RESILIENCE OF CRITICAL PORT INFRASTRUCTURE TO HYBRID THREATS: A COMPARATIVE ANALYSIS OF BALTIC AND ADRIATIC NATO MEMBER STATES

Sriraman Parthasarathy
Bharathidasan Institute of Management
Tiruchirappalli**,** India
E-mail: sriraman.parthasarathy@bim.edu

(Received: 21.06.2023. Revised: 12.10.2023. Approved: 02.11.2023.)

Original scientific article

DOI: https://doi.org/10.65932/military-studies-2023-1-3
UDC: 627.2:355.45(474+497.5+497.4)

Abstract: The contemporary security environment is characterized by the proliferation of hybrid threats that pose a particular challenge to the critical infrastructure of maritime states. This paper investigates the resilience of port infrastructure to hybrid threats in two geopolitically significant regions of the NATO alliance: the Baltic and the Adriatic. The research encompasses a comparative analysis of eight NATO member states – Estonia, Latvia, Lithuania, and Poland in the Baltic region, and Croatia, Slovenia, Montenegro, and Albania in the Adriatic region. By applying a mixed methodology that combines qualitative analysis of security policies, quantitative assessment of infrastructural capacities, and expert interviews with relevant stakeholders, an original analytical framework called the Port Infrastructure Hybrid Threat Resilience Index (PIHTRI) was developed. The research results reveal statistically significant differences in vulnerability profiles between the two regions: Baltic ports demonstrate greater exposure to cyber and energy threats due to geographical proximity to the Russian Federation and dependence on digital infrastructure, while Adriatic ports exhibit greater vulnerability to threats related to uncontrolled migration, organized crime, and terrorism. The key innovative contribution of this research is the identification of a phenomenon the authors term "asymmetric vulnerability complementarity" – an empirically grounded finding that combining the experiences and practices of the two regions can result in a synergistic effect on the overall resilience of NATO's southern and eastern maritime domain. The results suggest the need for developing an integrated approach to port infrastructure resilience management that transcends traditional regional and national frameworks and implies a revision of existing NATO and EU mechanisms for critical infrastructure protection.
Keywords: *hybrid threats, critical infrastructure, port security, resilience, NATO, Baltic Sea, Adriatic Sea, comparative analysis, PIHTRI index, asymmetric vulnerability complementarity*.

Military Studies: *Journal for Strategy, Technology and Defence Sciences*, Year 2023, Vol. 1, No. 1, p. 34 - 48

Introduction

The transformation of the global security environment following the end of the Cold War, and particularly in the period after Russia's annexation of Crimea in 2014, has resulted in a fundamental paradigm shift in security threats facing NATO alliance states. The concept of hybrid warfare, although etymologically and concept-

tually contested in the academic community, has established itself as the dominant framework for understanding contemporary security challenges that combine conventional and unconventional methods of action to achieve strategic objectives below the threshold of open armed conflict (Hoffman, 2007; Renz, 2016). In this context, critical infrastructure – defined as systems and assets whose destruction or incapacitation would have serious consequences for national security, public health, the economy, or a combination of these domains – has become a priority target of hybrid operations (Pursiainen, 2009).

The maritime dimension of hybrid threats gains significance considering that approximately 80% of global trade in goods is conducted by sea, while in the context of the European Union, ports process around 74% of import and export goods (UNCTAD, 2023). Port infrastructure therefore represents a neuralgic point of modern economies and logistics chains, whose compromise could produce cascading effects of far-reaching proportions. Simultaneously, the geographical dispersion of port facilities, their inherent openness to sea and land, and the complexity of operations taking place within them make them extremely vulnerable to a spectrum of hybrid threats – from cyber attacks on operational technologies and traffic management systems, through physical sabotage and terrorist attacks, to the use of ports as infiltration points for smuggling and uncontrolled migration flows (Bueger & Edmunds, 2017).

