higher levels of perceived individual (psychological) resilience. Emotional awareness was also pronounced, with a majority reporting attempts to remain rational when exposed to disturbing news.

Verification practices appear closely linked to perceived psychological resilience: individuals who actively evaluate information also perceive themselves as capable of resisting manipulation. Rather than knowledge alone, behavioural engagement in checking information seems to strengthen confidence in judgement. The results, therefore, suggest that perceived

resilience develops through repeated evaluative behaviour, as individuals construct a sense of informational competence through verification practices.

4.3. Cognitive Biases and Overconfidence (H3)

Despite high self-assessed resilience, psychological mechanisms may complicate this relationship. The third-person effect suggests that individuals often perceive others as more susceptible to manipulation than themselves, while the illusion of control may lead individuals to overestimate their ability to resist influence. Additionally, socially desirable responding may encourage participants to present themselves as rational and cautious information users.

These mechanisms indicate that perceived psychological resilience does not necessarily equal actual resistance. Manipulation frequently operates through emotional framing, identity alignment, and selective exposure rather than factual ignorance. Consequently, even individuals who report strong awareness of manipulation may remain vulnerable to influence. Therefore, the findings should be interpreted as evidence of perceived resilience and defensive practices rather than proof of complete immunity to cognitive manipulation.

Why, then, is there a problem of susceptibility to media manipulation? One theory that explains this is the “third-person effect”: “an individual who is exposed to a persuasive communication via the mass media will see this communication as having a greater effect on other people than on himself or herself” (Davison, 1983, p. 4). In other words, many people have the impression that they know more and that they are less susceptible to influence.

Another theory is the illusion of control: “An illusion of control was defined as an expectancy of a personal success probability inappropriately higher than the objective probability would warrant” (Langer, 1975, p. 311). This demonstrates that a high level of emotional awareness does not automatically imply the ability to fully regulate emotions. Just as a doctor may know a great deal about the harmful effects of cigarettes, it does not mean that he has the capacity for self-regulation when confronted with them.

Furthermore, a common theory in sociology and psychopathology is the tendency to give socially desirable responses (Crowne & Marlowe, 1960). It is socially desirable to say that one checks facts or remains rational. In reality, it is first difficult to admit irrational behaviour and ways of thinking to oneself; it is also difficult to become aware of that, and especially difficult to give an affirmative answer about one’s own impulsiveness.

Finally, manipulation does not operate solely through ignorance, but through identity polarisation, selective presentation of information, and the emotional amplification of beliefs. Being familiar with possible manipulation techniques does not mean that one cannot be manipulated. Of course, none of these theories necessarily implies that the responses are untrue

or incorrect; rather, they explain why people in general may be susceptible to manipulation even when they report a high level of perceived self-resistance.

4.4. Community (Horizontal) Resilience (H4)

Respondents consistently emphasised dialogue, mutual trust, and personal responsibility as foundations of resilience. Many reported willingness to discuss differing viewpoints, warn others about misinformation, and maintain open communication networks. Collective responsibility was widely endorsed as a mechanism for limiting the spread of false information. Such behaviour reflects an active rather than passive stance toward information dissemination. The findings suggest a pattern consistent with the expectations outlined in H4. Individual resilience appears to translate into collective resilience through social interaction. Rather than relying primarily on institutional authority, respondents construct resilience horizontally through peer discussions and shared norms of verification. Such interaction indicates that resilience is supported not only by individual capacities but also by the structure of social relationships.

This indicates a distributed resilience model: the community functions as a network of mutual correction in which manipulation is countered through communication. Interpersonal trust, therefore, plays a more central role than institutional trust in sustaining resilience within the observed group. This pattern aligns with the theoretical framework that conceptualises societal resilience as a socially embedded and communicatively sustained process.

4.5. Integrated Model & Implications (H5)

Taken together, the findings suggest a pattern consistent with the sequential mechanism proposed in H5. Institutional trust shapes media evaluation, which influences verification behaviour, leading to perceived individual resilience and ultimately to community resilience. Moderate institutional distrust did not weaken resilience; instead, it contributed to critical engagement with information. Verification behaviour functioned as the operational stage of resilience, while dialogue and mutual responsibility transformed individual resistance into collective protection. Open-ended responses further reinforced this mechanism. Respondents emphasised education, critical thinking training, and structured workshops as the most effective ways to strengthen resilience. They also highlighted personal responsibility and open discussion as essential components of a resilient information environment.

The model, therefore, suggests that resilience is not produced by increasing trust alone but by fostering evaluative competence and communicative interaction. Educational institutions play a key role by supporting verification skills and encouraging discussion, thereby strengthening both individual and collective resistance to cognitive manipulation. This study contributes primarily at the theoretical level by proposing and empirically illustrating a sequential model

of resilience formation. The results do not establish causal relationships but provide indicative evidence that supports further refinement and testing of the model.

4.6. Limitations

This study has several limitations that should be considered when interpreting the findings. The sample consisted of 64 students from a single university and was obtained through convenience and snowball sampling. Consequently, the results cannot be statistically generalised to the broader student population or to the general public.

However, the study employed an exploratory design to identify relationships among institutional trust, media evaluation, and perceived resilience, rather than producing population-level estimates. Within this framework, the sample size is adequate for descriptive analysis and allows theory-oriented analytical insights.

Therefore, the findings should be interpreted as indicative patterns within a specific academic community rather than representative conclusions. Future research should replicate the study with larger, more diverse samples to test the robustness and generalizability of the proposed resilience model.

CONCLUSION

Building on the theoretical framework that conceptualises resilience as a multidimensional, socially embedded process, this study sought to explore how students navigate a complex, often ambiguous information environment shaped by cognitive manipulation. By linking institutional trust, media evaluation, and verification behaviour, the research aimed to provide a more comprehensive understanding of how perceived resilience is formed in everyday contexts.

The findings of this study provide nuanced insight into how students perceive their resilience to cognitive manipulation in a contemporary information environment. While the results indicate relatively high levels of self-assessed awareness, verification behaviour, and engagement with information, it is important to emphasise that clear empirical relationships between key variables cannot be established within the limits of this research design. The findings should therefore be interpreted as indicative patterns rather than as evidence of measurable causal or statistical connections.

At the same time, the data reveal a consistent tendency among respondents to express confidence in their ability to recognise manipulation. Such self-assessments, however, should be approached with caution. Existing theoretical perspectives suggest that individuals often overestimate their own resistance to influence, while simultaneously perceiving others as more susceptible. In addition, the possibility of socially desirable responding cannot be ignored, as

individuals generally present themselves as rational, critical, and responsible information users. This raises the question of whether reported resilience fully corresponds to actual behaviour in real-world information contexts.

Despite these limitations, the findings remain highly relevant. They point to an important paradox: students appear capable of rejecting clearly identifiable misinformation, yet at the same time express a broader sense of uncertainty and distrust toward the information environment as a whole. Rather than indicating simple vulnerability, this suggests a more complex form of awareness in which respondents recognise that manipulation exists but may lack clear strategies for consistently identifying and responding to it.

Importantly, participants demonstrate a clear openness to learning and education. Their responses indicate a recognition of the challenges posed by disinformation and cognitive manipulation, as well as a willingness to better understand how such processes operate in practice. This suggests that resilience is not a fixed trait, but a developing capacity that depends on continued engagement, education, and critical reflection.

Furthermore, the strong emphasis on dialogue, mutual trust, and shared responsibility highlights the social dimension of resilience. Respondents do not perceive resistance to manipulation as solely an individual task, but as something that emerges through interaction, discussion, and collective awareness within a community.

In this sense, the study contributes to a broader understanding of resilience as a dynamic and socially embedded process. Although the findings cannot confirm direct relationships between variables, they offer valuable insight into how individuals navigate a complex information landscape, how they perceive their own capacities, and where potential gaps between perception and practice may exist. These insights provide a useful foundation for future research and, importantly, for developing educational approaches to strengthen both individual and collective resilience to cognitive manipulation.

REFERENCES

- Cohen, J. (1992). A power primer. *Psychological Bulletin*, 112(1), 155–159.
<https://doi.org/10.1037/0033-2909.112.1.155>
- Crowne, D. P., & Marlowe, D. (1960). A new scale of social desirability independent of psychopathology. *Journal of Consulting Psychology*, 24(4), 349–354.
- Cutter, S. L.; Barnes, L.; Berry, M.; Burton, C.; Evans, E.; Tate, E. & Webb, J. (2008). A place-based model for understanding community resilience to natural disasters. *Global Environmental Change*, 18(4), 598–606. <https://doi.org/10.1016/j.gloenvcha.2008.07.013>
- Davison, W. P. (1983). The third-person effect in communication. *Public Opinion Quarterly*, 47(1), 1–15.
- DeAngelis, T. (2024, April 1). *Teens are spending nearly 5 hours daily on social media. Here are the mental health outcomes.* *Monitor on Psychology*. American Psychological Association. <https://www.apa.org/monitor/2024/04/teen-social-use-mental-health>
- European Commission. (2022). *Special Eurobarometer 523: Corruption*. Publications Office of the European Union.
- European Commission. (2024). *Standard Eurobarometer 101: Spring 2024 – Public opinion in the European Union*. Publications Office of the European Union.
- Katsitadze, N., Kharadze, N., & Pirtskhalaishvili, D. (2025). The impact of social media on students' effective time management. *Baltic Journal of Economic Studies*.
<https://doi.org/10.30525/2256-0742/2025-11-1-200-210>
- Keck, M.; Bohle, H.-G. & Zingel, W.-P. (2012). Dealing with insecurity. Informal business relations and risk governance among food wholesalers in Dhaka, Bangladesh. *Zeitschrift für Wirtschaftsgeographie* 56 (1+2): 43–57.
- Keck, M. & Sakdapolrak, P. (2013). What is Social Resilience? Lessons Learned and Ways Forward. *Erdkunde*, 67(1): 5-19. <https://www.jstor.org/stable/23595352>
- Langer, E. J. (1975). *The illusion of control*. *Journal of Personality and Social Psychology*, 32(2), 311–328.
- Marjanović, A. & Smiljanić, D. (2025). Cognitive warfare - the human mind as the new battlefield. *Proceedings of the Defence and Security Conference*, 1(1): 84-114.
- Pelling, M. & High, C. (2005). Understanding adaptation: what can social capital offer assessments of adaptive capacity? *Global Environmental Change* 15 (4): 308–319.
<https://doi.org/10.1016/j.gloenvcha.2005.02.001>
- Schäfer, S.K., Supke, M., Kausmann, C., Schaubrich, L.M., Lieb, K. & Cohrdes, C. (2024). A systematic review of individual, social, and societal resilience factors in response to societal challenges and crises. *Communications Psychology*, 2(29).
<https://doi.org/10.1038/s44271-024-00138-w>

- Traerup, S. (2012). Informal networks and resilience to climate change impacts: a collective approach to index insurance. *Global Environmental Change* 22(1), 255–267.
<https://doi.org/10.1016/j.gloenvcha.2011.09.017>
- van Zoonen, W., Luoma-aho, V. & Lievonen, M. (2024). Trust but verify? Examining the role of trust in institutions in the sharing of unverified information on social media. *Computers in Human Behavior*, 150. <https://doi.org/10.1016/j.chb.2023.107992>

THE ROLE OF UNMANNED AERIAL SYSTEMS (DRONES) IN CONDUCTING INFORMATION OPERATIONS: A CASE STUDY OF THE RUSSO-UKRAINIAN WAR SINCE 2022

Dominik Dujic¹, Danijel Nekić², Tomislav Ivanjko³

¹University of Zagreb

Faculty of Humanities and Social Sciences

E-mail: dominik.dujic@morh.hr, dujicnovska@gmail.com

ORCID ID: <https://orcid.org/0000-0009-0006-4398-4400>

²Croatian Armed Forces

E-mail: danijel.nekic@morh.hr

ORCID: <https://orcid.org/0000-0002-1519-7251>

³University of Zagreb

Faculty of Humanities and Social Sciences

E-mail: tivanjko@m.ffzg.hr

ORCID ID: <https://orcid.org/0000-0002-0479-5395>

Abstract

Unmanned aerial systems (UAS), commonly known as “drones,” represent a significant evolution of the modern battlefield and are a key resource in contemporary military operations. Originally designed for reconnaissance and strike missions, they now play a prominent role in information operations alongside traditional combat activities. Their ability to operate in hostile environments and along the line of contact without directly exposing personnel to risk has enhanced their utility in the information environment, encompassing the adversary’s physical, virtual, and cognitive dimensions.

This paper examines how UAS are employed in information operations to achieve information dominance and shape desired narratives. Particular attention is given to

restricting adversary information flows, preventing the dissemination of disinformation (deception), and protecting one's own information. In this context, UAS support a wide range of tasks: intelligence collection, destruction of information infrastructure, psychological operations, actions in the electromagnetic spectrum, and media operations. In this way, risk to personnel is reduced, and the operational reach of units is extended, while battlefield information is transformed into media and psychological effects almost in real time.

The analysis is based on a case study of the Russo-Ukrainian war (2022–2025) and uses NATO doctrine AJP-10.1 (NATO, 2023) as its theoretical and doctrinal foundation. A qualitative approach is applied, grounded in open-source reports, video recordings, social media posts, and analytical studies, complemented by a SWOT analysis of the strengths, weaknesses, opportunities, and threats associated with the use of UAS in information operations. The results show that UAS effectively compress the “sensor–effect–narrative” loop, enabling continuous tactical-area coverage and sustained pressure on information nodes while simultaneously amplifying narratives. In conclusion, UAS function not only as force multipliers but also as accelerators of information operations, capable of placing an adversary in a position of information subordination and supporting the projection of desired narratives beyond the immediate area of operations.

Keywords: unmanned aerial systems; information operations; Russo-Ukrainian war; target audiences; case study; narrative.

INTRODUCTION

Technological development has enabled the exploitation of information in almost real time, regardless of one's location in the world. Alongside the expanded availability of information, systems designed to protect one's own information and deny an adversary access to it have also evolved. Information thus becomes an element of power through which public knowledge can be shaped to support the achievement of strategic objectives (Tudman, 2008). Since the beginning of humankind, technological development has accompanied warfare, and the possession of more advanced technology has often enabled a numerically weaker side to achieve success in military operations. As a result, information warfare has become an integral part of warfare, with its operational component consisting of conducting information operations.

Modern conflicts have shown that situational awareness and contemporary information flows are among the most important factors in the successful planning and execution of operations. The importance of information in military operations is reflected in doctrinal publications that guide military decision-makers, which designate one of the seven joint functions as “information” (Tackett, 2024). By identifying information as a joint function, doctrine unequivocally emphasises the importance of timely and accurate information used across all other functions, as well as its role in dedicated information activities to achieve desired

military objectives. In this context, information dominance, shaping desired narratives, and securing support from target audiences emerge as key goals of contemporary information operations.

In addition to acting against the adversary by disrupting or degrading its communications and information systems and complicating decision-making, it is essential to identify target audiences beyond the immediate area of operations. Information collected through all available means is disseminated to these audiences to support a desired narrative, thereby securing backing to achieve objectives by leveraging technological advances (Akrap, 2009). In this way, information operations seek to shape the perceptions, beliefs, and behaviour of different actors, with an emphasis on aligning physical effects on the battlefield with informational effects in the virtual and cognitive domains.

Russia's aggression against Ukraine, which began in 2014, demonstrated the importance of technology on the modern battlefield and how decisive the timely dissemination of information and/or disinformation can be when using selected platforms. With the escalation into open war in 2022, the effectiveness of unmanned aerial systems (UAS), commonly referred to as "drones", became even more pronounced, and these systems became a daily reality of the Russo-Ukrainian battlefield. Beyond their role in directly destroying adversary personnel, equipment, and infrastructure, a distinctive feature of this war is the information environment in which UAS have become dominant in generating informational effects. Particular emphasis is placed on UAS effects across the adversary's physical, virtual, and cognitive domains, whereby UAS enable the rapid conversion of tactical battlefield effects into informational and cognitive effects. This paper examines how UAS are employed in information operations during the Russo-Ukrainian war and the lessons learned from this conflict help inform models for their application in future conflicts.

The topic of UAS use in conflicts is present daily in scientific, professional, and public discourse; however, the informational dimension of their employment is not always adequately represented, even though it often has strategic value. Therefore, this article aims to clarify the role of UAS in conducting information operations and to assess their advantages and limitations, using the current war as a case. Accordingly, this study tests the hypothesis that UAS act as a multiplier of information capabilities by compressing the sensor-effect-narrative cycle, enabling tighter synchronisation of non-communicative information activities with communicative capabilities (PSYOPS and military public affairs), and amplifying cognitive effects across relevant audiences. The analysis is based on the Russo-Ukrainian war (2022–2025) and relies on NATO doctrine AJP-10.1 to unify terminology and analytical categories (NATO, 2023). Using a qualitative approach, the research draws on open-source reports, video recordings, social media posts, and analytical studies to assess the actions of both sides in the conflict. A complementary SWOT analysis structures the strengths, weaknesses, opportunities, and threats associated with the use of UAS in information operations.

1. METHODOLOGY

The qualitative method is the primary research approach in this study. It is applied as a case study of the Russo-Ukrainian war (2022–2025) to analyse the role of UAS in conducting information operations within the information environment. The theoretical and doctrinal framework is based on NATO doctrinal terminology and concepts related to the information environment, narratives, and target audiences, specifically the conduct of information operations through information capabilities and activities. The NATO publication *AJP-10.1 Allied Joint Doctrine for Information Operations* serves as the analytical starting point, ensuring consistency in terminology and analytical categories (NATO, 2023). Additionally, to substantiate the findings and enhance the objectivity of the analysis, information operations are also defined using other Allied and scholarly approaches.

The empirical material is sourced from open sources: publicly available analytical reports, professional studies, official statements, video recordings, and social media posts that contain or describe the use of UAS and their informational effects. The analysis is interpretative, employs source triangulation, and emphasises how the tactical effects of UAS are generated through information activities (such as physical destruction, jamming, and similar actions) that are subsequently translated into communicative and cognitive effects. It also focuses on the role of UAS-generated content in supporting military-strategic narratives conducted by STRATCOM through psychological operations and military public affairs. Episodes are purposively selected to cover different types of UAS-enabled information activities and are coded using an AJP-10.1-informed activity–audience–effect template; claims are validated through a “2+1” logic, relying on two independent sources plus an official statement and/or technical corroboration (e.g., geolocation, satellite imagery, or authenticated footage) where feasible.

SWOT analysis is used as a tool to synthesise findings rather than as a method of quantification. The SWOT elements are derived from the interpretation of patterns identified in the case study and the relevant literature. They are structured into internal factors (the strengths and weaknesses of UAS capabilities and their organisational employment) and external factors (opportunities and threats in the operational and information environments, including adversary countermeasures and communications systems).

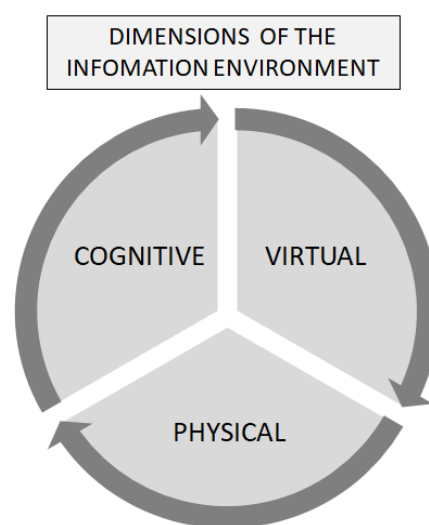
2. INFORMATION OPERATIONS

All actors in the information environment rely on information. Key individuals, civilians, the warring parties, and their weapons systems shape their actions according to the information available to them. Actors outside the area of hostilities, who form their perceptions based on available information, are also susceptible to information manipulation, and their support for one of the belligerents depends on the information they receive. It is therefore important that all information operations are conducted in a manner that supports a predefined narrative.

Timely and reliable information enables commanders to maintain situational awareness, including the adversary's disposition and intentions, other relevant actors, terrain characteristics, and the status of their own forces. The information environment (Figure 1), which NATO defines in AJP-10.1 as “*the environment composed of the information itself, individuals, organisations, and systems that receive, process, and convey information, and the cognitive, virtual, and physical space in which this occurs,*” is the space in which information operations take place (NATO, 2023, p. 68).

Figure 1

The information environment dimensions



Note. Made by authors, based on Modrzejewski (2018).

The information environment does not necessarily coincide with the area of combat operations; rather, information collected within the area of operations is either denied to or disseminated among all those it may influence. Coordinated action to manipulate such information can be considered information operations. Defining information operations is challenging because expert interpretations differ and there is no clear consensus, even within military organisations. According to information-security expert Nikola Brzica, information operations can generally be defined as “*the synchronisation and coordination activities of all capabilities that in any way deal with information*” (Brzica, 2022, p. 47). A broader definition is offered by Gordan Akrap, who describes information operations as “*a set of measures, actions, and activities undertaken against adversary information, information-communication systems, persons, and cognitive processes to destroy, disable, or slowing their functioning, or of taking control over their functioning, while simultaneously ensuring an*

appropriate level of protection of one's own information, cognitive processes, information-communication systems, and personnel” (Akrap, 2011, p. 42).

As early as 1998, the American information scholar Edward Waltz defined military information operations as: *“continuous military activities within the military information environment that enable, enhance, and protect the ability of friendly forces to collect, process, and use information to gain advantage across the full spectrum of military operations. Information operations include actions within the global information environment and the exploitation or denial of an adversary's information and decision-making capabilities”* (Waltz, 1998, p. 171). The United States, in its Joint Publication 3-13 Information Operations, defines them as *“the integrated employment of information-related capabilities, in concert with other lines of operation, to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own decision-making”* (Joint Chiefs of Staff, 2014, p. ix). This definition aligns with a more recent U.S. approach that describes information operations using the term “operations in the information environment” and defines them as military activities involving the integrated use of multiple information forces to influence behavioural drivers (Theohary, 2018).

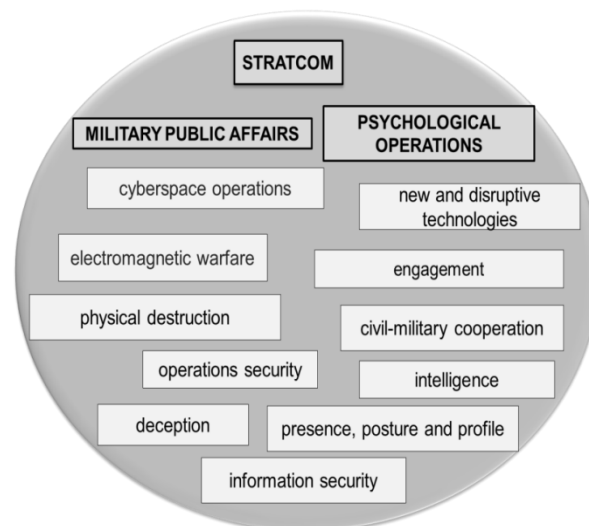
The most recent approved NATO definition of information operations further emphasises the staff function of planning and integration. Information operations are defined as *“a staff function to analyse, plan, assess, and integrate information activities in order to create desired effects on the will, understanding, and capabilities of adversaries, potential adversaries, and audiences in support of mission objectives”* (NATO, 2023, p. 25). This definition highlights the coordinated use of strategic communications, psychological operations, and military public affairs to achieve the greatest possible effect on target audiences within the information environment. In addition to these communication capabilities, NATO, in the same document, lists other military non-communication capabilities and techniques termed information activities, which it defines as *“activities conducted by any capability or means, aimed at creating a cognitive effect”* (NATO, 2023, p. 25).

In conducting information operations, coordination of the above-mentioned activities (Figure 2) is essential, as is a focus on the audiences to whom the operations are directed. It is important to emphasise that these are not all the activities that can be employed in information operations; only the most significant are highlighted. Whether dealing with a tactical example such as the destruction of a communications node, the dissemination of disinformation to an entire armed force, or a strategic campaign aimed at influencing the nations involved, it is essential to analyse whom information should be denied or disseminated to achieve the best result for the mission. Although this may involve an individual on the battlefield or an entire nation that one seeks to influence through information operations, the term audiences is used. NATO defines these audiences as *“individuals, groups, or entities whose interpretation of events and subsequent behaviour can*

influence the achievement of an end state” (NATO, 2023, p. 76). To facilitate coordination and ensure that the tactical, operational, and strategic levels are oriented towards the same cognitive outcome, a desired narrative is designated, previously defined and adapted to each level of action. NATO defines a narrative as “*a spoken or written account of events and information arranged in a logical sequence to influence the behaviour of a target audience*” (NATO, 2023, p. 10). Through information dominance achieved through successfully conducted information operations, one’s own narrative is imposed, and the desired ultimate state in the information environment is attained.

Figure 2

Information operations “bubble” – information activities that can be coordinated and integrated through information operations



Note. Made by authors, based on NATO’s AJP-10.1 (NATO, 2023).

Based on the above definitions, it can be concluded that information operations entail coordinated action within the information environment using all available and permitted means to achieve information superiority in the assigned area of operations. The purpose of such action is a cognitive effect in the form of imposing one’s own narrative, that is, influencing the adversary to act as desired.

3. UNMANNED AERIAL SYSTEMS – “DRONES” IN SUPPORT OF INFORMATION OPERATIONS

For terminological consistency, this study adopts the NATO definition of UAS. NATO defines a UAS as “a system whose components include the unmanned aircraft, supporting networks, and all equipment and personnel necessary to control the unmanned aircraft” (Kutuk, 2025, p. 14). In addition to Allied terminology, the specific features of Russian and Ukrainian terminology are considered comparatively, where necessary, to apply the analytical framework authentically to the research subject. Although the term “drones” is widely used in everyday language, in scientific and doctrinal contexts, it is advisable to use UAS, as it is more precise and explicitly includes all system components (platform, networks, equipment, and personnel).

Due to their flexibility, availability, and cost-effectiveness, UAS are becoming key assets of contemporary armed forces. Although these systems have a relatively short life cycle due to physical destruction and electromagnetic spectrum operations (e.g., jamming, interception), their low production cost (particularly for lower-class UAS) and effective use make them among the most recognisable means employed by both belligerents. While the primary tasks of UAS in modern warfare are conducting kinetic strikes against designated targets and intelligence, surveillance, and reconnaissance (ISR) for intelligence collection, in recent years, UAS have also been used on various battlefields worldwide for information operations (Nagorno-Karabakh, Iraq/Syrian Arab Republic - ISIS, etc.).

The primary purpose of employing UAS in information operations is dual: targeting domestic and international audiences to boost the morale of the population and secure support for the authorities’ war effort, or to sensitise international audiences in the struggle against the enemy; and targeting adversary audiences to undermine enemy morale and encourage revolt against their authorities, thereby influencing the will to continue the war. In the Russo-Ukrainian war, it is particularly noteworthy that UAS affect the deployment and survivability of more expensive weapons systems, which, due to the threat within the so-called UAS “kill zone,” are often forced out of zones of immediate risk (Nieczypor & Matuszak, 2025).

However, the relevance of UAS extends beyond the kinetic domain: in the information environment, they are a key enabler, enabling the secure collection, production, transmission, and disruption of data—that is, the generation of information that can subsequently be exploited to achieve desired effects. It is important to emphasise that UAS do not, as a rule, conduct information operations independently; rather, they provide a platform and sensor–communications infrastructure that supports the planning and execution of information-related activities. In the current war, so-called First-Person View (FPV) UAS are particularly prevalent; NATO classifies them as Class I. To clarify the distinctions among categories, Table 1 presents NATO’s classification of UAS into three classes based on mass, typical employment, operating altitude, and mission radius.

Table 1*NATO UAS Classification*

Class	Category	Normal employment	Normal operating altitude	Normal mission radius	Example platform
Class III (>600 kg)	Strike/Combat	Strategic/National	Up to 65,000 ft MSL	Unlimited (BLOS)	Reaper
Class III (>600 kg)	HALE	Strategic/National	Up to 65,000 ft MSL	Unlimited (BLOS)	Global Hawk
Class III (>600 kg)	MALE	Operational/Theatre	Up to 45,000 ft MSL	Unlimited (BLOS)	Heron
Class II (150–600 kg)	Tactical	Tactical Formation	Up to 18,000 ft AGL	200 km (LOS)	Watchkeeper
Class I (<150 kg)	Small (>15 kg)	Tactical Unit	Up to 5,000 ft AGL	50 km (LOS)	Scan Eagle

Note. Data based on Joint Air Power Competence Centre (2010). MSL = mean sea level; AGL = above ground level; LOS = line of sight; BLOS = beyond line of sight. (1 ft = 0.3048 m)

The most recognisable use of UAS is in supporting the communicative component of information operations, specifically psychological operations and military public affairs. Because they can approach the enemy without exposing friendly forces, these systems can collect real-time information about the adversary (most often video footage) that is then processed and disseminated to target audiences to influence them. STRATCOM directs and frames these activities according to a desired, predefined narrative. As part of the non-communicative component of information operations, UAS conduct information activities to deny the adversary unhindered access to information, thereby supporting the imposition of information dominance. In this way, information operations constitute a cycle of information exploitation in support of friendly forces, using all available means.

The use of these systems enables the generation of tactical effects through information activities, such as the destruction of information infrastructure, which are then transformed into strategic effects through communicative capabilities under STRATCOM oversight by timely informing audiences. In many cases, publicly available communication channels, including social media, feature FPV UAS videos depicting tactical effects against adversary personnel and equipment, which are used to support narratives of effectiveness, dominance, or adversary vulnerability. Thus, actions in the physical and virtual domains produce effects

in the cognitive domain, aimed at degrading adversary morale. For this purpose, information operations coordinate public affairs communications through the media exploitation of such content, often including the selective release of intelligence, surveillance, and reconnaissance (ISR) and battle damage assessment (BDA) material to shape perceptions and steer the interpretation of events.

The psychological effect of UAS arises from their very presence, as they create a sense of constant vulnerability; their sound evokes assumptions of lethal scenarios that may follow. Frequently, in addition to direct UAS attacks, this includes artillery fire, the arrival of so-called “kamikaze drones”, or detection followed by an offensive by enemy forces (Renic & Christensen, 2024). Beyond the traditional use of leaflets dropped for psychological effect, there are numerous examples of UAS-mounted audio equipment used for various purposes, such as conveying information to support the extraction of friendly forces or the capture of enemy personnel. Alongside communicative effects, an important aspect is protecting friendly information and denying or degrading adversary communications and information flows. These activities can be supported by UAS through physical effects on communications infrastructure, support for psychological operations (PSYOPS), and actions in the electromagnetic spectrum to protect friendly capabilities and suppress adversary ones. Finally, the ISR capability of UAS is one of its fundamental advantages, as it enables the collection, verification, and distribution of information relevant to planning, targeting, and effects assessment, thereby indirectly supporting information activities in the information environment.

4. CASE STUDY – THE RUSSO-UKRAINIAN WAR

In the relevant literature, the Russian approach to information warfare is often divided into information-psychological and information-technological components, with the former targeting audiences' will and perceptions and the latter focusing on the technical degradation of information systems and flows (Thomas, 2014; Giles, 2016). Ukraine, by contrast, has shaped its activities in the information environment through a combination of NATO doctrinal principles, adaptation to Russian patterns of action, and intensive exploitation of technological innovations (Schrijver, 2023). Since 2022, the war has been marked by the widespread use of UAS, which have made the battlefield more transparent and increased commanders' situational awareness. Accelerated production in Ukraine confirms the industrialisation of this capability (Nieczypor & Matuszak, 2025), while Russia has simultaneously expanded its capacities, albeit under structural and supply constraints and with an initial reliance on imports and commercial components (Marcinek & Han, 2023; Nieczypor & Matuszak, 2025).

Given their cost and vulnerability in an environment saturated with air defences, NATO-classified Class III platforms generally have limited employment due to their high cost

relative to lower-class UAS. In practice, Class I systems (especially FPV) are the most widespread because of their cost-effectiveness and mass producibility for tactical use. Systems that fall under Class II by weight (e.g., Shahed/Geran) are often used in Russian operations for strategic-reach missions, illustrating that a platform's doctrinal classification does not determine its level of effect. In accordance with AJP-10.1, the analytical focus of the case study is on information activities associated with UAS use, the audiences they target, and the desired and achieved effects across the cognitive, virtual, and physical dimensions of the information environment. In the Russian narrative, actions are framed as a “special military operation,” whereas the Ukrainian narrative emphasises the defence of the country with Allied support; accordingly, the key audiences are the domestic public, the adversary’s public and forces, and international audiences whose support or neutrality affects the objectives of the war. In the early stages of the invasion, Ukraine systematically leveraged the successes of the Bayraktar TB2 UAS through military public affairs, primarily via social media, including strikes on Russian armoured columns in the Brovary area (Perrigo, 2022). The release of selected ISR/BDA footage simultaneously boosted morale and reinforced perceptions of defensive capability, aiming to sustain international support. The Russian side sought to neutralise this effect by showcasing the destruction of Western and Ukrainian equipment, with a recognisable pattern emerging in the form of footage of Lancet (ZALA) loitering munitions operating in conjunction with reconnaissance UAS platforms (Farrell, 2023). Such a “two-sided” visual cycle (effect–content–narrative) demonstrates how tactical events are rapidly transformed into information directed at audiences. The continuation of the war has led to a significant evolution of information operations.

4.1. Operation “Spider Web” (1 June 2025): Deep UAS Strike and Integration of Information Activities

Operation “Spider Web” is a prominent example of UAS employment with strategic reach, where the physical effect is directly linked to communicative exploitation. It also illustrates the role of military public affairs: selected strike and BDA-related imagery was quickly released and amplified to frame the event and shape audience interpretation in line with STRATCOM objectives. According to publicly available sources, the attack took place on 1 June 2025, with FPV UAS launched from civilian trucks parked near the targeted military sites. The reported targets were air bases across the Russian Federation (see Table 2), including some more than 4,000 km from Ukraine (Dumont, 2025). A Ukrainian damage assessment reports losses exceeding USD 7 billion (Strategic Studies Department, 2025). The Ministry of Defence of the Russian Federation stated that Ukraine had carried out an attack with FPV drones against military airfields in several regions (Murmansk, Irkutsk, Ivanovo, Ryazan, and Amur oblasts). According to the Ministry, the attacks in Ivanovo, Ryazan, and Amur oblasts were “repelled.” At the same time, fires were recorded on several aircraft in Murmansk and Irkutsk oblasts (Ministry of Defence of the Russian Federation, 2025). Additionally, analytical commentaries cite satellite imagery and video recordings of the attack as evidence of damage to several aircraft (Dumont, 2025). Analytical literature

indicates that planning for the operation lasted approximately 18 months and involved smuggling a large number of FPV UAS, modular launch systems, and associated payloads, concealed within civilian logistics chains (Bondar, 2025).

Table 2

Overview of targeted airfields and reported effects during Operation “Spider Web”

Name of airfield	Oblast/ Region	Main aircraft types (stationed/ targeted)	Ukrainian claims (damaged/ destroyed)	Response/ statement of the Ministry of Defence of the Russian Federation (if specified)	Key statements from sources
Belaia	Irkutsk (Siberia)	Tu-22M3, Tu-95MS	Included in the total of over 40, the most distant target (over 4,000 km)	Attack confirmed by the regional governor	Included in the total of over 40, the most distant target (over 4,000 km)
Olenia	Murmansk	Tu-22M3, Tu-95MS, Tu-142	Included in the total of over 40	Attack reported by Russian media; active defences	Attack reported by Russian media; active defences
Ivanovo Severny	Ivanovo	A-50, Il-76	Included in the total of over 40; 1 A-50 destroyed	Attacks "repelled"	Included in the total of over 40; 1 A-50 destroyed
Diaguilevo	Ryazan	Tu-95MS, Tu-22M3	Included in the total of over 40	Attacks "repelled"	Attacks "repelled"
Voskressensk	Moscow	(Unspecified)	Included in the total of over 40	Unspecified	Unspecified

Note. Data based on Dumont (2025)

Impact assessments vary across sources: Ukrainian estimates indicate a substantial proportion of strategic platforms were damaged or destroyed, while the Russian Ministry of Defence reports that parts of the attack were repelled and confirms fires on several aircraft in the Murmansk and Irkutsk oblasts (Ministry of Defence of the Russian Federation, 2025). For this analysis, the doctrinal aspect is crucial: the ability of UAS to simultaneously generate a physical effect and credible visual material (ISR/BDA) for communicative exploitation with different audiences.

Figure 3

Spatial layout of the listed targets of Operation “Spider Web”



Note. Reprinted from “Significance and implications of Ukraine’s Operation Spiderweb”, by Strategic Studies Department, 2025. The map shows attacks in the airfields of Ivanovo, Ryazan and Amur.

From the perspective of information operations, Operation “Spider Web” produced multiple effects for different audiences, with FPV UAS serving as key enablers of both physical impact and communicative exploitation. In this episode, UAS acted as the strike vector, while available video recordings and subsequent effects assessments (BDA), including satellite confirmation and selected visual materials, enabled the rapid conversion of tactical-technical results into narrative and psychological effects (Dumont, 2025; Strategic Studies Department, 2025). As sources indicate real-time video transmission and remote control, UAS can also be considered part of the sensor component, thereby operationally compressing the “sensor–effect–narrative” chain through the simultaneity of effect and communicative exploitation. According to Ukrainian claims and analyses, the attack had a pronounced moral and symbolic impact and was presented as a “media victory” that supported the national narrative of resilience and initiative (Strategic Studies Department, 2025). For adversary audiences, the intended effect is to undermine perceptions of security and the ability to protect critical military infrastructure deep within the territory, with potential consequences for trust in military leadership and the effectiveness of defensive measures. For external audiences, the operation may signal the capabilities and endurance of Ukrainian forces, indirectly helping

maintain international support. The coding of this episode in accordance with AJP-10.1 (NATO, 2023) and the verification protocol (2+1) is presented in Table 3.

Table 3

Coding of the “Spider Web” episode according to AJP-10.1 (activity–audiences–effect) and the verification protocol (2+1)

Element	Summary (coding according to AJP-10.1)
Activity	- FPV UAS launched from civilian vehicles positioned near the targeted airfields in order to generate a physical effect; - Parallel production and distribution of visual evidence (video/BDA) for narrative exploitation (UAS as a strike vector and narrative enabler)
Audiences	- Domestic audience of Ukraine: morale and legitimacy; - Domestic audiences and stakeholders in Russia: perceptions of security and institutional competence; - International audiences/stakeholders: strategic signalling and the maintenance of support or neutrality; - Military and political actors: perceptions of vulnerability and control over strategic assets
Effect	- Cognitive and narrative effects: reinforcement of perceptions of capability and initiative (Ukraine); - Potential erosion of the sense of security and trust (Russia); - Signalling of capability and endurance to external audiences, accompanied by increased crisis-communication pressure due to the spread of verifiable strike footage
Evidence (2+1)	Two independent sources: - Dumont (2025) and Strategic Studies Department (2025); - Primary official statement: Ministry of Defence of the Russian Federation (2025). +1 technical verification (where feasible): satellite/BDA analyses and/or authenticated FPV video materials substantiating damage assessments

4.2. Psychological Operations (PSYOPS) on the Front Line

The ubiquity of FPV UAS on the battlefield creates a persistent sense of vulnerability and a distinct cognitive effect among personnel exposed to them. This perceived omnipresence fosters anticipatory stress and hypervigilance, as individuals must constantly fear being observed, targeted, or recorded. Sensor persistence and the constant threat of attack constrain movement, force the search for cover, and increase the psychological burden on soldiers and civilians alike, with the acoustic “signature” of UAS itself acting as a trigger for stress reactions (Maddox, 2025). In addition to standard kinetic effects, both sides occasionally

employ particularly “dramatic” forms of action to achieve psychological effects and media dissemination (see Table 4). In such cases, tactical action is deliberately designed to be communicable, producing emotionally salient imagery that extends the effect beyond the immediate target set to broader audiences. An example is the publicly documented use of incendiary payloads (so-called “dragon drones”), which at the same time raises questions of compliance with the law of armed conflict and risks to civilians and has become the subject of legal analyses (Coble & Hernandez, 2024).

Table 4

Illustrative PSYOPS techniques using UAS (target audience and primary effect)

PSYOPS Technique (UAS)	UAS Type / Payload	Target Audience	Primary Effect	Sources
Leaflets/messages (leaflet dropping)	Multirotor/FPV + leaflet capsule or container	Front-line soldiers / specific groups	- Erosion of morale - Encouragement of desertion	Lee & Cho, 2024
Audio messages (loudspeaker on UAS)	UAS + loudspeaker (sometimes also a microphone)	Front-line groups / encircled groups	- Inducement of surrender - Disruption of combat routine	Maddox, 2025; Mariner, 2020
“I Want to Live” (UAS-supported surrender)	Multirotor/FPV + communication channel; Visual control.	Individuals / small groups	- Increase in surrenders with reduced contact risk - Procedural credibility	Wallace & Reeves, 2023
Incendiary UAS (“dragon drones”) as a psychological effect	UAS with incendiary payload (e.g., thermite)	Enemy forces in cover; secondarily, broader audiences	- Intimidation - Coercion to abandon cover - Perception that there is no safe place	Coble & Hernandez, 2024
Ambient psychological effect (sound and constant presence)	Various UAS (especially FPV); acoustic stimulus	Combatants and civilians in the area of operations	- Chronic stress, exhaustion, decline in morale, restriction of movement.	Maddox, 2025; Renic & Christensen, 2024

To induce demoralisation and surrender, methods such as dropping leaflets and messages from UAS (Lee & Cho, 2024), broadcasting audio messages, and technologically enabled surrender procedures are employed. In this context, the Ukrainian project “I Want to Live” is particularly notable: surrender is coordinated through available channels, and UAS are used to guide individuals or small groups to a designated point, reducing contact risk and creating “procedural proof” that is subsequently exploited communicatively (Wallace & Reeves, 2023). Consequently, FPV UAS function not only as strike platforms but also as information-related capabilities that shape perceptions and behaviour across the physical and cognitive domains through surveillance, intimidation, and narrative amplification. Moreover, the

integration of UAS video feeds into command-and-control and open media ecosystems compresses the observe–orient–decide–act cycle and enables near-real-time narrative framing of tactical events for multiple audiences.

This convergence of ISR, precision engagement, and strategic communication complicates efforts to analytically separate military effects from information effects, particularly when recordings are selectively edited, contextualised, and redistributed to sustain credibility, impose reputational costs, or signal inevitability of defeat. At the tactical level, the routine availability of “proof-of-effect” imagery can influence operational tempo and risk calculus, incentivising actions that are not only militarily expedient but also communicatively advantageous. At the strategic level, repeated exposure to UAS-derived content may contribute to a cumulative perception of technological overmatch or battlefield transparency, shaping morale, compliance, and willingness to manoeuvre, even among forces not directly engaged when the content is disseminated.

4.3. Other Information Activities

In addition to their communicative capabilities (PSYOPS and military public affairs), UAS also support non-communicative information activities from the AJP-10.1 spectrum, such as deception, operational security, actions in the electromagnetic spectrum, physical destruction of critical information nodes, and “presence and posture.” In this context, UAS are most often used as ISR platforms (target detection and confirmation, effects monitoring), but also as payload carriers for jamming, deception, or attacks on infrastructure (Ito, 2025). To achieve information dominance, the information infrastructure in the Sumy and Kharkiv oblasts in eastern Ukraine was destroyed using UAS, combined with simultaneous electronic jamming of Ukrainian radio and television stations, constituting an information operation that combined physical destruction with electromagnetic warfare (Reuters, 2024; Polishchuk & Gurcov, 2025). The immediate effect was the interruption of TV and radio signals, aimed at isolating the population from information and degrading the distribution of official messages. Due to their extremely low radar cross-section, these systems have successfully destroyed particularly expensive radar systems and relay nodes, thereby disrupting the adversary’s information flows (Ito, 2025).

UAS decoys and deceptive systems are a salient example of information activities involving deception and saturation. Russian military doctrine refers to deception as *maskirovka* and employs it before all major operations (Kirichenko, 2025). In attack waves involving more complex and expensive Russian UAS (e.g., Shahed/Geran), inexpensive decoys (e.g., Gerbera/Parody) appear, mimicking the radar and flight profile of the target, forcing air defence and sensor systems to expend resources and increasing the probability of penetration by the “real” platforms (Anokhin & Faragasso, 2024). In this way, false information is generated, and adversary forces are deceived.

Actions in the electromagnetic spectrum include supporting data collection, jamming, and degrading communications flows (Roslan, 2022). An example is the use of the Orlan UAS as a relay and sensor platform and its integration into electromagnetic warfare systems such as Leer-3, which can jam GSM signals within a local radius while simultaneously supporting targeting and psychological effects (Mariner, 2020). These patterns show that UAS, in addition to direct firepower, function as an “information accelerator”: they shorten the collection–effect–distribution loop, facilitate the integration of information-related activities, and increase the capacity to steer narratives towards different audiences. In practice, this means that electromagnetic actions (e.g., jamming, spoofing, or denial of local connectivity) can be synchronised with kinetic strikes and mediated messaging to shape not only what adversary forces can do, but also what they can perceive, report, and credibly claim in the immediate aftermath.

5. SYNTHESIS OF FINDINGS: A SWOT PERSPECTIVE

In this paper, the SWOT analysis synthesises the findings. The listed elements refer to capabilities that form part of coordinated information activities, interpreted in relation to target audiences and narratives (see Table 5).

Table 5

SWOT analysis of UAS in support of information operations

Strengths (internal factors)	Weaknesses (internal factors)
• Low cost; mass use • Accessible civil–military production • Modularity (sensors/payloads/missions) • Reduced risk to personnel • Applicability at the tactical, operational, and strategic levels • Near–real-time data transmission • Compressed “sensor–effect–narrative” cycle • Visible psychological and media effects (effects assessment, documentation)	• Dependence on line-of-sight and beyond-line-of-sight links • Vulnerability to electromagnetic warfare (jamming and signal deception) • Weather-related constraints (meteorological conditions) • Interoperability issues and logistical fragmentation • Training requirements and standardisation of tactics, techniques, and procedures • Data overload and verification of content credibility • Operational security risk (exposure of procedures and locations)

Opportunities (external factors)	Threats (external factors)
• Development of doctrine and standard operating procedures • Integration with analytics and forensics (2+1 protocol) • Artificial intelligence for processing and anonymisation • Simulators and accelerated operator training • Influence on international (“distant”) audiences • Documentation of crimes and legitimisation of narratives • Operations beyond immediate range (satellite links, relays, autonomy) • Coalition support through content verification	• Adversary electromagnetic warfare and countermeasures • Air defence and counter-UAS measures • Interception and exploitation of data • Content manipulation (e.g., deep fakes and false attribution) • Supply chain constraints (chips, batteries, optics) • Legal and regulatory restrictions • Ethical and reputational risk (“backfire”) • Audience saturation (attention fatigue)

Strengths (internal factors)

Unmanned aerial systems (UAS) are characterised by relatively low acquisition costs and the potential for mass use, enabling saturation of both the battlefield and the information space. Modularity and a high proportion of civilian components facilitate rapid mission adaptation (e.g., ISR, BDA, message transmission, leaflet dropping, various sensors) while simultaneously reducing personnel risk, as operations are conducted remotely and deep within adversary territory. Near-real-time data transmission shortens the cycle from a tactical event to its exploitation as a narrative, thereby increasing the potential to influence domestic, adversary, and international audiences.

Weaknesses (internal factors)

The key weakness of UAS is their dependence on line-of-sight (or beyond-line-of-sight) communication links and data channels, making them highly vulnerable to electromagnetic warfare. Meteorological conditions further constrain operational effectiveness, while platform heterogeneity creates interoperability issues, logistical fragmentation, and challenges for standardising training. The availability of many platforms can lead to a “data overload” effect, in which the volume of data complicates timely validation and content selection. Finally, releasing material entails OPSEC risks, as it may compromise TTPs and sensitive capabilities.

Opportunities (external factors)

The effectiveness of UAS in information operations can be increased by developing and standardising doctrine and SOPs, and by integrating analytics and automated processing (including AI tools). This approach can shorten operator training, improve validation quality, and accelerate verification of material credibility (2+1). The ability to operate over the horizon expands the reach and scope of information exploitation, while verified content has particular value in influencing international audiences and documenting war crimes.

Threats (external factors)

The most significant threats arise from adversary electromagnetic warfare measures and counter-UAS capabilities, which can degrade data transmission, increase losses, and reduce operational continuity. Interception and exploitation of data enable content manipulation and the construction of counter-narratives, including sophisticated forms of deception. The use and distribution of content are constrained by supply chains and legal and ethical barriers; in cases of perceived disproportionality, information activity may result in a reputational “backfire.”

CONCLUSION

Over the past 20 years, Unmanned Aerial Systems (UAS) have become an integral part of every conflict, contributing to the evolution of the modern battlefield and emerging as a key resource for achieving victory. Although UAS are often associated with kinetic operations, they have also become indispensable for conducting information operations, supporting a wide range of tasks: intelligence collection, destruction of information infrastructure, psychological operations, operations in the electromagnetic spectrum, and media operations. In doing so, they reduce risk to personnel and extend the operational reach of units, while transforming battlefield information into media and psychological effects almost in real time.

Technological development has enabled the exploitation of information in near-real time, regardless of location, turning it into a source of power that shapes public knowledge and supports the achievement of one’s objectives. Modern conflicts have shown that situational awareness and the contemporary flow of information are among the most important factors in the successful planning and execution of operations, as demonstrated by the wars in Nagorno-Karabakh, Iraq/Syrian Arab Republic (ISIS), and the current Russo-Ukrainian conflict. The primary purpose of employing UAS in information operations across these conflicts has been dual: targeting domestic and international audiences to boost the morale of the population and secure support for the authorities’ war effort, or to sensitise international audiences in the struggle against the enemy; and targeting adversary audiences to undermine enemy morale and encourage revolt against their authorities, thereby influencing the will to continue the war. The current Russo-Ukrainian conflict has demonstrated that UAS can be used for a wide

range of tasks to generate effects across the physical, virtual, and cognitive domains, influencing target audiences.

The current Russo-Ukrainian conflict has demonstrated that UAS can be used for a wide range of tasks to generate effects across the physical, virtual, and cognitive domains, influencing target audiences. In this context, the findings support the initial hypothesis that UAS act as multipliers of information capabilities by compressing the sensor–effect–narrative cycle. They enable tighter synchronisation of non-communicative and communicative information activities and amplify cognitive effects across relevant audiences.

Experience to date in conducting information operations using UAS clearly shows that this trend will intensify, making UAS in information operations an indispensable element of future conflicts.

REFERENCES

- Akrap, G. (2009). Informacijske strategije i oblikovanje javnoga znanja. *National Security and the Future*, 10 (2), 77-151. <https://hrcak.srce.hr/80639>
- Akrap, G. (2011). *Informacijske strategije i operacije u oblikovanju javnoga znanja* [Doktorska disertacija. Sveučilište u Zagrebu, Filozofski fakultet].
- Anokhin, I., & Faragasso, S. (2024, December 18). *Russian decoy drones that depend on Western parts pose a great challenge to Ukrainian defenses*. Institute for Science and International Security (ISIS Reports). <https://isis-online.org/isis-reports/russian-decoy-drones-that-depend-on-western-parts-pose-a-great-challenge/>
- Bondar, K. (2025, June 2). *How Ukraine's "Spider Web" operation redefines asymmetric warfare*. Center for Strategic and International Studies (CSIS). <https://www.csis.org/analysis/how-ukraines-spider-web-operation-redefines-asymmetric-warfare>
- Brzica, N. (2022) *Suvremeno ratovanje – Asimetrični i hibridni rat u teoriji i praksi*. Zagreb: Despot Infinitus.
- Coble, K. S., & Hernandez, A. (2024, October 23). Ukraine Symposium – Dragon drones and the law of armed conflict. Lieber Institute West Point. <https://lieber.westpoint.edu/dragon-drones-law-armed-conflict/>
- Dumont, J.-F. (2025, June 3). Operation Spider Web: Strategic Analysis. European Security. <https://european-security.com/operation-spider-web/>
- Farrell, F. (2023, November 8). How Russia's homegrown Lancet drone became so feared in Ukraine. *The Kyiv Independent*. <https://kyivindependent.com/how-russias-homegrown-lancet-drone-became-so-feared-in-ukraine/>
- Joint Air Power Competence Centre. (2010, January). Strategic concept of employment for unmanned aircraft systems in NATO (UAS CONEMP). https://www.japcc.org/wp-content/uploads/UAS_CONEMP.pdf
- Joint Chiefs of Staff. (2014). Information operations (Joint Publication 3-13). U.S. Department of Defense.
- Kunertova, D. (2023). Drones have boots: Learning from Russia's war in Ukraine. *Contemporary Security Policy*, 44(4), 576–591. <https://doi.org/10.1080/13523260.2023.2262792>
- Kutuk, Y. (2025). *UAS (Unmanned Aircraft Systems): The force multiplier for law enforcement agencies and the potential contributor to stability policing*. NATO Stability Policing Centre of Excellence (NATO SP COE). <https://nllp.jallc.nato.int/iks/sharing%20public/uas-unmanned-aircraft-systems.pdf>
- Giles, K. (2016, November). *Handbook of Russian information warfare* (Fellowship Monograph No. 9). NATO Defense College.

- <https://www.ndc.nato.int/download/handbook-of-russian-information-warfare-by-keir-giles/>
- Hourani, L. (2025, June 2). ‘Closer to victory’ – Operation Spiderweb gives much-needed morale boost to Ukrainians after 3 years of full-scale war. *The Kyiv Independent*. <https://kyivindependent.com/closer-to-victory-ukrainians-celebrate-operation-spiderweb-targeting-russias-heavy-bombers/>
- Ito, T. (2025). Intelligence failures in the asymmetric war between Ukraine and Russia: A literature review of Ukraine’s drone attacks on Russian military infrastructure. *Security Intelligence Terrorism Journal (SITJ)*, 2(3), 262–273. <https://doi.org/10.70710/sitj.v2i3.63>
- Kirichenko, D. (2025, May 8). *The phony war: Ukraine and Russia’s decoy drones*. Center for European Policy Analysis (CEPA). <https://cepa.org/article/the-phony-war-ukraine-and-russias-decoy-drones/>
- Lee, S., & Cho, J. W. (2024, December 20). Ukraine military drops leaflets urging North Korean troops to surrender. *Radio Free Asia*. <https://www.rfa.org/english/korea/2024/12/20/north-korea-ukraine-leaflets/>
- Maddox, J. D. (2025, July 24). It’s time to think about (and fear) drones and psychological operations. *War on the Rocks*. <https://warontherocks.com/2025/07/its-time-to-think-about-and-fear-drones-and-psychological-operations/>
- Marcinek, K., & Han, E. (2023). *Russia’s asymmetric response to 21st century strategic competition: Robotization of the armed forces* (RR-A1233-5). RAND Corporation. https://www.rand.org/pubs/research_reports/RRA1233-5.html
- Mariner. (2020, June 7). Russian Army PsyOps units. *Militarnyi*. <https://militarnyi.com/en/articles/russian-army-psyops-units/>
- Ministry of Defence of the Russian Federation. (2025, June 1). Сегодня киевским режимом был совершен теракт с применением FPV-дронов... [Telegram post]. Telegram. (Retrieved January 18, 2026, from the URL below) https://t.me/mod_russia/53366
- Modrzejewski, Z. (2018). Information operations from the Polish point of view. *Obrona a strategie*, 18(1), 113–130. <https://doi.org/10.3849/1802-7199.18.2018.01.113-130>
- NATO. (2019, February). *Allied joint doctrine for the conduct of operations* (Allied Joint Publication AJP-3, Edition C, Version 1). https://www.coemed.org/files/stanags/01_AJP/AJP-3_EDC_V1_E_2490.pdf
- NATO. (2023). AJP-10.1 Allied joint doctrine for information operations. NATO Standardization Office. <https://www.gov.uk/government/publications/allied-joint-doctrine-for-information-operations-ajp-101>
- Nieczypor, K., & Matuszak, S. (2025, October 14). *Game of drones: The production and use of Ukrainian battlefield unmanned aerial vehicles*. OSW Centre for Eastern Studies

- (OSW Commentary). <https://www.osw.waw.pl/en/publikacje/osw-commentary/2025-10-14/game-drones-production-and-use-ukrainian-battlefield-unmanned>
- Perrigo, B. (2022, March 1). Ukraine's secret weapon against Russia: Turkish drones. *Time*. <https://time.com/6153197/ukraine-russia-turkish-drones-bayraktar/>
- Polishchuk, O., & Gurcov, N. (2025, February 21). *Bombing into submission: Russian targeting of civilians and infrastructure in Ukraine (Report)*. Armed Conflict Location & Event Data Project (ACLED). <https://acleddata.com/report/bombing-submission-russian-targeting-civilians-and-infrastructure-ukraine>
- Renic, N., & Christensen, J. (2024). *Drones, the Russo-Ukrainian War, and the future of armed conflict*. Djøf Publishing & Centre for Military Studies. https://cms.polsci.ku.dk/publikationer/droner-krigen-i-ukraine-og-fremtidens-konflikter/Drones_the_Russo-Ukrainian_War_And_the_Future_of_Armed_Conflict.pdf
- Reuters. (2025, June 12). Russia's Putin calls for quick development of drone forces. *Reuters*. <https://www.reuters.com/business/aerospace-defense/russias-putin-calls-quick-development-drone-forces-2025-06-12/>
- Reuters. (2024, February 6). Ukraine's Zelenskiy orders creation of separate military force for drones. *Reuters*. <https://www.reuters.com/world/europe/ukraines-zelenskiy-orders-creation-separate-military-force-drones-2024-02-06/>
- Rosław, G. (2022). Key issues related to the use of unmanned aerial systems. *Modern Management Review*, 27(4), 41–47. <https://doi.org/10.7862/rz.2022.mmr.21>
- Schrijver, P. (2023, September 12). Ukraine's fight on the front lines of the information environment. *Modern War Institute at West Point*. <https://mwi.westpoint.edu/ukraines-fight-on-the-front-lines-of-the-information-environment/>
- Strategic Studies Department. (2025, June 3). Significance and implications of Ukraine's Operation Spiderweb. *TRENDS Research & Advisory*. <https://trendsresearch.org/insight/significance-and-implications-of-ukraines-operation-spiderweb>
- Tackett, M. J. (2024). The joint functions: Theory, doctrine, and practice. *Joint Force Quarterly*, (115), 117–124. <https://digitalcommons.ndu.edu/joint-force-quarterly/vol115/iss3/18>
- TASS. (2025, November 12). Russia establishes Unmanned Systems Forces. *TASS*. <https://tass.com/defense/2042371>
- Theohary, C. A. (2018). Information warfare: Issues for Congress (CRS Report R45142). *Congressional Research Service*. <https://www.congress.gov/crs-product/R45142>

- Thomas, T. L. (2014). Russia's information warfare strategy: Can the nation cope in future conflicts? *The Journal of Slavic Military Studies*, 27(1), 101–130.
<https://doi.org/10.1080/13518046.2014.874845>
- Tuđman, M. (2008). *Informacijsko ratište i informacijska znanost*. Zagreb: Hrvatska sveučilišna naklada.
- Wallace, D., & Reeves, S. (2023, January 13). Ukraine Symposium – The “I Want to Live” Project and technologically-enabled surrender. *Lieber Institute West Point*.
<https://lieber.westpoint.edu/i-want-to-live-project-technologically-enabled-surrender/>
- Waltz, E. (1998). *Information warfare: Principles and operations*. Artech House.

III

Emerging and Disruptive Technologies in Warfare



www.sois-ft.hr

CYBER DEFENCE IN MODERN WARFARE

Dinu Ștefan-Cosmin

Independent researcher

E-mail: dinustefan948@gmail.com

Abstract

In the digital era, cyber defence has become a cornerstone of modern military strategy, fundamentally reshaping how states perceive and respond to threats. The present paper examines the evolving relationship between cyber operations and hybrid warfare, focusing on the operational, technological, and strategic challenges faced by armed forces. The paper draws on recent initiatives by NATO and the EU, as well as lessons learned from the war in Ukraine, to explore how cyberattacks, disinformation, and electronic warfare collectively affect command-and-control systems, situational awareness, and national resilience. Utilising a comparative and analytical approach, the paper highlights the increasing interdependence between military and civilian infrastructures in cyberspace, underscoring the need for coordinated defence policies, cross-domain interoperability, and enhanced public-private collaboration. The research also addresses the ethical and legal dimensions of cyber conflict, including issues of attribution, proportionality, and compliance with international law. The findings indicate that cyber defence has evolved from a purely technical concern to a multifaceted component of strategic deterrence. To ensure information superiority in future conflicts, there is a necessity for innovation, adaptability, and robust institutional coordination.

Keywords: Cyber Defence; Hybrid Warfare; NATO; Information Security; Critical Infrastructure; Resilience.

INTRODUCTION

Modern warfare is changing significantly due to new technologies, digital systems, and closer collaboration between military and civilian systems. While traditional battlefields remain important, modern conflicts are also taking place in new domains, such as cyberspace. Here, countries compete in politics, the military, the economy, and psychology, and sometimes this happens without an official declaration of war. Cyberspace is becoming an increasingly important arena for states to compete and demonstrate their strength without resorting to violence.

The digital revolution has changed how military power is generated, used and defended. The armed forces today rely heavily on networked information systems to support command and control, intelligence gathering, logistics, weapons systems, and operational coordination. Concurrently, civilian infrastructure such as energy grids, financial networks, transportation systems, healthcare services, and communication platforms is increasingly linked to military operations and national security. The extensive reliance on interconnected digital systems generates novel forms of risk. States are increasingly vulnerable to cyber operations capable of influencing strategic outcomes without producing physical destruction, loss of life, or triggering a conventional military response.

As a result, defending against cyberattacks has shifted from a specialised area to a key part of how states and alliances ensure security. Cyber operations can disrupt decision-making processes, reduce military readiness, erode public trust in institutions, and destabilise entire societies. Cyber conflict differs from traditional warfare because it is anonymous, fast, and can reach across the world. Attacks can be carried out remotely, making it hard to identify who is responsible, and they can happen at any time, both during and outside of war. This makes it difficult to distinguish between civilians and military forces, and it raises questions about the laws and morals that apply in such situations.

Furthermore, cyber capabilities are now an important part of the broader concept of hybrid warfare. This is when conventional military force is used alongside cyberattacks, electronic warfare, disinformation campaigns, economic pressure, and psychological operations. This means that organisations, such as states and non-state actors, can exploit weaknesses across multiple areas simultaneously. This makes it hard to determine who is responsible, how to address the problem, and how to prevent it from happening again. Recent wars, such as the war in Ukraine, have shown how cyber operations, disinformation, and electronic warfare can work together to alter the situation on the ground, shape public perception, and shift the balance of power among different groups.

In this context, cyber defence extends beyond mere network and information system protection. It has evolved into a strategic function that supports the prevention of attacks, the enhancement of system resilience, and effective crisis management. Addressing cyber threats requires more than technological solutions alone; it also demands robust inter-organisational cooperation, clear legal frameworks, and sustained international collaboration. Military institutions, government agencies, and private-sector organisations must coordinate their efforts to safeguard critical digital infrastructure. In contemporary conflicts, the timely exchange of information, coordinated action, and the capacity to adapt operational plans in response to emerging threats are essential. Such an approach enhances anticipatory capabilities and strengthens preparedness against potential adversarial actions.

This paper analyses the evolution of cyber defence within the context of modern warfare, focusing on technological transformation, operational integration, and normative challenges. It

examines the role of cyber defence across different forms of conflict, its impact on military operations, and its contribution to national resilience, while also addressing the ethical and legal issues associated with cyber operations. The analysis draws on recent institutional assessments and academic research highlighting the growing complexity of cyber threats and their strategic implications (Robinson et al., 2013; ENISA, 2025). By assessing recent developments, conceptual shifts, and lessons derived from contemporary conflicts, including the war in Ukraine, the study argues that cyber defence has evolved from a supporting technical function into a structural component of twenty-first-century strategic deterrence and the effective projection of military power.

1. RESEARCH METHODOLOGY

This study employs a qualitative analytical approach based on a structured review of academic literature, policy documents, and institutional reports issued by NATO, the European Union, and specialised cybersecurity organisations (ENISA, 2025; Kwan et al., 2025).

The war in Ukraine is used as a contemporary illustrative example to demonstrate the operational integration of cyber operations within hybrid warfare. The example was selected for its availability of open-source documentation and its strategic relevance to Euro-Atlantic security.

The analytical framework focuses on three main dimensions:

1. technological transformation of warfare.
2. operational integration of cyber capabilities in hybrid conflict.
3. strategic, ethical, and legal implications of cyber operations.

The paper is limited to open-source information and does not include classified operational data. Consequently, conclusions are formulated at the strategic and conceptual levels rather than at the tactical or operational levels.

2. TECHNOLOGY AND THE TRANSFORMATION OF WARFARE

Throughout history, new technology has changed warfare in many ways. From basic weapons and medieval siege engines to the mechanisation of armies during the Industrial Revolution and the introduction of nuclear weapons in the 20th century, each major technological change has fundamentally reshaped military strategy, thinking, and the balance between attack and defence. Warfare has evolved alongside societal development. It is driven by competition for resources, power and political influence in a chaotic international system where states seek survival and the advancement of interests. The long-term interaction between technological innovation and military adaptation has been extensively documented in strategic studies literature (Bhattacharjee, 2025).

The Industrial Revolution was a significant moment in military history. The development of mass production, railways, and advanced logistics facilitated rapid troop mobility. This transformed the war from a small, local conflict into a large-scale industrial confrontation. Over the following decades, weapons improved steadily. They went from muskets and cannons to automatic machine guns, long-range artillery, and eventually weapons of mass destruction. The Manhattan Project and the introduction of nuclear weapons after it changed the global balance of power. It also introduced the idea of using nuclear weapons to stop other countries from attacking, which made technology a key part of how countries would avoid war.

In the 21st century, technology has advanced rapidly. Digital technologies, artificial intelligence, self-driving systems, satellite networks and cyber capabilities are now changing the way wars are planned, fought and concluded. This broader technological transformation confirms that contemporary military power increasingly depends on information dominance, network integration, and precision engagement capabilities rather than mass alone (Balmuş et al., 2022). Modern militaries fight in environments where networks are critical. In these environments, it is vital to collect and share information quickly and to make decisions quickly and accurately. Precision-guided munitions, long-range missile systems, stealth platforms, and advanced sensor networks allow countries to hit targets far away with great accuracy. This means soldiers sent out are at lower risk, and military operations can be more effective.

The growth of unmanned and autonomous systems is one of the most obvious changes to modern warfare. Drones were initially used for reconnaissance and surveillance, but they have since evolved into advanced combat platforms capable of autonomous navigation, making precise strikes, and even performing coordinated swarm operations. Recent conflicts, particularly the war in Ukraine, demonstrate how small unmanned systems can generate effects comparable to those traditionally associated with large conventional platforms. This development has lowered barriers to entry for technologically capable states and altered prevailing metrics of military power. Adaptability, innovation, and rapid production capacity have become more significant than aggregate industrial output.

Simultaneously, cyber technologies have introduced a new kind of warfare. Cyber operations enable actors to disrupt critical infrastructure, manipulate information, and influence political and social stability without resorting to violence. Cyber tools differ from conventional weapons because they can operate continuously, cross borders, and often remain anonymous. This makes them very useful for strategic competition that is not armed conflict. The operational domain now includes cyberspace, where controlling data, networks, and information is a key source of power.

Despite their operational advantages, emerging technologies have generated new strategic and structural risks. The modern military and its effectiveness, as well as society's ability to address problems, now depend on complex, interconnected information systems. If these systems are stopped, whole societies can be paralysed. Energy grids, financial systems, transportation

networks, healthcare services and military communications are all connected to digital ecosystems. A cyberattack can therefore have significant effects on public trust, economic stability, and political legitimacy, even when no direct physical destruction occurs.

Furthermore, advances in range, accuracy, rate of fire, and lethality have altered the balance between offensive and defensive operations. The proliferation of modern sensors and precision-guided munitions has increased the vulnerability of concentrated troop formations. As a result, armed forces are compelled to disperse, fortify positions, and adapt their operational concepts. Recent operational analyses similarly indicate a return to dispersed formations and to continuous adaptation at the tactical level as forces attempt to survive persistent surveillance and precision-strike environments (Noorman, 2024). This transformation resembles earlier historical shifts, such as the introduction of rifled firearms in the nineteenth century, yet it is broader in scope and characterised by significantly greater technological sophistication.

In conclusion, technology has not just improved existing forms of warfare; it has fundamentally changed how warfare is conducted. Warfare today is faster, more connected, more information-driven, and more destructive. Concurrently, it is also less visible and has a bigger effect on society than it used to. It is critical to understand how technology has changed warfare to grasp the role of cyber defence in modern conflicts.

3. CYBER WARFARE AS A CORE DIMENSION OF MODERN CONFLICT

Cyber warfare is now one of the most important and complicated parts of modern conflict. It has completely changed how power is used and fought for in the international system. Cyber warfare differs from traditional warfare, which relies on physical force and control of territory. In cyber warfare, information, perception, and system integrity are the main strategic objectives. The use of digital technologies by states and non-state actors is increasing. This means that cyber operations are now an important part of modern military strategy and political competition.

Cyber capabilities enable actors to achieve strategic goals through a wide range of activities, from espionage and influence operations to the disruption and damage of critical infrastructure and military systems. Cyberattacks can be used to steal sensitive information about politics, the military, and the economy. They can also be used to damage industrial and energy systems, interfere with elections, and manipulate public opinion through disinformation campaigns. In addition, cyber attacks can weaken the command, control, communications, and intelligence (C3I) architecture of rival states. These activities can have the same strategic effect as conventional military operations, but without the associated political risks and costs.

One of the defining characteristics of cyber warfare is its persistence across the spectrum of competition. Analytical models of cyber threat characterisation emphasise the

multidimensional and evolving nature of cyber risks, which often operate below the threshold of armed conflict (Robinson et al., 2013). This condition of "permanent competition" blurs the traditional distinction between war and peace and challenges established deterrence models.

Recent wars show how important cyber warfare is. In the war in Ukraine, cyber operations have been closely linked with other military actions, electronic warfare, and strategic communication campaigns. Cyberattacks against government institutions, energy infrastructure, and communication networks have sought to disrupt military coordination, erode public confidence, and weaken national resilience. Simultaneously, online information campaigns have sought to change how international audiences perceive the conflict. This shows that cyber warfare extends beyond the technological domain; it involves cognitive and political domains.

Cyber warfare also makes it much harder to maintain peace and prevent aggression. It is difficult to attribute cyberattacks with certainty, which weakens traditional deterrence models. These traditional models are based on clearly identifying aggressors and credible threats of retaliation. Therefore, the relatively low cost of online services means that a wide range of people and organisations, including smaller states, proxy groups, and non-state organisations, can now access the same disruptive capabilities previously available only to major powers. This diffusion of capabilities renders cyber operations more frequent, diverse, and unpredictable, increasing the risk of uncontrolled escalation and miscalculation.

But cyber operations have their own limitations. Cyberattacks can disrupt systems and put users under pressure. But they often need systemic preparation and may not always work. In recent wars, cyber capabilities alone do not usually decide the outcome. Instead, they help amplify the impact of other operations and achieve broader strategic objectives. Their most important feature is that they can change how operations are carried out, limit the enemy's actions, and influence political decisions.

Cyber warfare is now a central part of modern conflicts. It is now critical for countries to be good at using the internet. This helps them obtain useful information, carry out their activities effectively, and protect themselves. Therefore, it is not just a technical necessity, but a strategic imperative for all modern armed forces to have strong cyber defence capabilities.

4. CYBER DEFENCE AND INFORMATION SHARING

In today's world, it is not possible to have good cyber defence on its own. Cyber threats are complex, fast and international. This means they need to be addressed in a joined-up way that goes beyond individual military organisations or national borders. Therefore, cyber defence is now a shared effort between the armed forces, government organisations, intelligence agencies, private companies, and other countries. European security policy research likewise emphasises that effective cyber defence requires coordinated civil-military cooperation and structured

information exchange across institutions and member states (Trimintzios et al., 2017). The most important part of this plan is that countries share information about cyber threats.

Recent European threat assessments further underline the increasing sophistication and coordination of cyber campaigns targeting both civilian and military infrastructure (ENISA, 2025). These developments reinforce the necessity of structured information-sharing mechanisms across institutional and national boundaries.

Information sharing is a fundamental mechanism for detecting, analysing, and responding to cyber threats. The timely exchange of threat intelligence and mitigation measures enables earlier identification of malicious activity, recognition of coordinated campaigns, and prevention of potential damage. When stakeholders maintain shared situational awareness, they are better positioned to prevent subsequent incidents, disrupt malicious actors, and enhance overall network security.

Sharing information has many benefits, not just for protecting technology. If partners regularly and openly share information, it helps build trust and strengthen cooperation over time. This trust is vital for effective joint operations against cyber threats, enabling coordinated responses across the military, government and civilian sectors. Cyber threats often cross-national borders and target both civilian and military infrastructure, making it impossible for any one country to defend itself. Therefore, collective cooperation is required to keep the country safe.

Information sharing also helps to prevent crime. When enemies see that countries and organisations are working together to detect and respond to cyberattacks quickly, they think it is more dangerous and costly to launch an attack. Monitoring is made more difficult, situational awareness is reduced, and it is harder to work together to defend against attacks. This makes it less likely that operations will be successful.

However, there are still significant challenges in effectively sharing information. There are often worries about data protection, privacy, how to label sensitive information, and protecting sources. These worries often stop organisations from sharing important information. Therefore, differences in legal systems, working practices, and technical standards make it difficult for partners to work together. Therefore, it is critical to balance openness with safety online.

As war evolves in the digital age, it is increasingly important to have information-sharing structures that can adapt and remain strong. Effective defence against cyber threats requires integrating new technologies with organisational adaptation. Such integration enables flexible, trusted, and responsive cooperative arrangements. Information sharing constitutes not only a central component of cyber defence but also one of its most powerful enabling mechanisms.

5. INTEGRATION OF CYBER DEFENCE IN HYBRID WARFARE

Modern conflicts typically involve a combination of conventional military force, cyber operations, electronic warfare, psychological operations, disinformation campaigns, economic pressure, and political subversion. This multidomain character enables state and non-state actors to exploit vulnerabilities across several domains simultaneously, thereby amplifying operational effects while limiting escalation risks. Within this operational environment, cyber defence has become an essential component of contemporary warfare.

Hybrid warfare makes it hard to tell the difference between war and peace, civilians and the army, and the home country and other countries. Cyber operations are vital in that situation. Cyberattacks can cause all sorts of problems for the military, elections, and public trust in institutions. These actions often occur below the level of armed conflict, making it hard to identify who is responsible and to respond.

Combining cyber operations with other military activities makes them more effective. Cyberattacks can prepare the battlefield by damaging air defence systems, disabling communication networks, and confusing decision-makers before kinetic strikes. Concurrently, disinformation campaigns can influence public opinion, erode civic responsibility, and reduce willingness to engage in political action. Electronic warfare constitutes an additional component of this process. It can stop radar, navigation and sensor systems from working. All these tools work together to attack the enemy in a coordinated way, making it difficult for them to understand, decide, and act.

Recent conflicts show how important this combined approach is. In the war in Ukraine, cyber operations, information warfare and electronic attacks have been closely coordinated with conventional military campaigns. This has shaped the operational environment and influenced both domestic and international audiences. The conflict shows that cyber defence is about more than just protecting networks. It is also about protecting the way decisions are made in the country, maintaining societal stability, and ensuring the military is effective.

The military and civilian infrastructures are becoming increasingly interdependent, making cyber defence more important in hybrid warfare. Energy systems, transportation networks, healthcare services, financial institutions, and communication platforms are all possible targets. If they are disrupted, this could have a knock-on effect on society as a whole. Accordingly, defence against cyberattacks requires not only military measures but also the protection of critical national infrastructure and the safeguarding of the population.

In this environment, cyber defence is crucial to strategic resilience. It helps prevent enemies from winning easily, makes it easier to handle emergencies by keeping services running, and makes the country more secure by protecting the things modern society relies on. Therefore,

the success of hybrid warfare strategies depends on both offensive capabilities and strong, adaptable cyber defence systems.

6. ETHICAL AND LEGAL DIMENSIONS OF CYBER CONFLICT

The rapid growth of cyber capabilities in modern warfare has created significant ethical and legal problems that international frameworks are not well-equipped to address. Cyber conflict differs from other military operations because it occurs in a world of anonymity, uncertainty, and interconnected civilian and military systems. This makes it harder to apply the usual rules of international humanitarian law and the laws of armed conflict.

One of the central legal challenges in cyber warfare is attribution, namely the determination of responsibility for cyber operations. Establishing the origin of a cyberattack is often difficult because attackers can conceal their identities, use compromised systems as intermediaries, or route operations through infrastructure across multiple jurisdictions. This uncertainty complicates the assignment of state responsibility and weakens deterrence, as harmful conduct is less likely to be constrained without reliable evidence. The attribution problem also raises significant ethical concerns about miscalculation and escalation, as erroneous accusations may trigger unintended conflict.

Another important issue is the rules of distinction and proportionality. International humanitarian law says that those fighting in a war must not mix up military targets with civilian ones. It also says they must ensure any use of force is reasonable, given the expected military advantage. In the online world, however, military and civilian systems are often closely connected. If a cyberattack targets military command-and-control networks, it may also affect civilian communications, healthcare systems, or energy infrastructure. This could have severe and indirect consequences for civilians. It is very difficult to judge what is fair in these situations because it is often impossible to predict how long cyber effects will last and how bad they will be.

The idea of necessity makes cyber operations even more complicated. Cyber weapons may be designed to produce temporary, reversible, or non-lethal effects, which are sometimes regarded as preferable to kinetic force. But these same tools can spread problems across connected systems, leading to economic downturns, humanitarian crises, and long-term harm to society. There are no clear rules on what targets are acceptable and how to achieve them in cyberspace. This means there is a legal grey area that actors may exploit.

Ethical concerns intensify as cyber operations increasingly rely on automation and artificial intelligence. Systems that can detect, respond to, or even initiate their own cyber actions raise questions about who is in control, who is responsible, and what is right and wrong. When decisions are handed over to computer programs, it becomes harder to determine who is responsible if something goes wrong. This challenge is similar to broader debates about

autonomous weapons, but it is exacerbated in the online world because it moves fast and is difficult to understand.

The international community has made some progress in addressing these challenges, though it remains limited. International efforts to clarify legal norms in cyberspace include the work of the United Nations Group of Governmental Experts (UN GGE), which has affirmed that existing international law, including the UN Charter, applies to state conduct in cyberspace. Recent comparative studies of global cybersecurity governance further demonstrate that states adopt differing normative interpretations of responsibility and sovereignty in cyberspace, complicating the development of universally accepted rules (Gargiulo et al., 2024).

Additionally, the Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations provides a comprehensive, though non-binding, academic interpretation of how international humanitarian law principles apply to cyber activities (Schmitt, 2017). While these initiatives contribute to normative clarification, they remain constrained by divergent state interpretations and the absence of binding enforcement mechanisms.

In this context, strengthening the normative framework governing cyber conflict is essential for maintaining international stability. The development of clear rules, transparency among actors, and confidence-building measures can reduce the risk of misperception and escalation. Ultimately, the effectiveness of cyber defence strategies depends not solely on technological capability but also on their consistency with international law and established ethical principles.

CONCLUSION: A- STRATEGIC IMPLICATIONS AND FUTURE TRENDS

Cyber defence has become a structural pillar of modern deterrence and hybrid warfare. Its effectiveness depends not only on technological capability but also on institutional coordination, legal clarity, and international cooperation. Contemporary security assessments demonstrate that cyber resilience increasingly determines strategic credibility and alliance cohesion (ENISA, 2025; Kwan et al., 2025).

Future research should focus on developing measurable indicators of cyber resilience and on clarifying normative thresholds governing cyber operations in armed conflict. As digital interdependence deepens, cyber defence will remain central to national security, operational effectiveness, and strategic stability.

REFERENCES

- Balmuş, C., Cramar, I., & Cramar, A.-A. (2022). The impact of technology on warfare. *International Scientific Conference "Strategies XXI"*, 18(1). 171-178.
<https://doi.org/10.53477/2971-8813-22-20>
- Bhattacharjee, S. (2025, 23 June). *The evolution of modern warfare: How technology is transforming the rules of war*. DefenceXP.
<https://www.natstrat.org/articledetail/publications/the-evolution-of-modern-warfare-how-technology-is-transforming-the-rules-of-war-212.html>
- ENISA. (2025, August). *ENISA Cybersecurity threat landscape methodology*. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/sites/default/files/2025-08/ENISA%20CTL%20Methodology_Updated%20August%202025.pdf
- Gargiulo, P., Giovannelli, D., & Sciacovelli, A. L. (Eds.). (2024). Cybersecurity governance and normative frameworks: Non-Western countries and international organisations perspectives. *Editoriale Scientifica*. https://ccdcoe.org/uploads/2024/10/Cybersecurity-Governance-and-Normative-Frameworks_Non-Western-Countries-and-International-Organizations-Perspectives.pdf
- Schmitt, M. (Ed.). (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge University Press.
- Kwan, C., Gratzner, N., Podiņš, K., & Tolppa, M. (Eds.). (2025). *17th International Conference on Cyber Conflict: The next step*. CCDCOE Publications.
- Noorman, R. (2024, 27 March). *The return of the tactical crisis*. Modern War Institute, United States Military Academy at West Point. <https://mwi.westpoint.edu/the-return-of-the-tactical-crisis/>
- Robinson, N., Gribbon, L., Horvath, V., & Robertson, K. (2013). *Cyber-security threat characterisation: A rapid comparative analysis*. RAND Europe.
- Trimintzios, P., Chatzichristos, G., Portesi, S., Drogkaris, P., Palkmets, L., Liveri, D., & Dufkova, A. (2017). *Cybersecurity in the EU Common Security and Defence Policy (CSDP): Challenges and risks for the EU*. European Parliamentary Research Service. [https://www.europarl.europa.eu/thinktank/hr/document/EPRS_STU\(2017\)603175](https://www.europarl.europa.eu/thinktank/hr/document/EPRS_STU(2017)603175)

AI AS A FORCE MULTIPLIER FOR FUTURE INTELLIGENCE OPERATIONS: FROM COLLECTION SUPERIORITY TO DECISION ADVANTAGE IN WAR

Zrinko Petener¹, Damir Stručić², Nikolina Mokricki³

¹Information Systems Security Bureau

E-mail: zrinko.petener@outlook.com

² Croatian Military Academy "Dr. Franjo Tuđman"

E-mail: dastrucic@gmail.com

³Croatian Military Academy "Dr. Franjo Tuđman"

E-mail: nikolnavukovic92@hotmail.com

Abstract

Artificial Intelligence (AI) is becoming essential for navigating the complex threats of information-centric warfare - accelerating data collection, enhancing multidomain integration, and shortening the detection-to-decision cycle. This paper explores the potential of AI as a force multiplier in operational environments characterised by high tempo, deception, information saturation, and communication disruption.

Rather than replacing human analysts or commanders, AI is positioned as a means of augmenting human cognition and decision-making. It supports faster data triage, enables predictive analytics, and helps detect weak signals across both kinetic and non-kinetic domains. Nonetheless, human judgment remains indispensable - particularly in interpreting context, applying ethical frameworks, and exercising strategic discretion. The enduring role of Human Intelligence (HUMINT) is also emphasised: while core collection remains a human task, AI can support surrounding activities such as optimising tasking and prioritising potential sources. At the core of this study is a conceptual model defining intelligence effectiveness through three interrelated components: Collection Superiority, Fusion Superiority, and Decision Superiority. The paper considers how AI-enabled systems might assist distributed analytical teams when guided by clear operational intent and implemented within accountable governance structures. The study seeks to contribute to ongoing efforts to integrate AI responsibly into defence intelligence practice. It highlights key areas for further exploration, including trust calibration,

adversarial testing through red-teaming, oversight of model evolution, and performance metrics that prioritise operational relevance alongside technical accuracy.

Together, these reflections suggest that AI can enhance the adaptability of human–machine teams to the demands of modern conflict - while reinforcing, rather than displacing, the human foundation of military intelligence.

Keywords: artificial intelligence; force multiplier; information-centric warfare; intelligence; intelligence analysis;

INTRODUCTION AND PROBLEM STATEMENT

In recent years, AI has been widely discussed as a defining technology for modern intelligence and military operations. In an era where "data overload" is the norm and speed is a weapon, the primary challenge has shifted: it is no longer about how much information we can collect, but how quickly we can process and interpret it. Consequently, AI is being studied, discussed, and applied as a force multiplier in intelligence operations – a tool to increase the speed of data processing and intelligence production in support of decision-makers.

However, much of the current public debate focuses on high-level programs run by the largest and most technologically advanced organisations. Such studies offer valuable insights but may be of limited utility for organisations that struggle with fragmented data, insufficient digital infrastructure, lower workforce knowledge, or limited budgets. This leaves a significant analytical gap: we still do not fully understand how AI can realistically support intelligence work in less developed and under-resourced organisations without replacing human judgment, which remains the foundation of intelligence work.

This article attempts to fill this analytical gap by offering a practical framework for AI integration that augments human intelligence work without replacing it. The central question is simple: under what conditions does AI actually make an intelligence team more effective without fundamentally changing or restructuring how intelligence work is done?

The core argument here is that AI is most powerful when applied to data-intensive, repetitive tasks such as triage, pattern recognition, and cross-referencing vast datasets. It is less useful when a task requires deep context, ethical nuance, understanding of human interaction, or strategic deception. For most organisations, success will not come from a centralised overall digital revolution, but from an incremental, human-centred approach that uses AI to ease the cognitive burden on intelligence professionals.

1. THEORETICAL FRAMEWORK AND KEY CONCEPTS

1.1. Force multiplier

In military studies, a force multiplier is commonly understood as a factor or combination of factors – such as capability, technological advancement, training, tactics, etc. – that enables a force to achieve effects disproportionate to its size. In other words, a force multiplier enables existing forces or resources to achieve greater operational results without increasing manpower.

In the context of intelligence, a force multiplier is a capability that increases output, speed, and, most importantly, the quality of decision-making without requiring additional personnel. A force multiplier has to enable an intelligence organisation to process more data in less time, ensuring better, not just more, intelligence support to decision makers. This is especially relevant in contemporary intelligence, where the crucial challenge is not lack of data, but the inability to process, exploit, and transform it into usable intelligence at the necessary speed. An intelligence organisation may possess access to vast quantities of data and still fail to gain an advantage if it cannot convert that data into usable knowledge quickly enough. A capability that allows the same analytical team to triage far larger datasets, correlate more sources, detect patterns earlier, or support decision-making faster than before does produce a meaningful multiplier effect.

This article argues that AI can be a force multiplier in intelligence operations by enabling better intelligence support for decision-makers with the same amount of human effort, but with a different focus. AI can perform work-intensive tasks instead of humans, freeing limited human resources, such as time and attention, for use in other stages of the intelligence cycle. If applied to those tasks, AI can enable intelligence organisations to digest far more data than possible before, with the same human resources. While presenting arguments in favour of increased AI application in intelligence work, this article also emphasises the need for caution. AI, when applied as a force multiplier, does not eliminate the need for judgment, nor does it guarantee that increased data-processing capability will automatically produce better intelligence. The multiplier effect of AI is strongest where repetitive tasks that require speed, scale, and consistency are decisive, and weaker where intelligence value depends on interpretation, contextual understanding and human judgement. If intelligence organisations can identify such tasks and apply AI in these areas, it can have a truly multiplying effect – making humans more efficient, not replacing them.

1.2. The Intelligence cycle and intelligence disciplines

Despite criticism – which will be mentioned in this article – that the traditional intelligence cycle is outdated and not applicable anymore in the age of AI because of its linear nature, this article argues in favour of its continued usefulness for all those organisations that are not able or willing to introduce AI within an all-encompassing transformation of the way in which they

conduct their intelligence activities. The intelligence cycle remains a useful analytical framework because it divides intelligence work into recognisable and definable functions: direction, collection, processing, analysis, and dissemination. It is nothing new that in practice, these functions often overlap, interact, and feed back into one another. Intelligence work is rarely a neat sequence of steps and stages as the textbook model of the intelligence cycle suggests. But this is not specific to AI's age. The blurring of borders between the stages of the intelligence cycle has always been the reality of intelligence operations. Nevertheless, the intelligence cycle provides a clear framework for identifying where AI can influence the overall process and where it can be best applied as a force multiplier.

This article uses the intelligence cycle as its baseline because it provides a clear framework for comparing the potential relevance of AI across different stages of intelligence work. As mentioned, some authors argue that the traditional cycle is too rigid and linear for the realities of fast-moving, networked, and multidomain operations. There is merit in that critique, but abandoning the cycle altogether would make it harder to assess where AI contributes most, and where its usefulness is limited.

Using the cycle in this way also underscores an important point of this article. The article claims that, if applied prudently, AI doesn't require a complete replacement of existing intelligence structures. On the contrary, the central assumption is that, for many organisations, the more productive question is how to integrate AI into the existing intelligence cycle to improve performance without requiring immediate organisational redesign. Preserving the cycle as an analytical frame is therefore closely connected to the article's broader argument in favour of gradual step-by-step AI integration into intelligence operations.

The article also relies on the taxonomy of the major intelligence disciplines – HUMINT, OSINT, IMINT/GEOINT, SIGINT, and MASINT- to assess the different levels of AI's applicability as a force multiplier across these disciplines. They involve different collection logic, data types, tradecraft, and relationships between humans and technology. Therefore, AI does not affect all intelligence disciplines equally. A technology that performs well in image analysis may be useless for source handling. A system that reduces burdens in signal analysis may be largely irrelevant to rapport-building or credibility assessment in HUMINT. An assessment of AI as a force multiplier must make these distinctions to move beyond abstract claims about intelligence in general and examine the specific functions and constraints of individual disciplines.

1.3. Augmentation versus automation

As this article argues for AI applications to augment the human workforce in intelligence, it is necessary to define the term and distinguish between augmentation and automation, which are similar but distinct. Automation means delegating a task to a machine with minimal or no human intervention. Augmentation, by contrast, refers to the use of technology to strengthen

human performance without removing the human from the loop. In intelligence work, this distinction is crucial. Some tasks in the intelligence cycle may truly be automated – i.e. automatic transcription, translation, image analysis, pattern or anomaly detection, etc.

Nevertheless, intelligence is also a process of evaluating reliability, interpreting evidence, understanding opponents' intentions, managing ambiguity, and ultimately providing intelligence support for decisions that may have strategic consequences. In these areas, the human role remains crucial. This article argues that AI cannot replace humans in these areas, but is most valuable when it reduces the burden of tasks that consume time and attention. By doing this, AI enables humans to allocate their limited time and attention to tasks that require analytical judgment and human responsibility in decision-making. AI can free analysts and collectors to spend more time on evaluation, synthesis, and strategic interpretation.

Where AI performs repetitive, high-volume, and technically bounded tasks, automation may be appropriate and highly valuable. Where intelligence value depends on judgment, ambiguity, credibility assessment, and contextual understanding, AI-augmented human judgment is required. This leads us to the crucial thesis of this article: AI can serve as a true force multiplier when it is integrated as an instrument of human-machine cooperation, rather than imagined as a high-tech replacement for the human role in intelligence.

2. METHODOLOGY AND RESEARCH DESIGN

This article is a qualitative study based on analysis and interpretation of publicly available doctrinal, strategic, and scholarly sources. It examines how official doctrine, policy documents, and selected scholarly studies describe the likely utility, limits, and conditions of AI use in intelligence work. The article is a conceptual analysis rather than an empirical, technical performance study.

The article relies on publicly available documents by intelligence and defence institutions, especially ODNI, NGA, GAO, the U.S. Army, the U.S. Marine Corps, the Joint Chiefs of Staff, the UK Ministry of Defence, and NATO-related material. Alongside these sources, the article also cites selected academic and policy documents relevant to specific intelligence functions.

The article uses the intelligence cycle as an analytical framework, then compares the roles of AI across the five major intelligence disciplines: HUMINT, OSINT, IMINT/GEOINT, SIGINT, and MASINT. By doing this, the article doesn't aim to explain AI's technological capabilities, but to show where AI is most useful at the stages of the intelligence cycle and how this usefulness differs across intelligence disciplines. In its comparative chapter on "AI and the INTs," the central argument that AI is a potential force multiplier for the augmented human workforce is tested against the specifics of each discipline.

To organise the argument, the article uses the triad of Collection Superiority, Fusion Superiority, and Decision Superiority. This triad is not presented as an official doctrinal model but rather as an analytical framework for evaluating where AI may generate practical advantage within the traditional intelligence cycle.

The article also develops the idea of a "modest approach" to AI integration. This concept is derived from the analysis of doctrinal and policy documents, which emphasise augmentation rather than overall automation, institutional and digital readiness, and step-by-step adoption over all-encompassing transformation.

The article intends to synthesise doctrine and literature into a coherent argument about how AI should be understood in intelligence work: not as a universal substitute for human professionals, but as a force multiplier that enables human analysts to focus on higher-order tasks.

3. THE RISE OF AI IN AN INFORMATION-CENTRIC ENVIRONMENT

The proceedings of the 2023 NATO Multidomain Operations (MDO) Conference in Copenhagen, Denmark, organised by NATO Allied Command Transformation, state that *"in the contemporary security landscape, conflicts are not confined to the battlefield alone; they extend into the realms of politics, economics, and information. Therefore, achieving strategic objectives necessitates a synchronised approach that integrates military actions seamlessly with diplomatic initiatives, economic measures and informational strategies. MDO becomes not just a military strategy but a holistic framework that aligns military operations with broader national and international objectives, fostering a unified response to multifaceted challenges"* (NATO Allied Command Transformation 2024, 22). In this environment, the character of warfare is changing rapidly, driven by the pace and ever-growing volume of information and technological change. Intelligence support for such operations, in which the volume of data that needs to be collected, analysed, and utilised to support decision-making is increasingly demanding, mandates the application of technological innovations to enhance its effectiveness. The integration of Artificial Intelligence (AI) into the intelligence cycle presents itself as such a tool of technological innovation that could act as a force multiplier for intelligence organisations, increasing their efficiency much beyond their numerical and organisational size and strength. The U.S. Intelligence Community defines AI as a "machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations or decisions influencing real or virtual environments. AI systems use machine- and human-based inputs to (A) perceive real and virtual environments; (B) abstract such perceptions into models through analysis in an automated manner; and (C) use model inference to formulate options for information or action" (Office of the Director of National Intelligence 2019, p. 3).

The realm of intelligence is by no means the only area for AI application in defence matters. As early as 2020. – which considering the pace of the evolution of AI seems ages ago – a U.S. Congressional Research Service report found applications for AI in defense in the areas of Intelligence, Surveillance, and Reconnaissance (ISR), Logistics, Cyberspace Operations, Information Operations and "Deep Fakes", Command and Control, Semiautonomous and Autonomous Vehicles, and Lethal Autonomous Weapon Systems (LAWS) (Sayler, 2020). The report concludes that "AI is expected to be particularly useful in intelligence due to the large data sets available for analysis" and argues that AI is conceptualised not as a substitute for human agency, but as a critical force multiplier designed to enhance the "detection-to-decision cycle" across multidomain environments. The report specifically mentions the example of project Maven, *"which is intended to incorporate computer vision and AI algorithms into intelligence collection cells that would comb through footage from uninhabited aerial vehicles and automatically identify hostile activity for targeting. In this capacity, AI is intended to automate the work of human analysts who currently spend hours sifting through drone footage for actionable information, potentially freeing analysts to make more efficient and timely decisions based on the data"* (Sayler, 2020, p. 10). Project Maven was established in 2017 with the objective of delivering flagship AI capabilities to the Department of Defense. Project Maven transitioned to NGA in 2023, where it became a Program of Record called Maven. Maven provides the cloud infrastructure, software capabilities, and AI that powers CDAO's Combined Joint All-Domain Command and Control (CJADC2) initiatives (Palantir, 2024). The cited statement from Palantir's investor website shows the evolution of Project Maven from the initial goal stated in the Congressional Research Service's report and the application of AI technologies in defence over the past years. The fact that Project Maven was established as early as 2017 highlights the maturity and evolution of AI integration into defence and military systems at all levels, especially in the realm of intelligence.

Other studies also advocate the necessity of profound change and the adaptation of existing intelligence systems to the contemporary operational environment, and the effective integration of AI into such systems as true force multipliers. One such study questions the applicability of the traditional intelligence cycle in current circumstances, arguing that "the traditional linear intelligence cycle, with its hierarchical bureaucracy, has limitations in fast-moving environments. This study proposes designing the intelligence cycle as a network in which nodes communicate constantly, in multiple directions, and in real time. In this model, the decision-maker or originator of the intelligence request actively participates in the process alongside the operator or analyst, unlike in the traditional linear cycle. The study recognises that a compelling illustration of adaptive intelligence in practice is Israel's use of AI-enabled fusion centres. During the May 2021 Gaza conflict, a senior colonel from Unit 8200 revealed that their team employed a form of 'data-science magic powder' to uncover previously unknown operatives by analysing social links and patterns. Tens of thousands of potential targets were flagged as Hamas or Islamic Jihad affiliates, dramatically enhancing the speed and precision of targeting decisions (Muhić, 2025). In the United States, the AIM Initiative – A Strategy for Augmenting Intelligence Using Machines (Office of the Director of National Intelligence,

2019) provides a framework for a long-term investment and transformation strategy, focusing on "AAA" technologies: Artificial Intelligence, process Automation, and IC officer Augmentation. The Initiative's Vision statement states that it seeks to secure and maintain a strategic competitive information advantage for the U.S. Intelligence Community through focused development and rapid adoption of AAA technologies. The Initiative aimed to guide the IC in accelerating its digital and analytics transformation by identifying mission use cases, building a coherent data ecosystem, acquiring appropriate AI tools, reshaping the workforce, adapting workflows, and changing the culture. The statement concludes that IC investments in cloud technology and data services have paved the road to harness the power of unique data collections and insights to provide a decision advantage at machine speed (Office of the Director of National Intelligence, 2019, p. 2). The AIM initiative recognises that the pace of data generation has long since exceeded the collective human understanding, necessitating a "whole-of-government" approach to leveraging private-sector investments in machine learning and natural language processing. As an illustration of the information overflow necessitating the adoption of new technologies, the Initiative cites the director of the U.S. National Geospatial-Intelligence Agency who has publicly estimated that at the current, accelerating pace of collection, the NGA would need over 8 million imagery analysts by 2037 to process all imagery data (Office of the Director of National Intelligence, 2019, p. 1). Another example states that in 2020, the U.S. military operated over 11,000 drones, with each one recording "more than three NFL seasons worth" of high-definition footage each day. However, the department lacks sufficient personnel and an adequate system for analysing data and deriving actionable intelligence. (Sayer 2020; 29).

Practical applications of these doctrines are evident in projects such as the aforementioned Project Maven, an Algorithmic Warfare Cross-Functional Team, which have conducted projects by applying AI to help a workforce that was significantly overwhelmed because of the incoming data, which included millions of hours of video, allowing human analysts to focus on higher-level strategic assessment rather than manual data sifting (Cho et al., 2020, p. 3).

Neither arguing the merits of such conclusions nor questioning the possibility of advanced AI applications in intelligence and military C2 systems, this article seeks to step back and examine the applicability of AI in less mature, less technologically advanced systems or organisations. While such initiatives and some scholars advocate a total shift in how intelligence operations are conducted, this article argues that, for many organisations, the most effective path is the AI-driven optimisation of the existing, proven traditional cycle. It examines the utility of AI application in all stages of the traditional intelligence cycle in the five major intelligence disciplines, as a tool for augmenting human effectiveness and output by reducing the possibility of human error and performing work-intensive tasks, thus reducing the workload on human intelligence collectors and analysts, while keeping the human always in the loop – acting as a true force multiplier by augmenting the effectiveness of humans, not replacing them. Faced with challenges of information overload and, at the same time, the need to keep up with the high pace of technology development, many defense and intelligence organisation, even entire

countries, might be overwhelmed by the complexity of initiatives such as the Maven Project, the enormous investments the AIM initiative calls for, and the comprehensive transformation of the way intelligence organisations conduct their work other analysis advocate. Therefore, many organisations will need to adopt an approach that incorporates AI augmentation into existing workflows and tasks, primarily to reinforce their workforce by handling work-intensive tasks and enabling collectors and analysts to focus their limited time and energy on high-level analysis, rather than processing ever-growing amounts of raw data. This more modest approach can still empower intelligence organisations and serve as a real force multiplier in achieving intelligence advantage or superiority in collection, analysis, and decision-making.

4. THE TRIAD OF SUPERIORITY

As stated before, the most demanding task of modern intelligence organisations is not to collect more data – in most cases, they are already overwhelmed by the volume of available data – but to achieve sufficient speed and precision in turning that data into actionable intelligence and foresight. To analyse the impact of AI as a force multiplier within the traditional intelligence cycle, this study uses a taxonomy of three interrelated pillars: Collection Superiority, Fusion Superiority, and Decision Superiority. These components represent the stages of the "detection-to-decision cycle," in which AI acts as a cognitive assistant to humans, ensuring timely data processing, the availability of intelligence, and the quality of the forecasts provided to human analysts.

4.1. Collection Superiority

Collection superiority, for the purposes of this article, is understood as the capability to acquire relevant data across multidomain environments while filtering out the "noise" of information overload. In the contemporary landscape, the primary constraint is not a lack of data but its "abundance"; as the ODNI observes, the "pace of data generation has long ago exceeded our collective human understanding" (Office of the Director of National Intelligence 2019, 1). AI-enabled collection systems provide the computational power needed to automate the processing of large datasets. By applying AI to the collection process, organisations can manage the volume of data to be collected, analysed, and utilised without overwhelming the human workforce.

4.2. Fusion Superiority

Fusion Superiority is the ability to integrate different, often contradictory data sets into a single, coherent *Common Operational Picture*. In official joint doctrine, fusion is defined as "a deliberate and consistent process of collecting and examining information from all available sources and intelligence disciplines to derive as complete an assessment as possible of detected activity" (Joint Chiefs of Staff 2022a, II-12). AI serves as a critical force multiplier of this pillar,

as it "drives operating efficiency and effectiveness, by enhancing decision-making, reducing cognitive load, and improving outcomes in repetitive and complex analytical tasks" (British Army, 2023, p. 7).

4.3. Decision Superiority

Decision Superiority is the ability to use information to gain an advantage by enabling decision makers – military commanders or leaders at the strategic level alike – to make faster and better-informed decisions than an opponent. To prevail in conflict, a commander's "decision and execution cycles must be consistently faster than the adversary's and be based on better information" (Joint Chiefs of Staff 2013, V-1). This "decision advantage" allows decision makers to "leverage the velocity, precision, and reliability of compute power, without sacrificing the ingenuity and flexibility of human intelligence" (British Army, 2023, p. 8). Effective implementation of AI will increase decision advantage by improving the speed and precision of decision-making. AI enables humans to exploit information rather than process low-level data. Humans cannot compete with the computing speed required to process the volume of data which is now available. This volume will continue to grow, further underscoring the necessity of AI. (British Army 2023, p. 8).

Together, these three pillars form a mutually reinforcing system. Improved collection provides the basis and raw data for accurate analysis and intelligence fusion, which, in turn, informs the operational picture required for superior decision-making. By maintaining the traditional structure of the intelligence cycle, this model ensures that AI augments human collectors, analysts, and decision-makers. At the same time, it ensures that critical human judgment remains relevant at every stage of the process.

5. THE *MODEST APPROACH* TO AI INTEGRATION IN INTELLIGENCE ORGANISATIONS

For many intelligence organisations, the most realistic and effective near-term path to AI adoption is not a total reconstruction, but rather the step-by-step integration of AI into existing workflows. This is especially applicable in areas where AI can reduce repetitive tasks, accelerate data triage, improve correlation analysis, and help transform raw data into processed, usable information. That conclusion is strongly supported by official U.S. and allied strategy documents, which repeatedly frame AI as a means of augmenting rather than displacing intelligence personnel. ODNI's AIM Initiative explicitly states that AI, automation, and augmentation technologies should "amplify the effectiveness of our workforce." At the same time, the UK Defence AI Strategy says AI should "reduce burdens and focus human talents on higher value functions" requiring "ingenuity, contextual thinking and judgement" (ODNI 2019, p. 3; UK Ministry of Defence 2022, p. 7).

Such a modest approach to AI integration arises especially from the reality of the institutions in question. Not every organisation possesses the institutional maturity, the technological foundation, such as digitalised, structured data, and the necessary workforce and skill sets to make a sudden leap into AI transformation. ODNI's AIM Initiative states that AI is not a substitute for an "enduring, secure, standardised, and measurable" digital infrastructure, and the GAO reports that the U.S. Department of Defense needs to complete additional steps to define and identify its AI workforce before being able to assess" its current workforce or forecast future requirements accurately. The UK Defence AI Strategy likewise warns of a "severe skills deficit" and says Defence data remain too often "stove-piped, badly curated, undervalued and even discarded" (ODNI 2019, p. 5; GAO 2024, pp. 28, 33; UK Ministry of Defence 2022, pp. 19-25).

While publicly available empirical data on AI integration in intelligence organisations and metrics on achieved improvements are – for obvious reasons – scarce, the consulted literature on the subject shows that AI is especially useful where intelligence work is dominated by size, repetitiveness, translation, tagging, object detection, anomaly screening, and pre-analytic structuring. The ODNI's OSINT strategy rates AI and generative AI as useful for identifying common themes and summarising large bodies of text, while warning that inaccuracies and hallucinations remain a source of concern and require mitigation. NGA's technology guidance identifies computer vision, data integration, automated tagging, and analytic suggestion services as central GEOINT needs where AI excels. (ODNI 2024, pp. 7–8; NGA 2020, pp. 12–13; IAEA 2022, pp. 95–97).

In this modest approach to AI integration, the human role remains central, especially in validation, interpretation, deception assessment, source criticism, and strategic judgment. ODNI's strategy states that the IC's job is to analyse data, connect disparate datasets, apply context, infer meaning, and make analytic judgments. HUMINT doctrine shows that rapport, cultural understanding, motivation assessment, and judgment of truthfulness remain exclusively human. The UK Defence AI Strategy makes the same distinction in different words: machines are good at "doing things right" quickly, whereas people are good at "doing the right things" in complex and incomplete situations. The stated viewpoints support AI as a force multiplier, but not as an omnipotent substitute for tradecraft (ODNI 2019, p. 4; FM 2-22.3 2006, pp. 139–142, 172; UK Ministry of Defence 2022, p. 16).

5.1. Defining the Modest Approach

In this article, the "modest approach" is understood as a model of AI integration characterised by incremental adoption, selective application to precisely defined tasks, continuous human oversight, and alignment with institutional capabilities and readiness. It does not, in principle, reject more ambitious forms of AI transformation, but it assumes that many intelligence organisations face issues with data quality, insufficient digital infrastructure, limited human workforce capabilities, and governance challenges. Considering these conditions, a force-

multiplying effect is most likely achieved when AI is integrated into specific functions, rather than attempting a complete and immediate redesign of an organisation.

For the use in this article, the modest approach should be understood as the incremental, selective, and human-centred integration of AI into existing intelligence workflows and the traditional intelligence cycle. In this regard, AI should be particularly applicable to functions such as processing, exploitation, translation, correlation, visualisation, and analytic support. The *modest approach* is not an official term in doctrine or an official document. It is a term coined to describe research findings from various official documents that advocate AI augmentation of existing systems, organisations, and workflows, rather than a sudden, total AI transformation. ODNI's AIM Initiative urges the community to "be big but be practical" and, in the short term, "adopt commercial and open-source narrow AI solutions." The UK Defence AI Strategy introduces a distinction between "AI Now" and "AI Next," stating that many immediate gains will come from proven techniques delivered rapidly to users, while more transformative capabilities are a separate and riskier path (ODNI 2019, pp. 3, 5; UK Ministry of Defence 2022, pp. 31–33). In simpler terms, the modest approach this article advocates calls for integrating AI into intelligence work where it is most applicable, most needed, and most efficient than human work. It can thus reduce the time and increase the accuracy of the workflow that transforms raw data into informed decisions. Most importantly, it calls for integrating AI without requiring a wholesale transformation of such organisations. Intelligence organisations need to identify tasks where AI can outperform humans, relieving humans of information overload and repetitive, menial labour.

5.2. Why a Modest Approach?

While the introduction of an all-encompassing AI system that could supercharge intelligence organisations might seem tempting, a modest approach to this ambition is necessary due to a common mismatch between AI ambition and institutional readiness. ODNI states that AI activities depend on a secure, standardised digital infrastructure and data ecosystem. The UK Defence AI Strategy says organisations must assess whether they have accessible, structured, and exploitable data; scalable computing; and models that are fit for purpose and can be updated quickly enough. Where these preconditions are not met, radical AI transformation is impossible and a potentially dangerous undertaking for the organisation (ODNI 2019, p. 5; UK Ministry of Defence 2022, p. 18).

The same rationale must be applied to limitations arising from the workforce's skills and capabilities in accepting and integrating AI into existing workflows. GAO reports that the National Security Commission on Artificial Intelligence identified DoD's AI talent deficit as one of the greatest impediments to DoD's AI readiness. The UK strategy similarly warns of a severe skills deficit and states that effective AI teams require data scientists, machine-learning engineers, and AI analysts. A modest approach is therefore not only technologically prudent but also organizationally realistic: it aligns adoption with the actual pace at which institutions

can build skills, management structures, and AI literacy (GAO 2024, pp. 4, 28, 32–33; UK Ministry of Defence 2022, pp. 19–21).

Other studies also seem to advocate a modest approach. The 2024 DoD Responsible AI Strategy states that a "balanced approach" is needed to deliver near-term impact while providing time for manpower and financial resourcing, increasing literacy, and decreasing adoption barriers (DoD, 2024, p. 18).

5.3. Mini-Case Study: Project SPOTTER and the Operational Logic of the Modest Approach

A useful example of a modest approach to AI integration is the UK Ministry of Defence's Project SPOTTER. In the 2022 *Defence Artificial Intelligence Strategy*, project SPOTTER is described as a machine-learning capability designed to "support and enhance imagery analysts' output" by automatically detecting and identifying objects in classified satellite imagery. According to the same document, the system allows locations to be monitored continuously for changes in activity, thereby enabling workload prioritisation and improving the efficiency and timeliness of image intelligence reporting. The strategy also notes that the application was built around a scalable, modular architecture tailored to analysts' requirements, rather than being presented as a stand-alone replacement for analysts (UK Ministry of Defence 2022, 42–43).

The 2024 *Defence AI Playbook* further explains the operational application of this capability. It explains that imagery analysis relies on trained analysts who must examine large numbers of images in order to identify relevant objects and changes. The AI-enabled solution is described as an imagery analysis capability that uses machine learning for object detection, prioritises images for the analyst, and automatically flags images with objects of interest or significant changes in areas of interest. Most importantly, the document states that the analyst remains responsible for interpreting what is seen and delivering actionable insight. This is precisely the logic of the modest approach in this article: AI is applied first to a restricted, data-intensive, and reviewable task within an existing workflow, while human judgment remains central to interpretation and decision support (UK Ministry of Defence 2024, 8).

For this article, the significance of SPOTTER lies in demonstrating that a selective, workflow-oriented, and human-supervised model of AI adoption has already been applied in practice. Judging by the publicly available data on project Spotter, AI implementation in this example didn't require a comprehensive transformation of the intelligence process, but rather the targeted insertion of AI into an existing work process where it could be most useful as an assistant to human analysts. The available information also doesn't imply that AI was implemented as a substitute for human judgment and decision-making. Instead, it shows how AI can function as a force multiplier by reducing the burden of scale, accelerating initial exploitation, and allowing analysts to focus on higher-value interpretation. In that sense, SPOTTER provides a strong practical illustration of the modest approach

5.4. First Use Cases

The described step-by-step, modest approach to AI integration in intelligence operations identifies several use cases where AI could deliver immediate, significant gains. Such use cases are predominantly found in data processing and exploitation. ODNI explicitly states that the U.S. intelligence community is applying AI, machine learning, and human-language technologies, and that generative AI can help identify themes and summarise large amounts of text. In IMINT/GEOINT, NGA identifies computer vision, automated tagging, data integration, and analytical suggestion services as concrete areas of need. In SIGINT, Marine Corps doctrine states that integrating collection, processing, and exploitation near the point of intercept reduces latency and helps users more quickly assess relevance. In activities that could be classified as MASINT, the IAEA says AI can increase efficiency in classification, pattern-finding, outlier detection, and sensor-fusion tasks (ODNI 2024, pp. 7–8; NGA 2020, pp. 12–13; MCRP 2-10A.1 2022, pp. 15–16; IAEA 2022, pp. 15, 95–97).

HUMINT, by its very nature, only partially fits the use-case requirements for AI integration. Publicly available HUMINT doctrine recognises source screening support, analytic support for source selection, digital reporting, cross-source corroboration, and visual analytic tools such as association matrices and link diagrams. It does not in any way support replacing the HUMINT collector's role. The modest approach is therefore especially well-suited to HUMINT's analytical tasks, such as screening, triage, translation, registry support, and corroboration. Source handling itself remains exclusively in the human domain (MCRP 2-10A.2 2025, pp. 14–15, 51–53; FM 2-22.3 2006, pp. 179–183).

Doctrine also suggests that early use cases should focus on tasks where the benefits are immediate, and the costs of error are more manageable. The UK Defence AI Strategy says the organisation should "learn by doing," undertaking simpler projects to deliver rapid gains and refrain from taking risks in more complex activities. It also recommends proven private-sector techniques, using Commercial Off-The-Shelf solutions where appropriate, delegating local responsibility for suitable "AI Now" solutions, and keeping more transformative "AI Next" work separate. That is perhaps the clearest official endorsement of the practical logic behind the modest approach (UK Ministry of Defence 2022, pp. 31–34).

5.5. The Human Analyst Under the Modest Approach

The human analyst does not lose his role in the modest approach; his role changes. Analysts spend less time on manual sorting and take on greater responsibility for validating machine outputs, assessing reliability, applying context, integrating across sources, and detecting deception. ODNI's ethics requirements call for human judgment and accountability, and for maintaining a critical perspective on the accuracy of AI output and on how errors are detected and communicated. The UK Defence AI Strategy makes a similar point: machines are efficient at processing large datasets, but people remain better at evaluating "complex, incomplete,

rapidly changing information" guided by values and judgment (ODNI 2020, pp. 1–2; UK Ministry of Defence 2022, p. 16).

This is especially visible in HUMINT activities. FM 2-22.3 requires collectors to build rapport, assess motivation, interpret cultural and nonverbal cues, and judge truthfulness. The same manual warns that excessive technical involvement can damage rapport and reduce the collector's ability to manage the encounter with the HUMINT source. A modest approach is therefore not only technologically prudent, but also advisable in the context of HUMINT tradecraft. It supports the idea that analysts and collectors should spend less time on low-value routine tasks – that can be better performed by machines – and more time on the parts of intelligence work that are still dominated by humans (FM 2-22.3 2006, pp. 139–142, 172; UK Ministry of Defence 2022, p. 7).

6. RISKS OF AI IMPLEMENTATION

As stated in many of the citations above, all doctrinal documents and studies on AI recognise the inherent risks of implementing AI in intelligence activities. While partially mitigated by the described modest approach, such risks persist even if an organisation refrains from premature leaps into all-out AI transformation.

The first risk is false confidence based on insufficient performance metrics. A RAND study shows that accuracy can be a poor metric when false negatives are much more costly than false positives, and ODNI's ethics framework requires attention to representativeness, error tolerance, and the consequences of inaccurate outputs. Measuring success only by technical precision or speed does not guarantee better intelligence (Ish et al., 2021, pp. 70–71; ODNI 2020, p. 2).

The second risk is tradecraft erosion through overreliance and amplified bias. OSINT research shows that both human and machine systems can over-select what is already visible. In other words, AI tools can reproduce distorted historical patterns or encourage analysts to defer too often to machine-produced outputs. This is why ODNI's governance and ethics documents insist on documenting limitations, model inventories, risk management, and oversight mechanisms rather than simply endorsing rapid adoption (McDermott, Koenig, and Murray 2021, p. 6; ODNI 2025, pp. 5–6).

The third risk is organisational fragmentation when an organisation follows a slower, more careful, step-by-step approach to AI implementation. Incremental adoption of AI tools, if not handled systematically, can result in disconnected local tools, incompatible workflows, or weakly governed experimentation. The UK strategy recognises this risk and tries to mitigate it by combining delegated local responsibility for "AI Now" solutions with central technical standards. ODNI as well requires governance structures, inventories, and approval processes, and the IAEA warns that limited false alarms and insufficient maturity constrain safe

operational use. (UK Ministry of Defence 2022, pp. 31–33; ODNI 2025, pp. 1–2, 5–6; IAEA 2022, pp. 95–97).

7. AI AND THE INTS

Artificial intelligence does not affect all disciplines of intelligence in the same way. It is strongest in areas where intelligence is burdened by data volume, repetitive comparison, translation, classification, anomaly screening, and correlation. It is weakest where collection and interpretation depend on human interaction, contextual judgment, or the authentication of ambiguous and potentially deceptive information. In all stages of the intelligence cycle, AI therefore seems most valuable in processing and exploitation, somewhat less useful in analysis, and least acceptable as a substitute for the human role in direction, source handling, and final decision-making. Official U.S. intelligence strategy supports these conclusions by presenting AI as a means to augment human expertise, connect disparate datasets, and accelerate work at machine speed, while preserving the human responsibility to apply context, infer meaning, and make judgments. (ODNI 2019, pp. 4–5, 7–8, 20–21).

The following chapter compares the applicability of AI in the basic intelligence disciplines – the INTs (HUMINT, OSINT, IMINT/GEOINT, SIGINT, and MASINT) in the traditional intelligence cycle: direction and tasking, collection, processing and exploitation, analysis, and dissemination/decision support. It seeks to test the central argument of this article that AI doesn't replace intelligence professionals but rather can act as a force multiplier by reducing cognitive burden, accelerating triage, improving cross-source correlation, and helping analysts focus scarce time and attention on the most relevant tasks and datasets.

7.1. AI in HUMINT

HUMINT is the clearest case in which AI should be understood as support, rather than a substitution for human activity. Marine Corps doctrine, for example, defines HUMINT as intelligence derived from information collected and provided by human sources, and stresses that HUMINT usually takes longer than technical collection because relationships with sources must be developed over time. The same doctrine argues that HUMINT can collect unique human perspectives that technical methods may not reach. Army HUMINT doctrine reinforces this point by treating screening as the systematic evaluation of individuals to determine whether they can meet intelligence requirements or match a source profile. Both cited sources suggest that AI's most realistic role in HUMINT lies in source screening, lead prioritisation, report triage, registry management, optical character recognition, translation, and cross-source correlation, rather than in the core interpersonal act of collection itself. (MCRP 2-10A.2 2025, pp. 14–15; FM 2-22.3 2006, p. 109; ODNI 2022, pp. 27–28).

The strongest case for AI utilisation in HUMINT concerns analysis and reporting support for HUMINT operations. Marine Corps doctrine states that intelligence analysis supports

CI/HUMINT source selection by identifying suitable individuals based on placement, access, or expertise, and it notes the use of visual analytic tools such as association matrices and link diagrams. HUMINT analysis also involves evaluating HUMINT reporting, assessing source credibility, and prioritising collection requirements. These are exactly the kinds of structured, repetitive, data-handling functions to which AI can plausibly add value. (MCRP 2-10A.2 2025, pp. 51–53; NAVMC 3500.100A 2013, p. 60; FM 2-22.3 22006, pp.179–183).

By contrast, the core task of HUMINT – collecting information through human interactions – remains unquestionably in the exclusive human realm. Army HUMINT doctrine judges that rapport-building, motivation assessment, cultural understanding, and the judgment of truthfulness are central skills a HUMINT collector must possess. It also warns that increased participation by analysts or technical experts may improve technical reliability but can reduce rapport and degrade the collector's ability to control the exchange and judge whether a source is telling the truth. A recent CIA *Studies in Intelligence* essay emphasises this point by arguing that AI-driven fabrication and disinformation will make HUMINT's role in establishing and testing source reliability more important, not less. All this supports a narrow but important conclusion: AI may strengthen the supporting functions to HUMINT collection activities, but rapport, recruitment, motivation assessment, contextual judgment, and source validation remain exclusively human. (FM 2-22.3 2006, pp. 139–142, 172; *Studies in Intelligence*, 2026, p. 9).

7.2. AI in OSINT

OSINT is the discipline in which AI's near-term utility is most obvious. The dominant problem in this discipline is not access to data, but the management of its almost unlimited volume, high speed of change, heterogeneity, and volatility. ODNI's current OSINT strategy defines OSINT as intelligence derived exclusively from publicly or commercially available information. The same strategy states that the U.S. Intelligence Community is already pioneering new uses of AI, machine learning, and human-language technologies for OSINT, and that generative AI is useful for identifying common themes or patterns and for quickly summarising large volumes of text. A RAND OSINT study complements this by showing that the OSINT cycle now depends heavily on acquisition, translation, aggregation, classification, authentication, contextualisation, social-network analysis, and geospatial analysis. (ODNI 2024, pp. 4–8; Williams and Blum 2018, pp. 25–32, 40–45).

At the same time, OSINT also illustrates that gains in the speed and volume of data handled are not equivalent to intelligence effectiveness. RAND's study shows that exploitation requires authentication, credibility evaluation, and contextualisation, while social-media data can be partial, unstable, multilingual, slang-heavy, and unrepresentative. The ODNI strategy itself warns that OSINT procedures must mitigate the risks of inaccuracies and hallucinations. Additional public literature highlights two further problems: First, digital open-source investigations are vulnerable to both human and machine bias, especially when highly visible

incidents distort attention. Second, AI-generated deepfakes create a more complex information environment in which AI is both the source of the challenge (by creating deepfake content) and the solution to the problem at the same time. AI is a genuine force multiplier in OSINT, accelerating collection, language handling, clustering, summarisation, and certain forms of network or geospatial analysis, but it becomes hazardous when automated outputs are treated as validated evidence. (ODNI 2024, pp. 5, 7–8; Williams and Blum 2018, pp. 28–32; McDermott, Koenig, and Murray 2021, p. 6; Helmus 2022, pp. 1, 9–10).