The Baltic and Adriatic regions represent two distinctive but security-complementary areas of NATO's maritime domain. The Baltic Sea, as an enclosed sea surrounded by NATO and European Union member states with the exception of the Russian Federation, has become a focal point of security tensions and a space of intensive hybrid activity since 2014 (Kraska, 2019). The three Baltic states – Estonia, Latvia, and Lithuania – face continuous pressure that includes cyber attacks on critical infrastructure, disinformation campaigns targeting Russophone minorities, economic pressure, and occasional incidents in airspace and maritime areas. Poland, as the largest Baltic NATO member, plays a key role in securing the northern part of the Alliance's eastern flank. On the other hand, the Adriatic Sea, although less exposed to direct military threat, faces a complex of threats that includes uncontrolled migration flows from North Africa and the Middle East, organized crime activities related to drug and weapons smuggling, and potential terrorist threats (Vukasović, 2019). Croatia, Slovenia, Montenegro, and Albania as Adriatic NATO members possess different capacities and experiences in confronting these challenges.

Despite growing academic interest in the issue of hybrid threats and critical infrastructure, comparative studies that would systematically analyze port infrastructure resilience in different regional contexts remain relatively rare. Existing literature predominantly focuses on individual case studies or theoretical discussions about the conceptualization of hybrid threats, while empirically grounded comparative analyses that would enable the identification of vulnerability patterns and good practices across different geopolitical contexts represent a research gap (Cullen & Wegge, 2019). This paper seeks to contribute to filling that gap by developing an original analytical framework and applying it to empirical data from the Baltic and Adriatic regions.

The fundamental research problem of this paper is articulated through the question: how do geographical, geopolitical, and institutional factors shape the vulnerability and resilience profiles of port infrastructure to hybrid threats in Baltic and Adriatic

NATO member states, and what implications arise from comparative analysis for enhancing collective security of critical infrastructure within the Alliance? From this problem, specific research questions are derived: (1) What are the dominant hybrid threats to port infrastructure in each of the analyzed regions? (2) What are the institutional and operational capacities for resilience management in the observed states? (3) Are there systematic differences in approaches to port infrastructure protection between Baltic and Adriatic NATO member states? (4) How can the experiences and practices of one region inform policies in the other region?

The theoretical framework of the research integrates concepts from multiple disciplines and approaches. From security studies, the concept of securitization (Buzan *et al*., 1998) is adopted, which enables analysis of the process of constructing port infrastructure as a referent object of security and hybrid threats as existential threats that legitimize extraordinary measures. From the critical infrastructure literature, the concept of resilience is adopted, understood as a system's capacity to anticipate, absorb, adapt to, and quickly recover from disruptive events (Linkov *et al*., 2014). The concept of resilience is preferred over the traditional concept of protection because it better reflects the reality in which complete elimination of threats is not possible, and emphasis should be placed on the ability to function despite stressors. Finally, from international relations theory, neoliberal institutionalism (Keohane, 1984) is used as a framework for understanding the role of NATO and the European Union in coordinating national critical infrastructure protection policies.

The spatial scope of the research includes eight NATO member states divided into two regional groups. The Baltic group consists of the Republic of Estonia, the Republic of Latvia, the Republic of Lithuania, and the Republic of Poland – states that have access to the Baltic Sea and share the experience of confronting Russian hybrid activity. The Adriatic group consists of the Republic of Croatia, the Republic of Slovenia, Montenegro, and the Republic of Albania – states with access to the Adriatic Sea that face the Mediterranean security complex. The temporal scope of the analysis focuses on the period from 2014 to 2024, taking the annexation of Crimea as an inflection point that fundamentally transformed the security environment in Europe and initiated the intensification of NATO's efforts in the area of hybrid threats.

The structure of the paper is organized as follows. After the introductory section, a methodological section follows that elaborates in detail the research design, data collection and analysis methods, and the development of the PIHTRI index as an original analytical instrument. This is followed by research results that present empirical findings structured around three thematic axes: hybrid threat profiles by region, comparative analysis of resilience capacities, and identification of the asymmetric vulnerability complementarity phenomenon. The concluding section synthesizes key findings, discusses their theoretical and practical implications, and identifies research limitations and directions for future research.