7.3. AI in IMINT/GEOINT

IMINT/GEOINT presents one of the strongest cases for AI as a force multiplier. The discipline is already organised around the exploitation and analysis of large visual and geospatial datasets. Doctrine defines GEOINT as the exploitation and analysis of imagery and geospatial information, and it recognises automated, semi-automated, and manual procedures in GEOINT processing. It identifies change detection, tracking, and battle-damage assessment as core GEOINT functions. NGA's technology priorities describe AI as a necessary force multiplier for advanced analytics and modelling, and state that computer vision is intended to detect, extract, and attribute features and objects in imagery and video. The GAO's discussion of Project Maven provides an example by describing a deployed computer-vision capability that analyses large volumes of ISR full-motion video to identify objects of interest. (JP 2-03 2017, pp. 8, 15, 58; NGA 2020, pp. 12–13; GAO 22022, p.15).

Here, too, however, limitations to AI intelligence production are pointed out. NGA's guidance emphasises the issues of high confidence under varying conditions, risk assessment, and contextualisation. Other research points out that object detection in imagery is difficult due to viewpoint variation, occlusion, clutter, illumination effects, and the explosive growth in image volume. Change detection faces challenges from noise, registration errors, and false alarms, even when deep learning has improved performance. This research concludes that AI is especially effective in IMINT/GEOINT exploitation, tagging, cueing, tracking, and change detection, but the human function remains vital for interpreting context, detecting deception, and assessing the relevance of collected IMINT/GEOINT information. (NGA 2020, pp. 12–13; NGA 2024, p. 1; and Han 2016, p. 1; Cheng et al. 2023, pp. 1, 15).

7.4. AI in SIGINT

In SIGINT, AI augmentation also seems highly applicable, as its doctrine already highlights processing and exploitation as central bottlenecks. Marine Corps doctrine states that the SIGINT process includes planning and direction, collection, processing and exploitation, analysis and production, dissemination and integration, and evaluation and feedback. The same doctrine notes that integrating collection, processing, and exploitation near the point of interception reduces latency and increases the speed at which the relevance of the collected data is assessed. The Army intelligence concept adds that future forces must transform raw and

processed data into actionable information at speeds beyond human capability. Official ODNI strategy reinforces this by identifying multimodal AI and spoken-language processing as priority areas to augment intelligence work. (MCRP 2-10A.1 2022, pp. 13–16, 86, 88; AFC Pam 71-20-3 2020, pp. 34, 57–60; ODNI 2019, pp. 20–21).

The strongest applications of AI in SIGINT, therefore, lie in signal classification, triage, anomaly detection, multilingual transcription support, and cross-modal fusion. But the limits are equally important. Public research shows that speech recognition systems perform poorly on accented speech and that voice processing and automatic speech recognition systems are vulnerable to adversarial attacks and manipulation. Marine Corps doctrine also makes clear that finished SIGINT analysis requires integrating traffic analysis, cryptanalysis, linguistic analysis, signal analysis, ELINT analysis, and radio geolocation into a fused product. This again shows that faster preprocessing is not the same as understanding final intelligence. The consulted studies support AI as a force multiplier in SIGINT support, but not as a replacement for human interpretation of intent, code words, cultural nuance, or strategic significance. (MCRP 2-10A.1 2022, p. 88; Hinsvark et al. 2021, p. 1; Abdullah et al. 2021, pp. 1–2, 13; Shi et al. 2019, pp. 1, 9).

7.5. AI in MASINT

MASINT might be a specific case, since it is entirely based on technically collected measurements of the physical characteristics (electro-optical, radar, radio-frequency, materials, nuclear radiation, and geophysical, etc.) of objects and events. ODNI defines MASINT as an intelligence discipline based on capturing and measuring the intrinsic characteristics (measurements, signatures, etc.) of objects and events, calling it the "INT of science" and stating that it is comparatively difficult to deceive. The Army intelligence concept explains why AI may play an important role in this discipline: it highlights the need to process high-volume, multimodal data, represent uncertainty, identify components and signals across modalities, optimise sensor subsets, and turn time-series data into actionable information. (ODNI 2022, pp. 1–7; AFC Pam 71-20-3 2020, pp. 57–60, 69, 102).

Public intelligence-specific research on MASINT is limited, so findings from other technical domains must be used. In this context, an IAEA report offers some insight, stating that AI can increase efficiency in safeguards tasks involving data classification, pattern detection, and outlier identification, including work on gamma-ray spectra and anomalous nuclear sources. The same source also warns that the technology is not mature enough to make autonomous decisions and that false alarms damage trust, while false negatives can have grave consequences. (IAEA 2022, pp. 15, 95–97).

7.6. Synthesis of findings

The review of AI's applicability across the five major intelligence disciplines notes that AI does not contribute to all disciplines in the same way and doesn't have the same effect at every stage of the intelligence cycle. Its strongest force-multiplier effects occur where intelligence work is dominated by scale, repetition, and data processing. Its contribution becomes weaker, where intelligence depends on interpersonal access, contextual interpretation, source validation, deception assessment, and broader strategic judgment. The comparative picture is summarised in Table 1.

Table 1

Comparative applicability of artificial intelligence across major intelligence disciplines

Intelligence discipline	Best AI use	Main value	Main limitation	Required human role
HUMINT	screening, triage, translation, report support, corroboration	workload reduction and support to source selection	rapport, motivation assessment, and truthfulness judgment cannot be automated	source handling, credibility assessment, contextual judgment
OSINT	clustering, summarisation, translation, entity extraction, network support	scale and speed in handling very large volumes of open information	verification problems, bias, hallucinations, deepfakes	authentication, contextualisation, source criticism
IMINT/GEOINT	object detection, tagging, tracking, change detection, cueing	faster exploitation of large imagery flows	false alarms, contextual ambiguity, vulnerability to deception and environmental variation	interpretation, relevance assessment, deception detection
SIGINT	classification, triage, anomaly detection, transcription, translation support	latency reduction and faster first-pass exploitation	adversarial manipulation, accented speech, dialect variation, difficulty of meaning extraction	fused interpretation, linguistic nuance, intent assessment
MASINT	anomaly detection, pattern recognition, sensor fusion, spectral support	pattern discovery in complex multimodal data	false negatives, false positives, limited public evidence, high sensitivity to validation	scientific judgment, operational interpretation, assessment of significance

Three conclusions arise from this comparison:

First, AI is a real force multiplier in data-rich, repetitive, and pre-analytic tasks. This is most visible in processing and exploitation, where AI can reduce cognitive burden, increase throughput, and convert large volumes of raw material into structured information for human review.

Second, AI's force-multiplier effect is weaker when tasks depend more on interpersonal judgment, credibility assessment, contextual interpretation, and deception detection. This explains why HUMINT is the least likely discipline in which AI might replace human roles and why, even in highly technical disciplines, AI should be regarded as an assistant rather than an autonomous decision-maker.

Third, institutional readiness strongly influences whether AI improves only speed and throughput or also the overall quality of intelligence support for decision makers. In organisations that lack structured data, digital infrastructure, and skilled personnel, the practical benefits of AI are more limited and require a step-by-step implementation approach.

What, then, does this chapter demonstrate for the article's central research question? It demonstrates that AI can indeed function as a force multiplier in the traditional intelligence cycle and across major intelligence disciplines, but not equally at all stages or across all disciplines. Its greatest utility is to assist intelligence organisations in coping with the problem of too much data, too little time, and too few human analysts to process it all manually. But the chapter also demonstrates that greater data volume processed is not identical to better intelligence. AI can accelerate collection support, exploitation, and preliminary analysis, yet the final value of intelligence still depends on human interpretation, judgment, and accountability. Therefore, the conclusion should be that AI will not replace intelligence professionals, but it can significantly strengthen them when integrated into a human-machine partnership and applied where its advantages are real.

Summarising the findings of the previous chapter on the applicability of AI in the stages of the intelligence cycle, the following conclusions present themselves:

In terms of direction and tasking, AI performs best as a tool to support the recognition and prioritisation of intelligence requirements. It can help identify data gaps, rank requirements, optimise collection management, and structure access to relevant data. It has to be emphasised that AI should be regarded only as a tool to aid these activities, but never as a substitute for human authority over requirements.

In conclusion, the differences between the intelligence disciplines are most underlined. HUMINT remains fundamentally human, while OSINT, IMINT/GEOINT, SIGINT, and MASINT present much better use cases for AI-assisted or even AI-conducted collection. However, even in these disciplines, various studies warn of the inherent risks that overreliance on technology, in general, and on AI, in particular, could pose.

The strongest force-multiplier effects appear in processing and exploitation. OSINT benefits from AI-enabled translation, clustering, summarisation, and classification. IMINT/GEOINT benefits from object detection, tagging, tracking, and change detection. SIGINT benefits from

signal classification, noise reduction, triage, and transcription/translation support. MASINT benefits from anomaly screening, spectral interpretation support, and sensor-fusion assistance. HUMINT also benefits here, but only in a much more limited sense. The strongest case for AI in data processing and exploitation can be made: AI reduces workload and helps convert large raw datasets into structured information for human review.

In analysis, AI remains valuable but still limited. Official U.S. strategy repeatedly describes the analyst's role as connecting datasets, applying context, inferring meaning, and making judgments. All findings support AI as an analytical assistant, not a substitute for intelligence tradecraft.

All these findings emphasise the difference between increased throughput and actual intelligence effectiveness. AI increases throughput: it can process more open-source content, screen more imagery, sort more signals, and flag more anomalies than humans. But the claim that AI independently improves the final quality of intelligence in a fully operational sense remains questionable, especially when credibility, deception, ambiguity, and broader context need to be assessed. AI is most applicable as a force multiplier for attention management and pre-analytic structuring, not for autonomous judgment.

Across the five major intelligence disciplines, the most defensible conclusion is that AI functions best as an augmenting technology rather than a substitute for human intelligence work. Its strongest force-multiplier effects appear in data-rich disciplines and stages of the cycle – especially OSINT, IMINT/GEOINT, SIGINT, and MASINT. HUMINT is a separate case. AI can offer support functions, but the core collection activity remains human.

CONCLUSION

The central conclusion of this article is that AI can function as a genuine force multiplier in intelligence operations, but only under specific conditions. Its greatest value lies in accelerating high-volume, repetitive, and pre-analytic tasks, especially in processing and exploitation, while leaving judgment-based functions to human professionals. Consequently, the utility of AI varies across the intelligence disciplines: it is strongest in OSINT, IMINT/GEOINT, SIGINT, and MASINT, and most limited in HUMINT, where rapport, credibility assessment, and contextual judgment remain crucially human roles. For many organisations, the most realistic path is not total AI transformation but a modest approach based on step-by-step implementation of AI for very specific tasks, while maintaining continuous human oversight and control of the intelligence cycle. Artificial intelligence has great potential to act as a force multiplier in future intelligence operations, but its greatest value lies in augmenting human work rather than replacing it. In contemporary information-centric operational environments, defined by speed, scale, and information overload, the challenge is not simply to collect more data but to transform enormous volumes of data into usable intelligence quickly enough to support superior decisions. AI is highly relevant to that challenge because it can accelerate this process

and improve the speed with which information moves through the intelligence cycle. In that sense, AI can make a significant contribution to collection superiority, fusion superiority, and ultimately decision superiority.

At the same time, this contribution is highly dependent on context. AI does not affect all intelligence disciplines equally, and increased throughput is not the same as better intelligence. AI may help organisations process more information, but it does not automatically produce a better understanding. The final value of intelligence still depends on human judgment and interpretation. This is most visible in HUMINT but also applies to all other intelligence disciplines.

Organisational context is also highly important in assessing the use of AI in intelligence operations and organisations. Not all organisations possess the same level of digital infrastructure, structured data, organisational capacity or workforce skills to adopt AI rapidly. For that reason, the authors argue in favour of a modest approach to AI integration. Rather than advocating a total transformation of intelligence organisations or abandoning the traditional intelligence cycle, many organisations will benefit more from incremental, selective, and human-centred adoption. The most effective path is often to optimise existing workflows by inserting AI where it delivers the greatest benefit: processing, exploitation, triage, analytical support, and cross-domain fusion. This approach is not against technical innovation; it is a way to align ambition with institutional reality.

Finally, responsible AI integration requires more than technical capability. It requires trust calibration, clear oversight, appropriate performance metrics, red-teaming, documentation of limitations, and attention to bias, opacity, false confidence, and dependence on automation. The true test of AI in intelligence is therefore not whether it can imitate human analytical behaviour in narrow tasks, but whether it can improve operational relevance without eroding intelligence quality or accountability.

AI can become a genuine force multiplier for future intelligence operations, but only if it is integrated into a disciplined human-machine partnership. Its role is not to displace the human foundation of intelligence, but to strengthen it. By reducing cognitive burden, accelerating fusion, and straightening the path from collection to decision, it can create a significant advantage. The future of intelligence will belong not to machines alone, nor to unchanged human systems, but to organisations capable of combining technological power with human reasoning.

AI is the one analyst every intelligence chief would like to have on the night shift: it does not blink, does not yawn, does not need coffee, cigarettes, or a trip to the bathroom, and its eyesight does not deteriorate after twenty years of staring at dim screens, grainy imagery, and unreadable spreadsheets. It does not complain about the volume of reporting, the quality of the source packet, or the fact that someone has again sent a mislabelled file in the wrong format. It will

patiently scan, sort, compare, flag, and correlate at machine speed without losing concentration. Yet for all these superhuman virtues, it still lacks one very human quality that intelligence ultimately depends on: judgment. That is why the ideal future is not an intelligence service run by sleepless machines, but one in which human analysts can leave the blinking, scrolling, and data-sifting to their tireless digital colleague. At the same time, they focus on what matters most - understanding, meaning, and decision.

REFERENCES

- Abdullah, H., Warren, K., Bindschaedler, V., Papernot, N., & Traynor, P. (2020). *SoK: The faults in our ASRs: An overview of attacks against automatic speech recognition and speaker identification systems*. arXiv. <https://doi.org/10.48550/arXiv.2007.06622>
- Cheng, G., & Han, J. (2016). A survey on object detection in optical remote sensing images. *ISPRS Journal of Photogrammetry and Remote Sensing*, 117, 11–28.
- Cheng, G., Huang, Y., Li, X., Lyu, S., Xu, Z., Zhao, H., Zhao, Q., & Xiang, S. (2024). *Change detection methods for remote sensing in the last decade: A comprehensive review*. *Remote Sensing*, 16(13), 2355. <https://doi.org/10.3390/rs16132355>
- CIA Center for the Study of Intelligence. (2026). *Studies in intelligence* (Vol. 70, No. 1, extracts, March 2026). <https://www.cia.gov/resources/csi/static/UNCLASSIFIED-Extracts-Studies-in-Intelligence-70-1-Mar2026.pdf>
- Headquarters, Department of the Army. (2006). *FM 2-22.3: Human intelligence collector operations*. <https://irp.fas.org/doddir/army/fm2-22-3.pdf>
- Helmus, T. C. (2022). *Artificial intelligence, deepfakes, and disinformation: A primer*. RAND Corporation. <https://www.rand.org/pubs/perspectives/PEA1043-1.html>
- Hinsvark, A., Delworth, N., Del Rio, M., McNamara, Q., Dong, J., Westerman, R., Huang, M., Palakapilly, J., Drexler, J., Pirkin, I., Bhandari, N., & Jette, M. (2021). *Accented speech recognition: A survey*. arXiv. <https://doi.org/10.48550/arXiv.2104.10747>
- International Atomic Energy Agency. (2022). *Artificial intelligence for accelerating nuclear applications, science and technology, and safeguards and verification*. <https://www-pub.iaea.org/MTCD/Publications/PDF/ART-INTweb.pdf>
- Ish, D., et al. (2021). *Evaluating the effectiveness of artificial intelligence systems in intelligence analysis*. RAND Corporation. https://www.rand.org/pubs/research_reports/RRA464-1.html
- Joint Chiefs of Staff. (2017). *Joint publication 2-03: Geospatial intelligence in joint operations*. https://irp.fas.org/doddir/dod/jp2_03.pdf
- McDermott, Y., Koenig, A., & Murray, D. (2021). Open source information's blind spot: Human and machine bias in international criminal investigations. *Journal of International Criminal Justice*, 19(1), 85–105.
- National Geospatial-Intelligence Agency. (2020). *NGA tech focus areas*. https://www.nga.mil/news/NGA_Tech_Focus_Areas_chart_path_for_geospatial_tec.htm
- National Geospatial-Intelligence Agency. (2024). *NGA launches GEOINT-specific artificial intelligence model accreditation pilot*. https://www.nga.mil/news/NGA_Launches_GEOINT-specific_Artificial_Intelligen.html

- Office of the Director of National Intelligence. (2019). *The AIM initiative: A strategy for augmenting intelligence using machines*.
<https://www.dni.gov/files/ODNI/documents/AIM-Strategy.pdf>
- Office of the Director of National Intelligence. (2020). *Artificial intelligence ethics framework for the intelligence community*.
https://www.intelligence.gov/assets/documents/pdf/ai/ai-ethics-framework-for-the-ic-1_0.pdf
- Office of the Director of National Intelligence. (2021). *MASINT primer*.
https://www.dni.gov/files/ODNI/documents/21-113_MASINT_Primer__2022.pdf
- Office of the Director of National Intelligence. (2024). *The INT of first resort: Unlocking the value of OSINT: The IC OSINT strategy 2024–2026*.
https://www.dni.gov/files/ODNI/documents/IC_OSINT_Strategy.pdf
- Office of the Director of National Intelligence. (2025). *Intelligence community directive 505: Artificial intelligence*. <https://www.dni.gov/files/documents/ICD/ICD-505-Artificial-Intelligence.pdf>
- Palantir. (2024, September 20). Palantir expands Maven Smart System AI/ML capabilities to military services. *Palantir Technologies Investor Relations*.
<https://investors.palantir.com/news-details/2024/Palantir-Expands-Maven-Smart-System-AI/ML-Capabilities-to-Military-Services/>
- United States Department of Defense. (2024). *Responsible artificial intelligence strategy and implementation pathway*. <https://media.defense.gov/2024/Oct/26/2003571790/-1/-1/0/2024-06-RAI-STRATEGY-IMPLEMENTATION-PATHWAY.PDF>
- U.S. Army Futures Command. (2020). *AFC pamphlet 71-20-3: Army concept for intelligence 2028*.
https://www.army.mil/article/242182/army_futures_command_concept_for_intelligence_2028
- U.S. Government Accountability Office. (2022). *Artificial intelligence: Status of developing and acquiring capabilities for weapon systems* (GAO-22-104765).
<https://www.gao.gov/products/gao-22-104765>
- U.S. Government Accountability Office. (2024). *Artificial intelligence: Actions needed to improve DOD's workforce management* (GAO-24-105645).
<https://www.gao.gov/products/gao-24-105645>
- United States Marine Corps. (2013). *NAVMC 3500.100A: Intelligence training and readiness manual*. https://www.marines.mil/portals/1/publications/navmc_3500.100a_2.pdf
- United States Marine Corps. (2022). *MCRP 2-10A.1: Signals intelligence*.
[https://www.marines.mil/Portals/1/Publications/MCRP%202-10A.1%20\(SECURED\).pdf?ver=eMRBwMdOdqN2bMGFMCnxTQ%3d%3d](https://www.marines.mil/Portals/1/Publications/MCRP%202-10A.1%20(SECURED).pdf?ver=eMRBwMdOdqN2bMGFMCnxTQ%3d%3d)

- United States Marine Corps. (2025). *MCRP 2-10A.2: Counterintelligence and human intelligence*. [https://www.marines.mil/Portals/1/Publications/MCRP%202-10A.2%20\(SECURED\).pdf?ver=NgVh3ByQV9uNRbF3RnJQxA%3D%3D](https://www.marines.mil/Portals/1/Publications/MCRP%202-10A.2%20(SECURED).pdf?ver=NgVh3ByQV9uNRbF3RnJQxA%3D%3D)
- UK Ministry of Defence. (2022). *Defence artificial intelligence strategy*. <https://www.gov.uk/government/publications/defence-artificial-intelligence-strategy>
- UK Ministry of Defence. (2024). *The Defence AI Playbook*. https://assets.publishing.service.gov.uk/media/65bb75fa21f73f0014e0ba51/Defence_AI_Playbook.pdf
- Williams, H. J., & Blum, I. (2018). *Defining second generation open source intelligence (OSINT) for the defense enterprise*. RAND Corporation. https://www.rand.org/pubs/research_reports/RR1964.html

ARTIFICIAL INTELLIGENCE AS A DISRUPTIVE TECHNOLOGY IN THE DESIGN OF NOVEL CHEMICAL AND BIOLOGICAL WEAPONS

Ante Vučemilović

Dr Franjo Tuđman Croatian Defense Academy, Ilica 256b, 10000 Zagreb, Croatia

E-mail: ante.vucemilovic1969@gmail.com

ORCID: <https://orcid.org/0009-0009-7825-2666>

Abstract

Disruptive technologies are “the force multiplier” most valued and sought after today across all five domains of modern warfare. They can overturn the course of warfare regardless of numerical advantage or unit equipment and significantly shape the theatre of military operations. The contribution of such technologies to warfare is not new; throughout history, they have strongly influenced the course and outcome of war. Artificial intelligence (AI) is generally considered a disruptive technology, as its tools and algorithms have enabled new forms of human activity and the design of various products and services, and it has entered all fields of science and human endeavour. Given the contemporary trajectory of global society, which compels the integration of various technologies, AI has also found its place in a range of dual-use technologies whose services and products can be applied to both beneficial and harmful purposes. The fusion of AI with dual-use technologies in the life sciences, such as molecular biology methods and core chemistry (synthetic chemistry), yields powerful capabilities for developing a range of products, from “smart drugs” to chemical and biological weapons. This review paper covers dual-use technologies that support the development of chemical and biological weapons and enhance their capabilities through AI.

The aim (objective) of this paper is to review and analyse key technological pathways by which artificial intelligence enhances dual-use capabilities in molecular biology and synthetic chemistry, and to highlight their potential security implications for the development of new biological and chemical weapons.

The contribution of this review paper is exclusively humanitarian, as it aims to raise awareness among society and the scientific community of the potential consequences of such activities.

Keywords: artificial intelligence; biological weapons; chemical weapons; disruptive technologies; dual-use technologies

INTRODUCTION

Disruptive technologies profoundly and radically transform business processes and human activities. Throughout human history, they have left a significant imprint and often anticipated humanity's future trajectory. A prominent illustration of this impact is the evolution of methods and modes of warfare. Today, disruptive technologies represent the key value driver - “the force multiplier” - most highly regarded and sought after across all five domains of contemporary warfare: land, maritime (sea), air, space, and cyberspace. Artificial intelligence (AI) is unquestionably classified as a disruptive technology. In its military and defence-related applications, AI has found widespread use across a broad spectrum of operational needs, including rapid analysis, sorting, and filtering of intelligence data, support for training simulations, and enhancement of cyber capabilities. Given the inherently integrative nature of AI technologies, which allows them to be combined with a wide range of other technological platforms, AI has also become increasingly embedded in life sciences applications. These include personalised approaches to diagnostics and therapy, as well as applications in synthetic chemistry that support clinical pharmacology in the discovery and development of so-called “smart drugs”. Conversely, all of the aforementioned technologies may also be misused for harmful and destructive purposes, potentially posing serious risks to human health and ecosystems. Such adverse outcomes may arise from inadequate process oversight, a lack of transparent and well-defined AI algorithms, insufficiently trained personnel, or the deliberate creation and deployment of expertise driven by unethical or inhumane intentions (Anyanwu et al., 2024; Mukherji & Oudenaarden, 2009; Russell & Norvig, 2022; Tugui & Zelinschi, 2024).

Methods of molecular biology and synthetic chemistry are among the most prominent examples of the rapid advancement of science and technology. From the perspective of the Biological and Toxin Weapons Convention (BTWC) and the Chemical Weapons Convention (CWC), these methods and technologies may also be employed for military purposes, namely in the development and production of weapons of mass destruction (Millett, 2010; DiEuliis & Giordano, 2018; Trump et al., 2023; Warmbrod et al., 2020).

The control of the use of the aforementioned methods could not be achieved solely through the establishment of international conventions; therefore, it became necessary to introduce, at the operational level, concepts and mechanisms capable of addressing this issue, most notably the framework of *dual-use* technology (Ashcheulova & Ambrosova, 2021; Beard et al., 2023).

The term *dual-use technology* refers to technologies that have legitimate civilian or scientific applications but may be misused for harmful purposes. In the life sciences, this concept

encompasses the development of biological weapons or other products derived from molecular biology methods that may adversely affect human health or the ecosystem, whether intentional or unintentional (Ashcheulova & Ambrosova, 2021; Novossiolova & Perkins, 2021; DiEuliis & Giordano, 2018).

In synthetic chemistry, this concept refers to the synthesis of chemical warfare agents as defined in the Chemical Weapons Convention (CWC) schedules, as well as their weaponisation and use for mass destruction. The integration of artificial intelligence with dual-use life sciences technologies - such as molecular biology and core chemistry (synthetic chemistry) can enable powerful capabilities for developing chemical and biological weapons.

The scope of this review encompasses dual-use technologies relevant to the acquisition of chemical and biological weapons, as well as to the enhancement of these capabilities through artificial intelligence. The aim of this paper is to provide an overview and analysis of the most recent, realistically attainable capabilities arising from the convergence of AI with contemporary methods of molecular biology and synthetic chemistry, including newly designed products that may serve as novel chemical and biological weapons.

1. MOLECULAR BIOLOGY METHODS, DUAL-USE RESEARCH OF CONCERN (DURC), AND CYBERBIOSECURITY

Contemporary methods of molecular biology have converged into three principal technological trajectories: the reading, writing, and editing of DNA. By combining Next-Generation Sequencing (NGS) methodologies with the Polymerase Chain Reaction (PCR) technique, it is now possible to read vast DNA sequences with high throughput and precision. The Clustered Regularly Interspaced Short Palindromic Repeats (CRISPR) approach, particularly when integrated with synthetic biology, has enabled significant advances in DNA editing. In contrast, synthetic biology primarily focuses on DNA manipulation through the design and construction of novel biological constructs. Artificial intelligence tools and algorithms support all three trajectories. The scientific benefits of DNA reading, writing, and editing for humans and society at large have a direct impact across five major domains of the life sciences: immunology, neuroscience, reproductive technologies, animal and plant agriculture, and infectious diseases. However, within these same areas of research, a range of ethical, legal, and security concerns has emerged, including apprehension that advances in these fields could give rise to novel forms of biological weapons with effects that differ from - and may be potentially more harmful than - those observed in the past (Beard et al., 2023; Li et al., 2023; Mao et al., 2021; Redman et al., 2016; Warmbrod et al., 2020).

To enable more effective oversight and clearer delineation of intentions, products, and knowledge-based services in the life sciences, the concept of *Dual Use Research of Concern* (DURC) was introduced in 2015. DURC defines a category of research from which products, scientific services, and technologies may potentially arise that, if misused, could cause harm

to humans or the environment. This concept is continuously active and subject to revision, serving to minimise the potential destructive misuse of biomedical research while simultaneously enhancing awareness, as well as moral and ethical responsibility within the scientific community (Ashcheulova & Ambrosova, 2021; Beard et al., 2023; Guraiib et al., 2024; Moritz, 2022).

Internet-based technologies and tools that have provided substantial support for beneficial research have simultaneously given rise to various forms of criminal activity. The implementation of legal frameworks that rely primarily on security risk assessments and general guidelines has proven insufficient to achieve satisfactory outcomes. Consequently, criminology - through its examination of criminal perspectives and behaviours - has contributed to the life sciences by informing the design of more effective security measures and supporting efforts to prevent and mitigate criminal activities (Elgabry, 2023).

From a biosafety perspective, these systems are vulnerable primarily because the DNA molecule itself functions as an information-bearing medium. The stages of DNA creation, manipulation, processing, and analysis are therefore exposed to potential criminal attacks. The operational threat matrix is analogous to that observed in conventional information technology and computing systems. As an information medium, DNA can encode or store malicious code, enabling the introduction of “contaminated” DNA sequences that function analogously to computer viruses or worms. Such sequences may remotely compromise interconnected systems and networks. This risk arises, for example, when sequencing processes are targeted using synthetically designed DNA - potentially generated with the assistance of artificial intelligence - that contains embedded malicious code capable of exploiting software vulnerabilities. Once such synthetic DNA is sequenced using next-generation sequencing (NGS) technologies and the resulting data are processed, the malicious code may be executed as an application, thereby compromising the computational systems used for sequence analysis (Elgabry, 2023; Liu et al., 2024; Shankar et al., 2024).

Cyberbiosecurity encompasses a comprehensive set of protective measures and is based on a multidisciplinary approach that integrates capabilities in cybersecurity engineering, physical security and privacy, infrastructure resilience, and security psychology (Mueler, 2020).

Cyberbiosecurity is based on the premise that cyber-biological attacks are conceptually similar to conventional cyber-attacks. However, they are constrained by the use of DNA as the underlying medium for information. Accordingly, the core measures implemented within cyberbiosecurity include: (1) security auditing and regular software updating; (2) verification of the authenticity and integrity of software packages; (3) protection of DNA sequencing samples throughout the entire workflow, from collection to sequencing; and (4) assessment of whether synthetic sequences could be decoded into malicious code prior to and during synthesis. In addition, oversight of DNA synthesis processes must be implemented to prevent the generation of DNA sequences that could enable the production of pathogenic organisms,

chimeric constructs, toxins, or other components that could subsequently be misused as biological weapons (Lyu, 2024; Shankar et al., 2024).

2. DESIGN OF NOVEL BIOLOGICAL WEAPONS USING MOLECULAR BIOLOGY METHODS ENHANCED BY AI

The rapid development of molecular biology methods, all of which are dual-use and disruptive, has shaped the design of new biological weapons. The focus of the new generation of biological weapons is primarily on developing methods and tools for the *gain-of-function* of a given (micro)organism. While *gain of function* may serve beneficial purposes, these same methods and tools can be used to “weaponise” benign natural microorganisms through various chimeric modifications of peptide, nucleotide, or combined origin, thereby transforming them into biological weapons (Beard et al., 2023; Berche, 2023; Sandbrink & Koblenz, 2022).

The gain-of-function capability is not theoretical but has been experimentally demonstrated as routine in potentially epidemic pathogens, such as avian influenza, Myxovirus influenzae and SARS and MERS coronaviruses. The origin of SARS-CoV-2 cannot yet be definitively classified as natural or artificial. Some observations support the possibility of this virus being artificially created. Specifically, the primary isolates are genetically highly homogeneous, differing by only two nucleotides, with no evidence of adaptive mutations. In addition, the main virulence factor, the Spike protein, contains a furin cleavage site, which has not been observed in any other known sarbecovirus. From a scientific perspective, it is also notable that, unlike the SARS and MERS epidemics, no intermediate host has been identified to date (Berche, 2023; Beard et al., 2023; Novossiolova & Perkins, 2021; Vennis et al., 2021).

The broader framework of biological weapons design extends beyond pathogenic microorganisms and encompasses all molecular-genetic research involving human cells, embryos, fetuses, adult humans, plants, and animals. The challenge lies in the lack of consensus within the scientific community regarding the scope and direction of such research, as even exploratory or non-targeted studies and experiments may yield highly concerning results, products, or organisms whose harmful effects could impact human populations and ecosystems (Beard et al., 2023; Guraiib et al., 2024; Kropf, 2024; Trump et al., 2023; Uhlenhaut et al., 2013).

2.1 Clustered Regularly Interspaced Short Palindromic Repeats (CRISPR)

CRISPR-Cas9 is a precisely designed laboratory method for editing DNA, RNA, or proteins that fundamentally “mimics” a natural bacterial genome-editing mechanism using the Cas9 endonuclease, which cleaves both DNA strands to initiate repair. Post-binding repair can proceed via two pathways: (1) non-homologous end joining, typically resulting in random insertions or deletions of DNA, or (2) homology-directed repair, in which a homologous

DNA sequence is used as a repair template. Homology-directed repair enables precise modifications, making it highly suitable for laboratory manipulations (Beljouw & Brouns, 2024; Redman et al., 2016).

In addition to CRISPR–Cas systems that target DNA or RNA, the capabilities of molecular engineering have been extended to proteins through CRISPR-associated proteases, termed Craspases, which, upon activation by a target RNA, cleave host proteins to induce various cellular effects (Beljouw & Brouns, 2024). CRISPR-controlled proteases are ideal candidates for molecular applications, including biotechnological uses such as molecular diagnostics, targeted protein cleavage, and bacterial detection (Beljouw & Brouns, 2024; Jiang & Doudna, 2017; Selvam et al., 2022). The capabilities of the *CRISPR-Cas9* system in gene correction and repair have been utilised in biomedical applications to modify sequences of the human genome at mutated loci, which may result in hereditary diseases such as muscular dystrophy, thalassemia, or the development of various cancers (Farokhi et al., 2024; Ito et al., 2024; Tabibian et al., 2024; Zhan et al., 2019).

On the other hand, regarding the integration of “gene knockouts” in individuals with cognitive impairment, autism, schizophrenia, or bipolar disorder - where the KCTD13 gene, which has undesirable effects, is suppressed via a gene knockout through genetic reengineering of iPS cells - the implications are different. Such a procedure could be fully classified as a *dual-use* application, as critical regions of the human genome could be intentionally disrupted to induce disorders or diseases (Kropf, 2024).

Concerns raised within the scientific community regarding these dual-use procedures centre on precision and the potential for off-target effects arising from population-level gene shifts, which could harm not only the individual but also the ecosystem (Jiang & Doudna, 2017; Farokhi et al., 2024). Moreover, a far greater concern is the engineering or editing of the human germline for the purpose of obtaining targeted traits in individuals, such as enhanced cognitive functions, athletic performance, or abilities relevant to the most demanding human activities, including those pertinent to the conduct of military operations (Farokhi et al., 2024; Mir Gani et al., 2022; DiEuliis & Giordano, 2018). Despite warnings from the scientific community, the method has already been used to engineer embryonic genomes, resulting in twin girls known as the CRISPR babies (Mir Gani et al., 2022; Cyranosky, 2019).

2.2 Next-generation Sequencing (NGS) in Nucleic Acid Amplification Technologies (NAAT)

Next-generation sequencing (NGS) is a technology used for rapid, efficient DNA sequencing. The technical workflow of NGS includes DNA fragmentation, library preparation, massively parallel sequencing, bioinformatic analysis, and variant interpretation. Quantitative analysis is performed using quantitative PCR (qPCR), in which the amplification process is monitored by measuring fluorescent signals to quantify DNA accumulation in real time. The final step is

massively parallel sequencing, which can be carried out using, for example, flow-cell-based sequencers such as the Illumina NGS sequencer or chip-based sequencers such as the Ion Torrent NGS sequencer (Qin, 2019; Kumar et al., 2019).

Analysis of large numbers of sequences can be performed in a very short time using AI algorithms and tools (Kumar et al., 2019; Nafea et al., 2024; Qin, 2019; Rodino & Simner, 2024; Stenzinger et al., 2024). One of the key outputs of the NGS methodology is the reading and comparison of different variants or mutations. These capabilities can yield critical bioinformatic data that may subsequently be misused for harmful purposes, for example, in the development of race- or ethnicity-specific weapons. For this reason, NGS is justifiably classified as a dual-use technology (Beard et al., 2023). The coupling of CRISPR and NGS methods results in a powerful technology for generating *gain-of-function* pathogenicity and thereby facilitating the creation of biological weapons (Beard et al., 2023; Berche, 2023).

Nucleic acid amplification technologies (NATTs) fundamentally consist of PCR-based and isothermal amplification methods. Depending on the target (DNA or RNA), various variants of this technology are used, including Loop-mediated Isothermal Amplification (LAMP), Recombinase Polymerase Amplification (RPA), Rolling Circle Amplification (RCA), Strand Displacement Amplification (SDA), and Nucleic Acid Sequence-Based Amplification (NASBA). NATTs play an important role in nucleic acid analysis, similar to NGS, and have multiple applications in infectious diseases, tumour aetiology and diagnosis, human genetic disease diagnosis, and the implementation of personalised therapeutics. Limitations of NATTs include false-positive and false-negative results, and they can be combined with editing technologies such as CRISPR and synthetic biology. NATTs are also classified as dual-use technologies (Wang et al., 2023; Wang et al., 2024).

2.3 Synthetic Biology and AI

Synthetic biology employs tools and techniques to design new genetic systems, cells, and organisms or to modify existing ones. The tools span a wide spectrum, from developing synthetic gene expression promoters to controlling communication among cells, tissues, and organs (DiEuliis & Giordano, 2018; Mukherji & Oudenaarden, 2009; Vučemić, 2019).

Synthetic biology is developing much more rapidly in areas supported by artificial AI tools. Machine learning, a branch of AI that focuses on developing algorithms and models that enable computers to learn from collected data and autonomously generate solutions, decisions, or predictions, is useful for process optimisation and the analysis of large datasets. Machine learning operates through the following steps: data collection, data processing and preparation, model training, model evaluation, and implementation. Its major limitation is data bias, which can lead to incorrect, harmful, and unfair decisions. Due to this limitation, machine learning can also be used in the design of novel sequences for the weaponisation of

existing pathogens and the development of biological weapons (Anyanwu et al., 2024; Beard et al., 2023; Goshisht, 2024; Kriegman et al., 2021).

The greatest contribution of AI to synthetic biology lies in the creation of artificial biological constructs. AI tools can predict how a newly created construct or DNA sequence will function and how its peptide products will perform (Anyanwu et al., 2024; Russell & Norvig, 2022; Tugui & Zelinschi, 2024). The capabilities and tools provided by ChatGPT-4 were evaluated through a dialogue between scientists and ChatGPT-4 on synthetic humans and humanoid robots. The dialogue aimed to analyse the potential, challenges, and ethical implications of current achievements and to predict directions in which synthetic biology specifically impacts modifications, enhancements, and harmful consequences for the human species. ChatGPT-4 systematized the following areas of influence of synthetic biology on the creation of the synthetic human and synthetic ecosystems: (1) gene therapy and genetic engineering, (2) regenerative medicine, (3) development of neuroscience and brain-computer interfaces, (4) personalized medicine, (5) development of new biomaterials in construction and textiles, (6) environmental bioremediation and terraforming, and (7) creation of synthetic ecosystems with potential extension to extraterrestrial ecosystems and space colonization (Jones et al., 2024; Tugui & Zelinschi, 2024).

All of the aforementioned fields, through their connection to dual-use technologies, border on the design of biological weapons. Synthetic constructs such as chimaeras, plasmids, and transposons generated using AI tools can weaponise otherwise harmless microorganisms, circumvent detection and diagnostic systems, and produce consequences characteristic of true weapons of mass destruction. The creation of novel biological forms and organisms through synthesised sequences represents a slippery slope argument (Kropf's case) on which developments may proceed in either beneficial or harmful directions, whether intentional or unintentional (Berche, 2023; Kropf, 2024; Sandbrink & Koblenz, 2022; Sanz et al., 2022; Smith et al., 2023).

3. SYNTHETIC CHEMISTRY, DUAL-USE POTENTIAL, AND AI

The fundamental concept for identifying and addressing dual-use risks and potentials in research and development is Responsible Research and Innovation (RRI). RRI encompasses all research activities that have a significant societal and environmental impact. Chemical research, whether in core chemistry or applied chemistry, falls within this framework. The concept is grounded in rigorous scientific knowledge and expertise and provides guidelines for good scientific practice that researchers are expected to follow. Ethical, legal, social, and environmental implications of design decisions in research and innovation contexts are shaped and evaluated through stakeholder discussions, including researchers, designers, managers, and entrepreneurs. An important principle promoted by the concept is that there is no single correct solution to ethical challenges and dilemmas; final judgments emerge from a deliberative, discursive process. The concept assumes that the key to making sound (ethical)

decisions in chemical research and development is not theoretical knowledge of ethics, but practical discursive skills cultivated through RRI education (Mehlich, 2023; Mroz et al., 2025).

When it comes to chemical warfare agents as the main components of chemical weapons, their synthesis falls within the domain of core chemistry, specifically organic chemistry. Although synthetic chemistry serves as a bridge between core and applied chemistry, in this work, it is considered part of core chemistry because it is based on fundamental organic chemistry that does not need to be strongly directed toward a specific application. In other words, the toxicological properties of new chemical compounds synthesised in research need not be known (and generally are not), as was the case historically with the synthesis of sarin, tabun, and soman, making this a “slippery terrain” within core chemistry. All of these and similar activities in the synthesis of organic compounds can be considered to have dual-use potential (Mroz et al., 2025; Vučemilović, 2019).

The applications of AI in chemistry have become increasingly popular in recent years, as evidenced by the exponential growth in related publications. This growth, however, is not uniform across all branches of chemistry. In analytical chemistry and the life sciences, for example, the use of AI has likely already passed the so-called “peak of inflated expectations” and the “trough of disillusionment.” The benefit of AI tools in a given field depends on the quantity and quality of available data, as well as the possibilities for their analysis. AI aids in discovering insights that could not be derived from existing knowledge and is also useful for processing large datasets and automating repetitive tasks. Accordingly, the greatest increase in AI applications is observed in analytical chemistry, biochemistry, and the life sciences. In the life sciences, this particularly pertains to the use of AI in the discovery of small molecules as potential “smart drugs.” This rise in AI usage in chemistry has also been facilitated by greater availability of software and hardware tools, as well as an increase in the number of researchers skilled in data generation and processing for AI applications (Baum et al., 2021; Mroz et al., 2025).

In addition to discovering new compounds, AI is used to predict the molecular properties of newly synthesised compounds, such as solubility, temperature, and melting point (Singh et al., 2024).

Perhaps the most interesting area in chemical compound synthesis that borders on dual-use technology is the discovery of “smart drugs.” Advances in AI efficiency remain rare, as utilising such products is extremely complex. Genuine progress in drug discovery using AI can only be achieved through improved understanding of biological systems and the subsequent generation of practically relevant data in sufficient quantities to enable the identification of new mechanisms of action that demonstrate adequate efficacy and safety in clinical applications (Bender & Ciriano, 2021).

4. DESIGN OF NOVEL CHEMICAL WEAPONS USING AI-ASSISTED SYNTHETIC CHEMISTRY

The fourth generation of chemical warfare agents, popularly known as Novichok agents and designated as *nerve agent A230*, *nerve agent A232*, and *nerve agent A234*, synthesised in the previous century, was considered the greatest achievement in the development of chemical weapons. This assessment was based on their toxicological properties, namely their extremely high toxicity. This group of agents is classified toxicologically as nerve agents and is reported to be five to ten times more toxic than VX. Given that these agents can exist not only in liquid form but also in the solid state as fine “nanopowders,” they are more effective than aerosolised liquid droplets and can evade conventional instrumental detection systems. Following the discovery of this group of chemical compounds, the scientific community believed that more toxic chemical warfare agents would not be discovered (synthesised) and that this represented a “peak” that could not be surpassed (Ledgard, 2012; Vučemilović, 2019).

At this point, a disruptive technology that fundamentally shifts the boundaries of research emerges, namely, artificial intelligence (AI). As this paper focuses on chemical and biological agents, it will present the direct connection between beneficial AI-enabled services and products, such as the discovery of “smart drugs,” and harmful services and products, such as the identification of novel chemical warfare agents, obtained using similar or even identical AI tools and algorithms (Urbina et al., 2022). In his work, Ananikov describes the top 20 technological directions of digital chemistry shaped by AI support. Notably, AI-assisted drug discovery ranks first on this list. AI can accelerate the identification of potential drug candidates by predicting biological activity and optimising lead compounds (Ananikov, 2024; Gangwal & Lavecchia, 2025).

A common characteristic of “smart drugs” and chemical warfare agents is that both are synthetic chemical compounds, and this shared property enables AI to use the same tools and algorithms to produce different outcomes, some beneficial and others highly harmful and destructive. This scenario highlights AI as not only a disruptive technology but also a dual-use technology (Gangwal & Lavecchia, 2025; Hurst & Bobier, 2025; Urbina et al., 2022). Evidence that such dual-use activities are not merely theoretical comes from a computational experiment conducted by *Collaborations Pharmaceuticals, Inc.*, a company engaged, among other activities, in machine learning models for toxicity prediction across various domains. This experiment was presented at the “Convergence” conference organized by the *Swiss Federal Institute for NBC (Nuclear, Biological, and Chemical) Protection – Spiez Laboratory*, established by the Swiss government to monitor developments in chemistry, biology, and enabling technologies that could have implications for the Chemical Weapons Convention (CWC) and the Biological Weapons Convention (BTWC) (Urbina et al., 2022; Urbina et al., 2023).

The experiment was conducted using a previously developed commercial de novo molecular generator, MegaSyn2, designed to predict the bioactivity of machine-learning-derived models to identify novel therapeutic inhibitors associated with human diseases. This generative model penalises predicted toxicity while favouring predicted bioactivity. In this experiment, the logic of the goal-directed process was reversed, and the model was configured to reward both toxicity and bioactivity. For the experiment, the AI was trained on drug-like molecules from public databases that are synthetically feasible and bioavailable. The generative model was then deliberately directed toward compounds similar to the nerve agents VX and Novichok. In less than six hours, the model generated 40,000 similar molecules. During this process, the AI also designed many other known chemical warfare agents, which were subsequently compared with and identified in public chemical databases. The newly generated molecules were predicted to be more toxic than publicly known nerve agents, based on estimated LD₅₀ values. By reversing the mode of use of this generative machine-learning model, it was effectively transformed from a beneficial tool in pharmacology into a generator for the discovery and conceptualisation of the synthesis of novel lethal chemical warfare agents (Hurst & Bobier, 2025; Urbina et al., 2022; Rubinic, 2023; Urbina et al., 2023).

DISCUSSION AND CONCLUSIONS

In this review article, an overview is provided of AI's capabilities as a disruptive, dual-use technology applicable to the design of novel chemical and biological weapons. Drawing on the latest scientific research and technological solutions, this work focuses exclusively on highly harmful and potentially catastrophic applications classified as weapons of mass destruction. With regard to biological weapons and molecular biology methods, AI - with its capabilities, tools, and developed algorithms - has been implemented across all three major directions of development: reading, writing, and editing DNA (Li et al., 2023; Ashcheulova & Ambrosova, 2021; Guraiib et al., 2024; Warmbrod et al., 2020).

The three main targets defined for harmful purposes are: the development of novel biological weapons, the creation of a synthetic human and unforeseen mutations in biomedical research, and the modification of ecosystems (including plants and animals) (Anyanwu et al., 2024; Beard et al., 2023; DiEuliis & Giordano, 2018; Gillum, 2024; Russell & Norvig, 2022; Trump et al., 2023) (Table 1).

Particular emphasis should be placed on the ability to design novel DNA constructs that generate functional, fully synthetic cells, microorganisms, and multicellular organisms. Such activities may have irreversible consequences for humans and may disrupt entire ecosystems. Evidence suggests that these capabilities are already feasible, as demonstrated by the fact that, under high-containment laboratory conditions, scientists have reconstructed previously eradicated pathogens (e.g., horsepox virus and the 1918 pandemic influenza virus) from

commercially available DNA fragments, thereby demonstrating the feasibility of recreating any virus solely from accessible genomic information (Sanz et al., 2022).

A particular threat is posed by *gain-of-function* research, as it offers a wide range of possibilities for the “weaponization” of nonpathogenic microorganisms by transforming them into a new class of biological weapons capable of circumventing modern systems of detection, diagnostics, and protection, analogous to “stealth technology” (Berche, 2023; Li et al., 2023; Vučemilović, 2019).

In such a technological environment, control and safety measures struggle to keep pace with the pace of discovery, particularly when accelerated by disruptive technologies. For this reason, in the context of scientific research and the digitalisation of the life sciences, it became necessary to develop, alongside biosafety and biosecurity measures, the concept of *cyberbiosecurity*. This measure is increasingly becoming part of military cyber defence in response to cyber warfare as the fourth dimension of conflict. Undoubtedly, in the near future, cyber-attacks in biomedicine will drive significant changes, similar to those observed in cyber warfare during modern military conflicts (Liu et al., 2024; Mueller, 2020; Shankar et al., 2024).

With the introduction of AI into the field of synthetic chemistry, chemical weapons have, intentionally or unintentionally, acquired a new dimension and perspective on CBRN threats. Pharmaceutical companies possess powerful technologies, such as AI-assisted molecular generators, supported by advanced tools and algorithms. The experiment presented at the “Convergence” scientific conference demonstrated that such dual-use technologies can also be employed in the development of new generations of chemical weapons (Table 1) (Hurst & Bobier, 2025; Rubinic, 2023; Urbina et al., 2023).

Therefore, one of the highest priorities within the scientific community is controlling the misuse of AI models to develop chemical, biological, nuclear, or radiological (CBRN) threats. Due to accelerated technological progress, assessments of real risks can no longer be conducted as they were 15–20 years ago over extended timeframes; instead, developers, regulators, and decision-makers must confront the fact that risk and threat thresholds need to be updated far more frequently than ever before (Pannu et al., 2025).

These developments have direct implications at the strategic CBRN level and for defence planning, particularly in the domains of CBRN threat assessment and operational capability, early warning and reporting (W&R) systems, first response, force protection (FP) within the theatre of military operations, as well as preventive, active, and countermeasure-oriented CBRN and medical interventions. At the strategic CBRN level, within the framework of the three foundational pillars—prevention, protection, and recovery—such newly synthesized agents and weapon systems necessitate substantial revisions in the conceptualization and implementation of defence against the full spectrum of CBRN threats. At the operational

level, when developing courses of action for CBRN environments within the theatre of military operations, it is essential to account for all scientific implications arising from artificial intelligence in the development of novel weapons of mass destruction (WMD).

In the development and revision of techniques, tactics, and procedures (TTPs), due consideration must be given to the capabilities and performance characteristics of CBRN assets, including:

- first response capabilities (particularly CBRN detection systems),
- response at the level of confirmation of CBRN incidents in the theatre of operations through CBRN identification measures,
- response capabilities for recovery following CBRN exposure.

Such capabilities must be reassessed and aligned with emerging threat landscapes shaped by the convergence of CBRN and AI technologies. This is of critical importance because newly engineered biological and chemical agents may readily circumvent existing systems of detection, protection, and even radiological, biological, and chemical decontamination, thereby significantly influencing operational outcomes in the theatre of military operations.

In the context of rapid “leap” developments driven by disruptive technologies and the convergence of AI and WMD, the model of lessons learned and their integration into doctrine requires enhanced attention, more frequent updating, stronger integration between the scientific community and defence systems, and increased investment in the development of CBRN defence capabilities (Vučemilović, 2019) .

In addition to control measures and the continuous updating of threat assessments, it is necessary to develop intelligence and counter-terrorism measures to monitor both state and non-state actors, as advances in digitalisation and data availability have enabled much faster adoption of new technologies, techniques, and procedures. This can be demonstrated through two key examples. The first is related to a study that leveraged cloud-computing resources to identify more than 100,000 novel RNA viruses, highlighting the accessibility and scale at which new pathogens can be discovered (Sanz et al., 2022; Vučemilović, 2019).

The second fact is the AI-driven generation of 40,000 entirely new toxic compounds with toxicity levels comparable to those of nerve agents (Hurst & Bobier, 2025; Urbina et al., 2023). Therefore, this comprehensive approach aims to foster greater awareness within society and the scientific community of the potential consequences of such activities.

ACKNOWLEDGMENTS

The author acknowledges the use of ChatGPT (OpenAI, GPT-5.3) to improve the language quality of this paper. The opinions expressed and arguments employed are solely those of the authors.

REFERENCES

- Ananikov, V. P. (2024). Top 20 influential AI-based technologies in chemistry. *Artif Intell Chem*, 2, 1-20. <https://doi.org/10.1016/j.aichem.2024.100075>
- Anyanwu, E. C., Okongwu, C. C., Olorunsogo, T. O., Ayo-Farai, O., Osasona, F., & Daraojimba, O. D. (2024). Artificial Intelligence in Healthcare: A Review of Ethical Dilemmas and Practical Applications. *Int Med Sci Res J*, 4, 126–140. <https://doi.org/10.51594/imsrj.v4i2.755>
- Ashcheulova, T., & Ambrosova, T. (2021). Dual-use technologies of concern in context of biosafety. *Inter collegas*, 8, 1-6. <https://doi.org/10.35339/ic.8.1.4-9>
- Baum, Z. J., Yu, X., Ayala, P. Y., Zhao, Y., Watkins, S. P., & Zhou, Q. (2021). Artificial Intelligence in Chemistry: Current Trends and Future Directions. *J. Chem. Inf. Model*, 61, 3197–3212. <https://doi.org/10.1021/acs.jcim.1c00619>
- Beard, S. J., Rees, M., Richards, C., & Rios Rojas, C. (2023). The Era of Global Risk: An Introduction to Existential Risk (pp. 173-199). Cambridge, UK. <https://doi.org/10.11647/OBP.0336>
- Beljouw, S. P. B., & Brouns, S. J. J. (2024). CRISPR-controlled proteases. *Biochem Soc Trans*, 52, 441–453. <https://doi.org/10.1042/BST20230962>
- Bender, A., & Ciriano, I. C. (2021). Artificial intelligence in drug discovery: what is realistic, what are illusions? Part 2: a discussion of chemical and biological data. *Drug Discov Today*, 26(4), 1040-1052. <https://doi.org/10.1016/j.drudis.2020.11.037>
- Berche, P. (2023). Gain-of-function and origin of Covid19. *Presse Med*, 52, 104167. doi.org/10.1016/j.lpm.2023.104167
- Cyranosky, D. (2019). What's next for CRISPR babies? *Nature*, 566(7745), 440-442. <https://doi.org/10.1038/d41586-019-00673-1>
- Dieuliis, D., & Giordano, J. (2018). Gene editing using CRISPR/Cas9: implications for dual-use and biosecurity. *Protein Cell* 9(3), 239–240. <https://doi.org/10.1007/s13238-017-0493-4>
- Dieuliis, D., Imperiale, M. J., & Berger, K. M. (2024). Biosecurity Assessments for Emerging Transdisciplinary Biotechnologies: Revisiting Biodefense in an Age of Synthetic Biology. *Appl Biosaf*, 29(3), 123-132. <https://doi.org/10.1089/apb.2024.0005>
- Elgabry, M. (2023). Towards cyber-biosecurity by design: an experimental approach to Internet of Medical Things design and development. *Crime Sci*, 12:3. <https://doi.org/10.1186/s40163-023-00181-8>
- Farokhi, M., & Bhansali, D. (2024). The Use of CRISPR/Cas9 in Cancer Immunotherapy. *J Stud Res*, 13(1). ISSN: 2167-1907
- Gangwal, A., & Lavecchia, A. (2025). Artificial Intelligence in Natural Product Drug Discovery: Current Applications and Future Perspectives. *J Med Chem*, 68, 3948–3969. <https://doi.org/10.1021/acs.jmedchem.4c01257>

- Gillum, D. R. (2024). Balancing Innovation and Safety: Frameworks and Considerations for the Governance of Dual-Use Research of Concern and Potential Pandemic Pathogens. *Appl Biosaf*, 1-10. <https://doi.org/10.1089/apb.2024.0033>
- Goshisht, M. K. (2024). Machine Learning and Deep Learning in Synthetic Biology: Key Architectures, Applications, and Challenges. *ACS Omega*, 9, 9921–9945. <https://doi.org/10.1021/acsomega.3c05913>
- Guraiib, M. M., Ross, A. L., Frewer, A., Sprumont, D., Shamsi Gooshki, E., Dzenowagis, J., & Reis, A. A. (2024). Oversight of Dual-Use Research: What Role for Ethics Committees? *Health Secur*, 22(4), 15-36. <https://doi.org/10.1089/hs.2023.0095>
- Hurst, D., & Bobier, C. (2025). Dual use research and artificial intelligence. *AI & Society*, 40:5547–5548. <https://doi.org/10.1007/s00146-025-02263-4>
- Ito, Y., Inoue, I., Nakashima, T., Zhang, H., Li, Y., Kasuya, Ho., Matsukawa, T., Wu, Z., Yoshikawa, T., Kataoka, M., Ishikawa, T., & Kagoya, Y. (2024). Epigenetic profiles guide improved CRISPR/Cas9-mediated gene knockout in human T cells. *Nucleic Acids Res*, 52, 141–153. <https://doi.org/10.1093/nar/gkad1076>
- Jiang, F., & Doudna, J. A. (2017). CRISPR–Cas9 Structures and Mechanisms. *Annu Rev Biophys*, 46, 505–29. <https://doi.org/10.1146/annurev-biophys.062215-010822>
- Jones, E. M., Marken, J. P., & Silver, P. A. (2024). Synthetic microbiology in sustainability applications. *Nat Rev Microbiol*, 22, 345–359. <https://doi.org/10.1038/s41579-023-01007-9>
- Kriegman, S., Blackistona, D., Levina, M., & Bongard, J. (2021). Kinematic self-replication in reconfigurable organisms. *PNAS*, 118(49), e2112672118. <https://doi.org/10.1073/pnas.211267211>
- Kropf, M. (2024). The ethically significant difference between dual use and slippery slope arguments, in relation to CRISPR-Cas9: philosophical considerations and ethical challenges. *Res Ethics*, 1–16. <https://doi.org/10.1177/17470161241240587>
- Kumar, K. R., Cowley, M. J., & Davis, R. L. (2019). Next-Generation Sequencing and Emerging Technologies. *Semin Thromb Hemost*, 45(07), 661-673. <https://doi.org/10.1055/s-0039-1688446>.
- Ledgard, J. (2012). The Preparatory Manual of Chemical Warfare Agents. 3rd edition. (pp. 123-126). UVKCHEM. USA.
- Li, T., Yang, Y., Qi, H., Cui, W., Zhang, L., Fu, X., He, X., Liu, M., Li, P., & Yu, T. (2023). CRISPR/Cas9 therapeutics: progress and prospects, *Signal Transduct Target Ther*, 8, 36. <https://doi.org/10.1038/s41392-023-01309-7>
- Liu, T., Zhou, S., Wang, T., & Teng, Y. (2024). Cyberbiosecurity: Advancements in DNA-based information security. *Biosaf Health*, 6, 251–256. <https://doi.org/10.1016/j.bsheal.2024.06.002>
- Mehlich, J. (2023). Addressing Dual-Use Potentials in Chemical Research and Innovation. *Chem Inter*, 45(3). <https://doi.org/10.1515/ci-2023-0303>

- Millett, P. (2010). The biological weapons convention: Securing biology in the twentyfirst century. *J Confl Secur Law*, 15(1), 25–43. <https://doi.org/10.1093/jcs/krq007>
- Mir Gani, T., Wani, A. K., Akhtar, N., & Shukla, S. (2022). CRISPR/Cas9: Regulations and challenges for law enforcement to combat its dual-use. *Forensic Sci Int*, 334, 111274. doi.org/10.1016/j.forsciint.2022.111274
- Moritz, R. (2022). Assessing dual use research of concern (DURC) - lessons learned from the United States government institutional DURC policy. *Can J Microbiol*, 68, 655–660. <https://doi.org/10.1139/cjm-2021-0344>
- Mroz, A., Basford A., & Hastedt, F., (2025). Cross-disciplinary perspectives on the potential for artificial intelligence across chemistry. *Chem Soc Rev*, 54, 5433. <https://doi.org/10.1039/d5cs00146c>
- Mueller, S. (2020). Facing the 2020 pandemic: What does cyberbiosecurity want us to know to safeguard the future? *Biosaf Health*, 3, 11–21. <https://doi.org/10.1016/j.bsheal.2020.09.007>
- Mukherji, S., & Oudenaarden, A. (2009). Synthetic biology: Understanding biological design from synthetic circuits. *Nat Rev Genet*, 10(12), 859–871. <https://doi.org/10.1038/nrg2697>
- Nafea, A. M., Wang, Y., Wang, D., Salama, A. M., Aziz, M. A., Xu, S., & Tong, Y. (2024). Application of next-generation sequencing to identify different pathogens. *Front Microbiol*, 14, 1329330. <https://doi.org/10.3389/fmicb.2023.1329330>
- Novossiolova, T., & Perkins, D. (2021). Life sciences professional responsibility in an age of dual-use research. *One Health Risk Manag*, 2, 75-80. <https://cyberleninka.ru/article/n/life-sciences-professional-responsibility-in-an-age-of-dual-use-research>.
- Pannu, J., Bloomfield, D., MacKnight, R., Hanke, M.S., Zhu, A., & Gomes G. (2025). Dual-use capabilities of concern of biological AI models. *PLoS Comput Biol*, 21(5), e1012975. <https://doi.org/10.1371/journal.pcbi.1012975>
- Qin, D. (2019). Next-generation sequencing and its clinical application. *Cancer Biol Med*, 16(1), 4-10. <https://doi.org/10.20892/j.issn.2095-3941.2018.0055>
- Redman, M., King, A., Watson, C., & King, D. (2016). What is CRISPR/Cas9? *Arch Dis Child Educ Pract Ed*, 101, 213–215. <https://doi.org/10.1136/archdischild-2016-310459>
- Rodino, K. G., & Simner, P. J. (2024). Status check: next-generation sequencing for infectious-disease diagnostics. *Clin Invest*, 134(4), e178003. <https://doi.org/10.1172/JCI178003>
- Rubinic, I., Kurtov, M., Rubinic, I., Likic, R., Dargan, P., & Wood, D., M. (2023). Artificial intelligence in clinical pharmacology: A case study and scoping review of large language models and bioweapon potential. *Br J Clin Pharmacol*, 90, 620–628. <https://doi.org/10.1111/bcp.15899>

- Russell, S., & Norvig, P. (2022). Artificial Intelligence: A Modern Approach, Fourth Edition Global Edition (pp 134-136). Pearson Education Limited. Harlow UK.
- Sandbrink, S. B., & Koblentz, G. D. (2022). Biosecurity risks associated with vaccine platform technologies. *Vaccine*, 40, 2514–2523. <https://doi.org/10.20892/j.issn.2095-3941.2018.005510.1016/j.vaccine.2021.02.023>
- Sanz, J. A., Dunlap, G., Nolan, N., & O’Leary, C. (2022). Biosecurity risks and governance in the age of synthetic biology. *MIT SPR*, 3, 136. 10.38105/spr.x3nlyr0fkc
- Selvam, K., Najib, M. A., Khalid, M. F., Ozsoz, M., & Aziah, I. (2022). CRISPR-Cas Systems-Based Bacterial Detection: A Scoping Review. *Diagnostics*, 12, 1335. <https://doi.org/doi.org/10.3390/diagnostics12061335>
- Shankar, D. D., Azhakath, A. S., Khalil, N., Sajjev, J., Mahalakshmi, T., & Sheeba, K. (2024). Data mining for cyber biosecurity risk management – A comprehensive review. *Comput Secur*, 137, 103627. <https://doi.org/10.1016/j.cose.2023.103627>
- Singh, A., Rai, S., Rao, K., & Rao, S. (2024). The Scientific Spectrum of AI, Enhancing the Future. (Silas, N. Chapter 13. AI in Chemistry, The Future of Scientific Discovery) (pp.192-198). Sankalp Publication, Bilaspur India.
- Smith, J. M., Hartmann, D., & Booth, M. J. (2023). Engineering cellular communication between light-activated synthetic cells and bacteria. *Nat Chem Biol*, 19, 1138–1146. <https://doi.org/10.1038/s41589-023-01374-7>
- Stenzinger, A., Vogel, A., Lehmann, U., Lamarca, A., Hofman, P., Terracciano, L., & Normanno, N. (2024). Molecular profiling in cholangiocarcinoma: A practical guide to next-generation sequencing. *Cancer Treat Rev*, 122, 102649. <https://doi.org/10.1016/j.ctrv.2023.102649>
- Tabiban, M., Moghaddam, F. S., Motevaseli, E., & Ghafouri-Fard, S. (2024). Targeting mRNA-coding genes in prostate cancer using CRISPR/Cas9 technology with a special focus on androgen receptor signaling. *Cell Commun Signal*, 22, 504. <https://doi.org/10.1186/s12964-024-01833-1>
- Trump, B., Cummings, C., Klasa, K., Galaitsi, S., & Linkov, I. (2023). Governing biotechnology to provide safety and security and address ethical, legal, and social implications. *Front Gen*, 13, 2022. <https://doi.org/10.3389/fgene.2022.1052371>
- Tugui, A., & Zelinschi, D. O. (2024). A New AI Dialogue Framework with ChatGPT: Exploring Synthetic Man within the Context of Synthetic Biology. *Preprints*, 1, 1-15. <https://doi.org/10.20944/preprints202404.1468.v1>
- Uhlenhaut, C., Burger, R., & Schaade, L. (2013). Protecting society Biological security and dual-use dilemma in the life sciences - status quo and options for the future. *Sci Soc*, 14(1), 25-30. <https://doi.org/10.1038/embor.2012.195>

- Urbina, F., Lentzos, F., Invernizzi, C., & Ekins, S. (2022). Dual Use of Artificial Intelligence-powered Drug Discovery. *Nat Mach Intell*, 4(3), 189–191. <https://doi.org/10.1038/s42256-022-00465-9>
- Urbina, F., Lentzos, F., Invernizzi, C., & Ekins, S. (2023). AI in Drug Discovery: A Wake-up Call. *Drug Discov Today*, 28(1), 103410. <https://doi.org/10.1016/j.drudis.2022.103410>
- Vennis, I. M., Schaap, M. M., Hogervorst, P. A., De Bruin, A., Schulpen, S., Boot, M. A., Van Passel, M., Rutjes, S. A., & Bleijs, D. A. (2021). Dual-Use Quickscan: A Web-Based Tool to Assess the Dual-Use Potential of Life Science Research. *Front Bioeng Biotechnol*, 9, 797076. <https://doi.org/10.3389/fbioe.2021.797076>
- Vučemilović, A. (2019). Oružja za masovno uništavanje: Kemijsko i biološko oružje (pp. 81-140). Sveučilište u Zagrebu, Ministarstvo Obrane Republike Hrvatske, Zagreb, Hrvatska. (Weapons of Mass Destruction: Chemical and Biological Weapons. University of Zagreb, Ministry of Defence of the Republic of Croatia, Zagreb, Croatia)
- Wang, M., Liu, H., Ren, J., Huang, Y., Deng, Y., Liu, Y., Chen, Z., Wang-NGai Chow, F., Leung, P. H. M., & Li, S. (2023). Enzyme-Assisted Nucleic Acid Amplification in Molecular Diagnosis: A Review. *Biosensors*, 13, 160. <https://doi.org/10.3390/bios13020160>
- Wang, Y., Chen, J., Yang, Z., Wang, X., Zhang, Y., Chen, M., Ming, Z., Zhang, K., Zhang, D., & Zheng, L. (2024). Advances in Nucleic Acid Assays for Infectious Disease: The Role of Microfluidic Technology. *Molecules*, 29, 2417. <https://doi.org/10.3390/molecules29112417>
- Warmbrod, K. L., Revill, J., & Connell, N. (2020). Advances in Science and Technology in the Life Sciences: Implications for Biosecurity and Arms Control (pp. 5-13). UNIDIR Geneva, Switzerland. <https://doi.org/10.37559/SecTec/20/SandT>
- Zhan, T., Rindtorffa, N., Betgea, J., Ebertb, M. P., & Boutros, M. (2019). CRISPR/Cas9 for cancer research and therapy. *Semin Cancer Biol*, 55, 106-119. <https://doi.org/10.1016/j.semcancer.2018.04.001>

ANNEX

Table 1

Overview of capabilities, products, and scientific services of molecular biology methods and synthetic chemistry in dual-use and military use applications.