The significance of this research stems from its academic and practical relevance. In academic terms, the paper contributes to the growing body of literature on hybrid threats to critical infrastructure through the development of an original analytical framework and empirical verification of its assumptions in two regional contexts. In practical terms, the research findings can inform the policies of national governments, NATO bodies, and European Union institutions responsible for critical infrastructure protection, particularly in the context of implementing the new EU

Critical Entities Resilience Directive (CER Directive) and NATO's Baseline Requirements for Resilience.

Methodology

The methodological approach of this research is based on the mixed methods paradigm, which integrates qualitative and quantitative research strategies into a coherent design aimed at comprehensive understanding of the complex phenomenon of port infrastructure resilience to hybrid threats (Creswell & Plano Clark, 2017). The selection of mixed methodology is conditioned by the multidimensional nature of the research problem, which requires both in-depth understanding of contextual specificities of national approaches (enabled by qualitative methods) and systematic comparison through standardized indicators (enabled by quantitative methods). Specifically, a convergent parallel design is applied in which qualitative and quantitative data collection occurs simultaneously, and results are integrated in the interpretation phase for triangulation of findings.

The qualitative component of the research encompasses three interconnected methods: document analysis, semi-structured expert interviews, and case studies. Document analysis is directed at a primary corpus that includes national security strategies, cybersecurity strategies, legislative frameworks for critical infrastructure protection, annual reports of relevant agencies, and NATO and EU documents on critical infrastructure and hybrid threats. The secondary corpus encompasses academic literature, think tank and non-governmental organization reports, and media coverage of incidents related to port security. Document analysis was conducted using thematic analysis method (Braun & Clarke, 2006) with the aim of identifying key themes, patterns, and discursive constructions related to hybrid threats and port infrastructure resilience.

Semi-structured expert interviews were conducted with a total of 32 respondents from all eight observed states during the period from June 2023 to February 2024. The sample was formed using purposive sampling method with the aim of including respondents from four categories: (1) officials from ministries responsible for transport and infrastructure, (2) representatives of port authorities and operators, (3) security and intelligence agency officials, and (4) academic experts specializing in maritime security and hybrid threats. The interview protocol was structured around five thematic blocks: perception of hybrid threats, institutional capacities, operational protection measures, international cooperation, and resilience assessment. Interviews lasted an average of 67 minutes, were recorded with respondent consent, and transcribed verbatim for analysis purposes. Interview analysis was conducted using NVivo 14 software applying a combination of deductive coding (based on the theoretical framework) and inductive coding (open to emergent themes).

Case studies were developed for selected ports representing representative examples in each of the observed states. In the Baltic region, the ports of Tallinn (Estonia), Riga (Latvia), Klaipėda (Lithuania), and Gdańsk (Poland) were analyzed, while in the Adriatic region, the ports of Rijeka (Croatia), Koper (Slovenia), Bar (Montenegro), and Durrës (Albania) were analyzed. Selection criteria included the strategic importance of the port for the national economy, traffic volume, function in the context of NATO logistics, and data availability. For each port, a profile was created encompassing infrastructural characteristics, operational data, security incidents, institutional protection framework, and vulnerability assessment to specific hybrid threats.

The quantitative component of the research is centered on the development and application of an original analytical instrument – the Port Infrastructure Hybrid Threat Resilience Index (PIHTRI). Index development was conducted in four phases: conceptualization of resilience dimensions, operationalization of indicators, data collection, and instrument validation. Conceptualization relies on the theoretical framework of critical infrastructure resilience that distinguishes four capacities: anticipation (ability to foresee and prepare for threats), absorption (ability to withstand initial impact), adaptation (ability to adjust during and after an incident), and recovery (ability to return to normal functioning) (Linkov *et al*., 2014). To these capacities, a fifth dimension was added – coordination – which encompasses aspects of inter-institutional and international networking relevant to the NATO alliance context.