CAPABILITIES	DUAL USE & MILITARY USE APPLICATIONS	PURPOSE	REFERENCES
DNA reading NGS, PCR	Mass sequencing, high-throughput DNA sequencing. DNA Amplification: Large-scale amplification of DNA. Identification of targeted genes within populations and ethnic races.	Development of biological and ethnic weapons.	<i>Beard et al., 2023; Berche, 2023; Nafea et al., 2024; Rodino & Simner 2024; Vučemilović, 2019,</i>
DNA writing SYNT BIO + AI	Synthesis of entirely new genetic systems, synthetic biomolecules, and organisms. <i>De novo</i> synthesis of viruses, peptides, plasmids, transposons, and chimaeras.	Development of biological and toxic weapons. Modification of abilities and functions in humans, animals, and plants. Design of synthetic ecosystems.	<i>Beard et al., 2023; Berche, 2023; Novossiolova, Perkins, 2021; Vennis et al., 2021; Kropf, 2024; Sandbrink, Koblentz, 2022; Sanz et al., 2022; Smith et al., 2023; Koblentz, 2022; Vučemilović, 2019.</i>
DNA editing CRISPR	Targeted protein cleavage, DNA sequence editing, and mutation detection. Integration of “knockout genes.” Creating “gain-of-function” modifications.	Development of pathogens, biological, toxic, and ethnic weapons. „Weaponising” non-pathogenic microorganisms. Design of human embryos - CRISPR babies.	<i>Kropf, 2024; Beard et al., 2023; Jiang, Doudna 2017; Farokhi et al., 2024; Mir Gani et al., 2022; DiEuliis, Giordano, 2018; Cyranosky, 2019.</i>
Synthetic chemistry +AI	<i>De novo</i> molecular generators, AI, and machine learning	Synthesis of new chemical warfare agents.	<i>Gangwal, & Lavecchia 2025; Hurst & Bobier, 2025; Rubinic, 2023; Urbina et al., 2023</i>

Note. NGS - Next-Generation Sequencing, PCR - Polymerase Chain Reaction, SYNT BIO - synthetic biology, AI - artificial intelligence, CRISPR - Clustered Regularly Interspaced Short Palindromic Repeats

ASSESSMENT OF THE IMPACT OF UNMANNED AERIAL VEHICLES ON NAVAL SURFACE WARFARE

Tomislav Sunko¹, Mihael Dedo², Lovro Strnad³, Stipe Brnadić⁴, Vilim Đura⁵, Zoran Medvidović⁶

¹ Croatian Defence Academy "Dr Franjo Tuđman", Zagreb, Croatia

E-mail: tsunko@morh.hr

ORCID: <https://orcid.org/0000-0002-9287-5642>

² Croatian Defence Academy "Dr Franjo Tuđman", Zagreb, Croatia

E-mail: mihael.dedo@morh.hr

ORCID: <https://orcid.org/0000-0002-5968-3171>

³ Dr. Franjo Tuđman Defense and Security University, Zagreb, Croatia

E-mail: lovro.strnad@sois-ft.hr

ORCID: <https://orcid.org/0009-0005-0478-875X>

⁴ Dr. Franjo Tuđman Defense and Security University, Zagreb, Croatia

E-mail: stipe.brnadice@sois-ft.hr

ORCID: <https://orcid.org/0009-0007-0405-7054>

⁵ Dr. Franjo Tuđman Defense and Security University, Zagreb, Croatia

E-mail: vilim.djura@sois-ft.hr

ORCID: <https://orcid.org/0009-0009-3682-5024>

⁶ Ministry of Defence, Croatian Navy, Split, Croatia

E-mail: zoran.medvidovic@morh.hr

ORCID: <https://orcid.org/0009-0000-4806-7843>

Abstract

Although Unmanned Aerial Vehicles (UAVs) and their deployment in warzones are not new, understanding their command and control, operational capabilities, and the advantages they provide is evolving daily, even with the smallest technological upgrades. Moreover, in the maritime domain, the broad consensus on the UAV threat to naval platforms often remains in the background, overshadowed by the media's greater focus on Unmanned Surface Vehicles (USVs). This paper explores the UAV threat to contemporary naval platforms to enhance

understanding of the associated risks, foster interpretation of changing tactics and procedures, and provide a concise, adequate overview of future Counter-Unmanned Aerial Vehicle (C-UAV) developments. Drawing on an analytical-synthetic approach to relevant scientific literature, the paper outlines the key attributes that make UAVs a threat to naval platforms. The paper then presents a timeline of notable naval incidents involving UAVs over the last few years, as reported by trusted international media sources, with particular focus on the Black and Red Seas. The incidents are categorised by their tactical aspects and subsequently linked to known UAV engagement tactics employed in these operational theatres. Furthermore, the paper describes the most prominent UAV models and their capabilities for maritime surface warfare, as demonstrated during the Russia-Ukraine War and Houthi attacks. In conclusion, UAV attributes, employment tactics, and emerging trends are summarised to provide a holistic review of the immediate risks to surface naval forces, the potential evolution of those risks, and the development of countermeasures, while also indicating directions for further research.

Keywords: Unmanned Aerial Vehicle (UAV), maritime surface warfare, threats to naval platforms, Russia-Ukraine War, Houthi attacks.

INTRODUCTION

Recent operational experiences highlight why UAVs have become a defining element of contemporary naval warfare. As noted by the Atlas Institute, NATO's traditional defence posture is increasingly strained by the proliferation of low-cost unmanned systems that can saturate air-defence networks and erode the conventional technological advantage of major naval powers (Satta, 2025). This shift is not merely theoretical - it is unfolding in active conflict zones. The January 2025 incident in the Red Sea, in which the USS *Stockdale* (DDG-106) successfully intercepted a low-flying Houthi attack UAV with five-inch naval gunfire, demonstrates both the operational maturity of UAV threats and the continuing need for adaptable, layered defensive responses at sea (Mongilio, 2025). These developments reveal a widening gap between traditional naval force design and the rapidly evolving landscape of unmanned aerial vehicle-enabled maritime warfare. To address these challenges, this paper provides a structured examination of how UAVs influence naval surface operations. The first chapter identifies and analyses the core threat attributes of UAVs, including affordability, detectability, payload diversity, and the limitations of existing shipboard defence systems. The second chapter presents a detailed timeline of notable UAV incidents over the past few years, focusing on the Black and Red Sea theatres. The third chapter evaluates the operational impact of these UAV engagements on surface vessels, comparing differences in mission profiles, defensive readiness, and tactical outcomes across the two maritime environments. Finally, the discussion and results synthesise these findings and conclude with the authors' thoughts on further developments and remaining challenges. This paper aims to synthesise the aforementioned approaches to provide readers with a holistic review of UAV threats to naval surface warfare and to outline key implications for future naval doctrine, force protection measures, and the development of effective counter-UAV (C-UAV) capabilities.

1. METHODOLOGY

The paper employs an analytical–synthetic research methodology grounded in the systematic review, comparison, and interpretation of publicly available and verified sources. First, relevant scientific literature, defence analyses, and open-source intelligence (OSINT) were examined to identify the key attributes that define UAV threats to naval surface platforms. Second, international media reports, operational statements, and incident databases, particularly those documenting events in the Black Sea and Red Sea, were compiled to construct a chronological timeline of notable UAV attacks or attempted strikes. These incidents were then categorised according to UAV type, target class, theatre characteristics, and tactical context. Third, a comparative analysis was conducted to evaluate discrepancies in UAV effectiveness across theatres, correlating platform vulnerability with factors such as air-defence capability, mission profile, and availability of integrated sensor networks. Limitations related to information clouded by the fog of war and derived from non-scientific literature were explained, considered in analyses, and mitigated by comparing two different theatres of operation and by examining the technical data of the attacked naval platforms and the most commonly employed UAV. Finally, the study synthesises data on prominent UAV models documented in the conflicts, assessing their operational capabilities and roles in shaping recent attack patterns. This methodological approach enables a holistic understanding of both UAV employment and naval susceptibility, informing an assessment of emerging trends and future C-UAV requirements.

2. THREAT ATTRIBUTES OF UNMANNED AERIAL VEHICLES

This chapter analyses attributes that make UAVs a threat to contemporary naval surface platforms. The special focus and most of the data presented below are based on an analysis of the Russia-Ukraine War and the employment of UAVs in it. This chapter aims to foster understanding of the UAV threat to naval platforms and, therefore, to pinpoint capabilities that must be considered when constructing or acquiring a counter-UAV (C-UAV) system.

- **Accessibility and affordability** - Specialised military UAVs can perform a wide spectrum of assault missions depending on range, guidance, and payload. Their development has proceeded along two main directions. Long-range, fixed-wing UAVs, priced from several million to several dozen million USD, such as the General Atomics MQ-9 Reaper, are, in effect, unmanned munitions carriers and are constantly evolving into ever more complex platforms (Bailey, 2025). Their primary task is to reduce risk to human aircrew, and their main tactical-technical trait is a large payload capacity. In contrast, inexpensive, one-way fixed-wing attack (OWA) UAVs such as the Iranian Shahed-136, or slow, commercial-off-the-shelf (COTS) rotary-wing UAVs that can carry a mortar grenade, are weapons in themselves and pose a risk to a naval platform's defence systems. These low-cost systems are the focus of this paper. With rotary-winged UAVs priced from a few hundred USD and OWA fixed-winged UAVs costing a few tens of thousands USD, their economy lies in the numbers. Ongoing trends make them even simpler and less complex, thereby reducing costs

(Saleh & Ziade, 2025). They have a low target-hit rate (for the Shahed, it is reported as 10%), but they compensate with operational numbers. The cost-effectiveness of large numbers of OWA UAVs can approach that of some of the most effective Russian missiles; furthermore, the saturation effect on detection sensors and air-defence systems, and the psychological effects of mass UAV attacks, are irreplaceable (Hollenbeck et al., 2025). The frequency of recent non-state actor use of this asymmetric tactic testifies to the widespread affordability of OWA UAVs (Saleh & Ziade, 2025).

- **Hard detectability** - The low detectability of small OWA and rotary-wing UAVs stems from several factors. First, their inherent design, i.e., small size and slow flight (especially rotary-wing UAVs), significantly reduces Doppler effects, while low flight enables exploitation of radar coverage gaps. For detection purposes, they are often categorised as low, slow, and small (LSS) targets (Liu, 2023). Second, their increasing simplicity and reduced costs have led to the use of UAV construction materials with low dielectric constants, most notably Styrofoam, which makes radar detection more difficult (Kartini et al., 2024). Third, many upgrades are deliberately intended to hinder detection across visual, acoustic, and radar domains (Rojhani & Shaker, 2024). Russian reporting indicates efforts to mimic birds using a UAV frame for certain land-target operations, in addition to Chinese efforts reportedly employing bird-like UAVs, or ornithopters, for intelligence missions (Khomenko, 2025; Saballa, 2024). Collectively, these factors allow UAVs to achieve significantly low signal-to-noise ratios (SNR) and increase the false-alarm probability. That can be especially dangerous in environments with strong clutter (De Quevedo et al., 2019). In those circumstances, UAV detection poses a significant challenge for naval platforms' defences and a substantial opportunity for adversaries to exploit. Additional detection challenges arise when UAVs employ smoke screens or other means to reduce visual and thermal signatures.
- **Lethality** - A crucial attribute of the UAV threat to naval platforms is their warheads. Mirroring UAV subcategories, warheads vary widely in type and mass. In the Russia-Ukraine War, during land operations, small rotary-wing UAVs have often carried hand grenades, mortar grenades or rocket-propelled grenade (RPG) (Anonymous, 2024). More advanced first-person view (FPV) systems that emerged later in the war have carried anti-tank, HEAT, fragmentation, or thermobaric warheads (Anonymous, 2024). Larger, fixed-wing OWA UAVs can carry warheads of several tens of kilograms (Albright et al., 2024; Kyiv Post, 2025). At first glance, many warheads may seem unlikely to inflict catastrophic damage on a naval vessel; however, the following chapter will analyse how even small but precise and sudden hits to critical points on a naval platform can have devastating operational effects. Moreover, the ongoing development of UAV warheads and UAVs capable of carrying missiles or laser devices must not be overlooked.
- **Swarming ability** - A swarm is a cohesive group of UAVs with a shared mission, performing collaborative work in navigation, communication, decision-making, and target engagement (Liu, 2023). Swarm collective actions can be distributed among UAVs and their collective behaviour is driven by artificial intelligence (AI) which connects them to advancements in the field of machine learning (ML), distributed learning (DL),

reinforcement learning (RL), high processing power, energy management, power supply and harvesting, and 6G connectivity (Javed et al., 2024). With advancements in these fields, the effectiveness of UAV swarms can be expected to grow, but so too does their vulnerability to electronic warfare (EW), cyber warfare (CW), and navigation warfare (NW). Notable examples of swarm employment include Turkey's anti-tank operations in Libya and by Israel in a UAV swarm attack against Syrian air defence (Javed et al., 2024). Deploying large numbers of UAVs in swarms can fully exploit saturation effects on sensor and weapon systems, thereby creating gaps in a naval platform's air defence by exploiting its vulnerabilities.

- **Naval platforms' defence limitations** - Not all UAV threat attributes stem from their intrinsic properties; some arise from the inadequate response capabilities of surface platform defence systems. For this analysis, they can be divided into three subsystems (Hood, 2021). First, a detection-sensor deficiency when interacting with stealth LSS targets was described above. Second, the cost disparity between contemporary hard-kill air defence measures and UAVs makes deploying such measures unsustainable against UAV attacks, given the magazine constraints of surface naval platforms (Tallis, 2024). Third, given UAV classification challenges, command and control (C2) systems are often constrained by ambiguous rules of engagement (ROE), which can vary further depending on a naval platform's position relative to United Nations Convention on the Law of the Sea (UNCLOS)-defined borders (Coffin, 2019). In recent years, significant advancements in hybrid C-UAV systems have been made. Several studies have examined hybrid counter-UAV detection systems. For example, Flórez et al. (2020) review detection and correlation techniques based on audio, RF, and video signals, while Sharma and Purohit (2025) categorise and compare different identification methods. Wentzel et al. (n.d.) present a validated hybrid C-UAV system architecture, while Zitar et al. (2023) focus on the newest advancements in machine-learning recognition for counter-UAV concepts and systems. C-UAV mitigation measures are usually subdivided into non-physical and physical mitigation. Non-physical mitigation includes GNSS spoofing, RF jamming, wideband and narrowband high-power electromagnetic waves (HP EM), low-power lasers (dazzlers) and high-power lasers. Physical mitigation, on the other hand, includes conventional and specialised munitions, various ground- and UAV-based nets, and counter-UAV measures. These measures, along with their advantages and shortcomings, are reviewed in Wentzel et al. (n.d.).

However, the majority of these potential concepts remain insufficient in near-shore conditions, particularly along indented and rugged coastlines, in choke points, at anchorages and in harbours lacking their own air defence capabilities (Hood, 2021).

This paper integrates previously published recommendations for developing future ship-based C-UAV systems (Liu, 2023; Rahman & Robertson, 2018; Zitar et al., 2023). Moreover, at the end of this chapter, the comprehensive approach summarises all recommendations within a single holistic systems framework, supported by analytical findings on UAV threat attributes and their relationship to threats to surface naval platforms, as discussed above.

This chapter outlines the general directions of UAV threat development, which is characterised by increasing autonomy in navigation, communication, and decision-making; mimicry-based designs; reduced overall size and thus detectability; and lower costs, leading to greater numbers of UAVs that can be operationally employed. At the same time, the effectiveness of these numbers increases due to advances in swarm algorithms, while the limitations of naval platform defence remain unchanged.

Based on the elaborated threat development, the paper proposes prescriptive recommendations for the development, integration, and employment of ship-based C-UAV systems. The evolution of radar, visual, thermal, and acoustic sensors should be tailored to the characteristics of low-flying, slow, and small (LSS) targets while remaining functional in strong-clutter environments and in the presence of electromagnetic and acoustic saturation. Research on micro-Doppler radar analysis for classifying ornithopters should continue (Rahman & Robertson, 2018). The integration of different sensors into hybrid sensor systems to mitigate their individual shortcomings is widely recognised (Zitar et al., 2023). System designers should leverage this approach to enable simultaneous engagement of many targets. They should consider developing a comprehensive database of UAV electromagnetic, thermal, visual, and acoustic signatures linked to these sensors. Furthermore, capability planners must design C-UAV weapon systems to be layered and cost-scalable, employing a mix of soft and hard countermeasures that reflect the cost and capability diversity of UAVs (Liu, 2023).

3. TIMELINE OF NOTABLE UAV INCIDENTS

This chapter reviews relevant media sources and compiles the most notable UAV incidents and attacks from the last four years, with a focus on the Russia-Ukraine War and Houthi attacks. The authors present a timeline below the text. From that timeline, the analysis in the following subchapter will proceed. Note that the attacks and incidents described are only those in which damage was caused or intended to be caused directly by UAVs, thus excluding cases where UAVs served solely as surveillance platforms for USV attacks. For this timeline, information from publicly available online sources was used. One of these sources is the official institutional website of US Central Command; most others are specialised naval portals that lack rigorous scientific methodology and therefore carry a risk of potential underreporting. In addition, readers should consider the possibility of misattribution regarding UAV involvement and the damage caused, due to both the fog of war and reporting errors.

- **October 2022.** On 29 October 2022, Ukraine conducted an unmanned raid on the Russian Black Sea Fleet headquarters at Sevastopol Naval Harbour. UAVs reportedly participated, but it remains unclear whether the reported Russian losses, mainly to harbour facilities, were caused by UAVs or unmanned surface vehicles (USVs). The UAV model employed was ironically called "*Alibaba drone*" - a twin-tail-boom, fixed-wing UAV of unknown origin (Rogoway & Payne, 2022; Rogoway, 2022).

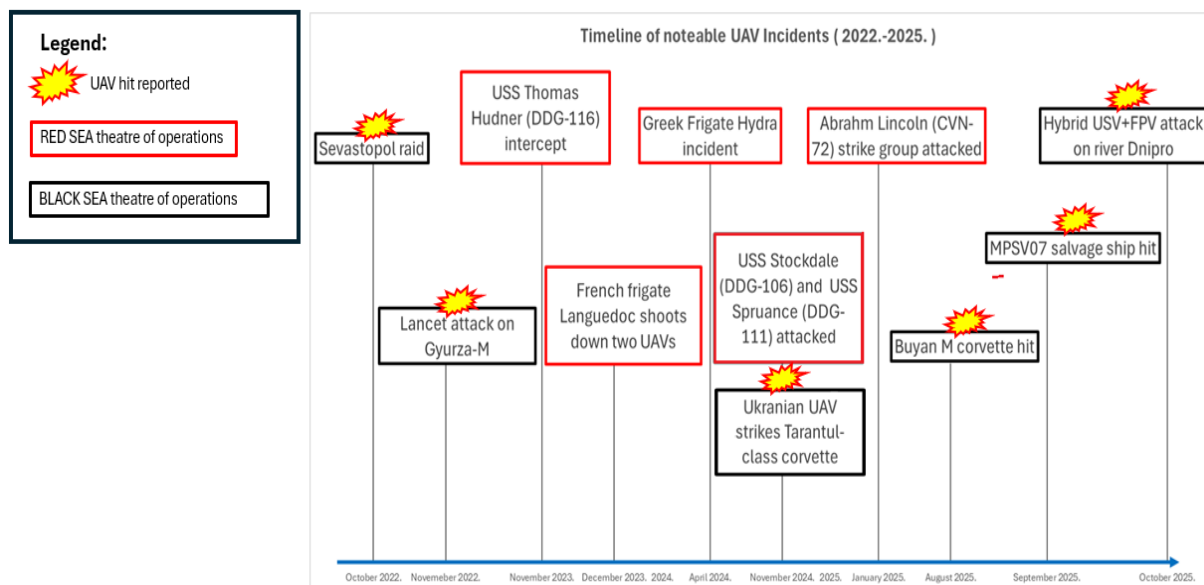
Although the revisions suggested consistency in terminology, particularly using "*unmanned aerial vehicle*" instead of "*drone*", the phrase "*Alibaba drone*" was left unchanged because it is a colloquial term.

- **November 2022.** On 4 November 2022, a Russian *Lancet*, an unmanned aerial vehicle, attacked a Ukrainian Gyurza-M-class patrol boat reportedly located in Kakhovsky Reservoir on the Dnieper River. Damage was reported. This marked the first recorded employment of a UAV against a surface naval target (Ozberk, 2025).
- **November 2023.** The *Arleigh Burke*-class destroyer USS *Thomas Hudner* (DDG-116) intercepted one UAV on 15 November 2023, launched from Houthi-controlled Yemeni territory, with no casualties (US CENTCOM, 2023). On 19 November 2023, a combined cruise-missile and UAV attack was fully intercepted by the same-class destroyer, USS *Carney* (DDG-64). On 23 November 2023, US DDG-116 shot down multiple one-way attack (OWA) UAVs fired from Houthi territory. The type of interceptor employed remains unknown (Ziezulewicz, 2023a).
- **December 2023.** On 11 December 2023, the French *FREMM* frigate *Languedoc* used *Aster 15* surface-to-air missiles to shoot down two UAVs launched by the Houthis (Vavasseur, 2023). The same type of interceptors was used by the British *Type 45* destroyer *HMS Diamond* on 14 December 2023 to repel a combined Houthi attack involving UAVs, cruise missiles, and ballistic missiles. The reported unit cost of the MBDA-manufactured *Aster 15* missile is estimated to be between 1 and 2 million GBP. The intercepted UAVs were presumably Iran-supplied *Shahed-136* models (NavyLookout, 2023). On 16 December 2023, US DDG-64 shot down fourteen UAVs over the Red Sea by unspecified means (Ziezulewicz, 2023b).
- **April 2024.** On 25 April 2024, the Greek frigate *Hydra*, deployed on an EU mission in the Red Sea, was involved in an incident with two UAVs, destroying one while the other escaped. The UAVs' intentions and the weapon employed remain unclear (Reuters, 2024).
- **November 2024.** On 6 November 2024, an unidentified Ukrainian attack UAV struck a *Project 12411 Tarantul* class corvette at the naval base in Kaspiysk, located on the shores of the Caspian Sea. This attack demonstrated Ukraine's capability to conduct UAV strikes against naval platforms at a range of up to 1,500 km (Kushnikov, 2024). On 11 November 2024, two *Arleigh Burke*-class destroyers, USS *Stockdale* (DDG-106) and USS *Spruance* (DDG-111), deployed in the Red Sea, were attacked by a combination of UAVs, cruise missiles and anti-ship ballistic missiles. All incoming threats were intercepted by unknown means (Mongilio, 2024).
- **January 2025.** On 30 January 2025, USS *Abraham Lincoln* (CVN-72) carrier strike group came under a combined ballistic missile, cruise missile and OWA UAV attack. During the engagement, US DDG-106 shot down a low-flying OWA UAV using 5-inch (127 mm) gunfire (Mongilio, 2025). This report provides more detailed information and accurately depicts the tactics discussed in the following chapters.
- **August 2025.** On 28 August 2025, Ukrainian OWA UAVs struck the Russian *Project 21631 Buyan-M* class corvette in the Temryuk Bay (Sea of Azov). The attack disabled the naval platform's radar systems, forcing her to withdraw (Ozberk, 2025).

- **September 2025.** On 11 September 2025, Ukrainian sources reported, and the Russians partially confirmed, that a Russian Project MPSV07 class, multifunctional salvage ship, was hit near Novorossiysk. The commanding bridge and electronic intelligence systems located on the monkey bridge were destroyed, and the ship was sent for repairs. Countermeasures taken, casualties, and the UAV model (beyond its domestic production) remain unknown (Fornusek, 2025).
- **October 2025.** On 21 October 2025, Ukraine launched a hybrid USV and FPV UAV attack. Domestically produced *Barracuda*-class USV deployed a group of FPV UAVs near the target vessel, reportedly making it inoperable. This attack represents a stepping stone toward more advanced hybrid unmanned attack techniques (Lerouvillois, 2025). On 4 October, Ukrainian Special Operations Forces struck a second *Project 21631 Buyan-M* class corvette in Lake Onega during her inland passage from the Baltic to the Caspian Sea, further demonstrating Ukraine's deep-strike capability and the vulnerability of Russian naval vessels. However, it remains unclear whether the attack was carried out by a UAV or a missile, and therefore, this strike is not included in the timeline (Xavier, 2025).

Figure 1

Timeline of Selected UAV Incidents in Maritime Operations



4. ANALYSIS OF UAV ATTACKS IN THE BLACK AND RED SEA

4.1. Differences in operational theatres

This chapter builds on the timeline presented in Figure 1 and further enriches the time-based approach with publicly available data from online OSINT sources. These sources, although used in other respected analyses (Learschi & Popa, 2025; Tallis, 2024) and supported by photographs and videos of damaged and destroyed naval platforms, are not immune to

underreporting, misattribution, and survivorship bias. Readers should therefore interpret this material with appropriate caution, in addition to the usual uncertainty inherent in battle damage assessment due to the fog of war. However, a clearer perspective can be gained by comparing the two theatres of operations, the naval assets involved, and their respective modes of employment.

From Figure 1, a peculiar observation can be made: the hit rate appears to be closely connected to the theatre of operations. Specifically, all recorded notable UAV attacks on naval platforms in the Black Sea have been successful, whereas there are no known cases of naval vessels being hit by UAVs in the Red Sea.

Table 1 highlights clear differences in the tactical employment of naval surface platforms, as the allied mission focuses on protecting maritime traffic through the contested Bab el-Mandeb choke point (Centre). Therefore, not all UAVs intercepted by allied naval platforms targeted them. Some UAVs targeted merchant traffic. In contrast, the mission of the Russian Navy during the early stages of the war in Black Sea was centred on power projection and joint operations. That role diminished once the Black Sea Fleet failed to secure sea control and was subsequently forced to retreat (Delanoë, 2024). The case of the *Project 21631 Buyan-M-class corvette demonstrated the vulnerability of naval surface assets employed in power-projection* missions without established sea control (Ozberk, 2025). Nevertheless, for the *Buyan-M*, air defence was not her primary mission at the time she was hit, unlike the allied naval platforms in the Red Sea, which served as theatre air defence platforms.

Table 1

Comparative tactical analysis of operational theatres and naval assets

	<i>Red Sea theatre</i>	<i>Black Sea theatre</i>
Maritime activity	Confrontation	Armed conflict
Conflict description	Asymmetric, versus a non-state actor (Houthi rebels)	Attrition war between sovereign states
Operational objective	Allied sea control	Both sides sea denial
Primary naval warfare areas	Anti-air warfare	Strike warfare
Core policies	Force protection	Power projection
Primary operational functions	Forces protection, civil-military cooperation	Fire, manoeuvre
Operation type	Freedom of navigation	Joint naval and ground operations

Most common naval unit	Task group (carrier task force)	Task element (single naval platform)
Most common platform class	Frigates, Destroyers, Cruisers	Versatile

Note. The table was created by the authors based on multiple sources (Cropsey, 2022; EUR-Lex, 2025; LaGrone, 2023; NATO, 2019; UK Ministry of Defence, 2025; Puspoayu et al., 2022).

4.2. Naval platforms losses: quality and quantity

In addition to sea control and mission objectives, a third factor influencing the hit rate in the Black Sea could be the size, capabilities, and organisation of the platforms involved. From the attack on the *USS Abraham Lincoln* (CVN-72) carrier strike group on 30th January 2025, the advantages of numerous platforms operating over a wide area with integrated sensors are clearly evident (Mongilio, 2025). The Buyan-M, Gyurza-M, and Project MPSV07 vessels, on the other hand, operated as independent tactical elements without the air defence umbrella of a larger platform after the attack on the Slava-class cruiser Moskva.

Since the previous analysis focused on notable incidents and attacks, the scope of the following research was expanded to include a classification of all recorded attempted Ukrainian aerial attacks on Russian Black Sea Fleet naval platforms, as well as all such platforms that were lost or damaged. Finally, as there are no known cases of UAV hits on naval vessels in the Red Sea theatre, civilian merchant vessels that were struck by UAVs have been classified and analysed to complement the comparison. All data were obtained from publicly available online databases, and the results are presented below.

Table 2 compares the size and capabilities of allied naval platforms that successfully evaded UAV attacks with those of Russian and Ukrainian naval platforms that were struck.

Table 2

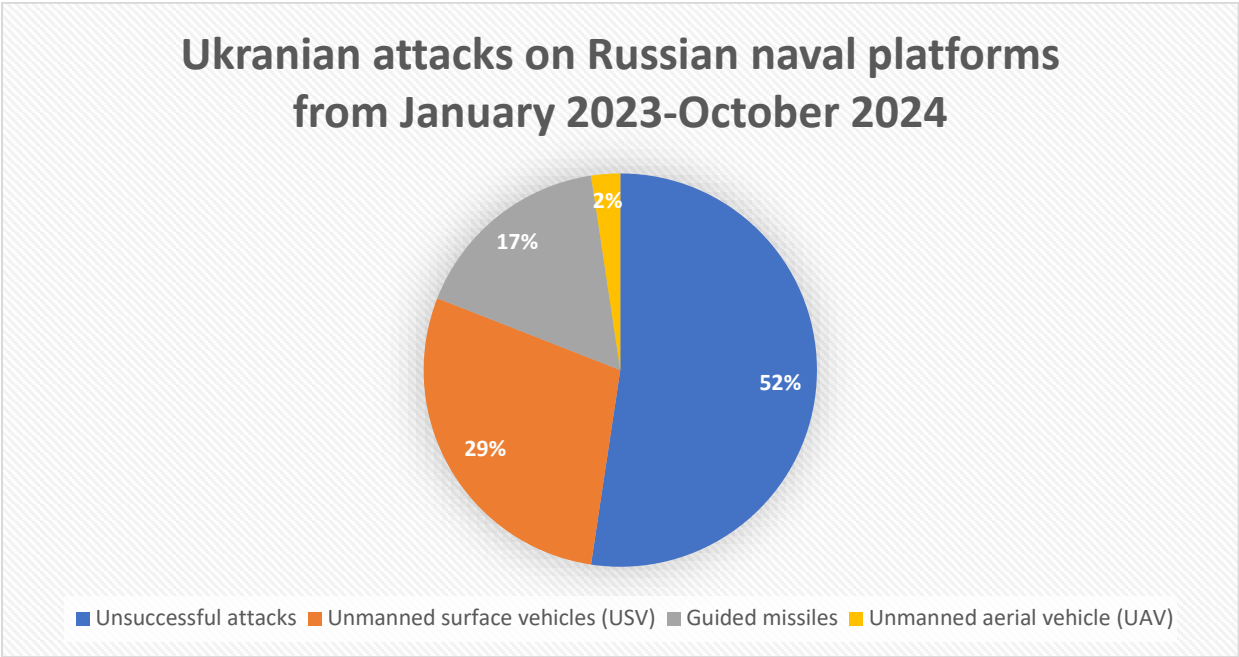
Comparison of naval platforms involved in notable UAV incidents and attacks

	<i>Arleigh Burke</i>	<i>FREMM</i>	<i>Type 45</i>	<i>Hydra</i>	<i>Gyruza-M</i>	<i>Project 2163 Buyan-M</i>	<i>Project 12411 Tarantul</i>	<i>Project MPSV07</i>
Country	United States	France	United Kingdom	Greece	Ukraine	Russia	Russia	Russia
Class	Destroyer	Frigate	Destroyer	Frigate	Patrol boat	Corvette	Corvette	Multifunctional salvage ship
Length overall (meters)	155.3	142.2	152.4	117	23	74.1	56.1	73
Full displacement (metric ton)	9 880 t	6 040 t	8 000 t	3 350 t	54 t	949 t	436 t	3634 t
Anti-air defence	SAM	Aster 15	Aster 15 Aster 30	RIM 7P-sea sparrow	/	2 Komar turret launchers with 16 9M39 Igla or 9M313 Igla-1	9K32/9K32M Strela-2/2M quad launcher	/
Close-in weapon systems	1 BAE Systems MK45 MOD 2 127 mm 1 Raytheon Mk15 Phalax block 1B with M61A1 20 mm	1 Oto Melara 76 mm, M621 20 mm	1 Vickers MK 8 mod 114 mm, 2 Raytheon Mk 15 Phalanx Block 1B 20 mm, 2 MSI ASCG with ATK Mk 44 30 mm Bushmaster	1 United defends Mk 45 mod 2 127 mm, 2 Raytheon Mk15 Phalax block 1 20 mm	2 Katran-M, 1 ZTM-1 30 mm/100	1 A-190 70 mm, 2 AK-630M duet 30 mm	1 AK-176 76 mm/59, 2 AK-630M 30 mm	/
Detection radar	Lockheed Martin SPY-1D E/F-band	Thales Herakles E/F-band	Signaal/ Marconi type 1046 D-band	Signaal MW08 Signaal/Magnavox DA08 F-G band	Furuno I-band	Pozitiv-M1, I-band	34K1 Monolit I-band	/

Note. Table created by the authors based on multiple sources (Jane's Group UK Limited, 2023; Tugs Towing & Offshore Newsletter, 2023).

The data in Figure 2 shows that fewer than half of Ukrainian aerial attacks were classified as hits on target. Furthermore, UAVs accounted for only one successful hit (i.e. 2%) during the stated period, and no notable UAV incidents were recorded in the Black Sea. Therefore, USVs and guided missiles have proven to be more effective.

Figure 2
Ukrainian attacks on Russian naval platforms



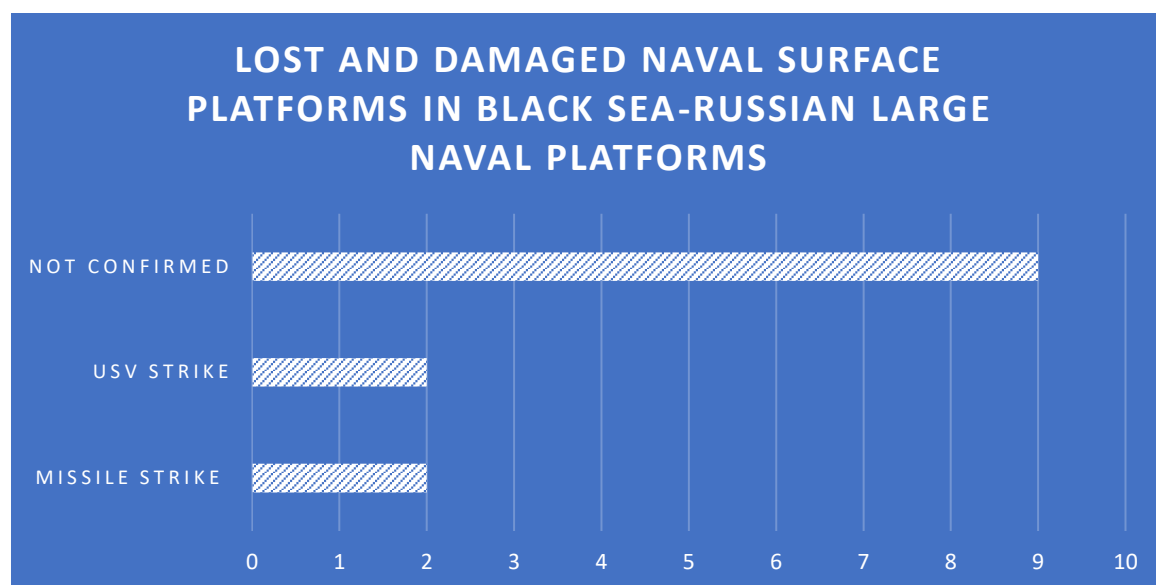
Note. Figure created by the authors based on Black Sea News (2024).

Of all Russian surface naval platforms attacked, the following figures analyse the weapons employed against large and small naval platforms. A previous analysis of the same dataset, conducted in spring 2024, found that five of eight large Russian platforms were destroyed by guided missiles. In that analysis, large platforms were defined as cruisers, submarines, landing ships, and minesweepers, while small platforms were defined as corvettes, patrol boats, and miscellaneous vessels (Tallis, 2024). Using this platform-size and vessel-type classification, Figures 3 and 4 present the analysis results for large and small naval platforms, respectively.

Figure 3 presents the distribution of causes of losses and damage to large naval platforms of the Russian Black Sea Fleet. The data indicate that guided missiles and unmanned surface vehicles account for most losses, while UAVs play a comparatively limited direct role against large naval platforms.

Figure 3

Causes of losses and damage to large naval platforms of the Russian Black Sea Fleet

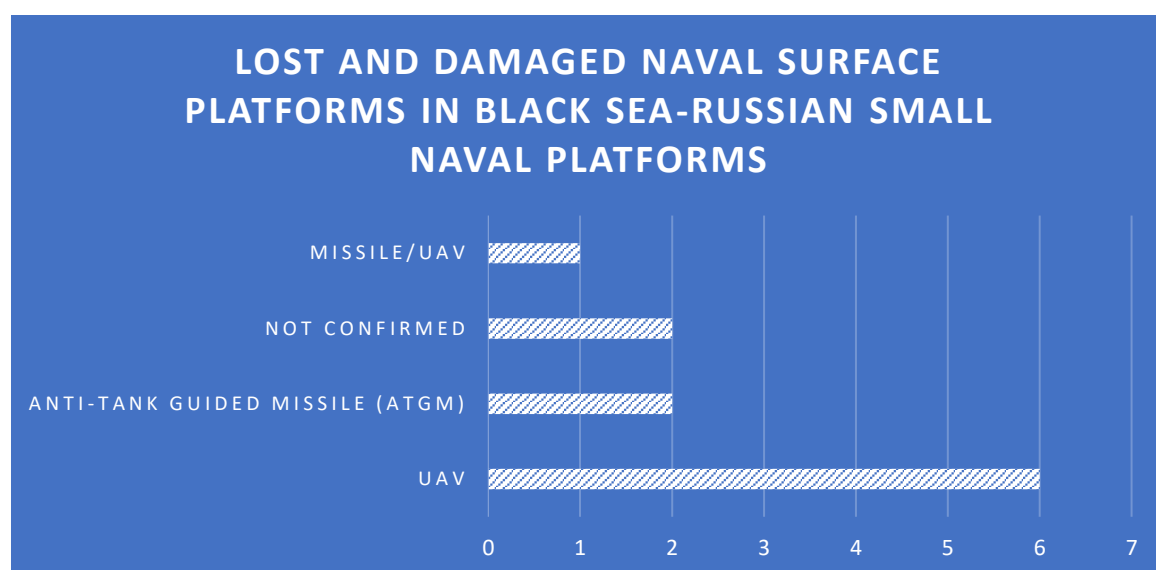


Note. Figure created by the authors based on Oryx (2022).

Figure 4 presents the distribution of causes of losses and damage to small naval platforms of the Russian Black Sea Fleet. The data indicate that UAVs and infantry-scale precision weapons account for a substantial share of damage events, whereas on larger vessels, guided missiles dominate.

Figure 4

Causes of losses and damage to small naval platforms of the Russian Black Sea Fleet



Note. Figure created by the authors based on Oryx (2022).

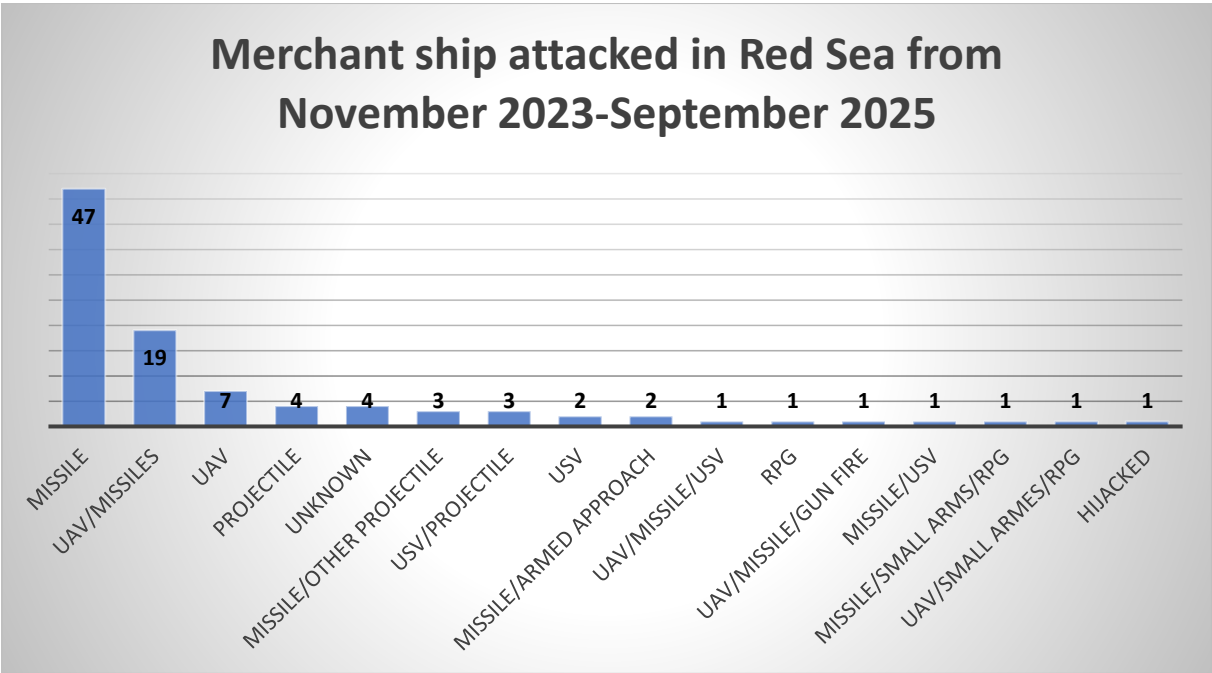
From these results, Tallis (2024) concluded two facts about the Black Sea theatre of operations:

- Guided missiles and USVs most effectively exploit the overall vulnerability of larger naval platforms.
- UAVs and infantry-scale weapons, such as Anti-Tank Guided Missiles, more often target smaller platforms.

Figure 5 presents an analysis of the attack methods employed by the Houthis against merchant vessels in the Red Sea area of operations, highlighting the significance of UAVs as attack assets in the absence of robust shipboard defences. Data illustrates the importance of UAVs primarily as a supporting element in missile and, occasionally, USV attacks in the Red Sea.

To contextualise UAV employment in the Red Sea in the absence of successful attacks on naval vessels, Figure 5 analyses weapons used against civilian merchant ships as proxy targets.

Figure 5
Weapons used against merchant vessels in the Red Sea



Note. Figure created by the authors based on Lloyd's List (n.d.)

Meanwhile, merchant maritime traffic in the Black Sea recorded 12 incidents in 2023 and 16 in 2024. Considering that 3,000 merchant vessels have transited the Ukrainian Black Sea ports of Odesa, Pivdenny, and Chornomorsk since July 2023, the "Maritime Threats and Security Trends Annual Incident Figures 2024" report labelled the area as low risk for merchant traffic. Means employed in these incidents remain unconfirmed (SAFETY4SEA, 2025).

This chapter concludes with two key statements:

- UAVs were the primary means of attack for Ukraine against Russian small naval platforms, including corvettes, patrol boats, and small support naval platforms.
- UAVs served as a supporting element in Houthi attacks, often operating in combination with guided missiles and USVs.

5. CAPABILITIES OF PROMINENT UAVs

This chapter presents prominent UAV models that have participated in attacks on surface naval platforms, such as the Ukrainian *Bayraktar TB2*, which is responsible for all confirmed successful UAV hits on Russian small vessels shown in Figure 4, and the *Lancet* unmanned aerial vehicle, which attacked the *Gyurza-M* patrol boat.

Other UAV models that may have participated in attacks on surface naval platforms remain unconfirmed. Ukrainian sources often refer to FPV kamikaze (one-way attack, OWA) UAVs when describing such strikes (Epstein, 2025). With reference to Ukrainian long-range UAV attacks in the Caspian Sea and possibly Lake Onega, the UAV with the greatest known range - the *FP-I*, presented in May 2025 - is discussed in (Safronov, 2025).

Russian forces, in contrast, reportedly conducted frequent patrols in the Black Sea, employing Iranian fixed-wing Mohajer-6 reconnaissance UAVs and Shahed-131/136 UAVs for OWA missions against naval platforms. Their range was extended by equipment installed on seized drilling platforms, which was later destroyed by Ukrainian special forces during Operation *Citadel* (BlackSea News, 2024). Table 3 presents a comparative analysis of the key operational capabilities of the UAVs mentioned above.

Table 3: Crucial operational capabilities of prominent UAVs

	<i>Bayraktar TB2</i>	<i>FP-I</i>	<i>Mohajer-6</i>	<i>Shahed-136/Geran-2</i>	<i>ZALA Lancet-3</i>
Country user	Ukraine	Ukraine	Russia	Russia	Russia
Country of origin	Turkey	Ukraine	Russia	Iran/Russia	Russia
Range	150 km	~1500 km	200 km	2000km	40 km
Payload	55 kg	50-120 kg	Mostly surveillance	40 kg	3 kg

Note. Table created by the authors based on multiple sources (Brahya, 2025; Chernysh et al., 2024; Shephard Defence Insight, 2025).

Combining data from the timeline and Table 3, the authors concluded that long-range OWA UAVs are getting more prevalent.

DISCUSSION AND CONCLUSION

The growing importance of UAVs in ground warfare is evident. Their development has set in motion the overall evolution of weapons, ordnance, and intelligence, surveillance, and reconnaissance (ISR) tools. UAVs have begun to replace or supplement the operational roles of hand grenades and mortars; anti-armour projectiles; tactical and long-range guided munitions; artillery fire correction; tactical air defence; and more (Tourret, 2025). Their direct impact of UAVs on naval surface warfare, however, although observable in contemporary crises such as Houthi attacks and the Russia-Ukraine War, is rarely discussed beyond general declarations of an emerging threat.

This paper explored the UAV threat to modern naval surface platforms through an analytical-synthetic approach, drawing on validated literature to identify key attributes that constitute a UAV threat to naval vessels. The evolution of the UAV threat was presented in a constructed timeline. Further tactical analysis highlighted the inherent vulnerability of small naval platforms with insufficient air-defence systems, while confirming the effectiveness of missile and USV attacks against larger platforms in the Black Sea.

However, the impact of UAVs on attacks against large surface platforms primarily manifests in support roles, such as monitoring and coordinating USV attacks or distracting and saturating air-defence systems during missile strikes. The case of the *Slava-class* missile cruiser *Moskva* underscores that, reportedly, advanced, distracted layered air-defence systems can be defeated by subsonic missile attacks (Waters, 2025). Without the air-defence umbrella provided by *Moskva* and other larger units sheltered in Novorossiysk, smaller units were easily destroyed by UAVs such as *Bayraktar TB2* (Tallis, 2024). A renewed analysis presented in this paper confirms Tallis's (2024) conclusion that missiles remain a crucial component of strikes against naval surface targets. Analysis also highlights the attrition effect of UAVs in saturating air-defence systems, which can lead to rapid overconsumption of magazine storage, rendering a naval platform defenceless if its air-defence capabilities are not scalable.

In the Red Sea theatre, no UAV hits on naval vessels were recorded. However, analysis of merchant traffic confirmed the primary role of missiles while highlighting a supporting role for UAVs, even when attacking unarmed or undefended targets. Houthi attacks further demonstrated the attrition effect by comparing the UAV threat with the air-defence measures employed by coalition naval vessels stationed there.

From the series of UAV attacks intercepted with high-value interceptors, the attack on 30 January 2025 is notable: the USS *Stockdale* (DDG-106) shot down a late-detected, low-flying UAV as part of a mixed missile-UAV Houthi attack. This incident demonstrated the

effectiveness of the naval platform's gun deck in intercepting UAVs under challenging conditions (Mongilio, 2025).

Advancements in UAV swarm attacks, the extended range of UAV strikes, such as the Ukrainian attack on a Caspian Sea naval harbour, and new hybrid tactics employing autonomous platforms, like the Ukrainian attack on 21 October 2025, which combined Barracuda-class USVs as carriers for FPV UAVs, pose growing threats to future naval platforms. This has led authors to conclude that such systems will need to share information with surface monitoring networks and employ micro-Doppler radar processing, fused with other sensors in a hybrid sensing subsystem, to provide data for layered soft- and hard-kill defences.

Lessons from ground-based C-UAV defence in Ukraine indicate that UAV protection is most effective when implemented from the individual infantry level and scaled up to larger units (SkyCTRL, 2025). Whether small naval surface platforms with limited air-defence capabilities should adopt this approach by installing small C-UAV systems or rely on a C-UAV umbrella provided by shore installations or larger platforms will depend on each navy's operational doctrine. However, considerations regarding cost scalability, the ability to scale systems efficiently, the abundance of counter-UAV weapons, and the effectiveness of sensor equipment, especially in indented and rugged coastlines, remain critical for future development and research.

REFERENCES

- Albright, D., Burkhard, S., Faragasso, D., & Spencer, S. (2024, 9 May). *Alabuga's Shahed 136 (Geran-2) warheads: A dangerous escalation*. Institute for Science and International Security. <https://isis-online.org/isis-reports/alabugas-shahed-136-geran-2-warheads-a-dangerous-escalation>
- Anonymous. (2024). *The role of small and medium UAVs in recent conflicts: Lessons and forecasting trends in the development of UAV forces in the military* (JCSP 50 – PCEMI 50). Canadian Forces College. <https://www.cfc.forces.gc.ca/259/290/950/286/Anon435.pdf>
- Bailey, J. (2025, 7 April). The world's best military drones in 2025. *AeroTime*. <https://www.aerotime.aero/articles/25712-worlds-best-military-drones>
- BlackSea News. (2024, 26 November). *Database of Ukrainian attacks on the occupied Crimea, Russian ships and facilities on the Black Sea coast in January–October 2024*. <https://www.blackseanews.net/en/read/226359>
- Brahy, J. (2025, 8 May). Ukraine may have used its new FP-1 deep-strike drone against Russia weeks before publicly acknowledging its existence. *Army Recognition*. <https://www.armyrecognition.com/focus-analysis-conflicts/army/conflicts-in-the-world/russia-ukraine-war-2022/ukraine-may-have-used-its-new-fp-1-deep-strike-drone-against-russia-weeks-before-publicly-acknowledging-its-existence>
- Center for Maritime Strategy. (2024, 18 July). *The Houthis, Operation Prosperity Guardian, and asymmetric threats to global commerce*. <https://centerformaritimestrategy.org/publications/the-houthis-operation-prosperity-guardian-and-asymmetric-threats-to-global-commerce/>
- Chernysh, V., Chornogor, O., Rad, A., Iaroslav, O., & Pavlo, K. (2024). *Russian unmanned systems: Current state, prospects of production and application* (Analytical report). Foreign Policy Council "Ukrainian Prism". https://prismua.org/wp-content/uploads/2024/08/Russian-Unmanned-Systems_%D1%83%D1%82%D0%BF.pdf
- Coffin, A. M. (2019). *To ROE or not to ROE: Small unmanned aerial vehicles and self-defense*. Naval War College. <https://apps.dtic.mil/sti/tr/pdf/AD1077939.pdf>
- Cropsey, S. (2022). Naval considerations in the Russo-Ukrainian War. *Naval War College Review*, 75(4), Article 4. <https://digital-commons.usnwc.edu/nwc-review/vol75/iss4/4>
- De Quevedo, Á. D., Urzaiz, F. I., Menoyo, J. G., & López, A. A. (2019). Drone detection and radar-cross-section measurements by RAD-DAR. *IET Radar, Sonar & Navigation*, 13(9), 1437–1447. <https://doi.org/10.1049/iet-rsn.2018.5646>
- Delanoë, I. (2024, 7 February). *Russia's Black Sea Fleet in the "Special Military Operation" in Ukraine*. Foreign Policy Research Institute. <https://www.fpri.org/article/2024/02/russias-black-sea-fleet-in-the-special-military-operation-in-ukraine/>

- Epstein, J. (2025, 28 August). Ukraine says it hit a Russian missile ship with flying explosive-packed drones. *Business Insider*. <https://www.businessinsider.com/ukraine-hit-russian-missile-ship-with-flying-drones-2025-8>
- EUR-Lex. (2025, 12 February). *European Union military operation to contribute to maritime security in the West Indian Ocean and in the Red Sea (EUNAVFOR Atalanta)*. <https://eur-lex.europa.eu/EN/legal-content/summary/european-union-military-operation-to-contribute-to-maritime-security-in-the-west-indian-ocean-and-in-the-red-sea-eunavfor-atalanta.html>
- Flórez, J., Ortega, J., Betancourt, A., García, A., Bedoya, M., & Botero, J. S. (2020). A review of algorithms, methods, and techniques for detecting UAVs and UAS using audio, radiofrequency, and video applications. *TecnoLógicas*, 23(48), 269–285. <https://doi.org/10.22430/22565337.1408>
- Fornusek, M. (2025, 11 September). Ukrainian drone disables rare Russian vessel patrolling Black Sea, intelligence says. *The Kyiv Independent*. <https://kyivindependent.com/ukrainian-drones-strike-rare-russian-vessel-patrolling-off-novorossiysk-intelligence-says-shows-footage/>
- Hollenbeck, N., Altaf, M. H., Avila, F., Ramirez, J., Sharma, A., & Jensen, B. (2025). *Calculating the cost-effectiveness of Russia's drone strikes*. Center for Strategic and International Studies. <https://www.csis.org/analysis/calculating-cost-effectiveness-russias-drone-strikes>
- Hood, C. (2021). *Counter unmanned aerial system defense for high-value units afloat pierside* (Master's thesis). Purdue University. https://hammer.purdue.edu/articles/thesis/Counter_Unmanned_Aerial_Defense_For_High_Value_Units_Afloat_Pierside/15057258
- Javed, S., Hassan, A., Ahmad, R., Ahmed, W., Ahmed, R., Saadat, A., & Guizani, M. (2024). State-of-the-art and future research challenges in UAV swarms. *IEEE Internet of Things Journal*, 11(11), 19023–19045. <https://doi.org/10.1109/JIOT.2024.3364230>
- Jane's Group UK Limited. (2023). *Jane's fighting ships 2023–2024*.
- Kartini, A.T., Irmawan, E., & Setiawan, F. (2024). Manufaktur UAV fixed wing menggunakan material styrofoam dengan metode lay-up fiberglass dan resin. *Teknika STTKD*, 10(1), 44–52. <https://doi.org/10.56521/teknika.v10i1.1054>
- Khomenko, I. (2025, 8 July). *Russia reportedly deploys bird-like spy drones to outsmart detection*. UNITED24 Media. <https://united24media.com/latest-news/russia-reportedly-deploys-bird-like-spy-drones-to-outsmart-detection-9706>
- Kushnikov, V. (2024, 6 November). Tarantul-class corvette was hit in the Caspian Sea. *Militarnyi*. <https://militarnyi.com/en/news/tarantul-class-corvette-was-hit-in-the-caspian-sea/>

- Kyiv Post. (2025, 20 May). Russia increases lethality of Shahed drones with 90-kilogram warhead. *Kyiv Post*. <https://www.kyivpost.com/post/53025>
- LaGrone, S. (2023, 19 December). "Operation Prosperity Guardian" set to protect ships in the Red Sea. *USNI News*. <https://news.usni.org/2023/12/18/operation-prosperity-guardian-set-to-protect-ships-in-the-red-sea-carrier-ike-in-gulf-of-aden>
- Lerouvillois. (2025). Ukrainian Barracuda unmanned boat launches FPV drone strike on Russian vessel in Dnipro. *Army Recognition*. <https://www.armyrecognition.com/focus-analysis-conflicts/army/conflicts-in-the-world/russia-ukraine-war-2022/ukrainian-barracuda-unmanned-boat-launches-fpv-drone-strike-on-russian-vessel-in-dniper>
- Liu, P. (2023). Research on detection and attack strategy against swarm of drones. In *Proceedings of the 2023 IEEE 11th Joint International Information Technology and Artificial Intelligence Conference (ITAIC)* (pp. 1648–1653). <https://doi.org/10.1109/ITAIC58329.2023.10408898>
- Lloyd's List. (n.d.). *Reported Houthi attacks in the Red Sea and Gulf of Aden*. <https://www.lloydslist.com/hot-topics/red-sea-risk/map-and-list-of-attacks>
- Mongilio, H. (2024, 12 November). Houthis attack two US destroyers leaving the Red Sea. *USNI News*. <https://news.usni.org/2024/11/12/houthis-attack-two-u-s-destroyers-leaving-the-red-sea-pentagon-says>
- Mongilio, H. (2025, 30 January). Crew of USS Stockdale shot down Houthi drones with 5-inch gun. *USNI News*. <https://news.usni.org/2025/01/30/crew-of-uss-stockdale-shot-down-houthi-drones-with-5-inch-gun-says-admiral>
- Navy Lookout. (2023, 16 December). Royal Navy destroyer HMS Diamond shoots down drone while escorting merchant ships in the Red Sea. *Navy Lookout*. <https://www.navylookout.com/royal-navy-destroyer-hms-diamond-shoots-down-drone-while-escorting-merchant-ships-in-the-red-sea/>
- NATO. (2019). *Allied Joint Doctrine for the Conduct of Operations: AJP-3(C)*. NATO Standardization Office. <https://www.almendron.com/tribuna/wp-content/uploads/2019/07/doctrine-nato-conduct-of-ops-ajp-3.pdf>
- Oryx. (2022, 24 March). *List of naval losses during the Russian invasion of Ukraine*. <https://www.oryxspioenkop.com/2022/03/list-of-naval-losses-during-2022.html>
- Ozberk, T. (2025, 1 September). Ukraine strikes Russian Project 21631 Buyan-M class corvette with drones. *Naval News*. <https://www.navalnews.com/naval-news/2025/09/ukraine-strikes-russian-project-21631-buyan-m-class-corvette-with-drones/>
- Popa, A., & Learschi, S. (2025, 15 April). Russia's strategic naval collapse (2022-2025) in the context of the war in Ukraine. *Maritime Security Forum*. <https://www.forumulsecuritatimaritime.ro/russias-strategic-naval-collapse-2022-2025-in-the-context-of-the-war-in-ukraine-2/>

- Puspoayu, E. S., Widodo, H., Ronaboyd, I., Lovisonnya, I., & Amiq, D. B. (2022). Legal classification on the armed conflict between Ukraine and Russia in light of international humanitarian law. *SHS Web of Conferences*, 149, 03020. <https://doi.org/10.1051/shsconf/202214903020>
- Rahman, S., & Robertson, D. A. (2018). Radar micro-Doppler signatures of drones and birds at K-band and W-band. *Scientific Reports*, 8(1), 17396. <https://doi.org/10.1038/s41598-018-35880-9>
- Reuters. (2024, 25 April). Greek military ship intercepts two Houthi drones in the Red Sea. *Reuters*. <https://www.reuters.com/world/greek-military-ship-intercepts-two-houthi-drones-red-sea-2024-04-25/>
- Rogoway, H. A., & Payne, T. S. (2022, 29 October). Ukraine unleashes mass kamikaze drone boat attack on Russia's Black Sea Fleet headquarters. *The War Zone*. <https://www.twz.com/ukraine-unleashes-mass-kamikaze-drone-boat-attack-on-russias-black-sea-fleet-headquarters>
- Rogoway, T. (2022, 20 August). Ukraine situation report: Shadowy long-range kamikaze drone strikes again. *The War Zone*. <https://www.twz.com/ukraine-situation-report-shadowy-long-range-kamakaze-drone-strikes-again>
- Rojhani, N., & Shaker, G. (2024). Comprehensive review: Effectiveness of MIMO and beamforming technologies in detecting low RCS UAVs. *Remote Sensing*, 16(6), 1016. <https://doi.org/10.3390/rs16061016>
- Saballa, J. (2024, 7 August). China unveils military spy drones disguised as birds. *The Defense Post*. <https://thedefensepost.com/2024/08/07/china-military-spy-drones/>
- Safet4sea. (2025, 17 January). RiskIntelligence: Threats against shipping in the Black Sea. *SAFETY4SEA*. <https://safety4sea.com/riskintelligence-threats-against-shipping-in-the-black-sea/>
- Safronov, T. (2025, 6 May). It can fly up to 1,600 km: Ukraine presents FP-1 attack drone. *Militarnyi*. <https://militarnyi.com/en/news/it-can-fly-up-to-1600-km-ukraine-presents-fp-1-attack-drone/>
- Saleh, Z., & Ziade, P. (2025, 29 May). A \$500 attack drone costs millions to repel: It's an economic war, and the West is losing. *The Globe and Mail*. <https://www.theglobeandmail.com/business/commentary/article-a-500-attack-drone-costs-millions-to-repel-its-an-economic-war-and-the/>
- Satta, M. (2025, 14 August). *Rethinking NATO's defence in the drone era*. Atlas Institute for International Affairs. <https://atlasinstitute.org/rethinking-natos-defence-in-the-drone-era/>

- Sharma, B., & Purohit, A. (2025). UAV detection and identification: A comparative review of current methods and future directions. In *Proceedings of the International Conference on Advancements in Computing Technologies and Artificial Intelligence (COMPUTATIA-2025)* (pp. 205–217). Atlantis Press. https://doi.org/10.2991/978-94-6463-700-7_17
- Shephard Defence Insight. (2025, 25 September). Bayraktar TB2. *Shephard*. <https://plus.shephardmedia.com/detail/bayraktar-tactical-uas/>
- SkyCTRL. (2025). *Anti-drone warfare: Insights from Ukraine's drone war*. <https://skyctrl.com/cuas-academy/anti-drone-warfare-ukraines-drone-war/>
- Tugs Towing & Offshore Newsletter. (2023, 17 May). Tugs & Towing News. *Tugs Towing & Offshore Newsletter*, 24(39), 1 -34. https://www.mastermariners.uk/public/Newsletter_39_2023.pdf
- Tallis, J. (2024, 31 July). The calm before the swarm: Drone warfare at sea in the age of the missile. *War on the Rocks*. <https://warontherocks.com/2024/07/the-calm-before-the-swarm-drone-warfare-at-sea-in-the-age-of-the-missile/>
- Tourret, V. (2025). *Design, destroy, dominate: Mass drone warfare as a potential military revolution*. French institute of international relations IFRI. https://www.ifri.org/sites/default/files/2025-06/ifri_tourret_drone_warfare_2025.pdf
- UK Ministry of Defence. (2025). *Allied Joint Doctrine for Maritime Operations: AJP-3.1(B)*. NATO Standardization Office. https://assets.publishing.service.gov.uk/media/67f3b07d53505b2ca44efeed/AJP_3_1_Maritime_Ops_EdB.pdf
- US Central Command. (2023, 15 November). *US Central Command statement on drone shoot down*. <https://www.centcom.mil/Media/Statements/Statements-View/Article/3599885/us-central-command-statement-on-drone-shoot-down/>
- Vavasseur, X. (2023, December 11). French frigate Languedoc used Aster 15 missiles against drones. *Naval News*. <https://www.navalnews.com/naval-news/2023/12/french-frigate-languedoc-used-aster-15-missiles-against-drones/>
- Waters, C. (2025, 31 March). Naval operations: Lessons from recent conflicts. *European Security & Defence*. <https://euro-sd.com/2025/03/articles/43406/naval-operations-lessons-from-recent-conflicts/>
- Wentzel, A., Cornils, J., Valentin, M., Heynicke, R., & Scholl, G. (n.d.). *Compact counter-UAS system for defeating small UAVs in complex environments*. NATO Science & Technology Organization. <https://publications.sto.nato.int/publications/STO%20Meeting%20Proceedings/STO-MP-SET-315/MP-SET-315-23.pdf>
- Xavier, W. (2025, 9 October). Ukraine claims successful strike on Russian warship in inland waters. *Baird Maritime*. <https://www.bairdmaritime.com/security/incidents/acts-of-war/ukraine-claims-successful-strike-on-russian-warship-in-inland-waters>

- Ziezulewicz, G. (2023a, 23 November). USS Thomas Hudner shoots down "one-way attack drones" in the Red Sea. *Navy Times*. <https://www.navytimes.com/news/your-navy/2023/11/23/uss-thomas-hudner-shoots-down-one-way-attack-drones-in-the-red-sea/>
- Ziezulewicz, G. (2023b, 16 December). USS Carney takes out drone swarm in the Red Sea. *Navy Times*. <https://www.navytimes.com/news/your-navy/2023/12/16/uss-carney-takes-out-drone-swarm-in-the-red-sea/>
- Zitar, R. A., Al-Betar, M., Ryalat, M., & Kassaymeh, S. (2023). A review of UAV visual detection and tracking methods (*arXiv:2306.05089*). *arXiv*. <https://doi.org/10.48550/arXiv.2306.05089>

IV

Applied Methodologies for Critical Infrastructure, Operational Systems, and Advanced Technologies



www.sois-ft.hr

METHODS AND APPLICATIONS OF MACHINE LEARNING FOR INTELLIGENT OBJECT DETECTION, CLASSIFICATION, AND TRACKING

Alojzije Culej¹, Andrija Ljulj², Igor Štambuk³

¹Croatian Armed Forces,
E-mail: alojzije.culej@morh.hr

²Dr. Franjo Tuđman Defense and Security University (SOIS FT),
E-mail: andrija.ljulj@sois-ft.hr,
ORCID: <https://orcid.org/0000-0003-4825-6796>

³Dr. Franjo Tuđman Defense and Security University (SOIS FT),
E-mail: igor.stambuk@sois-ft.hr,
ORCID: <https://orcid.org/0000-0001-6020-3238>

Abstract

This paper analyses modern algorithms for object detection, classification, and tracking in images and videos, applicable within optical systems on various military platforms, including unmanned aerial systems. It compares machine learning and computer vision methods, which are core to contemporary artificial intelligence. The objective is to evaluate these approaches by comparing the advantages and limitations of the most significant deep learning and neural network-based techniques, which enable efficient real-time data processing, a key requirement for autonomous control and navigation of unmanned systems. The analysis demonstrates that single-stage algorithms such as YOLO provide fast, sufficiently accurate detection suitable for real-time applications on platforms with limited computational resources, which is typical of unmanned systems.

As part of this work, selected object detection and tracking algorithms were implemented and tested in Visual Studio Code after installing the necessary machine learning and computer vision tools and libraries. Online tools such as RoboFlow were used to streamline image annotation and dataset preparation for model training. The YOLOv8 algorithm was used to detect, classify, and track tanks. The results indicate that open-source tools are feasible for developing and deploying advanced machine learning algorithms across both unmanned and

manned platforms for object detection, classification, and tracking. By integrating artificial intelligence, unmanned systems can autonomously detect, classify, and track various objects in complex and dynamic environments, thereby reducing the need for continuous human supervision.

Keywords: machine learning, object detection, object tracking, object classification.

INTRODUCTION

Object detection, classification, and tracking are essential components of modern computer vision systems used in military applications. These technologies enable the automated identification and monitoring of targets such as vehicles, aircraft, and personnel in complex and dynamic environments. By integrating machine learning and deep neural networks, object detection systems can achieve high accuracy even under challenging conditions, including low visibility or partial occlusion. Classification algorithms further enhance situational awareness by distinguishing between different types of objects and identifying potential threats. Object tracking ensures continuous monitoring of detected targets, providing real-time movement data critical for decision-making and threat assessment. Together, these methods form the foundation for advanced surveillance, reconnaissance, and autonomous defence systems.

The main goal of this work is to analyse and explore current methods and algorithms for object detection, classification, and tracking, to compare their performance and assess their applicability in military contexts. In addition, by applying several open-source algorithms, the study aims to demonstrate their practical implementation and effectiveness. The methodology used in this paper includes analysing and comparing various approaches and algorithms, followed by the development of machine-learning software using open-source tools such as OpenCV, Visual Studio, and Python. Finally, the acquired knowledge and experience are consolidated in the discussion and conclusion sections to enhance the use of available tools in military computer vision projects.

1. LITERATURE REVIEW

Porikli & Yimlaz (2012) review the key trends and methods in object detection and tracking for surveillance systems, highlighting their role in identifying meaningful events and automating video annotation and retrieval. It provides a taxonomy of popular approaches, discussing underlying concepts and limitations, to guide more effective integration in business-oriented video analytics. Du and Bobkov (2023) provided a comprehensive review of object detection and tracking algorithms, distinguishing between one-stage and two-stage detection paradigms and summarising representative methods within each category.

In contrast to survey-oriented studies, Bewley et al. (2016) focused on a lightweight and efficient tracking-by-detection framework for real-time scenarios. Their approach

demonstrated that accurate detection, combined with simple motion modelling and data association, can significantly improve multi-object tracking performance.

Ferreira et al. (2022) proposed an object tracking algorithm that combines random tree techniques with optical flow analysis, adapted by using Gaussian curvature to define minimal surfaces that represent object motion. Random trees are employed to eliminate redundant optical flow vectors, retaining only those essential for motion characterisation. The results demonstrate that the proposed method achieves accuracy and processing times comparable to the Lucas–Kanade and Horn–Schunck algorithms.

The work by Lee et al. (2014) examines the challenges of occlusion in object tracking, a critical issue in applications such as surveillance, human-computer interaction, and sports monitoring. It reviews state-of-the-art occlusion-handling methods, including motion modelling with Kalman and Particle filters, feature-based approaches, and multi-camera setups, classifies them into categories, and discusses key considerations such as motion model selection, image features, and emerging trends in occlusion resolution. The thesis by Kovač (2015) examines the current state and applications of artificial intelligence (AI), highlighting methods such as expert systems, machine learning, neural networks, evolutionary computing, and intelligent agents, with examples including virtual assistants, recommendation systems, and self-driving cars. The survey by Sankar et al. (2021) provides a comprehensive analysis of object detection and tracking in computer vision, focusing on deep learning-based methods, benchmark datasets, and recent developments in granular DL models. It reviews both generic and specific detection models, compares detector and tracker performance, highlights traditional and emerging applications, and discusses current challenges and future research directions, including the role of granular computing.

Ouardirhi et al. (2024) surveyed occlusion-handling techniques in smart video surveillance (SVS), emphasising their importance for improving object detection, tracking, and scene analysis in complex environments with minimal human intervention. By evaluating multiple benchmark datasets, the authors provided a comparative assessment of existing architectural solutions, identified persistent challenges, and outlined future research directions to enhance occlusion robustness in real-world SVS applications.

Unlu et al. (2019) presented an autonomous drone detection and tracking system that combines a static wide-angle camera with a turret-mounted zoom camera. Their multi-frame deep learning approach enables efficient detection of small aerial targets by simultaneously analysing both wide-angle and zoomed image planes, thereby reducing computational cost. The system integrates detection, tracking, and classification algorithms, along with operational protocols, to support robust UAV surveillance.

Vlahović (2024) developed a system for face detection and skin-tone recognition to recommend appropriate protective factors. The work combines theoretical foundations in

artificial intelligence, machine learning, and neural networks with a practical, Python-based implementation that detects faces, classifies skin tones, and generates corresponding recommendations for protective factors.

A review of challenges and methods in small object detection and tracking, a critical aspect of computer vision and visual surveillance, where limited appearance and distinguishing features make accurate tracking difficult, was presented. It categorises existing approaches, summarises relevant datasets and evaluation metrics, and discusses current challenges and future trends to enhance the performance and real-world applicability of surveillance systems (Mirzaei et al., 2023). A proposal of an improved target detection and tracking method that combines an enhanced Canny edge detection algorithm with morphological processing and an extended Kernel Correlation Filter (KCF) based on Kalman filtering was shown. By refining the convolution kernel and integrating nonlinear morphological filtering, the approach achieves clearer edge detection and, when tested on the video surveillance and OTB2013 datasets, demonstrates high accuracy in tracking moving targets (Xu et al., 2024).

The author builds a complete methodology that uses YOLOv8 to detect coloured sample objects (red, blue, yellow) and Deep SORT to track them over time, covering the dataset creation/annotation, training, and inference steps. He also details the practical adjustments needed, such as converting annotation formats and updating Deep SORT to be compatible with TensorFlow 2.x, to make the system work smoothly (Aksoy, 2025). The authors explain how to set up and use YOLOv8 with Python for real-time object detection and tracking on video, including loading pretrained models, running detection, and maintaining object trajectories via tracking logic (Gosthipaty & Raha, 2024). Dai et al. (2024) introduced a multimodal sensor fusion framework that combines YOLOv8-based visual detection with LiDAR measurements to improve perception in autonomous systems. The integration of real-time image-based detection and precise 3D spatial information enhances robustness across diverse environments and addresses challenges related to sensor alignment, ground segmentation, and computational performance.

Ultralytics (2025) described the Track mode as an extension of standard object detection, enabling multi-object tracking by assigning persistent identities to detected objects across video frames. The framework supports multiple built-in tracking algorithms, including BoT-SORT and ByteTrack, allows configuration through YAML files, and is compatible with Detect, Segment, and Pose models, thereby facilitating deployment in streaming and video-based applications.

Ghosh (2024) demonstrated the practical use of YOLOv8 for real-time object detection and multi-object tracking by integrating supported trackers such as BoT-SORT and ByteTrack to maintain consistent object identities across frames. The tutorial further illustrated how tracking outputs can be extended to object counting tasks, including full-frame counts, line-crossing detection, and zone-based analysis, using OpenCV drawing functions and region-based logic.

Howse and Joshi (2016) introduced OpenCV as an open-source, cross-platform computer vision library that provides high-level tools for image acquisition, processing, and analysis, with seamless integration into Python and scientific computing libraries such as NumPy and SciPy. Their work presented a progressive learning approach, covering topics from basic image processing and body-part tracking to advanced applications such as object removal, three-dimensional reconstruction, augmented reality, gesture recognition, and traffic sign detection.

Howse and Minichino (2020) provided a comprehensive treatment of OpenCV's Python bindings, guiding readers from foundational image and video processing techniques to advanced topics including object tracking, face detection, three-dimensional vision, augmented reality, and deep learning-based computer vision applications using OpenCV 4 and Python 3.

Roboflow (2025a) presented a web-based platform for image annotation, highlighting its role as a critical preparatory step in developing robust models for object detection, classification, and tracking.

This paper is organised as follows. After the introduction and literature review, Chapter 2 focuses on analysing and comparing current methods and algorithms for object detection, classification, and tracking. It compares various machine learning approaches and evaluates their effectiveness. Chapter 3 presents the implementation of the YOLO v8 algorithm for tank detection and tracking. Finally, Chapter 4 offers a conclusion, highlighting potential improvements in the use of the aforementioned tools and assessing future developments in this field.

Despite the extensive body of literature covering object detection, classification, and tracking, a clear gap remains between theoretical advancements and their practical implementation in defence-specific, real-time operational environments. Existing surveys predominantly focus on algorithmic taxonomies, performance comparisons, and benchmark evaluations. At the same time, comparatively little attention is given to integrating these methods within resource-constrained military systems. In particular, the practical feasibility of deploying modern deep learning models using accessible, open-source tools in real-world defence scenarios, such as unmanned platforms operating under real-time constraints, remains insufficiently explored.

This paper addresses this gap by moving beyond purely descriptive and survey-based analyses and providing a combined methodological and demonstrative contribution. Specifically, it not only analyses and compares state-of-the-art approaches, but also implements a complete workflow using open-source tools for dataset preparation, model training, and real-time deployment, with a focus on defence-relevant object detection and tracking. The contribution of this work is therefore twofold: applicative, through the validation of YOLOv8 in a realistic military-oriented use case, and demonstrative, by showing that advanced computer vision capabilities can be effectively developed and deployed using widely available tools. In doing

so, the paper bridges the gap between theory and practice and contributes to the operationalisation of machine learning methods in defence systems.

2. ANALYSIS AND COMPARISON OF CURRENT METHODS AND ALGORITHMS FOR OBJECT DETECTION, CLASSIFICATION, AND TRACKING

2.1. MACHINE LEARNING METHODS APPLICABLE TO OBJECT DETECTION, CLASSIFICATION, AND TRACKING

Machine learning is an interdisciplinary process in which computers learn from data using algorithms that identify patterns and generalise them to new situations. Its success largely depends on the quantity and quality of the data, since inadequate data can significantly reduce model performance. Machine learning is the capacity of systems to learn from problem-specific training data to automate analytical model building and solve associated tasks. Deep learning is a machine learning concept based on artificial neural networks. (Janiesch et al. 2021).

In accordance with Udousoro (2020), there are the following types of machine learning:

- Supervised learning, where the computer is being supplied with example input and their desired output, which learns a rule that is able to map inputs to outputs.
- Unsupervised learning where no label is given to the learning algorithm and it's allowed to determine the structure of its input.
- Semi-supervised learning lies between supervised and unsupervised learning, where the teacher gives an incomplete input or signal where some of the target outputs are missing, it can also be regarded as transduction.
- Reinforcement learning, where an environment interacts with the computer to be able to perform a certain goal without any input or interference from a teacher telling it what to do.

Culej (2025) compares different machine learning methods, as shown in Table 1.

Table 1

Machine learning methods comparison

Learning Method	Advantages	Disadvantages
Supervised learning	High accuracy, predictability, versatile application, and clear evaluation.	Requires a large amount of labelled data and poor adaptation to new patterns.
Unsupervised learning	No need for data labelling, discovers hidden patterns.	Unpredictable results, complex interpretation, lower precision.
Semi-supervised learning	Saves labelling resources and combines supervised and unsupervised learning.	Complex to implement, sensitive to the quality of the small labelled dataset
Reinforcement learning	Learning through interaction, adaptability to different environments, and sequential decision-making.	It can be slow and requires many trial-and-error iterations, making it difficult to define reward and penalty functions.

2.2. DEEP LEARNING

In recent years, deep learning has become one of the most important areas within machine learning, particularly in computer vision applications. Owing to their strong ability to learn from data, these methods are increasingly used for automatic object detection and tracking in various systems. In computer vision, deep learning models achieve outstanding results in tasks such as object recognition, semantic segmentation, and classification. Such approaches are applied in systems that use surveillance cameras, autonomous vehicles, or unmanned aerial vehicles, where it is crucial to quickly and accurately identify and track targets (Unlu et al., 2021). The advantage of deep learning lies in its ability to recognise patterns and features even in complex and visually ambiguous scenes. Popular algorithms, such as YOLO (You Only Look Once), enable real-time image processing, which is essential in applications where speed and reliability are key. In some cases, deep learning is combined with classical computer vision methods, such as optical flow algorithms. This combination can further enhance the accuracy and stability of tracking systems, especially in situations with limited computational resources (Ferreira et al., 2020).

2.3 COMPUTER VISION, METHODS AND ALGORITHMS FOR TARGET DETECTION, CLASSIFICATION AND TRACKING

2.3.1 Computer vision

By definition, computer vision is a field of artificial intelligence (AI) that leverages machine learning and neural networks to enable computers and systems to extract meaningful information from digital images, videos, and other visual data, and to make recommendations or take actions when anomalies or problems are detected. Its broad applicability is evident across numerous sectors. In industry, it is used for precise control of robotic systems, defect detection in manufacturing, and identification of production bottlenecks. In medical diagnostics, computer vision supports technologies such as CT imaging. In transportation, it enables the development of autonomous vehicles that can operate without human intervention. Security and surveillance applications include facial recognition at airports and protection against threats such as terrorism, while in the military, it is employed for weapon guidance and terrain analysis (Hrga, 2018).

2.3.2 Methods of object detection

Object detection and tracking are key processes in computer vision, aimed at identifying objects in visual data and tracking their movement over time. Detection involves recognising and localising objects in a single frame, while tracking refers to continuously following the same objects across a sequence of video frames (Zhao et al., 2015). These tasks are often performed using machine learning methods, particularly deep learning, in which algorithms such as convolutional neural networks (CNNs) enable object classification and the prediction of their positions in images and videos. In deep learning, object detection involves labelling

each object with its corresponding class and determining its bounding box, while tracking ensures that the object's identity is maintained across multiple frames (Pal et al., 2021).

The process of object detection and tracking in computer vision involves several key stages and incorporates a range of techniques, broadly categorised into classical methods and deep learning-based approaches. The object detection phase typically begins by identifying foreground objects using visual features. These initial hypotheses about object presence are then validated through classification, which assigns each detected entity to a class (Pal et al., 2021). Object detection approaches fall into three main categories:

- Appearance-based – utilise information such as colour, texture, and edges to recognise objects within an image. These methods are limited when objects are partially occluded (Zhao et al., 2015).
- Motion-based – analyse sequences of frames over time to identify moving objects. While useful, these methods are often unreliable in complex or dynamic scenes (Zhao et al., 2015).
- Deep learning-based – combine appearance and motion features using deep neural networks, achieving higher robustness and accuracy under diverse conditions (Pal et al., 2021).

Within deep learning, detection methods are categorised as one-stage or two-stage. In one-stage approaches, networks such as Yolo directly predict objects and their locations, enabling faster processing suitable for real-time applications. Two-stage networks first propose potential regions of interest, which are then classified and precisely bounded, offering higher accuracy, as in R-CNN (Region-based Convolutional Neural Network) architectures (Pal et al., 2021). The tracking phase follows detection, predicting future object positions, and linking objects across frames. Various algorithms, such as the Kalman filter and its nonlinear variants (e.g., Extended Kalman Filter and Particle Filter), are used to estimate motion based on prior parameters. In deep learning, tracking can be achieved through several approaches: some systems use features extracted from convolutional networks to improve detection association across frames, others use recurrent neural networks (RNNs) to track sequential changes over time. Embedding-based models help distinguish objects using learned representations, thereby enhancing tracking accuracy in dynamic environments (Pal et al., 2021).

The success of object tracking depends heavily on the quality of the initial detection, making careful selection of the detector and tracking method critical, given the nature of the data and application (Zhao et al., 2015). Tracking algorithms are divided into two-stage and one-stage methods. Object recognition in an image typically involves drawing a rectangle around each object and assigning a corresponding label, meaning that each object is classified and localised, not just the main object. Using the sliding window method would require applying deep neural networks to many image regions of different sizes, which is computationally intensive. To address this, researchers introduced the idea of recognising specific regions of interest (ROIs) likely to contain objects, allowing faster processing by focusing the network only on relevant areas.

The first such model, R-CNN, uses selective search to generate approximately 2000 candidate regions per image, which are then processed by a neural network to extract features and refine object localisation. Although R-CNN transforms detection into a classification problem, it suffers from slow training, high disk storage requirements, and slow inference. Fast R-CNN improved speed by processing the entire image in a single pass, though selective search remained time-consuming. The most advanced approach, Faster R-CNN, replaces selective search with a Region Proposal Network (RPN), which predicts likely object locations and significantly reduces the number of regions to check. These regions are then processed by the Faster R-CNN model, which includes additional layers for improved classification and localisation, making it faster and more accurate than previous models (Du & Bobkov, 2022). Although Faster R-CNN accelerated object recognition, it is still not fast enough for real-time detection. To address this, one-stage methods were developed that directly predict object positions and classes from an image. One of the best-known methods is YOLO.

Unlike two-stage algorithms like R-CNN, which first propose regions and then classify them, YOLO is a one-stage algorithm that performs detection and localisation in a single network without additional steps. This achieves significantly higher speed, up to ten times faster than Faster R-CNN, while maintaining good accuracy, making Yolo ideal for tasks requiring real-time processing, such as security cameras or autonomous vehicles. YOLO divides the image into an $S \times S$ grid, with each cell responsible for detecting whether an object is present within it. Each cell predicts the bounding box coordinates, object class, and a confidence score indicating the certainty of its prediction. Unlike older methods, Yolo does not use sliding windows or region proposals. Feature maps are divided into blocks; each block is classified, and non-maximum suppression is applied to remove duplicate bounding boxes for the same object. This results in a clear, final output. YOLO significantly simplifies and accelerates object detection by accurately identifying which objects are present and where they are in an image in a single pass (Du & Bobkov, 2022).

2.3.3 Object tracking methods

Object tracking algorithms in video are generally divided into two types: generative and discriminative methods. The most popular approach is the discriminative method, also known as tracking-by-detection; all algorithms described in this text are based on it. Beyond classical algorithms, object tracking can be categorised into correlation-filter-based methods (e.g., MOSSE – Minimum Output Sum of Squared Error) and deep learning-based methods (e.g., SORT – Simple Online and Realtime Tracking). Correlation is a concept from signal processing used to measure the relationship between signals. In computer vision, it is applied to measure similarity between regions of different images. Correlation filtering locates objects in video frames by comparing patterns for similarity. Before the advent of correlation filters and deep learning, traditional tracking algorithms were slow and less accurate.

MOSSE is one of the first successful correlation filters capable of tracking objects at high speed, up to 669 frames per second. MOSSE uses the Fast Fourier Transform (FFT) for rapid

image processing and filtering, efficiently locating the object's centre by identifying the peak correlation. On the other hand, the SORT algorithm does not use object features during tracking; it relies solely on the position and size of detection bounding boxes to estimate motion and associate objects across consecutive video frames. SORT consists of three main components: object detection (e.g., YOLO, R-CNN), a Kalman filter that predicts the object's position, and the Hungarian algorithm, which matches predictions to actual detections across successive frames. The Hungarian algorithm solves the problem of matching elements between two sets; in this case, it connects objects in the current and previous video frames. SORT is simple, fast, and capable of real-time operation when integrated with object detection, and it significantly improves tracking accuracy. This combination provides an effective balance between speed and precision (Du & Bobkov, 2022).

3. OBJECT DETECTION, CLASSIFICATION, AND TRACKING – YOLOV8 ALGORITHM EXAMPLE

3.1 Introduction

In this section, the YOLOv8 algorithm for object detection, classification, and tracking was used as an example of a fast and reliable algorithm. YOLOv8 is an advanced, real-time deep learning architecture designed for object detection, classification, and tracking. It is part of the Yolo family but introduces significant structural and training improvements over previous versions. The model uses a decoupled head, separating classification and bounding-box regression to improve accuracy and convergence speed. YOLOv8 employs anchor-free detection, which simplifies training and reduces computational overhead. The network is available in multiple size variants (n, s, m, l, x) to support a wide range of hardware constraints and speed-accuracy trade-offs. For object detection, YOLOv8 outputs bounding boxes, classes, and confidence scores with strong performance on both small and large objects. For image classification, YOLOv8 includes streamlined classification-only models that use efficient convolutional blocks tuned for high accuracy and low latency. For tracking, YOLOv8 integrates smoothly with ByteTrack, BoT-SORT, and other multi-object tracking frameworks, enabling robust identity preservation across video frames. The model introduces improved augmentation strategies, such as Mosaic and MixUp, to improve training stability. It also includes built-in support for exporting to ONNX, TensorRT, CoreML, and other deployment formats. YOLOv8's training pipeline emphasises simplicity, including automatic hyperparameter tuning and task-specific metrics. With these features combined, YOLOv8 delivers state-of-the-art performance across detection, classification, and tracking while remaining efficient and deployable in real-time applications. The entire procedure consists of the following steps: collecting a dataset of tank images, annotating the images, developing a training model using the YOLOv8 architecture, and applying the YOLOv8 model for object detection, classification, and tracking. All steps are presented in the following subsections. The main characteristics of the hardware used, along with other important training model parameters, are shown in Table 2.

Table 2

The main characteristics of hardware and important training model parameters

Hardware configuration	- AMD Ryzen 9 7940HX processor - Installed RAM 16 GB - CPU cores 16C/ 2.4 – 5.2 GHz - Graphics AMD Radeon™ 610M 2 CUs, up to 2.2 GHz
YOLOv8 variant	n
Image resolution	640x360
Batch size	16
Training duration	11h 35min
Data augmentation settings	Default settings for YOLOv8n

3.2 Picture set and annotation using Roboflow

The picture set of the main battle tank was developed using publicly available online sources. Some pictures were extracted from video streams using OpenCV and Python, by selecting specific frames. Initially, there were approximately 1,000 images, but after refinement and removal of similar and duplicate images, the final set consisted of 450 images. For picture set annotation Roboflow online tool was used. Roboflow is an online platform that simplifies the preparation of image datasets for computer vision projects. It provides intuitive tools for image annotation, supporting bounding boxes, polygons, keypoints, and segmentation masks. The interface allows users to label images collaboratively, making it easier to manage large datasets. Roboflow also automates dataset organisation by splitting images into training, validation, and test sets. It includes powerful preprocessing options, such as resizing, background removal, and class balancing. The platform offers extensive augmentation tools, such as rotation, flipping, noise addition, and colour adjustments, to improve model robustness. Roboflow converts datasets into formats compatible with common machine learning frameworks, including Yolo, COCO, TensorFlow, and PyTorch. The tool also hosts datasets in the cloud, enabling easy version control and sharing. Overall, Roboflow streamlines the entire data preparation pipeline, ensuring clean, high-quality image sets for effective model training (Roboflow.com, 2025b).

The result of picture annotation was annotation data for each picture, providing bounding-box coordinates for each tank. In this case, the picture set was divided into training and validation sets at a 75:25 ratio. An example of an annotated picture is shown in Figure 1.

Figure 1

An example of an annotated picture of tanks



Source: Picryl (n.d.).

3.3 YOLO v8 training model

The process starts by creating a new YOLOv8 model using a predefined structure, meaning it begins without any built-in knowledge. This model architecture defines how the system processes images and learns visual patterns. After the model is created, it is connected to a dataset configuration file that specifies where the images are located and which object categories it should learn to identify. The training phase then begins, during which the model repeatedly analyses the images, compares its predictions to the correct labels, and adjusts itself to improve accuracy. This training runs for many cycles, so the model can refine its understanding of shapes, colours, and object boundaries. Over time, it becomes better at recognising the objects it was trained on. Once training is complete, the model becomes a learned system that can detect those objects in new, unseen images. The next step is to convert this trained model into a format that can be used across different platforms. The chosen format is widely supported, making it easier to integrate the model into applications, including those running outside Python. This converted version enables faster, more flexible deployment in real-world situations. Overall, the workflow covers creating an empty model, training it on the image set, and preparing it for practical use. In YOLOv8, the model is evaluated on the validation set at the end of every training epoch to track its learning progress. After all training epochs are complete, a final validation run is performed to produce overall performance metrics. If early stopping is enabled, the validation results also help determine when to automatically stop training. Figure 2 shows the validation results for different images from the validation set.

Figure 2 Validation of the training model on the pictures from the validation set



Figure 3 shows the Yolo8 model's normalised confusion matrix. It shows that the model correctly detects a tank in 87% of cases and misses it in 13%. It also shows that the model misinterpreted the background for tanks, and this can be fixed by adding background pictures to the model without bounding boxes. In this way, the model can distinguish the tank from the background.

Figure 3 Yolo8 model normalised confusion matrix

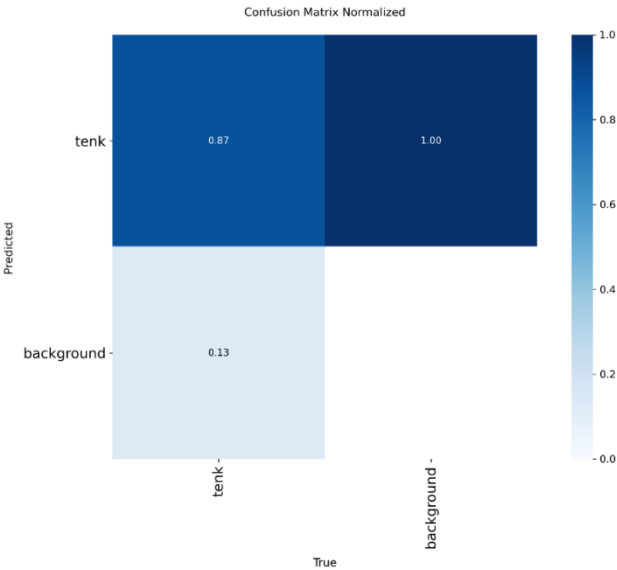
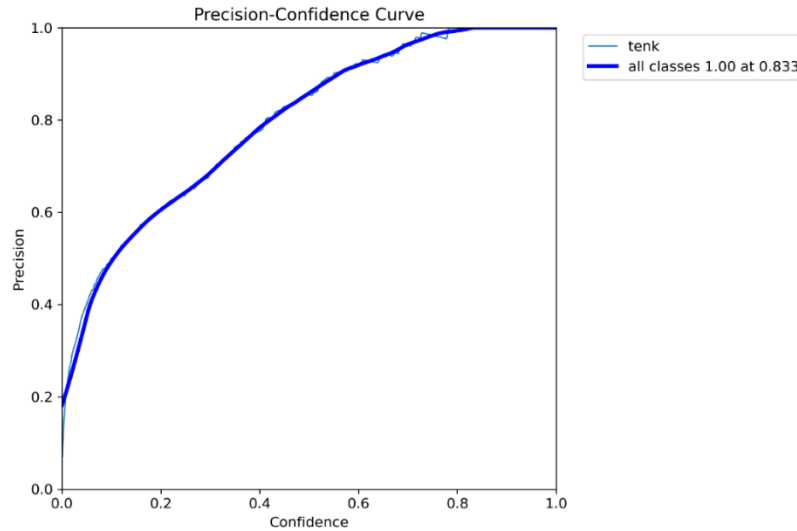


Figure 4 shows a precision confidence curve. For this model, a precision of 1.0 is achieved at a confidence threshold of 0.83; as confidence decreases, precision declines. Setting a higher

confidence threshold means higher precision, but fewer predictions. Therefore, the confidence threshold should be set to a balanced value between 0.45 and 0.65.

Figure 4 *Precision confidence curve*



The precision-recall curve is shown in Figure 5. X-axis, recall, represents the ratio of correctly detected objects to the total number of actual objects, while the Y-axis is the ratio of correct detections to the total number of positive predictions the model made. The curve is generated by varying the confidence threshold for a prediction. A higher area under the curve indicates better overall performance. It helps in choosing an optimal confidence threshold.

Figure 5 *Precision recall curve*

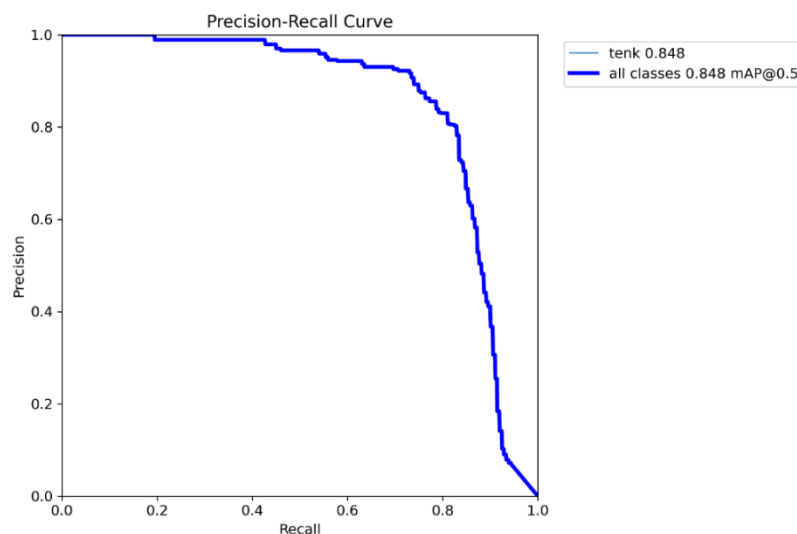
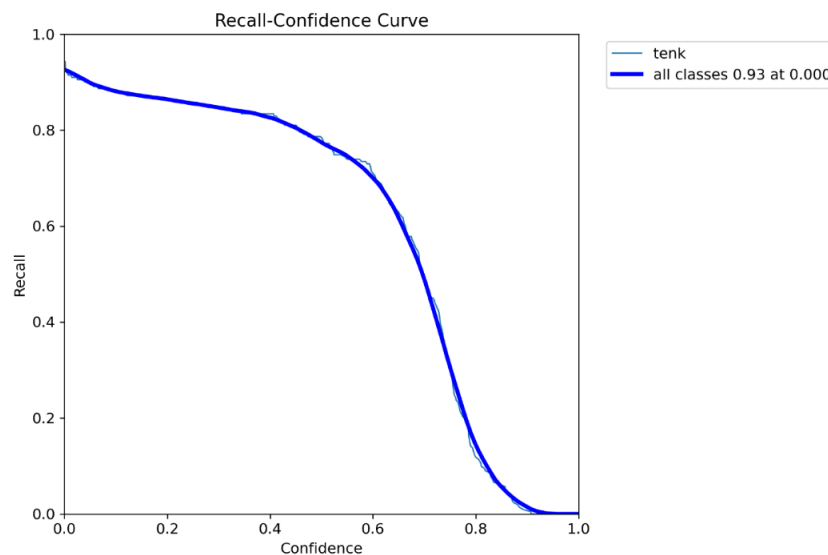


Figure 6 presents the recall confidence curve. The X-axis represents the confidence threshold, and the Y-axis represents recall. Recall measures the proportion of actual positive cases that the model correctly identifies (true positives) out of all actual positive cases. As the confidence

threshold increases, recall generally decreases because fewer predictions are accepted as valid, increasing the risk of missing some true positives. The curve illustrates the trade-off between accepting more predictions (higher recall, lower confidence) and being more certain about predictions (lower recall, higher confidence).

Figure 6

Recall confidence curve



In YOLOv8, `train/box_loss`, `train/cls_loss`, and `train/dfl_loss` are components of the total training loss that measure different aspects of the model's performance: `box_loss` measures bounding box accuracy, `cls_loss` evaluates classification correctness, and `dfl_loss` refines the box localisation precision. Metrics (precision and recall), pictures, and the aforementioned losses are shown in Figure 7. Precision is the ratio of correctly predicted positive instances to the total number of positive predictions made by the model. It shows how reliable the model's positive predictions are. High precision means the model makes very few false positive errors. After 150 epochs, the model's precision is above 0.8, which is acceptable. It can also be seen that different types of losses decrease as the number of epochs increases, which is a good sign of the model's improvement. However, it also shows that there is room to improve the model by increasing the number of epochs. Similar logic applies to recall, which is the ratio of correctly predicted positive instances to the total number of actual positive instances in the dataset. High recall means the model misses very few objects. As the number of epochs increases, both curves rise, indicating that the model is improving. The final metrics of the training model are presented in Table 3.

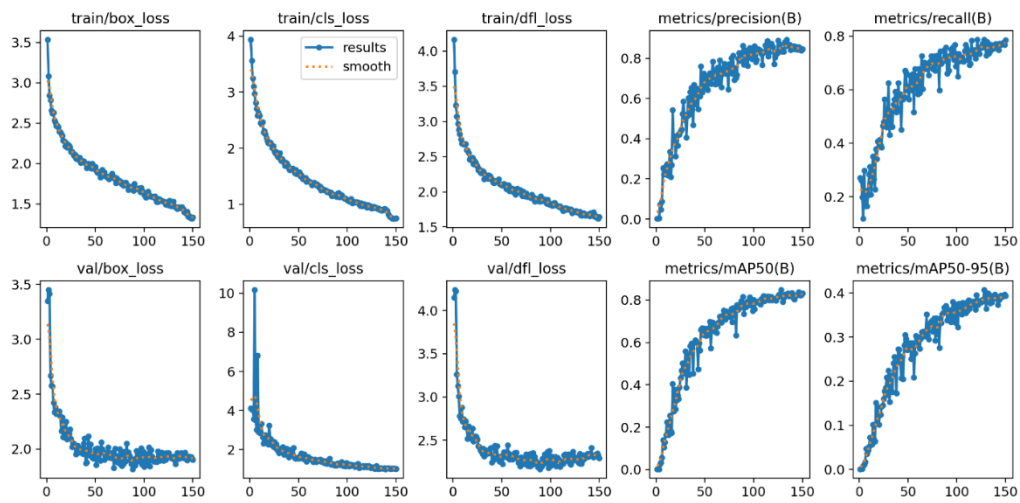
Table 3

The final metrics of the training model

Final precision (150 epochs)	0.84662
Final recall (150 epoch)	0.78479
maP@0.5	0.83196
maP@0.5:0.95	0.39396
Number of parameters	15
Inference time (FPS)	-

Figure 7

Model metrics

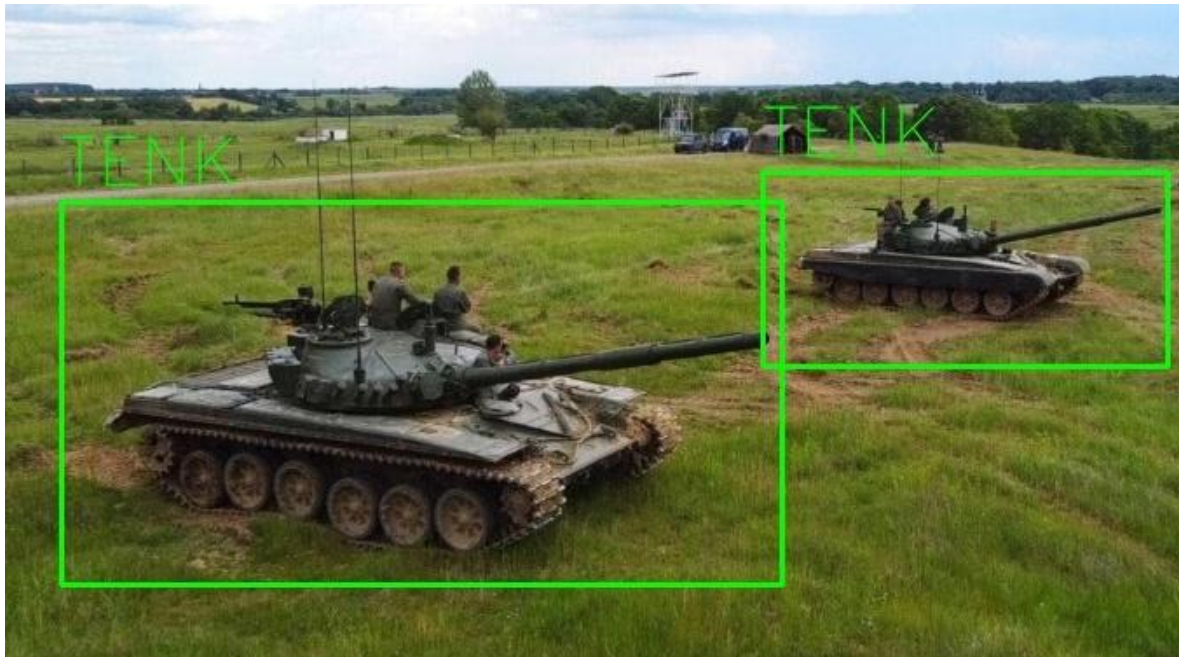


3.4 Using the Yolov8 training model on real pictures and video streams

After training the Yolov8 model on the tank dataset, it was possible to evaluate it on images and video streams not part of the training set. The model was checked on many new pictures and video streams. It shows a relatively good capability for detecting and classifying main battle tanks. Figure 8 shows the detection (and classification) of tanks, and ref (Ljulj, 2026) shows a video stream with detection and tracking of the tank across its frames.

Figure 8

Tank detection and classification example



Source: Dalmacija danas (2020)

As observed during further testing, the model has significant room for improvement. The dataset could be much larger, up to several thousand images, which would surely improve the model. The model will benefit from considering more pictures, viewing tanks from different angles and distances. Also, the model can be improved by increasing the number of epochs. Increasing the number of epochs in YOLOv8 training generally allows the model more time to learn from the data. With more epochs, the model can improve its accuracy, better fit complex patterns, and reduce prediction errors. The ideal number of epochs depends on the dataset size, complexity, and the rate at which the validation metrics stop improving.

The presented experimental results should be interpreted in light of several dataset-related limitations. The model was trained on a relatively small dataset of approximately 450 annotated images, which may not fully capture the variability of real operational environments, including different lighting conditions, viewing angles, distances, and background contexts. Consequently, the reported performance should be considered a preliminary proof of concept demonstrating the feasibility of applying deep learning-based object detection to the selected task rather than a fully generalised solution. A limited dataset size also increases the risk of overfitting, in which the model learns patterns specific to the training images rather than general object characteristics, potentially reducing performance on unseen data. To mitigate this risk and improve generalisation, future work should incorporate significantly larger and more diverse datasets, including additional negative samples and a wider range of environmental conditions.

CONCLUSION

This paper examined the application of artificial intelligence methods, with an emphasis on machine learning and computer vision, for object detection, classification, and tracking in both civil and military domains. Through analysis and comparison of various approaches, the key advantages and limitations of each were identified, along with an assessment of their practical applicability. As a representative solution, the single-stage deep learning method YOLOv8 was selected, and its effectiveness in detecting, classifying, and tracking defence-related objects was demonstrated.

The YOLOv8 model was developed and trained using open-source tools, including Python and the OpenCV library. The experimental evaluation demonstrates that the implemented detection model achieves a precision above 0.8 and correctly detects tank objects in approximately 87% of validation cases, indicating reliable performance for a single-class detection task. These results confirm that the applied approach provides a satisfactory balance between detection accuracy and computational efficiency for practical computer vision applications.

From a practical perspective, the achieved performance suggests that the proposed system can support real-time object detection and tracking on platforms with limited computational resources, such as unmanned aerial or ground systems. The model's ability to process images and video streams efficiently makes it suitable for deployment in surveillance, reconnaissance, and autonomous navigation systems, where rapid situational awareness is required.

However, several limitations remain. The model was trained on a relatively small dataset of approximately 450 annotated images, which may limit generalisation to diverse operational environments or unseen viewpoints. Additionally, the current implementation focuses on a single object class, thereby limiting the system's applicability to more complex multi-object detection scenarios.

Future research should therefore extend the model toward multi-class detection, enabling simultaneous identification of multiple objects within the same scene. Further work should also investigate robustness against adversarial perturbations and environmental variations, as well as domain adaptation techniques that improve performance when models are applied to data from different sensors or operational contexts. In conclusion, this work demonstrates that open-source tools can be used effectively to develop and implement machine learning-based solutions for object detection, classification, and tracking.

REFERENCES

- Aksoy, S. (2025). Object detection and tracking using YOLOv8 and DeepSORT. *Medium*. <https://medium.com/@serurays/object-detection-and-tracking-using-yolov8-and-deepsort-47046fc914e9>
- Bewley, A., Ge, Z., Ott, L., Ramos, F., & Upcroft, B. (2016). Simple online and realtime tracking. *Proceedings of the IEEE International Conference on Image Processing (ICIP)*.
- Culej, A. (2025). *Primjena umjetne inteligencije za detekciju i praćenje ciljeva na zračnim besposadnim sustavima* (Final thesis). Hrvatsko vojno učilište "Dr. Franjo Tuđman".
- Dai, Y., Kim, D., & Lee, K. (2024). An advanced approach to object detection and tracking in robotics and autonomous vehicles using YOLOv8 and LiDAR data fusion. *Electronics*, 13, 2250. <https://doi.org/10.3390/electronics13122250>
- Dalmacija danas. (2020, June 3). Splitska ekipa snimila reportažu o glavnom oklopnom vozilu Hrvatske vojske: Tenk M84-A4 Sniper. *Dalmacija danas*. <https://www.dalmacijadanas.hr/splitska-ekipa-snimila-reportazu-o-glavnom-oklopnom-vozilu-hrvatske-vojske-tenk-m84-a4-sniper/>
- Docs Ultralytics. (2025). *Multi-object tracking with Ultralytics YOLO*. <https://docs.ultralytics.com/modes/track>
- Du, K., & Bobkov, A. (2023). An overview of object detection and tracking algorithms. *Engineering Proceedings*. 33(1), 22. <https://doi.org/10.3390/engproc2023033022>
- Ferreira, R., Ferreira, J. C., & Neves, A. R. (2022). Object tracking using adapted optical flow. In *Information extraction and object tracking in digital video*. <https://doi.org/10.5772/intechopen.102863>
- Ghosh, A. (2024). *YOLOv8 object tracking and counting with OpenCV*. LearnOpenCV. <https://learnopencv.com/yolov8-object-tracking-and-counting-with-opencv/>
- Gosthipaty, A. R., & Raha, R. (2024). *Object tracking with YOLOv8 and Python*. PyImageSearch. <https://pyimagesearch.com/2024/06/17/object-tracking-with-yolov8-and-python>
- Hrga, M. (2018). *Računalni vid*. Elektronički zbornik radova Veleučilišta u Šibeniku.
- Howse, J., & Joshi, P. (2016). *OpenCV: Computer vision projects with Python*. Packt Publishing.
- Howse, J., & Minichino, J. (2020). *Learning OpenCV 4 computer vision with Python 3* (3rd ed.). Packt.
- Janiesch, C., Zschech, P., & Heinrich, K. (2021). Machine learning and deep learning. *Electronic Markets*, 31, 685–695. <https://doi.org/10.1007/s12525-021-00475-2>
- Kovač, L. (2015). *Umjetna inteligencija danas* (Doctoral dissertation). Sveučilište u Rijeci. <https://repository.ffri.uniri.hr/object/ffri:824>

- Lee, B. Y., Liew, L. H., Cheah, W. S., & Wang, Y. C. (2014). Occlusion handling in video object tracking: A survey. *IOP Conference Series: Earth and Environmental Science*, 18, 012097. <https://doi.org/10.1088/1755-1315/18/1/012097>
- Ljulj, A. (2026). *Tank detection and tracking* [Video]. YouTube. <https://www.youtube.com/watch?v=YKVZhuiMnOs>
- Mirzaei, B., Nezamabadi-pour, H., Raoof, A., & Derakhshani, R. (2023). Small object detection and tracking: A comprehensive review. *Sensors*, 23(15), 6887. <https://doi.org/10.3390/s23156887>
- Ouardirhi, Z., Mahmoudi, S. A., & Zbakh, M. (2024). Enhancing object detection in smart video surveillance: A survey of occlusion-handling approaches. *Electronics*, 13(3), 541. <https://doi.org/10.3390/electronics13030541>
- Pal, S. K., Pramanik, A., Maiti, J., & Mitra, P. (2021). Deep learning in multi-object detection and tracking: State of the art. *Applied Intelligence*, 51, 6400–6429. <https://doi.org/10.1007/s10489-021-02293-7>
- Porikli, F., & Yilmaz, A. (2012). *Object detection and tracking*. Mitsubishi Electric Research Laboratories.
- Picryl. (n.d.). The destroyed remains of Iraqi T-main battle tanks (MBT) litter an Iraqi military [Photograph]. Picryl. <https://picryl.com/search?q=the%20destroyed%20remains%20of%20iraqi%20t%20main%20battle%20tanks%20mbt%20litter%20an%20iraqi%20military>
- Roboflow. (2025a). *The fastest way to label computer vision datasets*. <https://roboflow.com/annotate>
- Roboflow. (2025b). *Everything you need to build and deploy computer vision applications*. <https://aiexpert.network/roboflow/>
- Udousoro, I. C. (2020). Machine learning: A review. *Semiconductor Science and Information*.
- Unlu, E., Zenou, E., Riviere, N., & Dupouy, P.-E. (2019). Deep learning-based strategies for the detection and tracking of drones using several cameras. *IPSI Transactions on Computer Vision and Applications*, 11.
- Vlahović, T. (2024). *Strojno učenje za detekciju i prepoznavanje lica* (Doctoral dissertation). Sveučilište u Zagrebu.
- Xu, J., Niu, S., & Wang, Z. (2024). Object tracking method based on edge detection and morphology. *EURASIP Journal on Advances in Signal Processing*, 45.
- Zhao, Y., Shi, H., Chen, X., Li, X., & Wang, C. (2015). An overview of object detection and tracking. In *Proceedings of the IEEE International Conference on Information and Automation*. <https://doi.org/10.1109/ICInfA.2015.7279299>

INITIAL DEPLOYMENT OPTIMIZATION OF TACTICAL MULTI-TECHNOLOGY TELECOMMUNICATIONS NETWORKS: A LITERATURE REVIEW

Mario Muñoz Fernández¹, Nina Skorin-Kapov²

¹Operational research, Spanish Army, C/ San Nicolás 11, Madrid, 28013, Spain

E-mail: mmunfel@pm.me

ORCID: <https://orcid.org/0009-0005-7382-5892>

²Universidad Politécnica de Cartagena member of European University of Technology

EUT+, Department of Statistics and Operations Research, C/ Dr. Fleming, s/n 30202

Cartagena, Spain.

E-mail: nina.skorinkapov@upct.es

ORCID: <https://orcid.org/0000-0002-2537-5867>

Abstract

Tactical telecommunications networks are critical infrastructure for establishing communications when permanent infrastructure has been destroyed or is inaccessible, particularly in disaster response, military operations, and expeditionary deployments. The initial deployment of these networks presents significant challenges. It requires integrating heterogeneous technologies, including high-frequency (HF) radio for beyond-line-of-sight communications, very high-frequency (VHF) and ultra-high-frequency (UHF) systems for mobile tactical coordination, satellite communications (SATCOM) for wide-area connectivity, and Internet Protocol (IP) radio links for high-capacity backhaul. The goal is to rapidly establish minimum operational coverage across the entire area of operations. This objective is compounded by severe operational constraints, including deployment time limits (typically hours to days), logistical restrictions on equipment transport, energy budget limitations, and the need to function under adverse conditions such as terrain shadowing, ionospheric variability, and electronic warfare threats.

This paper presents a two-part review of initial tactical network deployment. First, it characterises the main enabling technologies used in tactical and emergency deployments (HF radio, VHF/UHF systems, SATCOM, and IP radio links) and synthesises their deployment-

relevant capabilities and constraints. This technology-focused synthesis motivates the planning assumptions that must be embedded in realistic deployment models. Second, it reviews optimisation approaches for the tactical network initial deployment and related problems, classifying the literature by the optimisation methodology used and the communication technology considered (single-technology versus partial multi-technology integration).

Despite the breadth of existing work, a central gap remains: there is no unified framework for initial-deployment optimisation that jointly considers the full heterogeneous set of technologies typically required in tactical operations (HF, VHF/UHF, SATCOM, and IP radio links) under realistic operational constraints. This review consolidates the main technology-specific constraints that drive deployment modelling and shows that current optimisation studies largely remain technology-siloed or limited to partial hybrid integrations. It concludes by outlining immediate research directions toward integrated multi-technology formulations, hybrid algorithmic approaches that scale to realistic instances, and stronger validation methodologies that bridge the divide between doctrinal requirements and optimisation practice.

Keywords: Tactical communications; Initial deployment; Multi-technology networks; Coverage-first planning; Deployment optimisation; Military communications; Network optimisation.

INTRODUCTION

Modern military operations, disaster response scenarios, and emergency management activities increasingly depend on the rapid establishment of reliable telecommunications infrastructure in environments where permanent communications systems are unavailable, destroyed, or inaccessible. The need for a fast network stand-up is well recognised in tactical communications planning. Unlike conventional network planning, which assumes stable infrastructure and predictable demand patterns, tactical telecommunications must be deployed rapidly (often within hours) to provide immediate connectivity to distributed field teams operating across extended geographical areas (Shankar, 2019).

The fundamental challenge in tactical network deployment differs markedly from traditional network optimisation problems. During initial deployment, the primary objective is not to maximise throughput, minimise latency, or optimise routing efficiency, but to guarantee minimum operational coverage across the entire area of operations as rapidly as possible (Shankar, 2019). Field commanders, disaster response coordinators, and operational units require assured connectivity to maintain situational awareness, coordinate actions, and request support, even if available bandwidth is limited (North Atlantic Treaty Organization (NATO), 2024). In practice, a network providing near-complete coverage is often operationally inferior to one providing full coverage with suboptimal but functional connectivity, because early coverage enables time-critical coordination (NATO, 2024).

This coverage-first priority distinguishes initial deployment optimisation from the extensive body of research addressing post-deployment network optimisation, including topology modelling and reconfiguration in tactical internets and related networks (Zhang, 2022), as well as broader deployment and optimisation work in heterogeneous Wireless Sensor Network (WSN) contexts (Zhang & Guo, 2022). Post-deployment techniques can improve performance once connectivity is established, but they do not address the core question of where and how to initially deploy infrastructure to achieve full area coverage under operational constraints (Zhang & Guo, 2022).

Tactical telecommunications must operate in constrained environments characterised by strict time limits that mandate deployment completion within hours rather than days or weeks (Larsen et al., 2010). These constraints are reinforced by practical deployment considerations and cost/time trade-offs observed in heterogeneous wireless access deployments (Johansson et al., 2007). Operational dynamics also introduce uncertainty, because terrain effects and atmospheric variability may be imperfectly characterised pre-deployment (Michalak & Nowosielski, 2002; Witvliet, 2021).

No single communications technology can satisfy all the requirements of tactical operations. Operational resilience and complete area coverage, therefore, motivate heterogeneous architectures that leverage complementary strengths of multiple technologies (NATO, 2024). For example, HF supports beyond-line-of-sight connectivity under certain ionospheric conditions (Witvliet, 2021), VHF-band tactical radio networks enable mobile tactical coordination (Li & Vigneron, 2010), and satellite links provide wide-area reachback (Khan & Raheel, 2025). IP radio links provide high-capacity backhaul in deployment contexts (Johansson et al., 2007). This multi-layered logic is consistent with NATO communication and information systems (CIS) doctrine for integrating these systems into Allied joint operations (NATO, 2024).

Despite the maturity of optimisation methods and surveys in adjacent domains (such as metaheuristic-based deployment in WSNs (Abbas et al., 2024; Norouzi & Zaim, 2014; Liu et al., 2024), mesh node placement and transmitter placement approaches (Miche et al., 2025; Nicholas & Alderson, 2012), and emerging reinforcement learning for coverage (Zhao et al., 2025)) a critical gap remains. Existing approaches tend to optimise initial deployment for individual technologies or limited hybrid pairings, rather than jointly optimising the complete heterogeneous set commonly required in tactical and civil response operations (Tan et al., 2025; Li et al., 2020). This gap prevents systematic determination of an optimal technology mix, integrated node placement across technologies, and resource allocation under realistic constraints, and encourages sequential planning and expert judgment (NATO, 2024).

This paper presents a two-part review of initial deployment in tactical multi-technology telecommunications networks. In Part I, it characterises the principal technologies used in practice (HF radio, VHF/UHF systems, SATCOM, and IP radio links) and synthesises their

deployment-relevant characteristics and constraints, thereby making explicit the assumptions and restrictions that shape realistic planning. Part II reviews optimisation methods for deployment-phase decisions and organises the literature by the optimisation methodology used and the technology scope considered (single-technology versus partial multi-technology integration). The paper concludes by summarising the current state of research on full heterogeneous integration for initial tactical network deployment and by identifying the main open gaps that remain.

1. METHODOLOGY

This paper presents a comprehensive review of initial tactical network deployment in multi-technology telecommunications networks, with a dual-use perspective spanning military and disaster-response contexts (Shankar, 2019; Tan et al., 2025). The review is organised in two complementary parts that together capture both the technological landscape and the optimisation methods applied to initial deployment.

The first part of the review characterises the principal technologies employed in tactical network deployments (HF radio, VHF/UHF systems, SATCOM, and IP radio links), focusing on their deployment-relevant characteristics, capabilities, and operational constraints. This technology characterisation examines how each technology enables coverage across different operational scenarios and which practical factors (power requirements, deployment time, coverage range, environmental dependencies) constrain its use. Understanding these technology-specific factors is fundamental to formulating realistic optimisation problems, as they define the feasible decision space and the constraints that any deployment plan must respect.

The second part of the review examines research on deployment-phase optimisation decisions (node placement, site selection, technology selection, and configuration planning), rather than post-deployment optimisation in already operational networks (Zhang, 2022; Zhang & Guo, 2022). It focuses on how optimisation methods have been applied to initial deployment problems and how the scope of technology integration varies across existing works. The literature search targeted peer-reviewed academic sources and relevant technical and doctrinal publications on telecommunications, optimisation, and tactical and emergency communications from 2000 to 2025. The search emphasised venues where deployment optimisation is typically published (e.g., IEEE conferences/journals and related outlets), and it was complemented with defence-oriented and practitioner sources when they directly informed deployment requirements and constraints (NATO, 2024; Shankar, 2019).

Publications were included if they addressed at least one of the following in the context of establishing connectivity:

- Node placement/site selection or coverage-driven network establishment (Zhang & Guo, 2022; Nicholas & Alderson, 2012).
- Optimisation methods applied to deployment-phase decisions (Johansson et al., 2007; Norouzi & Zaim, 2014; Liu et al., 2024).
- Technology-specific deployment planning relevant to tactical or emergency contexts (Witvliet, 2021; Li & Vigneron, 2010; Khan & Raheel, 2025).
- Partial multi-technology integration for initial deployment, including hybrid satellite-terrestrial and unmanned aerial vehicle (UAV)-assisted approaches (Li et al., 2020; Tan et al., 2025; Zhao et al., 2025).

Publications were excluded if they focused exclusively on post-deployment optimisation (e.g., topology modelling without deployment decisions), protocol-only contributions without deployment implications, or methods not evaluated in ways that inform deployment planning decisions (Zhang, 2022). A total of 33 publications are included in the review that address the initial deployment optimisation of at least one relevant technology and/or method directly applicable to establishing tactical networks.

2. TECHNOLOGY CHARACTERIZATION FOR TACTICAL NETWORK DEPLOYMENT

Before optimisation methods can be meaningfully applied, the underlying technological landscape must be understood. This section synthesises the role of the main technologies discussed in the literature and identifies the deployment-relevant characteristics and constraints that shape tactical network planning. Understanding these factors - the coverage footprint of each technology, its power and logistical requirements, its sensitivity to environmental conditions, and its operational role - provides the essential foundation for optimisation models and constraints.

Table 1 summarises the roles of the main technologies discussed in the literature and the dominant deployment-relevant constraints emphasised in both military and civil-response contexts. The table is intended as an interpretive synthesis (not as performance benchmarking), consolidating recurring characteristics reported across the review.

Overall, technology-specific literature tends to treat deployment decisions within each technology independently. This is particularly evident in WSN-related node placement surveys and algorithms that are highly methodologically developed but typically assume homogeneous nodes and therefore do not reflect the doctrinal multi-layer, multi-technology reality of tactical communications (Abbas et al., 2024; Norouzi & Zaim, 2014; Zhang & Guo, 2022). A key finding from this part of the review is that technology characterisation reveals the constraints

and assumptions that must be embedded in subsequent optimisation formulations. For example, understanding the ionospheric dependence of HF radio informs whether frequency and timing decisions should be included in a deployment model, while understanding the role of relays in VHF/UHF networks highlights why node placement often becomes the central optimisation variable. By making these technology–constraint linkages explicit, planners can better formulate optimisation problems that are both methodologically sound and operationally realistic.

Table 1

Technologies and deployment-relevant constraints (synthesis)

Technology	Typical role in initial deployment	Key constraints emphasised in the literature
HF	Beyond-line-of-sight coverage where terrain blocks line-of-sight and when other infrastructure is unavailable or degraded (Witvliet, 2021).	Strong dependence on ionospheric conditions and frequency planning; uncertainty during early deployment; limited bandwidth for data-centric services (Michalak & Nowosielski, 2002; Witvliet, 2021).
VHF/UHF tactical radios	Mobile local communications and tactical coordination can be extended via relays and MANET features (Li & Vigneron, 2010; Peacock, 2007; Kaplan et al., 2022).	Terrain-driven coverage gaps; relay placement sensitivity; interference/frequency coordination in dense deployments; limited link budgets in obstructed terrain (Li & Vigneron, 2010; Larsen et al., 2010).
SATCOM	Wide-area connectivity and reachback when terrestrial connectivity is insufficient; backbone for dispersed units (Khan & Raheel, 2025).	Capacity limits, link budget constraints, and environmental attenuation; terminal positioning/visibility requirements and operational availability (Khan & Raheel, 2025; ITU-R, 2023).
IP radio links (microwave)	High-capacity backhaul/aggregation between nodes or to an operations centre when line-of-sight is feasible (Johansson et al., 2007).	Strict line-of-sight/Fresnel clearance; site accessibility; alignment and engineering effort; sensitivity to terrain and path obstructions (Johansson et al., 2007).

The next section builds on this technology characterisation. It reviews how the literature formulates and solves initial-deployment optimisation problems, with particular attention to the optimisation method used and the degree of multi-technology integration achieved.

3. OPTIMIZATION APPROACHES FOR INITIAL TACTICAL NETWORK DEPLOYMENT

Having characterised the technologies and their constraints, this section reviews how optimisation methods have been applied to initial deployment planning. The section classifies the related work according to the optimisation approach employed, the deployment problem addressed, and the extent of multi-technology integration achieved.

Table 2

Optimisation approaches used for deployment problems (synthesis)

Method family	Strengths (as used in the literature)	Typical limitations (as used in the literature)	References
Exact optimisation (mixed-integer linear programming / related)	Provides optimality guarantees for tractable instances and supports explicit modelling of constraints.	Scalability limits in realistic, high-dimensional deployment problems often require simplifications of propagation and combinatorics.	Nicholas (2016); Kumari & Srirangarajan (2024).
Metaheuristics (genetic algorithm, particle swarm optimisation, simulated annealing, hybrids)	Practical for large search spaces; flexible modelling; frequently used in node placement and coverage problems.	No optimality guarantee; sensitivity to parameter tuning; different benchmarks and models can limit comparability across studies.	Abbas et al. (2024); Barsagade et al. (2019); Duzel et al. (2024); Johansson et al. (2007); Khait & Hasson (2021); Khan & Raheel (2025); Kumari & Srirangarajan (2024); Larsen et al. (2010); Li et al. (2020);

Method family	Strengths (as used in the literature)	Typical limitations (as used in the literature)	References
			Liu et al. (2024); Miche et al. (2025); Nicholas & Alderson (2012); Norouzi & Zaim (2014); Zhang & Guo (2022)
Learning-based approaches (reinforcement learning, deep reinforcement learning)	Promising for dynamic, uncertain environments and for generating policies rather than single-shot solutions.	Requires extensive training data/simulation fidelity; transfer to operational settings and explainability are often open challenges.	Tan et al. (2025); Zhao et al. (2025)

A recurring pattern is that method development is more mature than end-to-end deployment realism. Many studies optimise abstracted coverage/connectivity models (common in WSN deployment) without embedding the full set of operational constraints typical in tactical and disaster-response deployments (Abbas et al., 2024; Zhang & Guo, 2022). Conversely, doctrinal and practitioner sources clearly emphasise the operational requirement for rapid, resilient stand-up, but they do not provide integrated mathematical frameworks spanning the heterogeneous technology set (NATO, 2024; Shankar, 2019).

Beyond the choice of solution method, a second organising dimension in the reviewed literature is the scope of the optimisation model's technology. Of the deployment-optimisation studies identified in this review, only nine explicitly optimise technologies commonly used in tactical networks. Table 3, therefore, focuses on these nine works and summarises which tactical communication technologies they consider: HF, VHF/UHF, SATCOM, and IP radio links.

Table 3*Technologies considered for optimisation in each reference*

Reference	HF	VHF/UHF	SATCOM	IP radio links
Khan & Raheel (2025)			X	
Larsen et al. (2010)		X		
Li & Vigneron (2010)		X		
Li et al. (2020)		X	X	
Miche et al. (2025)				X
Nicholas (2016)		X		
Nicholas & Alderson (2012)				X
Tan et al. (2025)		X		
Zhao et al. (2025)		X		

Note. The table presents nine selected works and summarises the tactical communication technologies they address, including HF, VHF/UHF, SATCOM, and IP radio links. Notably, none of the reviewed works considers HF communication.

In summary, Table 3 shows that even within the subset of studies that explicitly address tactical communications technologies, most contributions remain single-technology. Only one work considers a two-technology setting (VHF/UHF and SATCOM through UAV-assisted integration), while none addresses end-to-end heterogeneous optimisation across the full tactical stack. This limited degree of integration motivates the central research gap discussed next in Section 5: the absence of a unified initial-deployment optimisation framework that jointly considers HF, VHF/UHF, SATCOM, and IP radio links under realistic constraints.

4. IDENTIFIED GAP: FULL HETEROGENEOUS INTEGRATION FOR INITIAL DEPLOYMENT

Across the reviewed works, the central research gap is the absence of a unified framework for initial deployment optimisation that jointly considers the full heterogeneous set commonly

required in tactical operations (HF, VHF/UHF, SATCOM, and IP radio links) under realistic constraints (NATO, 2024; Shankar, 2019). The practical implication is that planners lack a systematic method to decide (i) which technologies should provide coverage in which subareas, (ii) where multi-technology nodes should be placed, and (iii) how limited time, energy, and personnel budgets should be allocated across the deployment tasks.

This gap matters in both military and civil-response settings. Doctrinally, multi-layer communications architectures are treated as a resilience requirement (NATO, 2024), while civil emergency communications research emphasises heterogeneous restoration and rapid service re-establishment under catastrophic disruption (Kishorbhai & Vasantbhai, 2017). The review indicates strong methodological building blocks (exact methods, metaheuristics, and emerging learning-based approaches), but it also shows that the “integration layer” (a single optimisation problem spanning all technologies and deployment resources) remains insufficiently addressed (Tan et al., 2025; Zhao et al., 2025).

CONCLUSION

This review analysed 33 publications (2000–2025) addressing initial deployment in tactical and emergency telecommunications networks, with a dual-use (military-civil) perspective. It comprises two complementary perspectives:

Part I (Technology Characterisation) synthesises the principal technologies (HF radio, VHF/UHF systems, SATCOM, and IP radio links) and their deployment-relevant characteristics, capabilities, and constraints. Understanding these technology-specific factors (coverage patterns, power requirements, environmental sensitivity) is essential for formulating realistic optimisation problems and appropriately constraining the solution space.

Part II (Optimisation Methods) reviews optimisation approaches for initial deployment, classifying research by the optimisation methodology used and the technologies considered. The reviewed corpus shows substantial maturity in the optimisation of single-technology deployments, particularly for terrestrial node placement and coverage problems, using exact optimisation and metaheuristic methods (Johansson et al., 2007; Larsen et al., 2010; Norouzi & Zaim, 2014; Liu et al., 2024; Zhang & Guo, 2022). Recent work also indicates growing interest in learning-based approaches for coverage and deployment decisions, especially in UAV-assisted or dynamic scenarios (Zhao et al., 2025; Tan et al., 2025).

At the same time, the findings highlight a persistent and operationally relevant gap. There is no unified framework that optimises initial deployment across the full heterogeneous set commonly required in tactical operations (HF, VHF/UHF, SATCOM, and IP radio links) under realistic constraints (NATO, 2024; Shankar, 2019). Existing multi-technology studies remain largely partial (e.g., hybrid satellite-terrestrial and UAV-assisted configurations) and typically

do not address integrated technology mix selection, multi-layer node placement, and resource allocation within a single decision framework (X. Li et al., 2020; Tan et al., 2025).

Based on this gap, the most immediate research directions are:

- Integrated multi-technology optimisation formulations that jointly capture technology selection, node placement, and configuration decisions, while reflecting doctrinal resilience requirements and real operational constraints (NATO, 2024; Shankar, 2019).
- Hybrid algorithmic approaches that combine exact optimisation for tractable subproblems with metaheuristics (and, where suitable, learning-based heuristics) to scale to realistic operational instance sizes (Johansson et al., 2007; Norouzi & Zaim, 2014; Zhao et al., 2025).
- Stronger validation methodologies that move beyond purely simulated evaluation toward cost-effective multi-tier validation, including calibrated propagation models, emulation, and opportunistic field measurements during exercises or deployments (Witvliet, 2021; Mehle & Ward, 2025).

These directions aim to bridge the current disconnect between (i) doctrinal and practitioner requirements for resilient, rapidly established communications and (ii) the predominantly technology-siloed optimisation literature, enabling decision support that is both operationally meaningful and methodologically sound (NATO, 2024; Shankar, 2019).

REFERENCES

- Abbas, N. A., Salman, M. A., & Mahdi, M. A. (2024). Deployment approach in WSNS using metaheuristic algorithm: A survey. *Al-Furat Journal of Innovations in Electronics and Computer Engineering*. <https://api.semanticscholar.org/CorpusID:272009647>
- Barsagade, S., Pradhan, P. P., & Bhattacharjee, S. (2019). Energy aware fault tolerant topology design for energy constraint sensor networks. In *2019 25th Asia-Pacific Conference on Communications (APCC)* (pp. 443-448). IEEE. <https://doi.org/10.1109/APCC47188.2019.9026492>
- Chandrasekhar, V., Andrews, J. G., & Gatherer, A. (2008). Femtocell networks: A survey. *IEEE Communications Magazine*, 46(9), 59-67. <https://doi.org/10.1109/MCOM.2008.4623708>
- Denisowski, P. (2020). *Understanding NVIS* (Educational Note). Rohde & Schwarz. https://cdn.rohde-schwarz.com/pws/campaigns/rsa/Rohde-Schwarz_Understanding-NVIS_v1.1.pdf
- Duzel, O., Saoud, B., Shayea, I., & Tulepova, G. N. (2024). Antenna optimization based on genetic algorithm. In *2024 IEEE 3rd World Conference on Applied Intelligence and Computing (AIC)* (pp. 511-517). IEEE. <https://doi.org/10.1109/AIC61668.2024.10730897>
- Halgamuge, M., Zukerman, M., Ramamohanarao, K., & Vu, H. (2009). An estimation of sensor energy consumption. *Progress in Electromagnetics Research B*, 12, 259-295. <https://doi.org/10.2528/PIERB08122303>
- International Telecommunication Union. (2023). *Propagation data and prediction methods required for the design of Earth-space telecommunication systems* (Recommendation ITU-R P.618-14). <https://www.itu.int/rec/R-REC-P.618-14-202308-I/en>
- Johansson, K., Zander, J., & Furuskar, A. (2007). Cost efficient deployment of heterogeneous wireless access networks. In *2007 IEEE 65th Vehicular Technology Conference - VTC2007-Spring* (pp. 3200-3204). IEEE. <https://doi.org/10.1109/VETECS.2007.655>
- Kaplan, M., Corrente, A., & Montalti, E. (2022). *An overview of MANET technologies advantages and disadvantages in the military*. FINABEL. <https://finabel.org/wp-content/uploads/2022/10/48.-An-Overview-of-MANET-Technologies-Advantages-and-Disadvantages-in-the-Military.pdf>
- Khait, Z. A., & Hasson, S. T. (2021). An optimization technique for wireless communication based on mesh topology. In *2021 7th International Conference on Signal Processing and Communication (ICSC)* (pp. 15-20). IEEE. <https://doi.org/10.1109/ICSC53193.2021.9673383>
- Khan, B. M., & Raheel, M. (2025). Optimization of satellite-based communication links. *PLOS ONE*, 20(4), e0315388. <https://doi.org/10.1371/journal.pone.0315388>

- Kishorbhai, V. Y., & Vasantbhai, N. N. (2017). AON: A survey on emergency communication systems during a catastrophic disaster. *Procedia Computer Science*, 115, 838-845. <https://doi.org/10.1016/j.procs.2017.09.166>
- Kumari, S., & Srirangarajan, S. (2024). Node placement and path planning for improved area coverage in mixed wireless sensor networks. *IEEE Robotics and Automation Letters*, 9(8), 6800-6807. <https://doi.org/10.1109/LRA.2024.3412590>
- Larsen, E., Landmark, L., Pham, V., Kure, Ø., & Engelstad, P. E. (2010). Optimized group communication for tactical military networks. In *MILCOM 2010 Military Communications Conference* (pp. 1905-1911). IEEE. <https://doi.org/10.1109/MILCOM.2010.5680404>
- Li, L., & Vigneron, P. (2010). Properties of mobile tactical radio networks on VHF bands (RTO-MP-IST-092). <https://apps.dtic.mil/sti/tr/pdf/ADA584166.pdf>
- Li, X., Feng, W., Chen, Y., Wang, C.-X., & Ge, N. (2020). Maritime coverage enhancement using UAVs coordinated with hybrid satellite-terrestrial networks. *IEEE Transactions on Communications*, 68(4), 2355-2369. <https://doi.org/10.1109/TCOMM.2020.2966715>
- Liu, X., Zhang, K., Zhang, X., Fiumara, G., & De Meo, P. (2024). A hybrid improved compressed particle swarm optimization WSN node location algorithm. *Physical Communication*, 67, 102490. <https://doi.org/10.1016/j.phycom.2024.102490>
- Mao, Y., You, C., Zhang, J., Huang, K., & Letaief, K. B. (2017). A survey on mobile edge computing: The communication perspective. *IEEE Communications Surveys & Tutorials*, 19(4), 2322-2358. <https://doi.org/10.1109/COMST.2017.2745201>
- Mehle, R. W., & Ward, T. E. (2025). High-frequency communications: Observations and recommendations from Project Convergence. *Line of Departure*. <https://www.lineofdeparture.army.mil/Journals/Field-Artillery/Field-Artillery-Archive/Field-Artillery-2025-E-Edition/High-Frequency-Communications/>
- Michalak, J., & Nowosielski, L. (2002). Integration of wireless HF systems with stationary systems. *NATO Regional Conference on Military Communications and Information Systems*. <https://www.researchgate.net/publication/258434455>
- Miche, F., Ebongue Fendji, J. L. K., Mafai, N. M., & Atemkeng, M. (2025). Towards a web simulator for optimizing the placement of mesh nodes in a wireless mesh network. *Procedia Computer Science*, 257, 684-689. <https://doi.org/10.1016/j.procs.2025.03.088>
- NATO. (2024). *AJP-6 Allied joint doctrine for communication and information systems* (Edition B, Version 1). NATO Standardization Office. https://www.coemed.org/files/stanags/01_AJP/AJP-6_EDB_V1_E_2525.pdf
- Nicholas, P. J. (2016). Optimal allocation of electromagnetic spectrum to support tactical wideband communications. *Military Operations Research*, 21(1), 21-39. https://mason.gmu.edu/~pnichol6/docs/spectrum_2016.pdf

- Nicholas, P., & Alderson, D. (2012). Fast, effective transmitter placement in wireless mesh networks. *Military Operations Research*. https://www.researchgate.net/publication/263451711_Fast_Effective_Transmitter_Placement_in_Wireless_Mesh_Networks
- Norouzi, A., & Zaim, A. H. (2014). Genetic algorithm application in optimization of wireless sensor networks. *The Scientific World Journal*. <https://doi.org/10.1155/2014/286575>
- Peacock, B. A. (2007). Connecting the Edge: Mobile Ad-Hoc Networks (MANETs) for Network Centric Warfare. *Defense Technical Information Center*. <https://apps.dtic.mil/sti/html/tr/ADA497761/index.html>
- Ruffieux, S., Gisler, C., Wagen, J.-F., Buntschu, F., & Bovet, G. (2018). TAKE - Tactical ad-hoc network emulation. In *2018 International Conference on Military Communications and Information Systems (ICMCIS)* (pp. 1-8). IEEE. <https://doi.org/10.1109/ICMCIS.2018.8398728>
- Shankar, M. A. (2019). Tactical communications planning. *Marine Corps Gazette*. <https://www.hoover.org/sites/default/files/2022-11/Tactical%20Communications%20Planning%20-%20MCG%20-%20Apr%202019.pdf>
- Tan, X., Liu, B., Li, C., Hussain, Z. K., Wang, K., Wang, K., Ye, M., Yang, D., & Mei, Z. (2025). Spatiotemporal optimization for communication-navigation-sensing collaborated emergency monitoring. *International Journal of Digital Earth*, 18(1), 2475517. <https://doi.org/10.1080/17538947.2025.2475517>
- Witvliet, B. (2021). Escaping the dead zone: A bottleneck in humanitarian ionospheric radio communications. In *IEEE Global Humanitarian Technology Conference (GHTC)*. IEEE. <https://doi.org/10.1109/GHTC53159.2021.9612415>
- Zhang, S. (2022). Topology structure model of tactical internet based on complex network. In *2022 4th International Conference on Frontiers Technology of Information and Computer (ICFTIC)* (pp. 1052-1055). IEEE. <https://doi.org/10.1109/ICFTIC57696.2022.10075320>
- Zhang, Y., & Guo, Z. (2022). A node placement optimization algorithm in heterogeneous WSN based on neighbor nodes. *Wireless Communications and Mobile Computing*. <https://doi.org/10.1155/2022/6820076>
- Zhao, L., Liu, X., & Shang, T. (2025). Maximizing coverage in UAV-based emergency communication networks using deep reinforcement learning. *Signal Processing*, 230, 109844. <https://doi.org/10.1016/j.sigpro.2024.109844>

CRITICAL INFRASTRUCTURE VULNERABILITY IN CRUISE SHIP OPERATIONS: STRUCTURAL PRESSURES AND RISK DIMENSIONS IN THE CENTRAL AND SOUTHERN PART OF THE EASTERN ADRIATIC

Josip Dorigatti

Dr. Franjo Tuđman Defense and Security University.

E-mail: josip.dorigatti@sois-ft.hr

Abstract

The rapid expansion of the cruise industry along the central and southern Adriatic east coast was initially characterised by a 25.75% increase in ship calls and a 46.07% increase in passenger movements between 2015 and 2019. This growth, reinforced by post-pandemic recovery trends in 2021–2024, has exposed an increasing imbalance between operational demand and maritime support infrastructure. This variance has implications for navigational safety, regional economic resilience, and environmental protection. Despite the cruise sector's substantial importance to Croatian tourism, cruise ship operations in the region have increasingly concentrated along informal coastal routes, often near environmentally sensitive and safety-sensitive areas that were not previously subject to dense maritime traffic.

This paper examines cruise ship routing practices, traffic intensity, and infrastructure gaps through an integrated analysis of AIS monitoring data, port traffic statistics, and a critical infrastructure vulnerability framework. Results show that cruise growth is driven by rising passenger volumes per call rather than by proportional increases in the number of cruise calls, intensifying the use of existing infrastructure. Standardised navigation within 3 M of the coast, along informal corridors, creates operational dependencies and reduces system flexibility during disruption.

The analysis demonstrates that navigational vulnerability arises from the interaction between incidental coastal navigation risks and structural pressures driven by industry growth and limited infrastructure adaptation. The paper proposes evidence-based recommendations focused on routing governance, traffic management, and infrastructure resilience applicable to the Adriatic and comparable cruise regions.

Keywords: Cruise navigation; Coastal operations; Critical infrastructure; Maritime governance; Adriatic Sea; Regulatory coordination

1. INTRODUCTION

1.1 Background: Cruise Industry Growth and Adriatic Expansion

The global cruise industry continues to expand following the COVID-19 disruption, with passenger volumes exceeding pre-pandemic levels (MedCruise Association, 2024). In 2023, global cruise passenger numbers reached approximately 31.7 million, a 7% increase from 2019. Industry projections indicate that this growth trajectory will continue, with global cruise passenger capacity expected to increase by around 10% between 2024 and 2028, driven by ongoing fleet expansion and sustained market demand (Cruise Lines International Association, 2024).

Within this global context, the Mediterranean has consolidated its role as one of the world's most important cruise regions, while the Adriatic Sea has emerged as one of its fastest-growing sub-regions. During the pre-pandemic period (2015–2019), cruise activity across the Mediterranean increased steadily; however, growth along the eastern coast of the central and southern Adriatic was notably stronger, particularly in passenger volumes. Cruise ship calls in this sub-region increased by approximately 25.8%, while passenger movements grew by more than 46%, significantly exceeding Mediterranean averages for the same period (Dorigatti et al., 2022). This differential growth indicates a redistribution of cruise capacity toward emerging Adriatic destinations, many of which are in environmentally sensitive coastal and island areas. Recent MedCruise (2024) statistics confirm that this trend has continued during the post-pandemic recovery phase. Adriatic ports have recorded sustained increases in both cruise calls and passenger movements relative to other Mediterranean regions, suggesting that Adriatic's role in cruise itineraries is structurally embedded in current industry deployment strategies. Importantly, this expansion has been accompanied by an increase in passenger concentration per call, reflecting the deployment of larger vessels and the intensified use of existing port and coastal infrastructure.

The economic implications of cruise tourism are particularly pronounced in Croatia. Tourism is a key pillar of the national economy, with the direct contribution estimated at approximately 11–12% of GDP, rising to around 24–25% when indirect and induced effects are included (Croatian Bureau of Statistics, 2024). In 2024, foreign tourism revenues exceeded €14 billion, emphasising Croatia's position as one of the most tourism-dependent EU member states (Croatian National Bank, 2024). While this economic reliance creates significant development opportunities, it also introduces structural vulnerability, as disruptions to cruise operations can rapidly cascade through coastal communities that depend on seasonal employment and related services.

Despite the rapid expansion of cruise activity, the development of maritime support infrastructure has progressed at a comparatively limited pace. No major expansion of Vessel Traffic Service (VTS) coverage has been implemented in the central or southern parts of the eastern Adriatic, while formal navigational routing infrastructure has remained largely unchanged. This misalignment between traffic growth and infrastructure development creates conditions of critical infrastructure vulnerability, understood as the reduced ability of essential systems to reliably support operational demands under both normal and disrupted conditions (Rinaldi et al., 2001).

Against this background, cruise ship navigation in the Adriatic can no longer be viewed solely as a tourism or port management issue. Instead, it reflects a complex interplay among global industry dynamics, regional traffic concentration, economic dependence, and maritime infrastructure capacity. This paper addresses this gap by examining cruise ship navigational practices in the central and southern part of the eastern Adriatic through an integrated analysis of traffic data, navigational practices, and infrastructure characteristics to identify emerging structural vulnerabilities and their implications for maritime safety, resilience, and governance.

1.2 Research Context and Objectives

Cruise ship accidents remain rare in the Adriatic Sea, and no major cruise-related incidents have been recorded to date (European Maritime Safety Agency, 2024). Nevertheless, the region hosts a high concentration of environmentally and culturally sensitive areas, including multiple UNESCO World Heritage Sites, Natura 2000 Marine Protected Areas, and national and nature parks such as Brijuni, Kornati, and Mljet National Parks, as well as Telašćica and Lastovo Nature Parks (UNESCO, 2023).

The growing concentration of cruise operations within environmentally sensitive coastal zones, combined with vessel interactions and gaps in maritime support infrastructure, increases the potential consequences of navigational incidents, particularly environmental damage. These conditions suggest the existence of systemic risk that requires formal assessment. While the absence of major accidents may indicate a high level of safety, it does not eliminate the potential for structural vulnerability arising from traffic intensity, operational practices, and infrastructure limitations.

To address this issue, the paper examines cruise ship navigation in the central and southern part of the eastern Adriatic through an integrated analytical approach combining three complementary data sources:

- Empirical traffic monitoring: AIS analysis of cruise ship movements during three representative periods (August - October 2014, May - July 2015 and May - October 2022), used to identify routing patterns, vessel interactions, and traffic spatial concentration.

- Infrastructure vulnerability assessment: Systematic analysis of gaps in routing infrastructure and procedures, Vessel Traffic Service (VTS) coverage, and navigational aid deployment.

The primary research objective is to demonstrate how the interaction between rising cruise activity and comparatively limited infrastructure development can generate systemic vulnerability in maritime regions. Based on this analysis, the paper proposes evidence-based mitigation measures applicable not only to the Adriatic Sea but also to other emerging cruise destinations facing similar operational and environmental constraints.

2. METHODOLOGICAL APPROACH AND DATA SOURCES

This study employs a mixed analytical approach that combines AIS-based traffic analysis, port-level cruise statistics, and a critical-infrastructure vulnerability perspective. Cruise ship movement data were obtained from AIS records for two representative periods (2014–2015 and 2022) to identify routing practices, spatial concentration, and coastal navigational behaviour (Dorigatti et al., 2022, 2025). The selected AIS datasets (2014–2015 and 2022) were chosen to capture established cruise traffic patterns and their persistence over time. The 2022 dataset validates earlier findings from the 2014–2015 period, based on processed and analysed AIS data (Perić, 2016), and extends the analysis under conditions of continued and intensified cruise activity, enabling assessment of the stability and evolution of routing practices and traffic concentration.

Port traffic statistics for the period 2021–2024 were analysed to examine cruise passenger movements, cruise calls, and passengers-per-call ratios, allowing differentiation between growth driven by visit frequency and growth driven by operational scale (MedCruise Association, 2024).

3. CRUISE OPERATIONS AND ROUTING PRACTICES IN COASTAL WATERS

3.1 Operational Characteristics Creating Infrastructure Dependencies

Cruise operations differ fundamentally from conventional maritime sectors (cargo shipping, tanker operations and ferries) in ways that intensify infrastructure dependencies and create specialised safety challenges:

Itinerary-Driven Operations

Cruise companies operate fixed circular itineraries with predetermined port sequences, specific calling windows, and committed passenger schedules (Dorigatti et al., 2022; Rodrigue & Notteboom, 2009). These routes may be difficult to reroute when infrastructure disruptions occur, when passages are temporarily restricted, or when congestion develops, particularly in

confined coastal corridors. Passengers purchase specific itineraries; operational constraints cascade through fleet schedules, causing economic losses (revenue loss, repositioning costs) and reputational damage (customer dissatisfaction, booking cancellations). A single port closure or navigational route restriction affects multiple cruise lines simultaneously across their entire seasonal schedule.

Coastal Navigation Preference

Cruise operators deliberately operate through scenic coastal areas to enhance passenger experience. This deliberate coastal preference, driven by commercial optimisation to enhance passenger satisfaction, imposes navigational constraints and increases reliance on coastal infrastructure.

Passenger Concentration

Most modern cruise ships carry 3,000–5,500 passengers and 1,000–2,000 crew members, resulting in concentrated human communities of 4,500–7,500 people per vessel (Cruise Lines International Association, 2024). This passenger concentration distinguishes cruise operations from distributed cargo shipping, in which incidents affect only the ship and its cargo. A cruise ship incident creates simultaneous hazards to thousands of people, rescue/evacuation demands, and cascading impacts on regional emergency services.

Seasonal Concentration

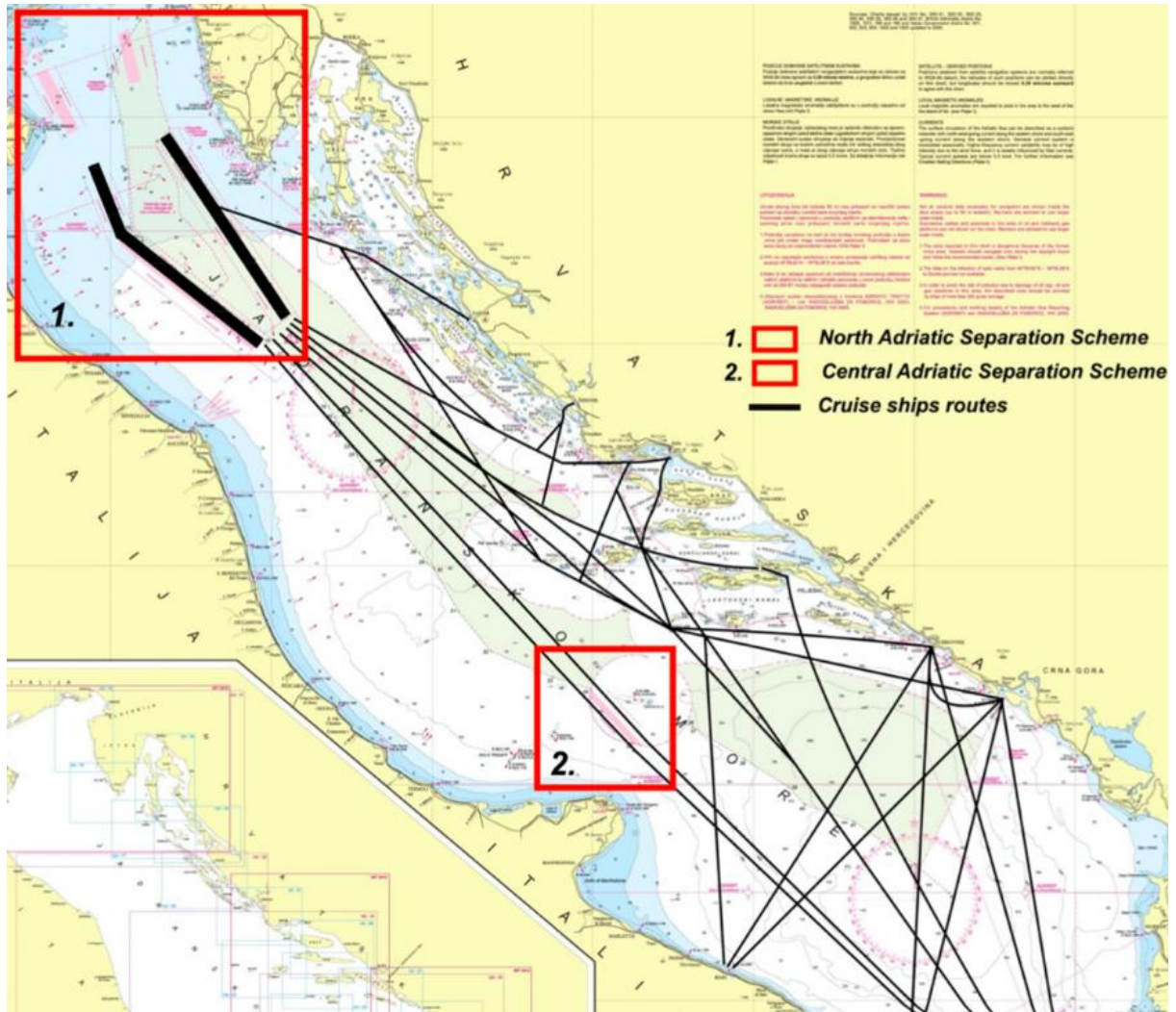
Peak cruise activity occurs from May to October, resulting in predictable periods of increased traffic intensity and pressure on port and traffic management systems (MedCruise Association, 2024). During the peak season, individual ports such as Dubrovnik and Split approach or reach their stated passenger capacity limits, while maritime infrastructure, and associated support infrastructure, largely developed under pre-expansion demand assumptions, operate under increased stress. Infrastructure with limited capacity for peak demand may have limited flexibility to accommodate emergencies, such as temporary port closures, navigational corridor closures, or navigational restrictions due to grounding, collisions, pollution, or SAR (Search and Rescue) events.

3.2 Established Navigational Practice and Infrastructure Gaps

Systematic cruise ships navigational practice AIS analysis reveals standardised coastal routing patterns that deliberately deviate from formal longitudinal corridors and Traffic Separation Schemes.

Figure 1

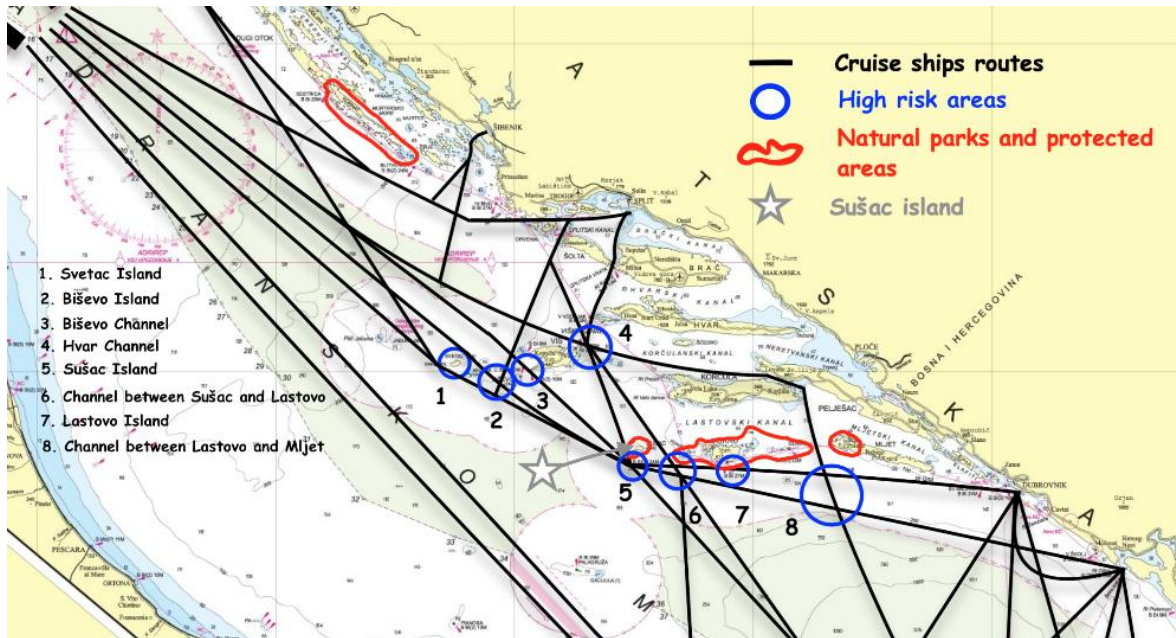
Cruise traffic on the Adriatic east coast illustrates the divergence between formal routing schemes and observed coastal navigation patterns.



Note. Black lines indicate cruise ship routes; red squares indicate Traffic Separation Schemes: (1) North Adriatic Separation Scheme and (2) Central Adriatic Separation Scheme (Dorigatti et al., 2022).

Figure 2

Cruise ships' routes and high-risk zones in the central and southern part of the eastern Adriatic highlight the spatial overlap between cruise routes and environmentally sensitive areas.



Note. Black lines represent cruise ship routes; red curves indicate marine protected areas; the grey star marks the island of Sušac; blue circles denote areas of high navigational risk (Dorigatti et al., 2022).

In 2022, documented routing data show:

- Central Adriatic Separation Scheme usage: 172 transits by cruise ships
- Informal outer island coastal corridor usage: 422 transits by cruise ships
- Preference ratio: 2.45:1 for the informal coastal corridor over the formal scheme

This strong preference for informal corridors reflects the deliberate cruise ship's choice to provide scenic routing despite increased navigational complexity and points to the absence of regulated coastal routing systems and procedures in the area of research.

3.3 Structural Drivers of Vulnerability: Root Cause Analysis

The analysis identifies three interdependent structural drivers that collectively amplify navigational and infrastructure-related vulnerability in the central and southern part of the eastern Adriatic. These drivers emerge from the interaction between cruise traffic growth trends, operational practices, and the pace of infrastructure and governance adaptation.

Driver 1: Routing Concentration and Lack of Formal Alternatives

AIS analysis indicates that, in the absence of officially established and standardised coastal routing systems, cruise ships operating in the central and southern parts of the eastern Adriatic tend to follow voluntarily adopted coastal routes (Dorigatti et al., 2022). Over time, these routes, particularly along the outer island bridge connecting major northern Adriatic ports with destinations in the central and southern Adriatic, have evolved into informal transit corridors, shaped by repeated operational practice rather than formal designation.

This routing concentration does not reflect dependence on predefined regulatory infrastructure; rather, it reflects a structural gap: the absence of formally supported routing alternatives. As cruise traffic increases, the reliance on these informal corridors reduces operational flexibility. In situations involving temporary navigational restrictions, port congestion, or degraded traffic management capability, the lack of clearly defined, coordinated official and alternative routes may limit effective traffic redistribution and coordinated responses, potentially affecting multiple operators simultaneously.

Driver 2: Capacity Divergence – Demand Growth versus Infrastructure Development

Cruise traffic growth in the central and south part of the eastern Adriatic has significantly outpaced the development of supporting maritime infrastructure. While passenger volumes have increased notably over the past decade, the number of cruise calls has grown more moderately, indicating a shift toward larger vessels and higher passenger loads per call. Latest port statistics show that, in several major Adriatic ports, passenger growth in 2024 substantially exceeded growth in cruise calls, and in some cases passenger volumes increased even where call numbers stagnated or declined. This trend reflects intensifying operational demand without a corresponding increase in visit frequency (MedCruise Association, 2024).

This misalignment is evident across several infrastructure components:

Vessel Traffic Service (VTS): No substantial expansion of VTS coverage has been implemented in the central and southern parts of the eastern Adriatic. Existing systems largely retain their original operational scope, despite increased traffic density and interaction complexity in coastal waters; there are no new reporting points or traffic management procedures in areas with elevated traffic density.

Routing infrastructure: No new formally established routing schemes, such as Recommended routes, Routes to be avoided, Seasonal routes, Precautionary Areas, Areas To Be Avoided or No-Go Areas, have been introduced, despite the concentration of cruise traffic in specific coastal corridors. The absence of additional schemes or precautionary routing measures suggests limited adaptation of formal routing governance to evolving operational conditions.

Navigational aids: Deployment of additional navigational aids along frequently used maritime corridors has remained limited, with most systems reflecting pre-expansion traffic assumptions.

Driver 3: Regulatory Fragmentation across Multiple Jurisdictions

The Adriatic maritime operations take place within a multi-jurisdictional regulatory environment involving several national maritime administrations, including those of Croatia, Italy, Montenegro, Albania, and Greece. While each administration applies established regulatory and operational frameworks within its jurisdiction, differences in national approaches to traffic management, detection and response procedures, and infrastructure planning have created a complex regional coordination environment. Recognition of these coordination challenges has prompted institutional development; the EUREKA (2023) project, established under the EU Strategy for the Adriatic-Ionian Region (EUSAIR) framework and led by the Croatian Ministry of the Sea, Transport and Infrastructure, was specifically designed to harmonize Vessel Traffic Service (VTS) procedures, standardize maritime safety practices, and coordinate ship reporting systems (ADRIREP) across the four maritime administrations.

From a critical infrastructure perspective, multi-jurisdictional fragmentation can complicate the development of region-wide strategies for coordinated planning for safety, security and environmental measures. Although this structure does not imply regulatory inadequacy, it highlights both the challenges and the strategic value of enhanced regional cooperation in supporting infrastructure development, maintaining consistent safety standards, and responding effectively to emerging operational challenges.

4. CRITICAL INFRASTRUCTURE VULNERABILITY: INCIDENTAL AND STRUCTURAL DIMENSIONS

4.1 Theoretical Foundations and Mechanisms of Vulnerability

In this study, critical infrastructure is understood to include both physical assets (ports, VTS systems, navigational aids) and non-physical systems (routing governance, traffic management frameworks) that are essential for maintaining safe and reliable maritime operations. Critical infrastructure vulnerability, as defined in the security and resilience literature, refers to situations in which essential systems are unable to reliably meet operational demands under normal or degraded conditions (Rodrigue & Notteboom, 2009). In the context of cruise ship operations in the Adriatic, vulnerability does not arise from individual infrastructure deficiencies, but from the interaction of multiple reinforcing mechanisms. Three such mechanisms are identified.

Mechanism 1: Operational Concentration Risk

Modern cruise vessels typically carry more than 5,000 passengers and crew, so navigational incidents can affect a large number of people simultaneously. This concentration increases demands on search and rescue, evacuation, medical response, and port support functions, particularly in geographically constrained coastal areas. Beyond immediate safety implications, such incidents may generate cascading effects across tourism-dependent coastal communities, where cruise activity supports seasonal employment and associated services.

Mechanism 2: Route Dependency

In the study area, cruise ships tend to follow a limited number of coastal corridors shaped by operational preferences rather than by formally designated routing schemes. When disruptions occur, such as temporary navigational restrictions, reduced Vessel Traffic Service (VTS), or port closures, the effectiveness of traffic redistribution may be limited. This reduction in operational flexibility can simultaneously affect multiple operators and increase the overall system's exposure.

Mechanism 3: Infrastructure Interdependence

Cruise ship operations rely on a network of interdependent infrastructure elements, including ports, traffic monitoring systems, routing systems, and navigational aids. Limitations in one component can arise within the system (Rodrigue & Notteboom, 2009). For example, gaps in VTS coverage may constrain the monitoring of vessel interactions or limit coordination during overtaking and head-on situations. Similarly, the absence of formally established routing measures limits the ability to manage traffic flows dynamically during disruptions.

Taken together, these mechanisms illustrate systemic vulnerability driven by demand growth that has outpaced infrastructure adaptation, resulting in sustained operational pressure and reduced tolerance for disruption.

4.2 Economic and Strategic Implications for Tourism-Dependent Regions

Croatia's high reliance on tourism amplifies the consequences of maritime disruptions. While tourism's direct contribution to GDP is estimated at approximately 11–12%, the broader tourism-related share of gross value-added reaches around 24–25%, among the highest in the European Union (Croatian Bureau of Statistics, 2024). In this context, cruise operations are a visible, spatially concentrated component of coastal economic activity.

Disruptions affecting maritime traffic and the cruise industry, such as incident-driven operational restrictions, navigational corridor closures, terminal capacity reductions, or port

closures, can therefore have effects extending beyond the maritime domain to Safety, Environmental, and Socio-Economic impacts.

Environmental and Safety Impacts:

- environmental degradation of high-value marine ecosystems (including national parks, nature parks, UNESCO World Heritage Sites, and Natura 2000 marine protected areas) resulting from navigational incidents such as collisions, groundings, and pollution.
- high operational pressure on search and rescue operations and emergency response
- maritime accident investigation, salvage operations, and liability costs

Socio-Economic Impacts:

- international competitiveness and destination reputation
- investment confidence in tourism and maritime infrastructure
- shipping company operational costs
- regional tax, local, port and terminal revenues,
- associated service industries (provisioning, crew services, waste management, maintenance), etc.

From a critical infrastructure perspective, these economic connections reinforce the strategic relevance of cruise navigation and coastal maritime systems, positioning them not only as transport and tourism assets but as components of broader societal resilience.

5. RESULTS

5.1 Cruise Traffic Intensity: Passenger Movements, Cruise Calls, and Operational Density

To distinguish between cruise traffic growth driven by increased visit frequency and growth driven by operational scale, cruise passenger movements, cruise calls, and passengers-per-call ratios were analysed together for major ports in the central and southern Adriatic.

Table 1 presents cruise passenger movements, cruise calls, and passengers-per-call ratios for the period 2021–2024, including both cumulative growth and recent year-on-year change (2023–2024) (MedCruise Association, 2024). The results show that while cruise calls increased across all analysed ports, passenger volumes grew at a consistently higher rate. This divergence is evident in both the long-term recovery period and the most recent growth phase, indicating an increase in cruise operations rather than simply traffic growth.

Table 1

Passenger Movements, Cruise Calls, and Operational Density (2021–2024). Evolution and Growth of Cruise Traffic Intensity in Major Adriatic Ports

Port	Indicator	2021	2023	2024	Growth 2021–2024 (%)	Growth 2023–2024 (%)	Trend Interpretation
Dubrovnik / Korčula	Passengers	116,975	549,041	632,513	441%	+15.2%	High-volume hub, nearing saturation
	Calls	191	489	625	227%	+27.8%	Call growth accelerating
	Passengers / Call	~612	~1,123	~1,010	65%	-10.1%	Density stabilising
Split	Passengers	89,148	388,204	497,856	458%	+28.3%	Strong scale-driven growth
	Calls	105	305	336	220%	+10.1%	Calls lag passenger growth
	Passengers / Call	~849	~1,272	~1,480	74%	+16.3%	Intensifying operations
Zadar	Passengers	10,164	174,573	248,462	2,35%	+42.3%	Rapid expansion
	Calls	30	159	220	633%	+38.4%	Strong growth
	Passengers / Call	~339	~1,098	~1,130	233%	+2.9%	High, stabilising density
Šibenik	Passengers	8,164	29,78	33,133	306%	+11.3%	Gradual growth
	Calls	43	90	83	93%	-7.8%	Fewer calls
	Passengers / Call	~190	~331	~399	110%	+20.5%	Shift to larger vessels
Rijeka	Passengers	903	37,725	43,405	4,71%	+15.1%	Recovery-driven growth
	Calls	1	20	30	2,90%	+50.0%	Volatile growth
	Passengers / Call	~903	~1,886	~1,447	60%	-23.3%	High variability

Note. Adapted from data in MedCruise Association (2024).

5.2 Cruise Traffic Growth and Spatial Concentration

Analysis of cruise traffic distribution confirms a strong spatial concentration of cruise activity within a limited number of Adriatic ports and coastal corridors. Dubrovnik/Korčula, Split, and Zadar collectively account for most cruise passenger movements, reinforcing their role as primary hubs in regional cruise itineraries. This concentration extends beyond port areas to associated approach routes and coastal navigation corridors, which accommodate repeated transits by high-capacity vessels operating on fixed schedules. AIS-based analysis indicates that cruise ship movements remain highly clustered along specific coastal routes, particularly within 3 M of shore (Dorigatti et al., 2022). As traffic intensity increases, these corridors accommodate a growing number of large vessels within constrained spatial and time windows, increasing the frequency and complexity of vessel interactions.

5.3 Divergence Between Cruise Calls and Passenger Volumes

The divergence between cruise calls and passenger volumes represents a key structural characteristic of recent cruise expansion. Passenger growth increasingly outpaces call growth, resulting in higher operational density per visit. This pattern indicates that infrastructure stress is driven less by the number of port calls than by vessel size, passenger concentration, and the simultaneity of operations.

This divergence reduces system flexibility by increasing dependency on existing port capacity, traffic management arrangements, and coastal routing practices. As a result, even minor disruptions, such as schedule delays, port congestion, or temporary navigational restrictions, can have amplified operational consequences.

5.4 Implications for Coastal Navigation and Traffic Management

Higher passenger loads per call translate into increased demands on pilotage, berthing operations, passenger handling, and emergency preparedness, particularly during peak season. At the same time, the concentration of cruise transits along coastal corridors increases the frequency of overtaking, crossing, and multi-ship encounter situations, especially in areas where cruise traffic overlaps with ferries, fishing vessels, and recreational craft. The increasing frequency of overtaking, crossing, and multi-ship encounters in constrained coastal corridors reflects dynamic risk conditions similar to those identified in collision risk modelling studies (Dorigatti et al., 2025). The combination of intensified operations and limited formal coastal routing measures increases navigational complexity and reduces tolerance for disruption, placing additional demands on bridge teams and traffic management systems.

5.5 Infrastructure Stress Indicators

Despite rising operational demand, support for maritime infrastructure has not expanded proportionally. Vessel Traffic Service (VTS) coverage in the central and southern Adriatic remains largely unchanged; formal coastal routing measures have not been introduced in high-density corridors, and the deployment of additional navigational aids has been limited. Consequently, rising traffic intensity is absorbed primarily through intensified use of existing infrastructure rather than through capacity expansion or system adaptation.

These conditions indicate the emergence of systemic infrastructure stress, reinforcing the structural nature of navigational vulnerability identified in the vulnerability framework.

6. DISCUSSION AND COMPARATIVE ANALYSIS

6.1 Incidental and Structural Dimensions of Navigational Vulnerability

The results presented in Section 5 indicate that navigational vulnerability in Adriatic cruise operations cannot be attributed to a single source or mechanism. Instead, vulnerability emerges through the interaction of two complementary dimensions: incidental, situation-dependent risks associated with coastal navigation practices, and structural pressures arising from long-term growth trends in cruise operations.

Incidental vulnerability has been documented in earlier research through the analysis of developed cruise ship routing practices in coastal waters, frequent vessel interactions, navigation in confined and environmentally sensitive areas, and proximity to shorelines and marine protected zones. These conditions generate localised, time-specific risk exposure, particularly during periods of high traffic density, limited manoeuvring space, or reduced situational awareness. Such vulnerabilities are operational and situation-dependent, shaped by navigational decision-making and traffic encounters, and influenced by the availability and effectiveness of supporting maritime infrastructure. Situation-dependent risks are consistent with established maritime risk literature, which emphasises the role of traffic encounters, operational context, and system configuration in shaping navigational risk exposure (Mazaheri et al., 2015).

The present study adds a structural dimension to this understanding. As shown by the traffic intensity indicators in Section 5.1, recent cruise growth in the central and southern parts of the eastern Adriatic is driven more by passenger volumes per call than by proportional growth in the number of cruise calls. This shift reflects clear industry trends toward larger vessels, higher passenger concentrations, and the seasonal intensification of operations. While these trends do not directly create navigational hazards, they increase the consequences of incidental risks by increasing the number of people, assets, and services affected by any disruption.

Structural vulnerability, therefore, does not replace incidental vulnerability; rather, it magnifies it. Under conditions of high operational density, even minor disruptions, such as temporary port closures, navigational restrictions, schedule delays, or reduced traffic management capability, may expand across multiple operators and ports, reducing system flexibility and resilience. In this sense, vulnerability increasingly reflects the characteristics of the system as a whole, rather than isolated failures or individual incidents.

6.2 Passenger Concentration and Escalation of Consequences

Passenger concentration represents a critical factor linking incidental and structural vulnerability in cruise ship operations. As shown by the passenger-per-call ratios presented in Section 5.1, cruise vessels operating in the Adriatic routinely carry several thousand passengers and crew per port visit. This concentration distinguishes cruise operations from other maritime sectors, in which traffic growth is more evenly distributed across vessels and over time.

From a navigational and infrastructure perspective, higher passenger concentration increases the potential severity of outcomes from navigational incidents, operational disruptions, or emergencies. Groundings, collisions, fires, or extended port closures involving cruise ships can simultaneously affect thousands of passengers, place substantial demands on search-and-rescue services, port authorities, emergency response systems, and local transport networks, and generate significant environmental and reputational impacts.

In tourism-dependent regions such as the Adriatic coast, these effects extend beyond the maritime domain. Disruptions to cruise operations can cascade into wider economic and social impacts, affecting seasonal employment, port revenues, service industries, public confidence and reputation. As a result, passenger concentration acts as a multiplier of vulnerability, transforming localised navigational risks into system-wide challenges with implications for coastal resilience and security.

6.3 Implications for Critical Infrastructure and Coastal Security

The combined presence of incidental navigational risks and emerging structural pressures supports framing cruise navigation as a critical infrastructure concern rather than solely a maritime safety issue. Maritime safety and security are increasingly interlinked, particularly in coastal and high-density traffic areas, where operational disruptions can escalate into broader economic and societal impacts (Goerlandt & Montewka, 2015). While traditional safety assessments focus on accident prevention and compliance at the vessel level, this study's findings highlight how routing practices, traffic intensity, and infrastructure capacity interact to shape system-level vulnerability.

In this context, maritime routing governance, traffic management systems, and navigational support infrastructure function as non-physical critical infrastructure, emphasising the safe and

reliable operation of coastal sea routes and ports. The absence of formally established routing measures, limited expansion of Vessel Traffic Service coverage, and reliance on informal coastal corridors reduce the system's ability to absorb shocks and adapt to disruptions, particularly under high operational intensity.

From a defence and security perspective, the identified vulnerabilities extend beyond maritime safety. Concentration of cruise traffic along limited coastal corridors, combined with limited infrastructure flexibility, increases the system's sensitivity to disruption. Such disruptions, whether caused by accidents, technical failures, or external interference, may affect critical economic functions, emergency response capacity, and environmental protection systems in tourism-dependent coastal states. In this context, coastal maritime transport systems function as critical infrastructure components whose resilience is directly linked to national economic stability and crisis response capability

These findings have relevance beyond the Adriatic case study. Other cruise regions experiencing rapid growth under similar geographic and institutional constraints may encounter comparable patterns of vulnerability. Early recognition of the interaction between incidental and structural risk factors, combined with proactive integration of navigational governance into critical infrastructure planning, may help prevent the escalation of vulnerability as cruise traffic continues to expand.

7. RECOMMENDATIONS

The findings of this study indicate that navigational vulnerability in Adriatic cruise operations arises from the interaction between incidental, situation-specific navigational risks and structural pressures driven by long-term growth and operational intensification. From a risk management perspective, effective mitigation requires proportional and cost-effective measures that address both operational exposure and systemic vulnerability, rather than isolated controls (Talley, 2012). Effective mitigation, therefore, requires a layered approach that addresses both dimensions simultaneously. Measures focused exclusively on operational behaviour or solely on infrastructure expansion are unlikely to deliver durable risk reduction if implemented in isolation.

The recommendations below are structured accordingly and are consistent with internationally recognised principles for ship routing, vessel traffic management, and bridge team operations, as reflected in IMO routing guidance, IALA VTS principles, and established industry practice (International Association of Marine Aids to Navigation and Lighthouse Authorities, 2015; International Maritime Organization, 2019).

7.1 Institutional and Regulatory Measures

Formalisation of coastal routing structures

Formally establish Recommended Routes in high-density coastal corridors to provide a structured traffic framework aligned with prevailing navigational practice. The introduction of Recommended Routes creates the foundation for complementary measures, including Routes to Be Avoided and routing restrictions, which can only be meaningfully defined once primary traffic flows are formally recognised.

Strengthening of Vessel Traffic Service (VTS) coverage

Expand VTS monitoring capability in the central and southern Adriatic through the introduction of additional reporting points and enhanced surveillance of complex traffic situations. Improved monitoring of overtaking, crossing, and multi-ship encounters is particularly important in near-shore corridors where cruise traffic overlaps with ferries, fishing vessels, and recreational craft.

Route declaration in high-risk coastal areas

Require cruise vessels above an agreed tonnage threshold to submit planned coastal transit routes when operating in identified high-risk corridors. The passage plan should include deviation criteria and contingency options to support better coordination during periods of congestion, disruption, or degraded traffic management capability.

Optimisation of transit timing

Where operationally feasible, prioritise daylight transits through confined or environmentally sensitive passages and avoid peak periods of local traffic activity. Improved timing reduces exposure to incidental risks associated with reduced visibility and traffic congestion.

Bridge system configuration and situational awareness

Optimise Electronic Chart Display and Information System (ECDIS) and Automatic Radar Plotting Aid (ARPA) settings for confined coastal navigation, with particular attention to target detection, filtering, and guard zone configuration. Enhanced system setup supports early identification of close-quarters situations and improves response capability during complex encounters. Taken together, these recommendations emphasise that reducing navigational vulnerability in cruise operations requires simultaneous action at the operational, regulatory, and infrastructure levels. Structural measures aimed at routing governance and traffic management improve system resilience and tolerance to disruption, while operational measures reduce exposure to incidental navigational risks. Coordinated implementation of both is essential to prevent the escalation of vulnerability as cruise traffic intensity continues to increase in the Adriatic and comparable regions.

7.2 Integrated Perspective

By framing cruise navigation as a critical infrastructure concern, the study highlights how maritime routing governance, vessel traffic management, and navigational support systems function as non-physical infrastructure underpinning the safe and reliable operation of coastal sea routes. In tourism-dependent regions such as the Adriatic, vulnerabilities in this system extend beyond maritime safety, affecting economic resilience, environmental protection, and public confidence.

The findings underscore the need for a coordinated and proportional response that addresses both incidental and structural dimensions of vulnerability. The development of routing measures, the targeted expansion of traffic management capabilities, and the enhancement of operational practices must be pursued in parallel and, where possible, through regional coordination mechanisms. Although the Adriatic serves as the primary case study, the observed patterns are relevant to other cruise regions experiencing rapid growth under similar geographic and institutional constraints. Early recognition of emerging structural pressures, combined with systematic management of incidental navigational risks, may help prevent the escalation of vulnerability as cruise traffic intensifies.

8. CONCLUSION

This study examined cruise ship navigational practices in the central and southern parts of the Adriatic through an integrated analysis that combined AIS-based traffic data, operational case studies, and a critical-infrastructure vulnerability perspective. The results show that recent cruise expansion in the region is characterised not only by increased traffic volumes, but by a marked intensification of operations, reflected in rising passenger volumes per port call and sustained concentration of cruise activity along near-shore coastal corridors.

The analysis confirms that navigational vulnerability in Adriatic cruise operations arises from the interaction of two complementary dimensions. First, incidental, situation-specific vulnerability emerges from developed navigational practices in coastal waters, including traffic interactions, navigation in confined spaces, and proximity to environmentally sensitive areas. These risks are spatially and operationally dependent and have been documented in earlier research as characteristic of cruise ship operations in complex coastal environments.

Second, the study identifies an additional layer of structural vulnerability driven by long-term industry trends. Growth in passenger volumes per call, seasonal concentration of operations, and reliance on infrastructure designed for lower traffic intensity amplify the consequences of incidental risks. Under these conditions, even minor disruptions, such as port closures, navigational restrictions, or degraded traffic management capabilities, may affect multiple operators and ports, reducing system flexibility and resilience.

Importantly, structural vulnerability does not replace incidental navigational risk; rather, it magnifies its impact. The combination of high passenger concentration, increased use of informal coastal corridors, and limited adaptation of routing governance and traffic management infrastructure increases the cruise system's sensitivity to disruption, even in the absence of major accidents or technical failures.

These findings highlight the relevance of cruise navigation within the broader framework of critical infrastructure protection and national resilience in maritime-dependent regions.

REFERENCES

- Cruise Lines International Association. (2024). *State of the cruise industry report 2024*. <https://cruising.org/news/state-cruise-industry-report-2024>
- Croatian Bureau of Statistics. (2024). *Turizam u 2023. -- Statistička izvješća 1731* [Tourism in 2023 -- Statistical Reports 1731]. <https://podaci.dzs.hr/hr/podaci/turizam/>
- Croatian National Bank. (2024). *Balance of payments -- statistical data and tourism revenues (current and capital account)*. <https://www.hnb.hr/en/statistics/statistical-data/rest-of-the-world/balance-of-payments>
- Dorigatti, J., Perić, T., & Jelić Mrčelić, G. (2022). Cruise industry trends and cruise ships' navigational practices in the central and southern part of the Adriatic east coast affecting navigational safety and sustainable development. *Applied Sciences*, 12(6884). <https://doi.org/10.3390/app12146884>
- Dorigatti, J., Perić, T., & Jelić Mrčelić, G. (2025). Cruise ship navigational practices in the central and southern part of the Adriatic east coast -- Biševo and Svetac island region. *Transactions on Maritime Science*, 14(2), xx--xx. <https://doi.org/10.7225/toms.v14.n02.s06>
- Perić, T. (2016). *Evaluation model of sanitary wastewater pollution from cruise ships in the Adriatic Sea*. PhD thesis. University of Rijeka.
- European Maritime Safety Agency. (2024). *Consolidated annual activity report 2023*. <https://www.emsa.europa.eu/publications/item/5256-emsa-consolidated-annual-activity-report-2023.html>
- Goerlandt, F., & Montewka, J. (2015). Maritime transportation risk analysis: Review and analysis in light of some foundational issues. *Reliability Engineering & System Safety*, 138, 115--134. <https://doi.org/10.1016/j.ress.2015.01.024>
- International Association of Marine Aids to Navigation and Lighthouse Authorities. (2015). *Vessel traffic services manual (VTS manual)*. Saint-Germain-en-Laye: IALA.
- International Maritime Organization. (2019). *General provisions on ships' routeing*. London: IMO.
- Mazaheri, A., Montewka, J., Kujala, P., & Matusiak, J. (2015). A dynamic risk analysis of ship--ship collision in a fairway. *Reliability Engineering & System Safety*, 138, 78--93. <https://doi.org/10.1016/j.ress.2015.01.025>
- MedCruise Association. (2024). *Cruise activities in MedCruise ports: Statistics report 2024*. Rome: MedCruise Association. <https://www.medcruise.com/>
- EUREKA Project (2023). *Adriatic-Ionian joint approach for development and harmonisation of maritime safety procedures (EUREKA)*. <https://eureka.adrioninterreg.eu/>

- Rinaldi, S. M., Peerenboom, J. P., & Kelly, T. K. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems Magazine*, 21(6), 11--25. <https://doi.org/10.1109/37.969131>
- Rodrigue, J.-P., & Notteboom, T. (2009). The cruise industry: Itineraries, not destinations. *Port Technology International*, 44, 013--016. <https://www.porttechnology.org/wp-content/uploads/2019/05/013-016.pdf>
- Talley, W. K. (2012). *Maritime safety, security and piracy*. London: Informa Law. <https://doi.org/10.4324/9780203805183>
- UNESCO. (2023). *World heritage and marine protected areas in the Adriatic*. Paris: UNESCO. <https://whc.unesco.org/en/marine-programme/>

A MULTI-CRITERIA DECISION FRAMEWORK FOR ASSESSING ENVIRONMENTAL INFLUENCES ON WILDFIRE DETECTION

Ena Sarajlić¹, Maja Braović², Hrvoje Karna¹, Ljiljana Šerić², Damir Krstinić²

¹ Dr. Franjo Tuđman Defense and Security University, Zrinjsko-Frankopanska 207a, 21000 Split, Croatia

E-mail: ena.sarajlic@sois-ft.hr, hrvoje.karna@sois-ft.hr

ORCID: 0009-0004-1646-4210 (Ena Sarajlić), 0000-0003-4299-3963 (Hrvoje Karna)

² Faculty of Electrical Engineering, Mechanical Engineering and Naval Architecture, University of Split, Ruđera Boškovića 32, 21000 Split, Croatia

E. E-mail: maja.braovic@fesb.hr, ljiljana.seric@fesb.hr, damir.krstinic@fesb.hr

ORCID: 0000-0002-3655-3534 (Maja Braović), 0000-0002-6390-1899 (Ljiljana Šerić), 0000-0002-9946-6630 (Damir Krstinić)

Abstract

Timely and accurate wildfire detection is a critical component of civil security, as it enables rapid interventions to protect human lives, ecosystems and infrastructure. Climate change has intensified summer droughts across Mediterranean countries, driving a surge in wildfire frequency and severity; Croatia's coast is among the hardest-hit regions and relies on an artificial-intelligence-based early-detection and surveillance system monitored by firefighters. This preliminary study analyses a sample of 100 images of events detected as possible wildfires by this surveillance system, but rather than assessing detection accuracy, it examines the correlation between these detections and key weather parameters recorded near the event locations. This multi-criteria decision analysis (MCDA) was conducted during the 2025 off-season (October–November), and it accounts for the system's high-recall strategy, which prioritises avoiding missed wildfire events over minimising false alarms. These preliminary findings can inform future multi-criteria decision analyses, provided they are based on larger samples and more balanced datasets (e.g., including more confirmed wildfires from peak summer months). While this study focuses on civil security and protection, the methodology transfers readily to national security and military contexts, where reliable fire detection supports operational readiness, asset protection, and situational awareness. With minimal adaptation, the framework can integrate into broader surveillance and decision-support

systems, interfacing with remote sensing platforms, unmanned systems, and command-and-control infrastructure.

Keywords: multi-criteria decision analysis (MCDA); SAW; TOPSIS; wildfire surveillance; image processing; decision-support systems; civil protection

INTRODUCTION

The world's climate is changing, and Croatia's coast is among the hardest-hit regions, facing a sharp rise in both wildfire frequency and intensity. While the majority of wildfires are caused by intentional or accidental human intervention (Mamut, 2011), and climate change alone cannot be blamed for every forest fire that occurs, the increase in global temperature levels can and does impact wildfire intensity and duration indirectly through its influence on the environment (e.g., wind speed, vegetation cover and the size of water obstacles). The most extreme examples of wildfires in Croatia in the last few decades include the 2008 wildfire in the Kornati National Park that claimed the lives of 12 firefighters and left one seriously injured (Stipaničev et al., 2008), the 2017 wildfire near Split that was stopped only 4 km from the city centre (Čavlina Tomašević et al., 2022), and a string of wildfires in 2025 (Hojsak, 2025). This increase in wildfire activity has not been restricted to Croatia only, but has spread all around the countries in the Mediterranean basin, including in Albania (Çela et al., 2025), Algeria (Curt et al., 2020), Greece (Stefanidis et al., 2022), Italy (Bacciu et al., 2025), Montenegro (Nikolić et al., 2023), Portugal (Silva et al., 2023), Spain (Liz-López et al., 2024), Turkey (Tariq et al., 2023), etc.

Decision-making in complex, uncertain scenarios, such as wildfires or battlefields, poses a formidable challenge in both real and virtual environments. Decisions depend on several interdependent variables whose interactions are difficult to model and predict, but whose influence on the final output can be approximated.

This study presents preliminary findings on the correlation between detections from an existing artificial intelligence (AI) based wildfire surveillance system and key weather parameters recorded near flagged event locations. The system in question, OIV Fire Detect AI (Bugarić et al., 2025; OIV, 2026), is developed at the Faculty of Electrical Engineering, Mechanical Engineering and Naval Architecture at the University of Split, Croatia, and is actively used by Croatian firefighters. OIV Fire Detect AI supports firefighting efforts by using video surveillance and image processing to detect wildfire smoke early, triggering alarms that firefighting teams can either confirm or dismiss. The surveillance system is installed at numerous strategic locations overlooking Croatian forests and is essential amid shifting Mediterranean climate patterns.

The idea of using weather analysis to predict fire potential or intensity is not novel and has been examined and implemented by various institutions and researchers. The Canadian Forest

Fire Weather Index (FWI) System (Natural Resources Canada, 2026) uses daily observations of temperature, relative humidity, wind speed and precipitation in order to determine the relative potential for wildland fire. USA's National Fire Danger Rating System (Jolly et al., 2024; Forest Service, U.S. Department of Agriculture, 2025) uses factors such as air temperature, relative humidity, rainfall, wind speed, solar radiation, snow cover and fuel moisture to determine the severe fire danger index. Australian McArthur Mk5 Forest Fire Danger Meter (Noble et al., 1980; CSIRO, 2026) uses air temperature, relative humidity, wind speed and drought effects to forecast fire danger in Australian forests. The Croatian wildfire risk index (Stipaničev et al., 2022) uses the Canadian FWI System, combined with wind speed and direction (correlated with slope and aspect), and calculates the relative influence of specific parameters on the overall risk index value using optimised genetic algorithms. (Di Giuseppe et al., 2025) used available data on fire fuel in order to increase the fire prediction accuracy and decrease false alarm rate, and employed data on temperature, dewpoint temperature, wind speed, precipitation, etc. (Nikolić et al., 2023) used multi-criteria GIS decision analysis (GIS-MCDA) of nine different natural and anthropogenic factors in order to determine the susceptibility to wildfires for two different regions in Montenegro. The weather-related factors the authors used in their analysis were temperature and precipitation. (Mohammadi et al., 2014) used logistic regression to analyse multiple factors influencing the occurrence of forest fires, and the climate-related ones were temperature and annual precipitation. It can be concluded that weather analysis is extremely important for predicting potential wildfire occurrence and intensity, and it is a field of research that is continually investigated and improved.

This paper is structured as follows. Section 2 outlines the methodology of the proposed approach and presents preliminary correlations between AI-based wildfire detections and weather parameters recorded at locations near flagged events. Section 3 discusses two multi-criteria decision-making (MCDM) methods, namely Simple Additive Weighting (SAW) and the Technique for Order Preference by Similarity to Ideal Solution (TOPSIS), which can be used to further analyse the previously obtained correlation results. Section 4 addresses the potential limitations of the presented approach and outlines directions for future work. Section 5 provides the conclusions.

1. METHODOLOGY

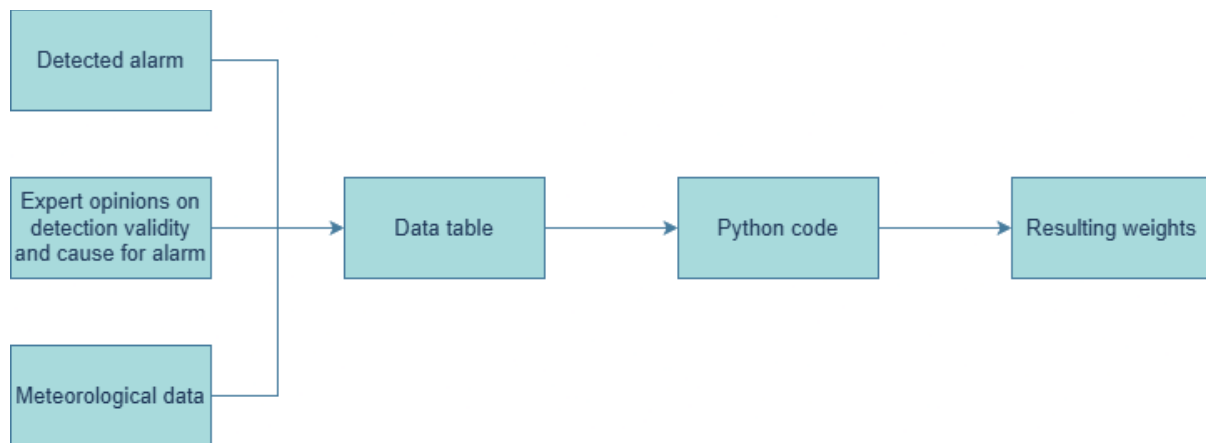
Many factors can affect the occurrence and intensity of wildfires. In this section of the paper, we present an analysis of the correlation between detections from an existing AI-based wildfire surveillance system and key weather parameters (e.g., temperature, relative humidity, wind gusts, precipitation and wind speed) recorded near flagged event locations. To analyse this correlation, logistic regression (Bewick et al., 2005; Erener et al., 2016) was used.

The goal of the logistic regression analysis is to determine the relative importance of various weather variables in accurately detecting wildfire smoke. The images used were all flagged by the wildfire detection system OIV Fire Detect AI (Bugarić et al., 2025; OIV, 2026) as positive

detections, but not always; some were false alarms. For every image with an alarm, additional information was collected. Three experts provided opinions on the validity of each alarm and on what they believed triggered it. Furthermore, meteorological data were gathered for each image. All of that information was combined into a single data file, which was then read by a Python script (Python Software Foundation, 2026) that calculated the weights for each collected environmental variable. The flowchart of the entire process is shown in Figure 1.

Figure 1

The process of obtaining weights



Data and Study Area

We collected operational data using the OiV Fire Detect AI wildfire monitoring system deployed across multiple locations in Croatia. The system uses cameras installed in mountainous, coastal, and island regions, including Biokovo, Hvar, Imotski, Knin, and Komiza. These cameras capture environmental images and transmit them to an AI-based algorithm that detects potential wildfire smoke and generates alerts.

This research collected a dataset of 100 alarm images captured by 9 cameras at the aforementioned locations during October and November 2025. Some locations have multiple cameras, each named by the location and an ordinal number. These alarm images contained the following information:

- camera location (e.g., Biokovo 1 and Hvar 1),
- date and time of the alarm,
- raw expert evaluations from three human experts on whether there is smoke in the image or not,
- a description of the phenomenon observed (by the same three human experts) in each of the images (e.g., clouds, fog, lighting effects, raindrops, smoke, etc.), and
- meteorological variables retrieved for the time/location of each image.

Meteorological variables were retrieved from the Open Meteo API (Zippenfenig, 2023) and matched to the alarm timestamp and location. The meteorological variables analysed in this research were: temperature at 2m (°C), relative humidity at 2m (%), wind gusts at 10m (km/h), precipitation (rain) (mm), wind speed at 10m (km/h), and wind speed at 80m (km/h). These variables were selected because they are available via the Open Meteo API, are physically related to smoke visibility and atmospheric conditions, and are commonly used in wildfire occurrence/risk modelling (Satir, 2016).

An assortment of phenomena contributes to the alarm condition (e.g., clouds, fog, lens flare, raindrops on the lens, and smoke), indicating the complexity of optical detection systems in mountainous coastal areas (Barmpoutis et al., 2020).

Labelling and class definitions

To provide expert labels for smoke presence across all alarm images, three independent human experts reviewed the images and assigned numerical ratings. The ratings used for the reviews were as follows: "0", indicating absolute certainty that smoke was not present and that the alarm was a false positive; "1", indicating absolute certainty that smoke was present; and "0.5", indicating some degree of uncertainty or partial smoke. In addition to providing a numerical value for their review, the experts also provided qualitative descriptions of what they saw in the images (e.g., clouds, smoke, fog, light effects). Because the experts' experience and reliability may have varied, their evaluations were combined using a weighted aggregation method.

The heuristically determined weights for the experts were 0.2, 0.4, and 0.4, giving greater weight to Experts 2 and 3. The weighted wildfire presence score for image i is defined by:

$$\text{fire_score_w}^{(i)} = 0.2x_1^{(i)} + 0.4x_2^{(i)} + 0.4x_3^{(i)} \quad (1)$$

where $x_1^{(i)}$, $x_2^{(i)}$ and $x_3^{(i)}$ are the numeric evaluations from Experts 1–3, respectively. The Python code reads the data file, converts the columns containing expert evaluations to numeric values, and calculates the weighted score for each row.

Depending on the weighted score, each of the 100 images is categorised into one of three categories, as shown in Table 1.

Table 1

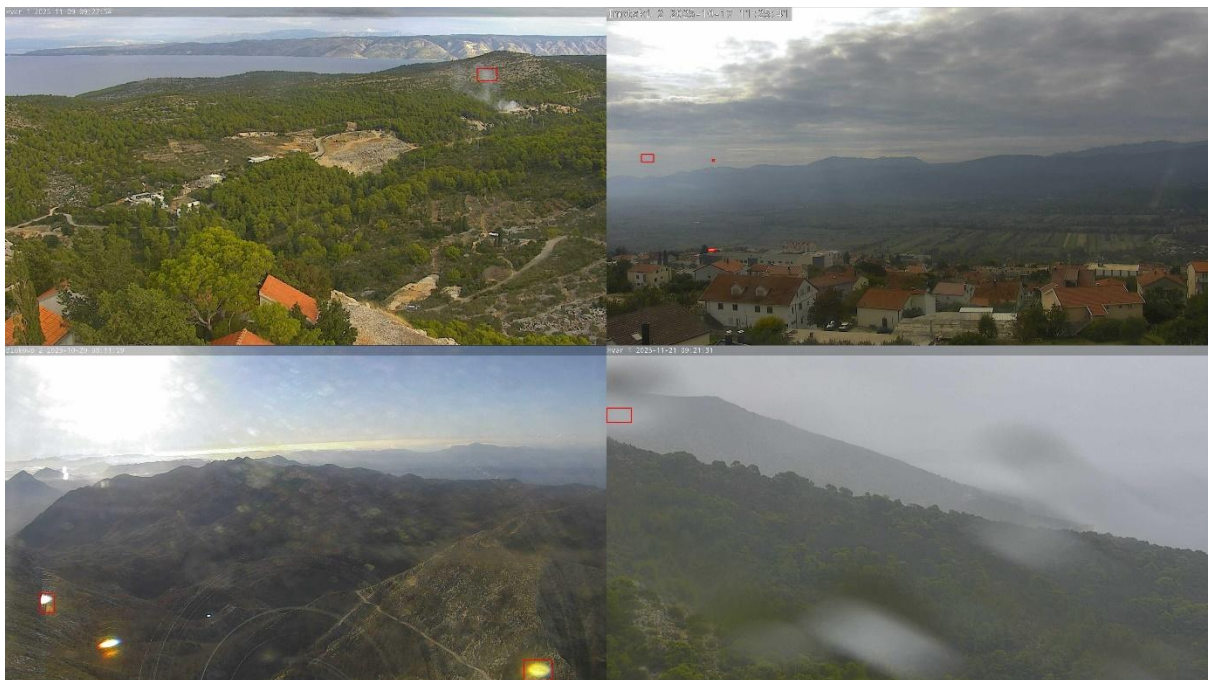
Labels assigned to alarms based on the calculated fire weights

Label	Calculated fire score	Expert consensus
True Positive (TP)	$\text{fire_score_w} \geq 0.8$	high expert consensus that smoke is present
True Negative (TN)	$\text{fire_score_w} \leq 0.2$	high consensus that no smoke is present
Mixed	$0.2 < \text{fire_score_w} < 0.8$	ambiguous or disputed cases

Examples of images for all three categories are shown in Figure 2.

Figure 2

Examples of images in different categories



Note. Top left: true positive, top right: mixed, bottom left and bottom right: true negative.
Source: Authors.

The "Mixed" category includes difficult-to-evaluate cases in which experts either disagree or are unsure whether smoke is present. For the logistic regression and weight determination, only the clearly labelled TP and TN subsets are utilised, thereby providing robust ground-truth data. The target variable y , where $y = 1$ for TP and $y = 0$ for TN, is the binary classification variable.

Weight derivation

The relationship between environmental conditions and accurate alarm detection is modelled using logistic regression. The independent variables are the six meteorological parameters, and the dependent variable is the alarm classification, using expert-weighted labels (TP or TN).

Let $X \in R^{(n \times 6)}$ denote the matrix of meteorological observations for n alarms, and $y \in 0,1^n$ the corresponding binary labels (1 = TP, 0 = TN). The logistic model is:

$$\log \left(\frac{P(y = 1 \vee X)}{1 - P(y = 1 \vee X)} \right) = \beta_0 + \sum_{j=1}^6 \beta_j x_j \quad (2)$$

where x_j are the standardised meteorological variables and β_j are the regression coefficients. To ensure the data had a zero mean and unit variance, it was pre-processed using scikit-learn's StandardScaler (Pedregosa et al., 2011). The logistic model is then fitted with L2 regularisation using the LBFGS solver (Liu & Nocedal, 1989; *Logistic Regression*, 2026).

The sign of each coefficient indicates the direction of influence. Positive values indicate that higher values increase the likelihood that an alarm will be a TP rather than a TN, and vice versa.

The absolute coefficients are then normalised to obtain MCDA-compatible importance weights:

$$w_j = \frac{|\beta_j|}{\sum_{k=1}^6 |\beta_k|} \quad (3)$$

These weights have two important properties: they add up to 1, and they reflect the relative influence implied by the regression, regardless of the sign of the coefficient. In MCDA terms, they represent the relative importance of each criterion for distinguishing expert-weighted true smoke alarms from non-smoke alarms under the studied conditions (Choo et al., 1999).

2. MCDA METHODS AND IMPLEMENTATIONS

The normalised absolute logistic regression coefficients can be directly applied to various established MCDA processes. Two methods are considered applicable to wildfire detection: SAW and TOPSIS (Hwang & Yoon, 1981). The following sections detail the application of these methods for two main use cases: per-alarm weather difficulty and site-level difficulty. In each case, the alarms and sites are regarded as alternatives, the six meteorological parameters as criteria, and the regression-determined weights represent the relative importance of each criterion.

Weather Difficulty Score

The goal of single alarms is to determine a weather difficulty score and, if applicable, a rank, indicating how favourable the meteorological environment is for accurate alarm detection. There are two complementary MCDA applications possible for determining the weather difficulty score for single alarms:

a) SAW (Simple Additive Weighing)

SAW uses the calculated weights directly:

1. Taking the six meteorological values x_{ij} (temperature, humidity, gusts, rain, wind 10 m, wind 80 m) for each alarm i
2. Normalising each criterion across alarms (e.g. min-max or z-score), and transforming to "benefit form" where larger values are indicative of more favourable conditions for accurate detection
3. Computing the SAW score

$$S_i^{SAW} = \sum_{j=1}^6 w_j x_{ij}^{(norm)} \quad (4)$$

using the normalised regression weights w_j .

Alarms can then be ranked by the S_i^{SAW} score, and alarms with lower scores are associated with higher difficulties and unfavourable weather conditions.

b) TOPSIS (Technique for Order Preference by Similarity to Ideal Solution)

TOPSIS better captures the distance of each alarm from the "optimal" and "worst" weather conditions, thereby improving detection accuracy and complementing SAW.

Using the weights, the steps are:

1. Constructing the decision matrix consisting of alarms (rows) and six criteria (columns).
2. Normalising the matrix (e.g. vector normalisation).
3. Multiplying each criterion column by the corresponding weight w_j .
4. Defining a positive ideal point A^* (best value on each criterion) and a negative ideal point A^- (worst values), adjusted to the benefit/cost direction.
5. Computing each alarm's distance to A^* and A^- and the coefficient of relative closeness

$$V_i = \frac{S_i^-}{S_i^- + S_i^*} \quad (5)$$

Here, S_i^* and S_i^- are computed using Euclidean distances from both the positive and negative ideal solution. V_i is the total reference score for each alternative A_i (Chakraborty, 2022). Alarms with higher V_i are closer to optimal weather conditions for accurate detection, whereas those

with lower values are closer to the worst meteorological regime for detection accuracy. TOPSIS provides an explicit expression of the "ideal-worst" reference weather conditions.

Site-Level Difficulty Score

For different camera positions, the objective is to calculate and rank the detection difficulty based on local climatic conditions. Each position is an alternative described by statistical summaries (e.g., seasonal averages) of the six meteorological parameters. Once again, the same MCDA methods can be used.

a) SAW

SAW again uses the calculated weights directly:

1. Computing representative site profiles (e.g. median temperature, humidity, gusts, rain, wind 10 m, wind 80 m during the fire season).
2. Normalising each criterion across different sites and adjusting the direction so that higher transformed values represent more favourable conditions for accurate detection.
3. Computing

$$S_{site}^{SAW} = \sum_{j=1}^6 w_j x_{site,j}^{(norm)} \quad (6)$$

to obtain a site difficulty index, where lower values indicate more challenging sites for the existing algorithm.

This core can guide the selection of additional equipment or algorithms for specific locations labelled as difficult.

b) TOPSIS

TOPSIS can further enhance the comparison of sites by allowing for the positioning of each site relative to a hypothetical "ideal" detection climate (e.g., moderate humidity, low gusts, moderate winds aloft) and a "worst" climate profile (e.g., high gusts, extreme humidity regimes that favour fog and low clouds). Using regression-based weights, the steps are:

1. Building the site-by-criterion matrix.
2. Normalising the matrix.
3. Defining ideal and anti-ideal site profiles A^* and A^- based on best/worst observed or expert-defined conditions.
4. Computing each site's closeness coefficient V_{site} .

Sites with low V_{site} are "close to worst" meteorological regimes for accurate detection and thus prime candidates for additional sensors (e.g., temperature and humidity sensors) or algorithmic changes.

By using the same derived weight vector for per-alarm and site-level analyses, the MCDA layer is consistent across the operational and strategic horizons, and SAW and TOPSIS can provide increasing degrees of analysis and understanding.

3. RESULTS AND DISCUSSION

The analysis of meteorological influences on the accuracy of the wildfire detection algorithm yielded regression-derived importance weights that characterise the algorithm's sensitivity to different environmental conditions. The calculated regression coefficients are shown in Table 2.

Table 2

Table of resulting coefficients β

Criterion	Coefficient	Absolute value
Temperature 2m (°C)	0.108	0.108
Relative humidity 2m (%)	0.831	0.831
Wind gusts 10m (km/h)	−0.548	0.548
Rain (mm)	−0.016	0.016
Wind speed 10m (km/h)	−0.026	0.026
Wind speed 80m (km/h)	−0.256	0.256

The coefficients with positive values (humidity, temperature) indicate that higher values increase the likelihood that an alarm will be a TP rather than a TN, while negative values (rain, wind speed 10m, wind speed 80m, and wind gusts 10m) indicate the opposite.

These coefficients β were then normalised, and the results are shown in Table 3.

Table 3

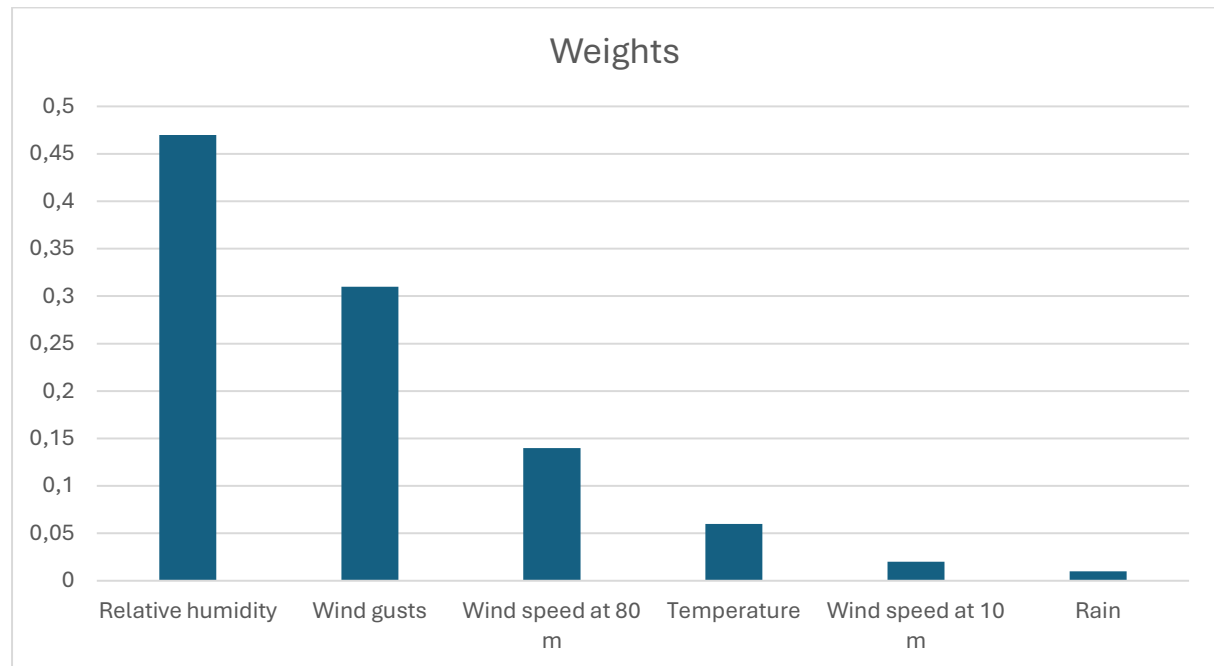
Table of normalised weights for each criterion w_j

Criterion	Approximate weight
Relative humidity 2m (%)	0.466
Wind gusts 10m (km/h)	0.307
Wind speed 80m (km/h)	0.144
Temperature 2m (°C)	0.060
Wind speed 10m (km/h)	0.014
Rain (mm)	0.009

The resulting weights sum to 1 and reflect the relative influence implied by the regression, regardless of the sign of the coefficient. The resulting weights ranked by importance are shown in Figure 3.

Figure 3

Calculated weights sorted from most influential to least influential



The results revealed that relative humidity and wind-related parameters have the greatest effect on detection accuracy, whereas temperature and precipitation have a lower influence. These weights can then be integrated into two MCDA frameworks (SAW and TOPSIS) to quantify and rank detection difficulty both for individual alarms and across monitoring sites, as stated in the previous section. By enabling the use of both SAW and TOPSIS, it creates a decision-support tool with multiple layers that helps determine when conditions are challenging for optical smoke detection systems and guides future adaptations to improve their deployment.

Limitations

While the presented methodology has certain limitations, these are particularly relevant when used as a decision-support tool in high-stakes contexts such as civil protection and military security.

A primary limitation of the proposed methodology is its reliance on a relatively small sample of alarms recorded over a very short period and in a limited area. The dataset is unbalanced because most alarms are classified as true negatives (TN). In contrast, a minority are classified as mixed or true positives (TP) due to the time interval between image captures. Therefore, the reliability of the regression coefficients and the derived MCDA weights under seasonal,

regional, and yearly variations is called into question. Using large datasets of alarms recorded over multiple years, seasons, and areas could yield better, more accurate results.

The framework relies solely on six environmental parameters, limiting its scope. Although the six selected meteorological variables are readily available in real time and physically significant, they represent only a very limited subset of relevant environmental parameters. Other parameters can influence results, such as time of day, direct sunlight, and solar geometry (Zhu et al., 2025). Additionally, the environmental parameters utilised were obtained via an Open Meteo API and were not directly measured by sensors located near the cameras. These parameters can significantly influence the radiometric and textural features of smoke, clouds, and fog captured by cameras.

Furthermore, there were limitations in the labels and the handling of ambiguities. The regression used to determine the MCDA weights ignores all ambiguous ("Mixed") alarms and focuses exclusively on clearly labelled True Positives (TPs) and True Negatives (TNs). While this helps ensure high-quality labelling for binary classification, it omits the exact instances that are operationally critical: images on which experts disagree or are uncertain. The datasets could also be expanded with additional labels, such as False Negatives (FNs), i.e., images where smoke was present but not detected by the algorithm.

Finally, the results are algorithm-specific. The derived weights reflect the sensitivity of a specific optical smoke detection algorithm applied to a specific camera network and configuration. Other algorithms may display very different sensitivities to humidity, wind, and precipitation. For this reason, comparative studies should be performed across different algorithms with weights calculated independently for each. An analysis can then be conducted on how the selection of detection algorithms affects the system's detection fidelity under various meteorological conditions.

Future work

From a military applications perspective, the framework has the potential to develop decision-support modules for training safety, range management, and protection of critical assets. Scenario-specific detection difficulty indices can be treated as a single criterion in a larger MCDA model that includes other criteria such as operational costs, required training and mission readiness. For example, formal comparisons of different scheduling options for live-fire exercises (at different times of the year, at different hours of the day, or in different locations) can be made in terms of fire-detection reliability and operational constraints.

There is a basis for theoretical integration with command-and-control (C2) and situational awareness systems. In this context, the meteorology-based detection difficulty indices would be one of many layers of information (intelligence, operations, logistics, meteorology, etc.) and future research could investigate formal relationships between the proposed MCDA module

and upper-level decision models (such as dynamic resource allocation, sensor tasking, and multi-stage emergency responses).

CONCLUSION

The presented methodology addresses decision-making in complex situations and the use of computer-aided systems to support it. The problem and methodology presented in this paper can be applied to a range of decision-making problems under uncertainty.

The problem of decision-making, especially in cases of exposure to: a) the influence of a large number of factors, b) large amounts of data, and c) time-critical activities, represents a special challenge. Making accurate, fact-based decisions under given conditions is of the utmost importance in situations that can result in human casualties, threats to social and/or ecological systems, and significant material losses. This paper presented an example of applying one such approach, based on MCDA, to wildfire detection, using the SAW and TOPSIS methods. The data used to create the decision framework were collected from optical sensors (surveillance cameras), meteorological procedures (condition indicators), and expert inputs (human judgment). The presented model serves as a proof of concept, demonstrating the effectiveness of establishing a correlation between wildfire occurrence and key parameters, i.e., meteorological conditions, at the observed locations.

The authors intend further to develop the model across a range of problem classes, using larger, more diverse datasets, primarily for application in the field of defence and security.

REFERENCES

- Bacciu, V., Salis, M., Arca, B., Pellizzaro, G., Ascoli, D., Delogu, G. M., Eftychidis, G., Chuvieco, E., Gitas, I., & Viegas, D. X. (2025). Shifting to a holistic approach in national wildfire management policies: The Italian case. *iForest - Biogeosciences and Forestry*, 18(4), 163. (world). <https://doi.org/10.3832/ifor4786-018>
- Barmpoutis, P., Papaioannou, P., Dimitropoulos, K., & Grammalidis, N. (2020). A Review on Early Forest Fire Detection Systems Using Optical Remote Sensing. *Sensors (Basel, Switzerland)*, 20(22), 6442. <https://doi.org/10.3390/s20226442>
- Bewick, V., Cheek, L., & Ball, J. (2005). Statistics review 14: Logistic regression. *Critical Care*, 9(1), 112. <https://doi.org/10.1186/cc3045>
- Bugarić, M., Krstinić, D., Šerić, L., & Stipaničev, D. (2025). Current Trends in Wildfire Detection, Monitoring and Surveillance. *Fire*, 8(9). <https://doi.org/10.3390/fire8090356>
- Čavlina Tomašević, I., Cheung, K. K. W., Vučetić, V., Fox-Hughes, P., Horvath, K., Telišman Prtenjak, M., Beggs, P. J., Malečić, B., & Milić, V. (2022). The 2017 Split wildfire in Croatia: Evolution and the role of meteorological conditions. *Natural Hazards and Earth System Sciences*, 22(10), 3143–3165. <https://doi.org/10.5194/nhess-22-3143-2022>
- Çela, G., Gjoni, A., Doko, A., Kadria, F., Rexhepi, I., & Jaupaj, O. (2025). Meteorological Analysis of Extreme Fires in Albania during the Period 2019–2025. *Journal of Geography, Environment and Earth Science International*, 29(12), 61–73. <https://doi.org/10.9734/jgeesi/2025/v29i12983>
- Chakraborty, S. (2022). TOPSIS and Modified TOPSIS: A comparative analysis. *Decision Analytics Journal*, 2, 100021. <https://doi.org/10.1016/j.dajour.2021.100021>
- Choo, E. U., Schoner, B., & Wedley, W. C. (1999). Interpretation of criteria weights in multi-criteria decision making. *Computers & Industrial Engineering*, 37(3), 527–541. [https://doi.org/10.1016/S0360-8352\(00\)00019-X](https://doi.org/10.1016/S0360-8352(00)00019-X)
- CSIRO. (2026). *McArthur Mk5 Forest Fire Danger Meter*. <https://www.csiro.au/en/research/disasters/bushfires/Mk5-forest-fire-danger-meter>
- Curt, T., Aini, A., & Dupire, S. (2020). Fire Activity in Mediterranean Forests (The Algerian Case). *Fire*, 3(4). <https://doi.org/10.3390/fire3040058>
- Di Giuseppe, F., McNorton, J., Lombardi, A., & Wetterhall, F. (2025). Global data-driven prediction of fire activity. *Nature Communications*, 16(1), 2918. <https://doi.org/10.1038/s41467-025-58097-7>
- Erener, A., Mutlu, A., & Sebnem Düzgün, H. (2016). A comparative study for landslide susceptibility mapping using GIS-based multi-criteria decision analysis (MCDA), logistic regression (LR) and association rule mining (ARM). *Engineering Geology, Special Issue on Probabilistic and Soft Computing Methods for Engineering Geology*, 203, 45–55. <https://doi.org/10.1016/j.enggeo.2015.09.007>

- Forest Service, U.S. Department of Agriculture. (2025, December 1). *National Fire Danger Rating System (NFDRS)* [Text].
<https://research.fs.usda.gov/firelab/projects/firedangerrating>
- Hojsak, T. (2025, December 11). *NERO Fire Brief: Extreme Wildfire Event in Pisak-Mimice, Croatia – June 2025 – NERO*. <https://nero-network.eu/news/nero-fire-brief-extreme-wildfire-event-in-pisak-mimice-croatia-june-2025>
- Hwang, C.-L., & Yoon, K. (1981). Methods for Multiple Attribute Decision Making. In C.-L. Hwang & K. Yoon (Eds.), *Multiple Attribute Decision Making: Methods and Applications A State-of-the-Art Survey* (pp. 58–191). Springer.
https://doi.org/10.1007/978-3-642-48318-9_3
- Jolly, W. M., Freeborn, P. H., Bradshaw, L. S., Wallace, J., & Brittain, S. (2024). Modernising the US National Fire Danger Rating System (version 4): Simplified fuel models and improved live and dead fuel moisture calculations. *Environmental Modelling & Software*, 181, 106181. <https://doi.org/10.1016/j.envsoft.2024.106181>
- Liu, D. C., & Nocedal, J. (1989). On the limited memory BFGS method for large scale optimisation. *Mathematical Programming*, 45(1), 503–528.
<https://doi.org/10.1007/BF01589116>
- Liz-López, H., Huertas-Tato, J., Pérez-Aracil, J., Casanova-Mateo, C., Sanz-Justo, J., & Camacho, D. (2024). Spain on fire: A novel wildfire risk assessment model based on image satellite processing and atmospheric information. *Knowledge-Based Systems*, 283, 111198. <https://doi.org/10.1016/j.knosys.2023.111198>
- Logistic Regression*. (2026). Scikit-Learn. https://scikit-learn/stable/modules/generated/sklearn.linear_model.LogisticRegression.html
- Mamut, M. (2011). Veza prirodnogeografske i sociogeografske osnove Dalmacije s ugroženošću otvorenog prostora požarom. *Sumarski List*, 135.
- Mohammadi, F., Bavaghar, M. P., & Shabanian, N. (2014). Forest Fire Risk Zone Modeling Using Logistic Regression and GIS: An Iranian Case Study. *Small-Scale Forestry*, 13(1), 117–125. <https://doi.org/10.1007/s11842-013-9244-4>
- Natural Resources Canada. (2026). *Canadian Forest Fire Weather Index (FWI) System*. <https://cwffis.cfs.nrcan.gc.ca/background/summary/fwi>
- Nikolić, G., Vujović, F., Golijanin, J., Šiljeg, A., & Valjarević, A. (2023). Modelling of Wildfire Susceptibility in Different Climate Zones in Montenegro Using GIS-MCDA. *Atmosphere*, 14(6). <https://doi.org/10.3390/atmos14060929>
- Noble, I. R., Gill, A. M., & Bary, G. a. V. (1980). McArthur's fire-danger meters expressed as equations. *Australian Journal of Ecology*, 5(2), 201–203. <https://doi.org/10.1111/j.1442-9993.1980.tb01243.x>
- OIV. (2026). *OIV Fire Detect AI*. <https://oiv.hr/en/services-and-platforms/oiv-fire-detect-ai/>

- Pedregosa, F., Varoquaux, G., Gramfort, A., Michel, V., Thirion, B., Grisel, O., Blondel, M., Prettenhofer, P., Weiss, R., Dubourg, V., Vanderplas, J., Passos, A., Cournapeau, D., Brucher, M., Perrot, M., & Duchesnay, É. (2011). Scikit-learn: Machine Learning in Python. *The Journal of Machine Learning Research*, 12(null), 2825–2830.
- Python Software Foundation. (2026). *Python documentation*. Python Documentation. <https://docs.python.org/3/>
- Satir, O. (2016). Modelling Long Term Forest Fire Risk Using Fire Weather Under Under Climate Change in Turkey. *Applied Ecology and Environmental Research*, 14(4), 537–551. https://doi.org/10.15666/aeer/1404_537551
- Silva, P., Carmo, M., Rio, J., & Novo, I. (2023). Changes in the Seasonality of Fire Activity and Fire Weather in Portugal: Is the Wildfire Season Really Longer? *Meteorology*, 2(1), 74–86. <https://doi.org/10.3390/meteorology2010006>
- Stefanidis, S., Alexandridis, V., Spalevic, V., & Luiz Mincato, R. (2022). Wildfire Effects on Soil Erosion Dynamics: The Case of 2021 Megafires in Greece. *The Journal "Agriculture and Forestry"*, 68(2). <https://doi.org/10.17707/AgricultForest.68.2.04>
- Stipaničev, D., Bugarić, M., Šerić, L., Krstinić, D., & Božić-Štulić, D. (2022). Site-Specific Wildfire Risk Index in Croatian Wildfire Monitoring and Surveillance System. *Environmental Sciences Proceedings*, 17(1). <https://doi.org/10.3390/environsciproc2022017034>
- Stipaničev, D., Španjol, Z., Vučetić, M., Vučetić, V., Rosavec, R., & Bodrozić, Lj. (2008). *The Kornati fire accident facts and figures – configuration, vegetation and meteorology*. 387–396. <https://doi.org/10.2495/FIVA080381>
- Tariq, S., ul-Haq, Z., Mariam, A., Mehmood, U., & Ahmed, W. (2023). Assessment of air quality during worst wildfires in Mugla and Antalya regions of Turkey. *Natural Hazards*, 115(2), 1235–1254. <https://doi.org/10.1007/s11069-022-05592-5>
- Zhu, W., Niu, S., Yue, J., & Zhou, Y. (2025). Multiscale wildfire and smoke detection in complex drone forest environments based on YOLOv8. *Scientific Reports*, 15, 2399. <https://doi.org/10.1038/s41598-025-86239-w>
- Zippenfenig, P. (2023). *Open Meteo Weather API*. <https://zenodo.org/records/14582479>

NUMERICAL SIMULATION OF FUEL CELL INTEGRATION IN MILITARY AUV AS AN ALTERNATIVE TO BATTERY SYSTEMS

Jure Penga¹, Ena Sarajlić¹, Bruno Ševo², Željko Penga², Luka Mihanović¹

¹ Dr. Franjo Tuđman Defense and Security University, Zrinsko-Frankopanska 207 a, 21000 Split, Croatia

E-mail: jure.penga@sois-ft.hr, ena.sarajlic@sois-ft.hr, luka.mihanovic@sois-ft.hr

ORCID: 0009-0007-6608-5798 (Jure Penga), 0009-0004-1646-4210 (Ena Sarajlić), 0000-0001-6082-4835 (Luka Mihanović)

² University of Split, Faculty of Electrical Engineering, Mechanical Engineering and Naval Architecture, R. Boškovića 32, 21000 Split, Croatia

E-Mail: bruno.sevo.00@fesb.hr, zeljko.penga@fesb.hr

ORCID: 0009-0006-3456-7373 (Bruno Ševo), 0000-0001-7331-9432 (Željko Penga)

Abstract

The development of Autonomous Underwater Vehicles (AUVs) has created a new generation of tools for the modern military to accomplish a wide range of missions, including maritime surveillance, mine countermeasures, reconnaissance, and search-and-rescue. The REMUS 100 AUV, introduced to the Croatian Navy in 2016, is a prime example of a small AUV designed to conduct shallow-water seabed searches and mine-countermeasures missions. At present, the REMUS 100 AUV is powered by lithium-ion batteries, which limit its endurance. The main goal of this study is to assess whether the current power source for the REMUS 100 AUV can be replaced with a fuel cell, enabling the AUV to operate for the same duration or for an extended period without affecting its hydrodynamic performance.

To start, a three-dimensional Computational Fluid Dynamics (CFD) model of the REMUS 100 hull and propeller was developed to quantify hydrodynamic resistance and propulsive power, with a focus on a cruise speed of 2 m/s. The CFD-derived thrust and torque were then converted into mechanical power demand and, subsequently, into electrical power requirements for the onboard energy system. Based on these results, a simple model was created to evaluate the currently implemented lithium-ion battery system against a Proton Exchange Membrane Fuel

Cell (PEMFC) system with the equivalent power output. Preliminary results indicate that a properly sized fuel cell system should be capable of extending mission duration at the expense of increased integration complexity. The study presents a quantitative roadmap for transitioning from battery-only to hybrid/fuel-cell architectures to enhance the operational capability of naval autonomous systems.

Keywords: CFD propeller-hull interaction; REMUS 100; fuel cell power system; power and energy modelling; autonomy enhancement; Croatian Navy

INTRODUCTION

Autonomous Underwater Vehicles (AUVs), such as the REMUS 100, have evolved into essential components of the contemporary naval force, supporting a variety of mission roles, including maritime surveillance, mine countermeasures, reconnaissance, and search-and-rescue in littoral environments. Since 2016, the REMUS 100 has supported seabed searches and mine countermeasure operations for the Croatian Navy. The successful completion of these tasks depends upon reliable coverage of extensive shallow-water areas and predictable energy consumption. Currently, the REMUS 100 uses lithium-ion batteries as its primary power source, limiting its autonomy. Therefore, the logistics of recharging, replacing, and safely handling the batteries during prolonged, intense military use represent significant constraints.

Given the inherent limits of battery systems, alternative energy sources are being explored that may offer higher effective energy density for onboard storage. One viable option is the PEMFC. PEMFC systems can offer improved reliability, decreased turnaround time between missions, and quieter-than-conventional-battery operation while submerged. When paired with high-pressure hydrogen storage, systems utilising PEMFCs have demonstrated the potential to achieve nearly twice the energy density of conventional batteries. Studies have shown that improvements of up to approximately 80% in energy density may be possible at hydrogen storage pressures around 700 bar (Deutsch et al., 2022).

Alongside advances in mission systems and autonomy, significant research has focused on developing hydrodynamic models of torpedo-shaped AUVs, such as the DARPA-SUBOFF hull, using CFD (Safari et al., 2022). While some studies have utilised RANS-based CFD to calculate hydrodynamic coefficients for AUVs and improve 6-DoF dynamic models, they have demonstrated that CFD-calculated values can yield significantly better representations of surge, heave, and pitch dynamics than empirical methods alone. For REMUS-type AUVs, studies on dynamic modelling and manoeuvrability have emphasised the need to accurately estimate drag and moments across the AUV's entire operating envelope (Sakaki & Kerdabadi, 2020). Such hydrodynamic models establish the relationship between the motion of the AUV, the amount of propulsive power required, and ultimately the amount of energy that must be supplied to the onboard power system. As those studies mainly focused on manoeuvrability and the simple

calculation of hull drag, this paper focuses on the interaction between the propeller, hull, and appendages to make the simulation as realistic as possible.

At the same time, lithium-ion batteries' inability to support long-range, long-endurance underwater operations has led to growing interest in incorporating fuel-cell-based power systems into AUVs. Fuel cells have higher specific energy than conventional batteries, and when coupled with appropriate hydrogen and oxygen storage solutions, they can effectively double a vehicle's range and endurance, though at the expense of increased integration complexity due to high-pressure storage and balance-of-plant issues. Several recent studies on AUV/UAV energy systems demonstrate that hydrogen-fuelled cells can outperform lithium-ion packs for missions requiring long-term, sustained power, provided that sufficient storage and balance-of-plant engineering are applied. For naval AUVs, this represents a promising pathway to reduce the recovery rate, increase on-station time, and enhance tactical flexibility in demanding operations.

Considering the above papers, the present work combines a CFD-based hydrodynamic analysis of the REMUS 100 with appendages with an energy-system comparison between the current lithium-ion battery configuration and a hypothetical fuel-cell-based alternative.

A three-dimensional RANS simulation utilising the $k-\omega$ SST turbulence model was conducted for the REMUS 100 hull with appendages and propeller. These simulations estimated the drag and the propulsive power required for the REMUS 100 AUV at a speed used in common missions. The hydrodynamic results obtained from the CFD simulations were used to generate power demand profiles and, from these, the corresponding hydrogen and oxygen consumptions for a PEMFC system. As such, a direct comparison of the achievable endurance of the current battery system and the hypothetical fuel-cell-powered REMUS 100 AUV can be made under realistic mission conditions. By linking CFD-derived hydrodynamics to energy storage and conversion models, this study aims to quantify how a fuel-cell-powered REMUS 100 AUV can extend mission duration and improve operational effectiveness in naval applications compared with batteries.

1. CFD CALCULATION BACKGROUND

Geometry

The geometry of the REMUS 100 was extracted from the figure, and the characteristics are shown in the Technical Specifications for the REMUS 100 (AMC Search, 2025). The first step was to identify the main characteristics that could be openly disclosed. The geometrical characteristics of the REMUS 100 are shown in Figure 1.

Figure 1

Side view of the REMUS 100 (left) and REMUS 100 at sea (right)



Source: AMC Search (2025).

Additional valuable information provided with the technical specifications is shown in Table 1.

Table 1

Main characteristics that have been used to define the geometry

Parameter	Value	Unit
Diameter	190	mm
Length	1700 to 2100	mm
Main battery capacity	1	kWh
Speed	0.5 to 2.6 (depending on configuration)	m/s
Endurance	Up to 10	h

Source: AMC Search (2025).

The geometry was reverse-engineered with CAD software. The extracted hull geometry is shown in Figure 2.

Figure 2

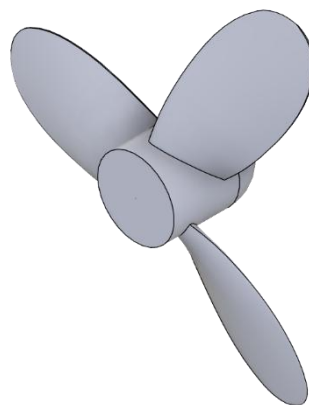
Geometry of the REMUS 100 extracted from the available data.



As for the propeller, since the data was not available, we implemented one similar to the one shown in the provided data. The chosen propeller is the Wageningen B 3.35, as shown in Figure 3. Because the standard calculation for this propeller type yields a diameter larger than required, the geometry was created at 1400 mm and scaled 1:10, resulting in a final propeller diameter of 140 mm.

Figure 3

Geometry of the Wageningen B 3.35 propeller



After generating the geometry of the REMUS 100 hull with appendages, it was necessary to consolidate them. The consolidated geometry is shown in Figure 4.

Figure 4

Consolidated REMUS 100 and B 3.35 propeller geometry.



Although it was interesting to have appendages on the hull of REMUS 100, the minor appendages created a significant problem for generating a proper mesh, resulting in slightly simplified geometry shown in Figure 5.

Figure 5

Modified REMUS 100 geometry with highlighted areas of geometry simplification



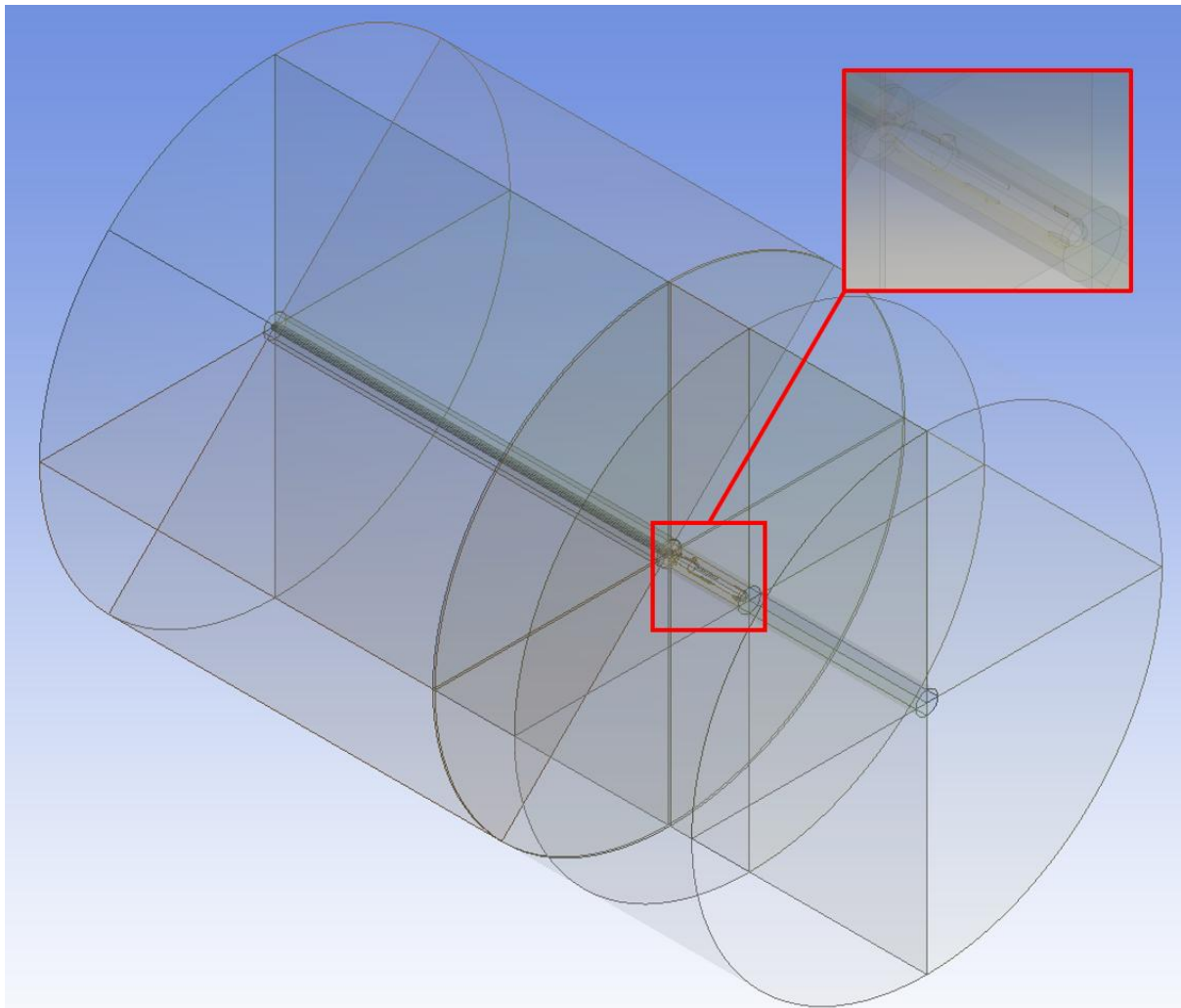
2. NUMERICAL DOMAIN

Geometry

The numerical domain for the CFD simulation was taken from Xu et al. (2024), with the only difference being that the domain was cylindrical rather than rectangular. The numerical domain is visible in Figure 6.

Figure 6

Numerical domain for the CFD calculation with details of the domain in proximity to the REMUS 100 and propeller geometry.



As the domain was complex, it was necessary to use the so-called "slicing" to get the proper minimal orthogonal quality of the mesh in the required regions for proper simulation. The main limitation in mesh quality was the use of an unstructured tetrahedral mesh near the REMUS 100, followed by a region with a combination of tetrahedral and hexahedral elements, which

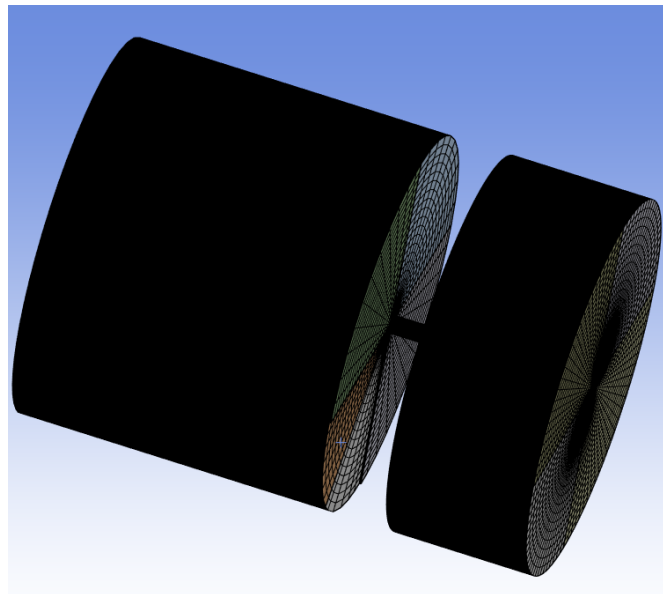
significantly reduced mesh quality. The solution to that problem was to "move" low-quality cells to the outer part of the mesh, which doesn't have fluctuations in terms of speed and flow direction. This ensured accurate results for the drag, thrust, and torque on the hull and propeller.

Mesh

The fluid domain consists of two parts: static and rotating. The static domain was sliced, as mentioned in 3.1. Geometry to ensure proper mesh quality. The numerical domain was divided into 3766678 elements in total, with a minimal orthogonal quality of 0.1, which is reached in most of the domain. The domains that have orthogonal quality larger than 0.1 are shown in Figure 7.

Figure 7

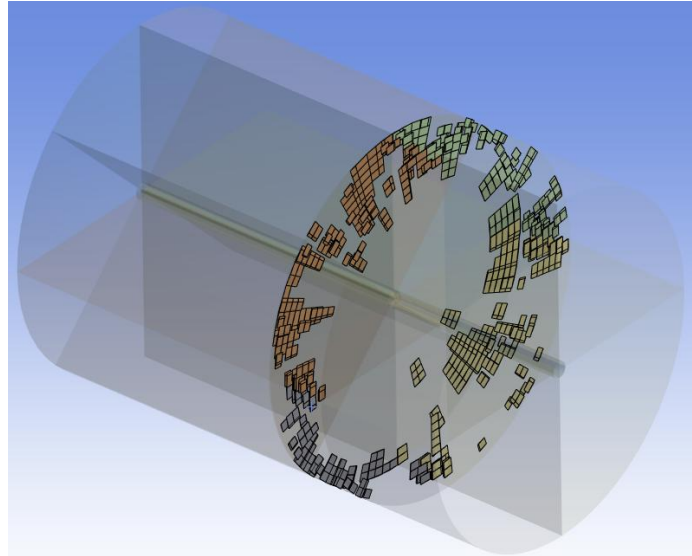
Numerical domain that fully complies with the required minimal orthogonal quality.



As shown in Figure 7, the mesh quality near the propeller hull exceeds the required minimum orthogonal quality of 0.1. The minimal orthogonal quality appears only in the outer part of the mesh, as shown in Figure 8, which is an additional benefit for claims that poor outer-element quality doesn't affect the accuracy of the solution.

Figure 8

Elements of the numerical domain that don't comply with the minimal orthogonal quality

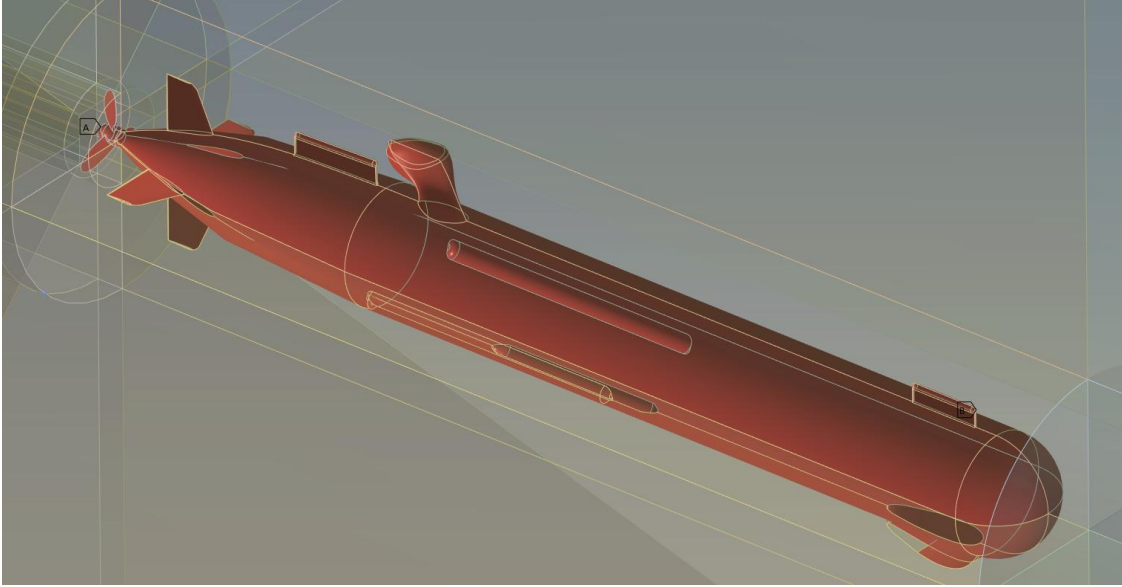


Boundary conditions

Boundary conditions are set as a velocity inlet and a pressure outlet in the direction of fluid flow (from the front to the back of the REMUS 100). The cylindrical exterior is set as a wall, and the hull and propeller are defined separately to calculate the required drag, thrust, and torque. It is important to note that the domain consisted of two parts (rotational and stationary) that required intersection, and the fluids were given named selections, fluid stationary and fluid rotating, to separate them and facilitate later setup. The hull and propeller domains are visible in Figure 9.

Figure 9

Hull and propeller named selections for calculating drag, thrust, and torque.



Governing equations

The full setup and calculations were conducted in ANSYS 2025 R2 within the Fluent module with solver options set as double precision. The flow was modelled using the $k-\omega$ SST two-equation RANS model, which solves transport equations for the turbulent kinetic energy k and the specific dissipation rate ω , with an eddy-viscosity formulation that includes shear-stress transport and blending between $k-\omega$ and $k-\epsilon$ behaviour (Menter, 1994).

The main equations that describe the $k-\omega$ SST model are written below:

1. Turbulent kinetic energy k equation.

$$\frac{\partial(\rho k)}{\partial t} + \frac{\partial(\rho u_j k)}{\partial x_j} = \frac{\partial}{\partial x_j} \left[(\mu + \sigma_k \mu_t) \frac{\partial k}{\partial x_j} \right] + P_k - \beta^* \rho k \omega \quad (1)$$

2. Specific dissipation rate ω equation (SST form).

$$\frac{\partial(\rho \omega)}{\partial t} + \frac{\partial(\rho u_j \omega)}{\partial x_j} = \frac{\partial}{\partial x_j} \left[(\mu + \sigma_\omega \mu_t) \frac{\partial \omega}{\partial x_j} \right] + \alpha \frac{\omega}{k} P_k - \beta \rho \omega^2 + 2(1 - F_1) \rho \sigma_{\omega 2} \frac{1}{\omega} \frac{\partial k}{\partial x_j} \frac{\partial \omega}{\partial x_j} \quad (2)$$

3. Eddy viscosity (shear-stress-transport form).

$$\mu_t = \rho \nu_t = \frac{\rho a_1 k}{\max(a_1 \omega, S F_2)} \quad (3)$$

Where S is the invariant measure of the strain-rate tensor.

Input parameters for the simulation

The numerical simulation was transient, with the main conditions set as shown in Table 2.

Table 2

Input parameters for the CFD simulation of the REMUS 100 and B3.35 propeller

Parameter	Value	Unit
Velocity	2	m/s
Number of propeller revolutions	2165	rpm
Time step	0.000222	s
Angle movement of the propeller for each time step	2.88	deg

3. HYDRODYNAMIC RESULTS OF NUMERICAL ANALYSIS

The numerical simulation showed a drag of 19 N on the hull at a speed of 2 m/s. The equivalent thrust required 2165 rpm and a torque (Q) of 0.4 Nm. The time step was calculated as time for the 2.88 deg of revolution, where the required mechanical power can be calculated as:

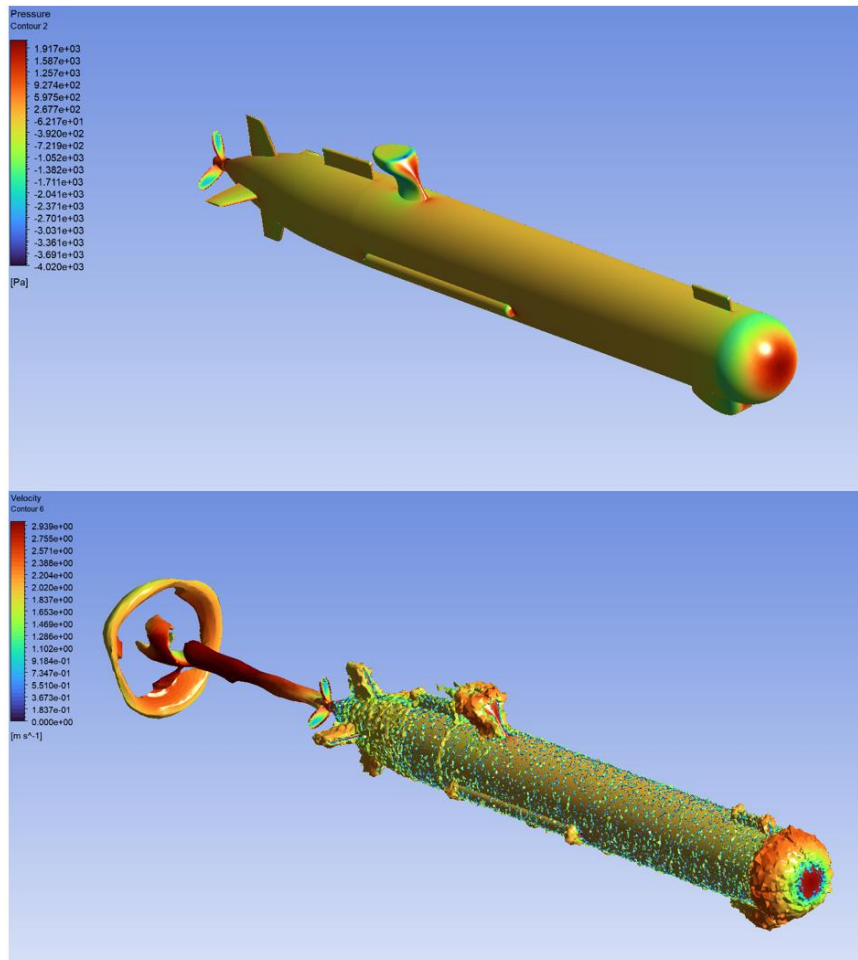
$$P_{prop} = Q \omega = Q * \frac{2\pi n}{60} \quad (4)$$

$$P_{prop} = 90.687 \text{ W} \quad (5)$$

In Figure 10, the pressure distribution across the hull and propeller is shown.

Figure 10

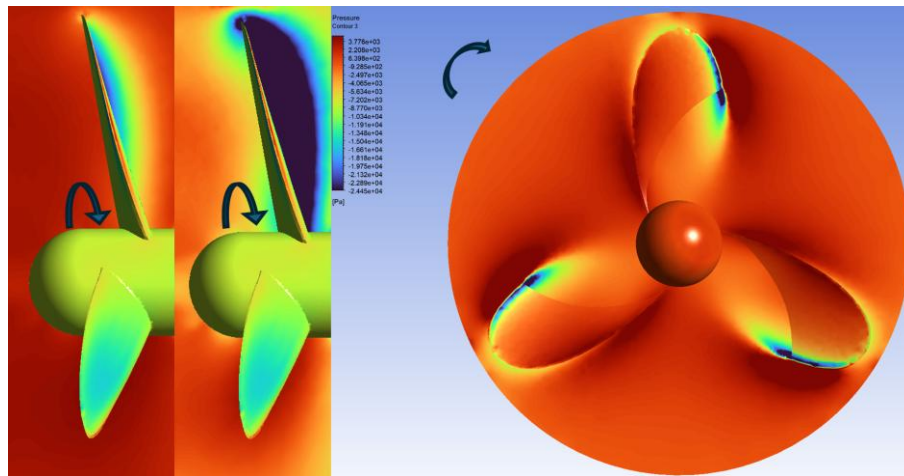
Pressure distribution (top) and vortex distribution (bottom) across the hull and propeller.



As shown in Figure 10 and in the pressure distribution across the hull of REMUS 100, the appendages significantly influence drag, along with the submersible bow. The pressure difference ranges between -4020 Pa and 2123 Pa on the hull and -36912 and 29936 Pa on the propeller. Propeller pressure distribution on the front and aft of the propeller, together with the cross-section, is visible in Figure 11.

Figure 11

Pressure distribution across the propeller and rotating domain cross-section on the propeller



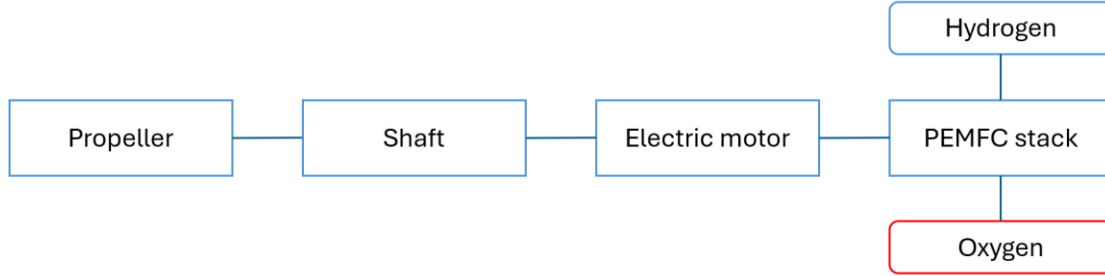
The propeller distribution is behaving as expected, generating the thrust required to overcome the drag of the REMUS 100 hull. Based on the visual inspection, this propeller is not optimised for the hull, which may reduce the system's efficiency compared to the original propeller on the submersible.

4. CALCULATION OF THE EQUIVALENT PROTON EXCHANGE MEMBRANE FUEL CELL SYSTEM REQUIREMENTS

As REMUS uses a 1 kWh battery package, it is interesting to compare it with a proton exchange membrane fuel cell (PEMFC) system with an equivalent storage capacity. Another key point is the possibility of adding fuel tanks without requiring external insulation, since tanks store only gas, unlike the battery system, which is susceptible to electrical discharge when it comes into contact with salt water. The main difference between the battery system and the PEMFC system is that the PEMFC system requires two tanks to store hydrogen and oxygen. To calculate the appropriate energy requirements, refer to the diagram in Figure 12. It represents all the components required to calculate losses from the fuel cell to the propeller.

Figure 12

Block diagram of the mechanical power flow (left to right).



As the required mechanical power on the shaft has been calculated in the previous chapter to be 90.68 W, it is important to add all other losses from the propeller to the PEMFC stack. The mechanical power on the propeller can be calculated as follows:

$$P_{prop} = P_{PEMFC} \eta_{PE} \eta_{motor} \eta_{shaft} \quad (6)$$

Where the losses consist of:

η_{PE} – Power-electronics efficiency

η_{motor} – Motor efficiency

η_{shaft} – Magnetic bearing efficiency

Where the PEMFC stack power can be calculated with the following expression:

$$P_{PEMFC} = \frac{P_{prop}}{\eta_{PE} \eta_{motor} \eta_{shaft}} \quad (7)$$

The losses in the REMUS 100 are predefined for each drivetrain component, as these components have standard losses (HII, 2025).

Efficiency of the electric motor (direct drive brushless motor):

$$\eta_{motor} = 0.9 \quad (8)$$

Efficiency of the magnetic bearing:

$$\eta_{shaft} = 0.96 \quad (9)$$

Efficiency of the power electronics:

$$\eta_{PE} = 0.94 \quad (10)$$

After the defined efficiencies, it is easy to calculate the required PEMFC stack power:

$$P_{PEMFC} = \frac{90.68}{0.94 * 0.9 * 0.96} \quad (11)$$

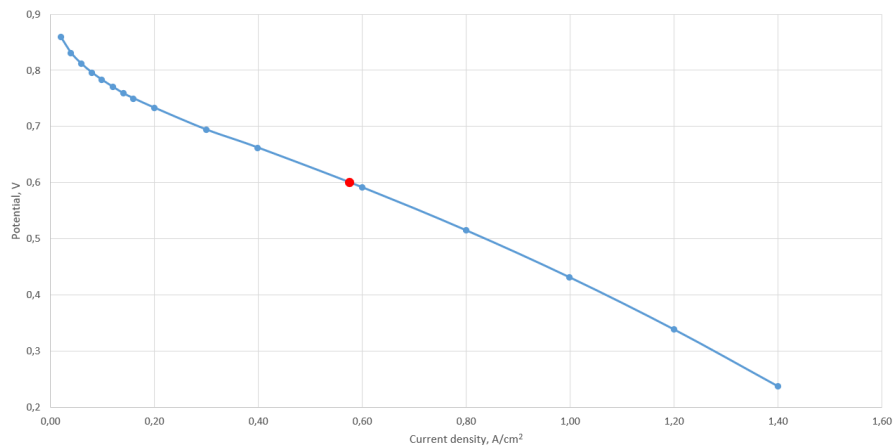
$$P_{PEMFC} = 111.69 \approx 120 \text{ W} \quad (12)$$

As this system has a 24 V battery pack, an interesting component to consider in the PEMFC system is a DC-DC converter. A single-cell PEMFC has a lower potential than the battery pack; in our case, the load is 0.6 V.

To measure the performance of the PEMFC stack, we will approximate the results with existing data from Penga (2022). The polarisation curve of the analysed configuration is shown in Figure 13.

Figure 13

Polarisation curve for the experimentally tested fuel cell.



Source: Penga (2022)

As shown in the polarisation curve in Figure 13, the planned working load is indicated by the red dot. The dot indicates that the current density is 0.576 A/cm² at a potential of 0.6 V. To deliver 120 W, we need to calculate the number of cells and the active area per cell required.

If we want to reach the required potential with the stack, we need to have:

$$n_{PEMFC} = \frac{24}{0.6} = 40 \quad (13)$$

As 40 single cells is a considerable amount (especially as the required current of 3 A in total wouldn't require a large active area), the approach is to reduce the potential to 12 V and implement 20 single cells, which will bring 12 V with a DC-DC converter to step up the voltage to 24 V.

To calculate the active area, we use the following equation:

$$A = \frac{I_{tot}}{I_{spec}} \quad (14)$$

Where I_{tot} represents total current and I_{spec} represents the current density on the working load.

With a 12 V working potential, we require 10 A to achieve the required power of 120 W.

In that case, the active area of every single cell in the PEMFC stack is as follows:

$$A = \frac{10}{0.57} = 17.54 \text{ cm}^2 \approx 20 \text{ cm}^2 \quad (15)$$

The chosen active area is higher to round up and add additional energy overhead. The final PEMFC stack consists of 20 single cells, each with an active area of 20 cm². The commercially available stack with similar power is shown in Figure 14.

Figure 14

PEMFC stack with 200 W of output power for unmanned aerial vehicles.



Source: Fuel Cell Store (2025)

The operating efficiency of the chosen PEMFC stack is:

$$\eta_{PEMFC} = \frac{U_{work}}{U_{OCV}} \quad (16)$$

Where the U_{work} represents the potential of the working load for a single cell, and U_{OCV} represent the open circuit potential (maximal theoretical potential) for a single cell. Because

the theoretical open-circuit potential is 1.23 V and the working potential is 0.6 V, the efficiency of such a system is approximately 50%.

The last part to calculate is the fuel capacity, along with a comparison between the battery and the hydrogen-powered REMUS 100. Because there was no official data on the battery package area, similar systems were used for comparison of energy density. The energy density of the Li-ion battery system ranges from 300 to 600 Wh/L (Ufine, 2025), decreasing to 210 to 420 Wh/L when unusable void space is accounted for, assuming an additional 30% volume around the battery package. Unlike batteries, hydrogen can vary its energy density by being pressurised to different levels. The normal pressure of the hydrogen in systems like REMUS 100 ranges from 350 to 700 bar. This means that the energy density of pressurised hydrogen can range from 700 to 900 Wh/L at 350 bar and from 1300 to 1400 mW/L at 700 bar (Damaco, 2025). The downside of the PEMFC system is that it requires hydrogen and oxygen tanks to operate. The benefit of the tanks is their cylindrical shape, which can potentially improve energy storage efficiency in a system such as the REMUS 100, which also has cylindrical geometry and therefore helps fully utilise the tanks' available storage. An example of a hydrogen tank is shown in Figure 15. Additional components that are required to sufficiently operate the PEMFC can be also optimised to reduce required space and increase the utilisation of the required equipment to power the PEMFC and, lastly, efficiency of such a system is 50%, which means that the effective power of the hydrogen drops to 350 to 450 Wh/L for 350 bar and 650 to 700 Wh/L for 700 bar.

Figure 15

Carbon-hydrogen tank for a pressure of 350 bar.



Note. Source: Hyfindr (2025).

If we add an oxygen tank, the energy density is split in half, bringing us to a realistic range of 325-350 Wh/L.

The energy density of the PEMFC system is stable, whereas that of the battery fluctuates significantly. The energy density comparison between the PEMFC and battery systems shows an increase of more than 50% in favour of the PEMFCs, even when using the lowest energy density. At the very optimistic, highest energy-density of 420 Wh/L, the battery system would exceed the PEMFC system; such values are rarely achievable in practice. More realistic energy densities for batteries used in AUVs are in the range of 220-300 Wh/L, with roughly 350 Wh/L achievable only through highly optimised battery systems. Under realistic assumptions, PEMFC already offers an advantage in energy density at this stage of development.

With respect to safety, the hydrogen and oxidant are stored in closed, pressure-rated tanks and piping, so there is no direct contact between the reactant gases and the surrounding seawater under normal or flooded-hull conditions. In the event of seawater ingress into the vehicle, the presence of sealed tanks means that the reactants themselves do not introduce additional environmental contamination hazards, and any potential safety risk is limited to controlled pressure-relief and venting strategies rather than uncontrolled mixing with water. Nevertheless, detailed failure-mode analysis, leak detection, and vent routing are beyond the scope of the present system-level study and are assumed to follow established marine and hydrogen safety standards.

CONCLUSION

In this study, a three-dimensional RANS CFD model of the REMUS 100 hull with all relevant appendages and a Wageningen B 3.35 propeller was developed to quantify drag, thrust, and torque at a representative cruise speed of 2 m/s, yielding a total drag of 19 N and a required propulsive power of approximately 90.7 W. These hydrodynamic results were then used to derive the electrical power demand and to compare a baseline lithium-ion battery system (1 kWh nominal capacity) with a PEMFC-based energy system sized for equivalent power. Realistic assumptions regarding component efficiency and volumetric energy density have been used. The PEMFC configuration has the potential to increase usable energy by more than 50% compared to the existing battery pack, thereby significantly increasing the endurance of AUV systems with the shift from battery power to PEMFCs.

The combination of CFD simulation and energy-system modelling provides a useful framework for high-accuracy performance predictions and highlights critical hydrodynamic areas, such as increased drag, propeller behaviour, and detailed flow around the hull, at only a fraction of the cost of experimental testing. This is particularly valuable when efficient and quiet operation is required, since the propeller geometry can be modified locally to reduce cavitation risk and, consequently, the acoustic signature. Regarding the PEMFC system, the present analysis shows that such an architecture offers a more stable and predictable volumetric energy density compared to the battery system, can remain inactive for long periods with limited self-discharge, and tends to exhibit increasing energy-density advantages as vehicle size (and thus available storage volume) increases.

In the current design, the PEMFC system achieves a stable volumetric energy density of 325-350 Wh/L. This already represents an improvement over the realistically packed AUV battery systems, even with a conservatively modelled PEMFC configuration. If this technology advances in autonomous underwater vehicles, such as the REMUS 100, customised storage could be designed to significantly reduce unused interior volume. Reactant tanks could be more tightly integrated with other subsystems or even placed outside the pressure hull, since they don't require insulation from seawater, which could reduce the volume required inside the hull, provided that structural, buoyancy, and safety constraints are taken into consideration. The overall energy density of a PEMFC system largely depends on tank pressure and storage configuration, and could be further increased with optimisation of tank construction and placement for the REMUS 100 hull. In addition, the broader PEMFC field offers alternative liquid fuels, such as formic acid, that combine high energy density with more effective utilisation of available tank volume in AUVs

The main limitations of the present approach are that the results still require experimental hydrodynamic validation and that the PEMFC model doesn't account for detailed stack dynamics or the influence of confined spaces on performance. Further work should therefore focus on experimental validation of the CFD-based hydrodynamics simulation, testing of the PEMFC system under realistic AUV operational cycles and more detailed studies of system integration with the focus on the PEMFC kinetics, thermal management, generated water during the current production, together with the fuel storage and safety measurements for such a system.

ACKNOWLEDGEMENTS

The authors of this paper would like to acknowledge financial support from the projects STIM-REI 2.0 PK.1.1.10.0005 and ATASYS IP-UNIST-06.

REFERENCES

- AMC Search. (2025). Technical specifications REMUS 100. *AMC Search*. Retrieved January 28, 2026, from <https://www.amcsearch.com.au/source-assets/images/REMUS-100.pdf>
- Damaco. (2025). The energy density of hydrogen: A unique property. *Demaco Cryogenics*. Retrieved January 29, 2026, from <https://demaco-cryogenics.com/blog/energy-density-of-hydrogen/>
- Deutsch, C., Thuné, S., Terán Espinoza, A., & Kutteneuler, J. (2022). *Fuel cells in practice: Challenges and benefits for AUVs*. In OCEANS 2022 (pp. 1–6), Chennai, India, February 21–24, 2022. <https://kth.diva-portal.org/smash/record.jsf?pid=diva2%3A1658702&dsid=2682>
- Fuel Cell Store. (2025). PEM fuel cells for drones, UAVs, and robotics. *Fuel Cell Store*. Retrieved January 29, 2026, from <https://www.fuelcellstore.com/fuel-cell-stacks/uav-fuel-cell-stacks>
- Garrido Pellicer, A. (2015). *Estimación de los coeficientes hidrodinámicos de vehículos autónomos submarinos mediante CFD* [Master's thesis, Universitat Politècnica de Catalunya]. <http://hdl.handle.net/10317/4657>
- HII. (2025). REMUS 100E specifications. *HII – Hydroid*. Retrieved January 29, 2026, from https://hii.com/wp-content/uploads/2023/03/REMUS-100E-3-31-22_web.pdf
- Hyfindr. (2025). Type III carbon fiber cylinders 3.5 L. *Hyfindr*. Retrieved January 29, 2026, from <https://hyfindr.com/en/shop/products/spectronik-accessories-carbon-fiber-cylinders-3-5l>
- Menter, F. R. (1994). Two-equation eddy-viscosity turbulence models for engineering applications. *AIAA Journal*, 32(8), 1598–1605. <https://doi.org/10.2514/3.12149>
- Penga, J. (2022). *Modeliranje i eksperimentalno ispitivanje svežnja gorivnog članka za primjenu u brodskom energetsom sustavu* [Master's thesis, Sveučilište u Splitu, Fakultet elektrotehnike, strojarstva i brodogradnje]. <https://urn.nsk.hr/urn:nbn:hr:179:515519>
- Safari, F., Rafeeyan, M., & Danesh, M. (2022). Estimation of hydrodynamic coefficients and simplification of the depth model of an AUV using CFD and sensitivity analysis. *Ocean Engineering*, 263, 112369. <https://doi.org/10.1016/j.oceaneng.2022.112369>
- Sakaki, A., & Kerdabadi, M. S. (2020). Experimental and numerical determination of the hydrodynamic coefficients of an autonomous underwater vehicle. *Scientific Journals of the Maritime University of Szczecin*, 62(134), 124–135. <https://doi.org/10.17402/427>

- Ufine (2025). What Is the Energy Density of a Lithium-Ion Battery? *Ufine Battery*.
<https://www.ufinebattery.com/blog/what-is-the-energy-density-of-a-lithium-ion-battery/>
- Xu, Y., Shi, W., Song, Y., & Hou, H. (2024). Hydrodynamics of a Remora-inspired autonomous underwater vehicle approaching and docking to a benchmark submarine. *Ocean Engineering*, 291, 116447. <https://doi.org/10.1016/j.oceaneng.2023.116447>

AERODYNAMIC AND THERMAL CFD MODELING FOR PERFORMANCE ENHANCEMENT OF A PEM FUEL CELL POWER SYSTEM FOR UAVS

Željko Penga¹, Bruno Ševo¹, Jure Penga², Ena Sarajlić², Luka Mihanović²

¹ University of Split, Faculty of Electrical Engineering, Mechanical Engineering and Naval Architecture, R. Boškovića 32, 21000 Split, Croatia

E-Mail: zeljko.penga@fesb.hr, bruno.sevo.00@fesb.hr

ORCID: <https://orcid.org/0000-0001-7331-9432> (Željko Penga), <https://orcid.org/0009-0006-3456-7373> (Bruno Ševo)

² Dr. Franjo Tuđman Defence and Security University, Zrinsko-Frankopanska 207 a, 21000 Split, Croatia

E-mail: jure.penga@sois-ft.hr, ena.sarajlic@sois-ft.hr, luka.mihanovic@sois-ft.hr

ORCID: <https://orcid.org/0009-0007-6608-5798> (Jure Penga), <https://orcid.org/0009-0004-1646-4210> (Ena Sarajlić), <https://orcid.org/0000-0001-6082-4835> (Luka Mihanović)

Abstract

The use of proton exchange membrane fuel cells (PEMFCs) in unmanned aerial vehicles (UAVs) requires careful consideration, as their integration can significantly affect aerodynamic behaviour and heat generation. The objective of this research project was to develop a computational fluid dynamics (CFD) model that incorporates aerodynamic and thermal analyses of a UAV with an integrated PEMFC power system. To develop the CFD model, a computer-aided design (CAD) model similar to Northrop Grumman X-47B UAV, with a wingspan of 0.75 m, was created, featuring an internal compartment to accommodate a 100 W PEMFC stack. As the UAV's original airfoil was unavailable, aerodynamic performance was evaluated for a symmetric wing airfoil and a modified NACA 6409 airfoil, with and without the PEMFC stack, at angles of attack of 0° and 5°. A thermal analysis of the UAV was also completed using a CFD model. In the thermal analysis, the PEMFC stack was modelled as a porous zone with volumetric heat generation representative of real-world operating conditions.

The thermal analysis revealed a significant increase in the temperature of the airflow passing through the PEMFC stack from the inlet to the outlet. The temperature increase varied throughout the flow region, depending upon the position within the flow field and the amount of heat generated at that location. It appears that if the geometry of the flow field and coolant channels is properly dimensioned, this temperature variation could enhance fuel cell performance. Overall, the results indicate that it should be possible to integrate PEMFC

systems into UAV platforms while maintaining favourable aerodynamic and thermal characteristics.

Keywords: Unmanned Aerial Vehicles (UAVs); Proton Exchange Membrane Fuel Cells (PEMFCs); Aerodynamic Analysis; Thermal Management Analysis; Computational Fluid Dynamics (CFD)

INTRODUCTION

A significant advantage of the presented hybrid architecture over conventional battery-only configurations is the ability to use a high-specific-energy fuel cell to extend the UAV's flight time. Fuel cells have been considered for use in aviation because they do not produce noise, vibrations, or high thermal signatures associated with combustion engines and can potentially increase the endurance of electric or hybrid platforms (Pan et al., 2019; Rostami et al., 2022; González-Espasandin et al., 2014).

Flying-wing configurations, particularly those with demonstrator layouts similar to the Northrop Grumman X-47B, may serve as ideal prototypes for integrating advanced power systems into stealth-oriented wings and blended-wing body configurations (Palmer et al., 2006). These platforms exhibit favourable lift-to-drag ratios and low radar cross-sections when properly optimised and therefore make good templates for designing derivative versions at various scales (Palmer et al., 2006). In this investigation, a 0.75 m-wingspan UAV, similar to the Northrop Grumman X-47B, will be used as a testbed to assess the impact of internal hybrid-power integration on aerodynamic performance and energy demand at a small scale.

At the scale of the present investigation, the Reynolds number effect, the internal volume constraint, and geometric details, such as fuselage openings for intake and exhaust, are critical issues; therefore, aerodynamics and system integration must be treated in a tightly coupled manner (Palmer et al., 2006). To characterise the scaled configuration, the external flow will be simulated using Computational Fluid Dynamics (CFD) with ANSYS Fluent to predict lift and drag at a nominal cruise speed of 25 m/s, as well as under other operating conditions.

For the initial configuration, with a symmetric wing cross-section, the computed lift at a freestream velocity of 25 m/s was very low. To achieve lift levels suitable for practical operation, a second configuration employing a NACA 6409 airfoil was investigated. This revised design exhibited a substantial increase in lift under the same operating conditions compared with the reference geometry. These results demonstrate that appropriate airfoil selection and planform shaping can significantly enhance the wing's aerodynamic performance relative to the original design, while also providing additional flexibility for internal integration.

Once the aerodynamic baseline has been determined, the PEMFC stack is installed in the UAV's longitudinal cavity to ensure adequate airflow for oxygen supply and heat removal (Palmer et al., 2006; Rostami et al., 2022).

Concurrently with the aerodynamic evaluation, the investigation identifies the limitation of flight time in large-scale UAVs and proposes a hybrid power system comprising an open-cathode PEM fuel cell stack and a smaller lithium-ion battery. The lift and drag data obtained from external-flow CFD simulations are used to determine the power requirements for each flight regime, thereby establishing the required performance of the hybrid power source (Depcik et al., 2020).

A PEM stack with a nominal power output of 100 W and a maximum power output of up to 120 W is selected as the primary long-duration energy source, while the battery serves as a buffer to absorb transient spikes in energy demand during take-off, aggressive manoeuvres, or payload transients (Pan et al., 2019; Rostami et al., 2022). With this division, the battery size and mass are substantially reduced, thereby relaxing the mass and volume constraints that generally limit the endurance of battery-centric designs (Depcik et al., 2020; González-Espasandin et al., 2014).

To quantify interactions between the power system and the airframe, detailed CFD of the internal fuselage flow is conducted in addition to external-flow simulations. In the internal simulation, the PEMFC stack is modelled as a porous region with a specified pressure drop and a volumetric heat source to represent electrochemical heat generation. Thus, simultaneous assessment of oxygen availability, cooling efficiency, and the aerodynamic impact of ducts and embedded equipment is possible.

By comparing the initial and optimised geometries with and without the integrated stack, the analysis provides a systematic overview of the trade-offs between propulsion-system integration and aerodynamic performance (Rostami et al., 2022; Pan et al., 2019).

1. UAV CAD MODELS

Geometry

The geometry of the UAV, similar to the Northrop Grumman X-47B UAV, was downloaded as STL data from the internet and then reverse-engineered into a STEP file. As shown in Figure 1, the STEP file has been modified internally to add a longitudinal bore through the UAV's body, extending from the front to the rear, to accommodate a 100 W PEM fuel cell stack within the airframe. The selected fuel cell stack was the G-HFCS-100W12V from Fuel Cell Store. The external dimensions were changed to match the UAV geometry while maintaining the same volume as the original PEM fuel cell stack.

Figure 1

(a) Isometric view of the Northrop Grumman X-47B UAV STL file, (b) isometric view of the Northrop Grumman X-47B UAV STEP file, (c) isometric view of the Northrop Grumman X-47B UAV STL and STEP file for comparison, (d) front view of the Northrop Grumman X-47B UAV STL and STEP file for comparison

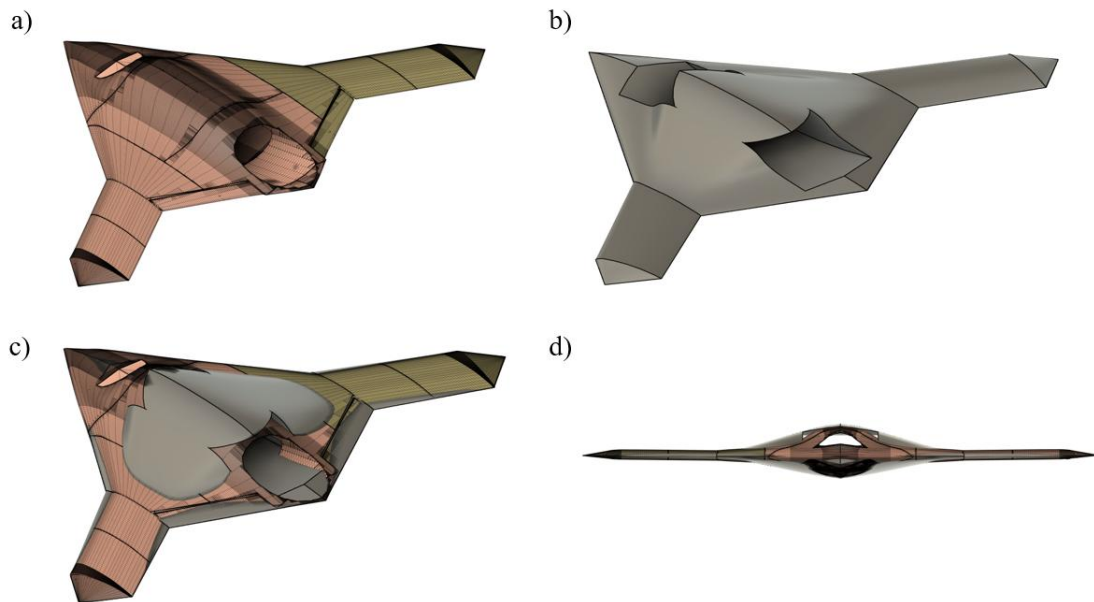
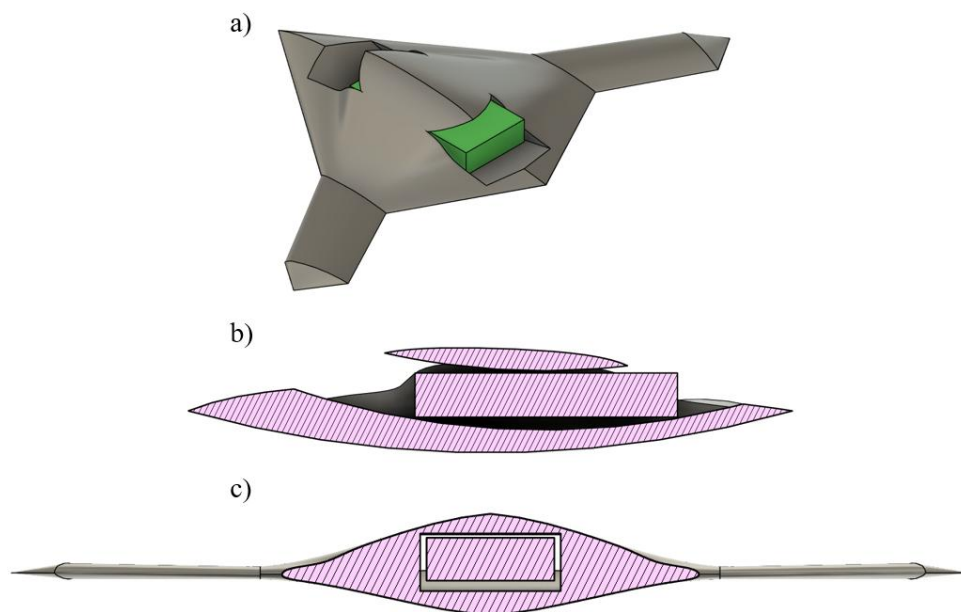


Figure 2

(a) Isometric, (b) side cross-sectional, and (c) frontal section views of the Northrop Grumman X-47B UAV. The integrated PEM fuel cell stack is represented by the green bounding box in each orientation



In

Figure 2, the green box represents a PEM fuel cell stack with the same volume as the G-HFCS-100W12V model from Fuel Cell Store. From the views presented, it is evident that this type of PEM fuel cell stack can be accommodated within the UAV's internal space.

Regarding the UAV wing cross-section, the initial geometry used a symmetrical airfoil. To improve lift performance, a NACA 6409 airfoil with a 9% thickness-to-chord ratio was used. In the following section, a CFD analysis of the UAV using both the original symmetrical airfoil and the NACA 6409 cross-section is presented and discussed.

Figure 3

Cross-sectional view of the symmetrical wing (left) and the modified wing with a NACA 6409 (9%) airfoil profile (right).



COMPUTATIONAL FLUID DYNAMIC ANALYSIS

The UAV geometry was imported into DesignModeler™, where a computational fluid domain was established around the UAV (with or without the PEMFC stack).

Boundary conditions

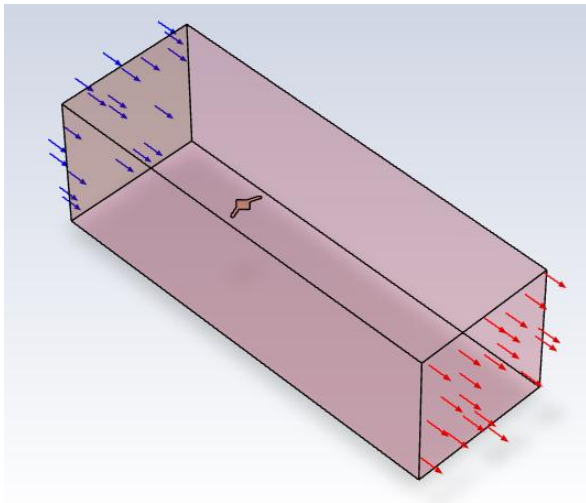
The boundary conditions for the computational domain were defined by specifying a velocity inlet on the front-left face (blue arrows on Figure 4) and a pressure outlet on the rear-right face (red arrows on Figure 4). All other faces were specified as walls. A uniform inlet velocity of 25 m/s was imposed. To establish a baseline, simulations were first performed for both UAV configurations without the PEMFC stack at angles of attack of 0° and 5°. For the UAV equipped with a PEMFC stack, simulations were performed at an angle of attack of 5° for two cases: one using the original geometry and the other using a modified wing geometry. The PEMFC stack was modelled as a porous zone with porosity 0.5, while graphite material properties were assigned to the solid parts of the stack. Considering a PEMFC power output of 100 W and an assumed operating efficiency of 50%, the corresponding heat output was estimated at approximately 100 W. Accordingly, a volumetric heat source of 149 253 W/m³ was applied to the PEMFC stack, based on a total stack volume of 6.7 x 10⁻⁴ m³.

Uniform volumetric heating is justified for a properly designed fuel cell flow field, where the current density is uniformly distributed across the entire active area. This ensures that reaction and Joule heating are also uniformly distributed. Using a dynamic heat source and a variable-wing design with flaps would require transient simulations, which are not relevant at this stage.

The current design focuses solely on determining lift and drag forces for a fixed fuselage geometry to confirm that the UAV can generate sufficient lift to support the mass of the aircraft, fuel cell stack, and auxiliaries. The simulations were initialised with a uniform temperature of 293 K. The computational domain measures 11.7 m in length, 3.8 m in height, and 4 m in width. The upstream section extends 3.75 m, and the downstream section 7.95 m, both exceeding the recommended values reported in the literature. The UAV is positioned at the centre of the domain in terms of both width and height.

Figure 4

Geometry of the computational fluid domain with defined inlet and outlet



Mesh

Due to the highly complex geometry, the mesh was generated using Fluent Meshing with poly-hexcore cells. Each mesh consists of approximately 5.6 million elements, with a minimum orthogonal quality of 0.15 and a maximum skewness of 0.7. Local face sizing was applied to the UAV surfaces, with a maximum element size of 1 mm. In addition, a local refinement box was created around the UAV with a maximum mesh size of 10 mm. To accurately capture near-wall physics, a 10-layer boundary layer was added around the UAV, with a first-layer thickness of 1 mm. For meshes that include the box representing the PEMFC stack, body sizing was applied to the box, with a maximum element size of 1 mm.

Figure 5

Side cross-sectional view of the mesh around the UAV

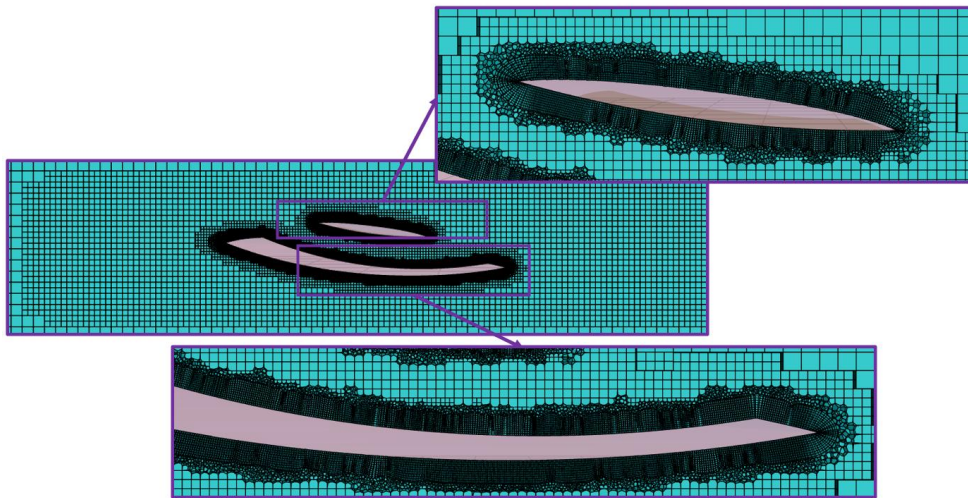


Figure 6

Top cross-sectional view of the mesh around the UAV

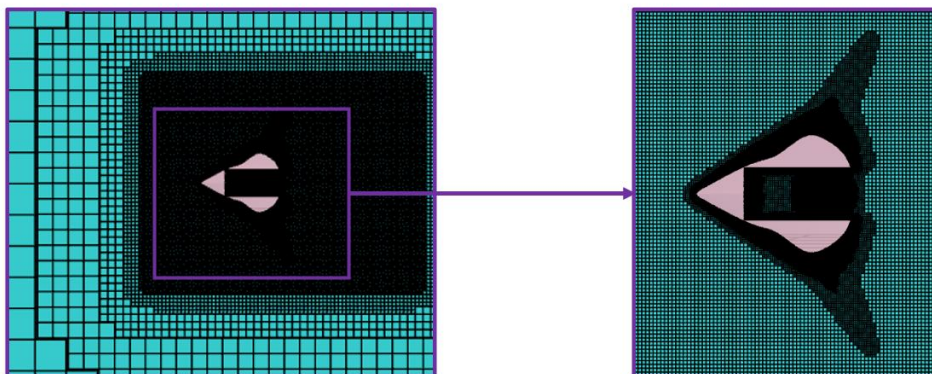
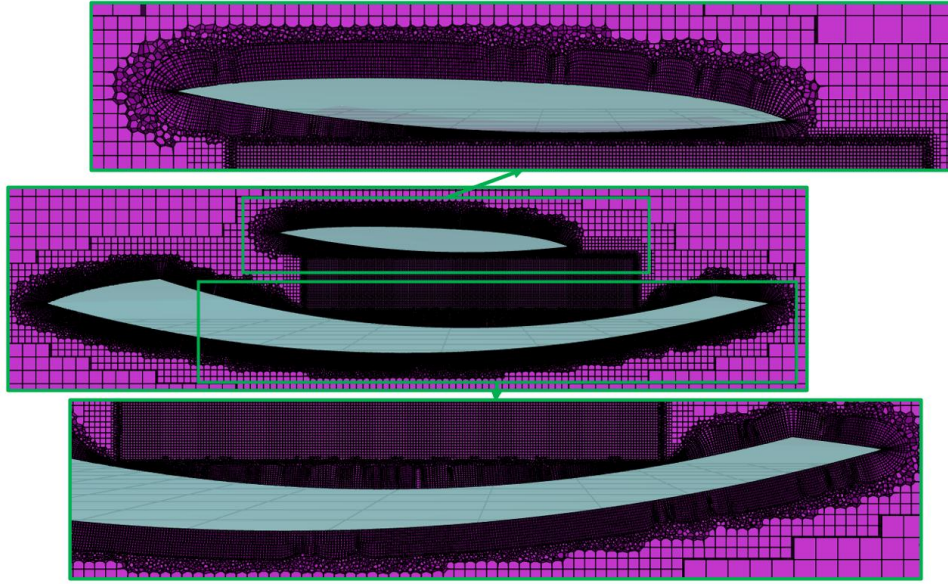


Figure 7

Side cross-sectional view of the mesh around the UAV and the box that represents the PEMFC stack



Governing equations

All simulations and numerical analyses were performed using ANSYS Fluent 2025 R2. Turbulence effects were represented by the standard k - ω empirical model, which is based on model transport equations for the turbulent kinetic energy (k) and the specific dissipation rate (ω) (Wilcox, 1998).

The turbulent kinetic energy, k , and the specific dissipation rate, ω , are obtained from the following transport equations:

$$\frac{\partial(\rho k)}{\partial t} + \frac{\partial(\rho k u_i)}{\partial x_i} = \frac{\partial}{\partial x_j} \left(\Gamma_k \frac{\partial k}{\partial x_j} \right) + G_k - Y_k + S_k + G_b \quad (1)$$

and

$$\frac{\partial(\rho \omega)}{\partial t} + \frac{\partial(\rho \omega u_i)}{\partial x_i} = \frac{\partial}{\partial x_j} \left(\Gamma_\omega \frac{\partial \omega}{\partial x_j} \right) + G_\omega - Y_\omega + S_\omega + G_{\omega b} \quad (2)$$

In these equations, G_k represents the generation of turbulent kinetic energy due to mean velocity gradients. G_ω represents the generation of ω . Γ_k and Γ_ω represent the effective diffusivity of k and ω , respectively. Y_k and Y_ω represent the dissipation of k and ω due to

turbulence. All of the above terms are calculated as described below. S_k and S_ω are user-defined source terms. G_b and $G_{\omega b}$ account for buoyancy terms.

The effective diffusivities for the k - ω model are given by

$$\Gamma_k = \mu + \frac{\mu_t}{\sigma_k} \quad (3)$$

$$\Gamma_\omega = \mu + \frac{\mu_t}{\sigma_\omega} \quad (4)$$

where σ_k and σ_ω are the turbulent Prandtl numbers for k and ω , respectively. The turbulent viscosity, μ_t , is computed by combining k and ω as follows:

$$\mu_t = \alpha^* \frac{\rho k}{\omega} \quad (5)$$

2. RESULTS

The data in Tables 1 and 2 indicate that the modified UAV design utilising the NACA 6409 airfoil with a 9% thickness-to-chord ratio produces greater lift than the original wing design. This improvement is evident in the pressure distributions shown in Figure 8 (0° angle of attack) and Figure 9 (5° angle of attack).

The pressure distribution over the top and bottom surfaces of the original wing design was nearly identical; therefore, very little lift was generated. However, due to the increased pressure differential between the upper and lower surfaces of the modified wing, the modified design produced much greater lift.

Table 1

Values of lift and drag forces for the original geometry

Attack angle	0°	5°
Drag force [N]	1.08	1.5
Lift force [N]	-0.56	12

Table 2

Values of lift and drag forces for the modified geometry

Attack angle	0°	5°
Drag force [N]	1.3	1.97
Lift force [N]	6.8	20

Figure 8

Pressure distribution across the UAV surface and cross-section of the wing for original geometry at 0° attack angle a) and b), and for the modified geometry at 0° attack angle c) and d)

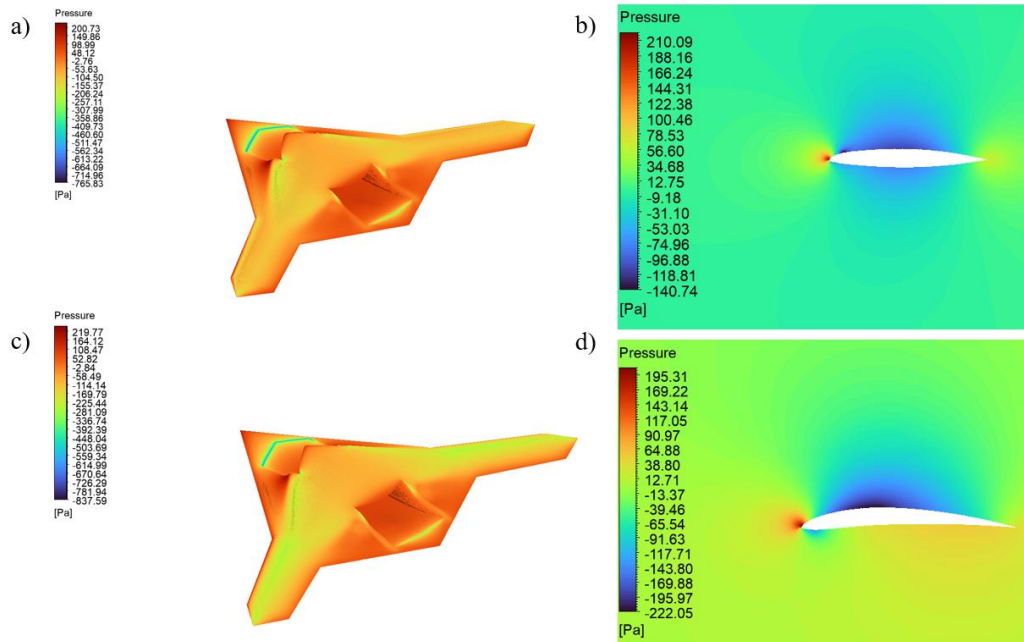
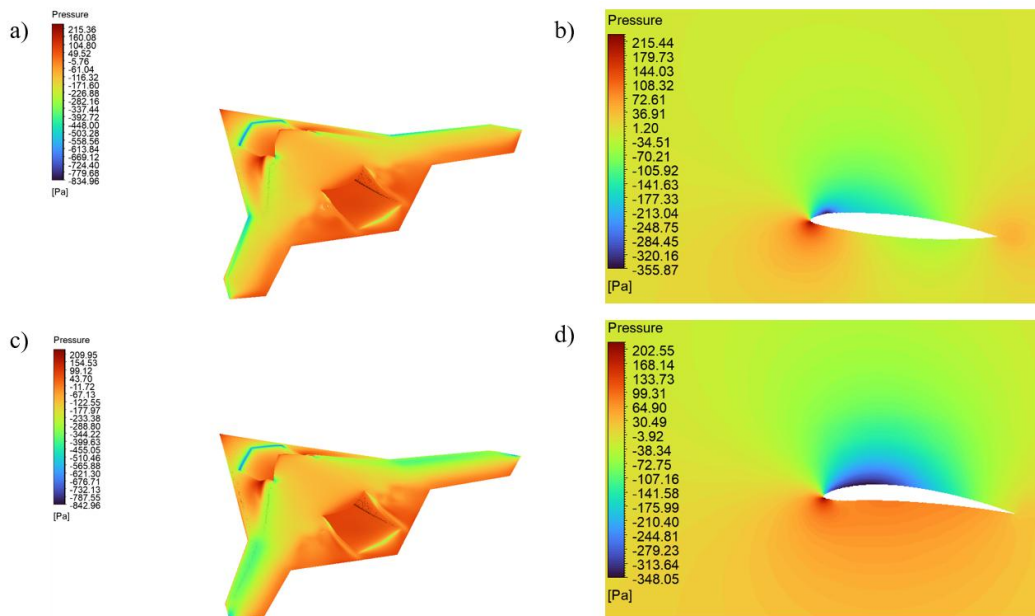


Figure 9

Pressure distribution across the UAV surface and cross-section of the wing for original geometry at 5° attack angle a) and b), and for the modified geometry at 5° attack angle c) and d)



A comparison of Table 3 with Tables 1 and 2 indicates that the inclusion of the PEMFC stack within the UAV hole has only a minor effect on the aerodynamic performance. Specifically, both the lift and drag forces remain largely unchanged after integrating the PEMFC stack into the UAV structure.

Table 3

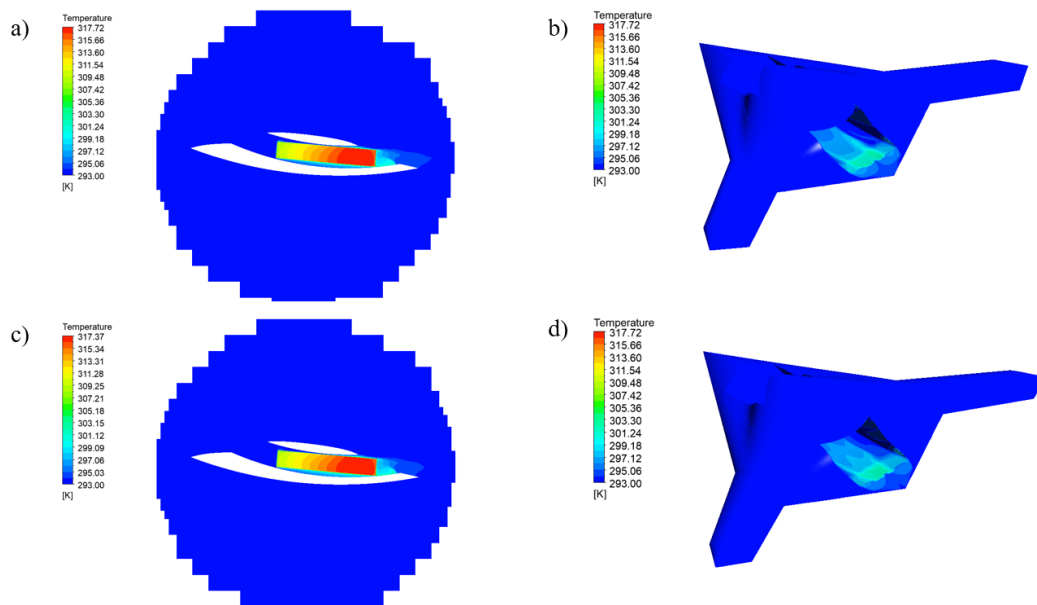
Values of lift and drag forces for both geometries with PEMFC stack at 5° attack angle

	Original Geometry	Modified Geometry
Drag force [N]	1.2738	1.78
Lift force [N]	10.783	19.38

Figure 10 illustrates the progressive heating of the incoming airflow as it passes through the PEMFC stack. While most studies aim to maintain a uniform temperature distribution across the PEMFC active area, recent studies (Penga et al., 2017, 2019) suggest that a variable temperature flow field can enhance PEMFC performance. However, achieving such performance improvements requires careful *optimisation of the flow-field* geometry to maintain 100% relative humidity across the entire active area.

Figure 10

Temperature distribution across the PEMFC stack mid-plane (a) and over the UAV surface (b) for the original geometry, and across the PEMFC stack mid-plane (c) and over the UAV surface (d) for the modified geometry



3. CONCLUSION

This study provides an overall assessment of the aerodynamic and thermal characteristics of a UAV platform incorporating a PEM fuel cell power system, using Computational Fluid Dynamics (CFD). A new internal geometry was developed to support a 100W PEMFC stack, and the aerodynamic characteristics of the UAV were compared for both a symmetric wing airfoil and a modified NACA 6409 airfoil. It was determined that adopting the NACA 6409 airfoil significantly increased lift force compared with the original symmetric wing airfoil design, particularly at low angles of attack. This increase was primarily attributed to larger pressure differences between the upper and lower wing surfaces.

It was also shown that incorporating the PEMFC stack into the UAV airframe had only a minimal effect on the UAV's aerodynamics compared with configurations without the fuel cell system. The presence of the fuel cell did not appear to degrade or otherwise adversely affect the aerodynamic performance of the UAV.

Thermal analysis showed that incoming airflow removed heat from the PEMFC stack, creating a temperature gradient along its active area. In addition, such a non-uniform temperature distribution could provide beneficial effects depending on the optimised geometry of the flow field and coolant channels.

These results demonstrated that PEMFC systems can be successfully integrated into UAVs without degrading their aerodynamic efficiency and can provide adequate thermal management via passive airflow cooling. The future of this work will focus on optimising the internal flow field and coolant channel geometries to enhance humidification across the active area of the PEMFC stack cells, and on expanding the analysis to include coupling with electrochemical performance and variability under flight conditions.

Overall, the results indicate that a carefully engineered combination of airframe optimisation and hybrid power-system integration can mitigate the aerodynamic penalties of fuselage openings and embedded components while realising the endurance benefits of a fuel-cell-based architecture. An improved NACA-based wing demonstrates that sufficient lift can be maintained at 25 m/s even with internal ducts, provided that their size and placement are co-designed with the surrounding flow field. For defence and security missions that demand long-endurance, autonomous operations with low signatures, such a configuration represents a promising step toward more persistent, energy-efficient UAVs compatible with UCAV-derived flying-wing concepts.

ACKNOWLEDGEMENTS

The authors of this paper acknowledge financial support from the projects STIM-REI 2.0 PK.1.1.10.0005 and ATASYS IP-UNIST-06.

REFERENCES

- Depcik, C., Kreutzer, C., Rugh, J., & Rousseau, A. (2020). Comparison of lithium ion batteries, hydrogen fueled proton exchange membrane fuel cells, and free piston engines for small unmanned aerial vehicle power plants. *Energy Conversion and Management*, 211, 112764.
- González-Espasandín, Ó., Leo, T. J., & Navarro-Arregui, M. (2014). Fuel cells: A real option for unmanned aerial vehicles propulsion. *International Journal of Energy Research*, 38(3), 399–413.
- Palmer, M., Gaitonde, A. L., & Holder, D. W. (2006). A comparative study of four UCAV wing layouts. In *25th International Congress of the Aeronautical Sciences (ICAS 2006)* (Paper 020). International Council of the Aeronautical Sciences.
- Pan, Z. F., An, L., & Wei, Z. (2019). Recent advances in fuel cells based propulsion systems for unmanned aerial vehicles. *Applied Energy*, 240, 473–485.
- Penga, Ž., Pivac, I., & Barbir, F. (2017). Experimental validation of variable temperature flow field concept for proton exchange membrane fuel cells. *International Journal of Hydrogen Energy*, 42(41), 26084–26093.
- Penga, Ž., Radica, G., Barbir, F., & Nižetić, S. (2019). Coolant induced variable temperature flow field for improved performance of proton exchange membrane fuel cells. *International Journal of Hydrogen Energy*, 44(20), 10102–10119.
- Rostami, M., Amidpour, M., & Asoodar, M. A. (2022). Introducing and evaluation of a new propulsion system for unmanned aerial vehicles based on fuel cells. *International Journal of Hydrogen Energy*, 47(44), 19078–19093.
- Wilcox, D. C. (1998). *Turbulence modeling for CFD*. DCW Industries, Inc.



www.sois-ft.hr