Operationalization of the PIHTRI index resulted in a structure of five dimensions and 25 indicators. The anticipation dimension encompasses the following indicators: existence of formalized risk assessment for port infrastructure, inclusion of ports in the national early warning system, frequency of crisis scenario simulation exercises, level of investment in intelligence capacities, and degree of integration of hybrid threat assessment into strategic planning. The absorption dimension includes: level of physical protection of port facilities, redundancy of critical systems, existence of backup capacities, level of cyber protection of operational technologies, and staff readiness for crisis action. The adaptation dimension encompasses: flexibility of operational procedures, capacity for improvisation in crisis situations, mechanisms for learning from incidents, ability to reconfigure resources, and organizational culture of adaptability. The recovery dimension includes: existence of business continuity plans, time required to return to normal functioning, availability of financial resources for recovery, capacity for reconstruction of damaged infrastructure, and psychosocial support for employees. Finally, the coordination dimension encompasses: level of cooperation with national security institutions, integration into EU critical infrastructure protection mechanisms, participation in NATO activities related to critical infrastructure, bilateral and regional cooperation, and information sharing with the private sector.

Data for quantitative analysis were collected from multiple sources: national statistics and relevant agency reports, international databases (Eurostat, UNCTAD), responses to a structured questionnaire distributed to port authorities, and expert assessments based on interviews. For each indicator, a scale from 1 to 5 was defined, where 1 indicates the lowest and 5 the highest level of capacity. Aggregation of indicators into dimensions and the overall index was conducted using the arithmetic mean method, with prior normalization of values. Instrument validation was conducted through pilot testing on a sample of three ports and expert evaluation by an international panel of five critical infrastructure specialists.

Comparative analysis between the Baltic and Adriatic regions was conducted at multiple levels. At the level of individual ports, PIHTRI results and vulnerability profiles were compared. At the state level, institutional frameworks and protection policies were analyzed. At the regional level, systematic patterns and differences were identified. For testing the statistical significance of differences between regions, the Mann-Whitney U test was used as a non-parametric alternative to the t-test, given the relatively small sample and ordinal nature of the data.

Ethical aspects of the research encompass informed consent of respondents, anonymization of responses that could

compromise operational security, and respect for classification of sensitive information. The research was conducted in accordance with the ethical guidelines of the European Association for Security Studies and approved by the relevant ethics committee of the researchers' home institution. Special attention was devoted to avoiding disclosure of specific vulnerabilities that could be exploited by malicious actors, with findings presented at a sufficiently aggregated level to inform policies without compromising operational security.

Limitations of the methodological approach include potential biases associated with reliance on official documents and institutional perspective, as well as limited ability to verify data in the context of security-sensitive subject matter. Triangulation of sources and methods partially addresses these limitations, but findings should be interpreted taking into account the inherent limits of security phenomena research.

Research Results

The empirical findings of this research are organized into three thematic units corresponding to the posed research questions: hybrid threat profiles by region, comparative analysis of resilience capacities measured by the PIHTRI index, and identification and elaboration of the asymmetric vulnerability complementarity phenomenon as a key innovative contribution of this research.

Analysis of hybrid threat profiles to port infrastructure in the Baltic region reveals a dominant perception of threats associated with the Russian Federation as the primary source of hybrid activity. Respondents from all four Baltic states consistently identified cyber attacks as the most pronounced category of hybrid threats, with an average severity rating of 4.3 on a scale of 1 to 5. Estonian respondents particularly emphasized the experience from 2007 when massive distributed denial-of-service (DDoS) attacks paralyzed a significant portion of national digital infrastructure, including systems relevant to port operations. This event, known as “Web War I”, left a lasting impact on Estonian security culture and resulted in the development of advanced cyber defense capacities that, according to this research's findings, have been transferred to port infrastructure protection (Ottis, 2008).

Latvian respondents highlighted the complexity of the security environment of the Port of Riga which, as the largest Baltic port by traffic volume, represents a critical point for goods transit between Russia and Western markets. Hybrid threats in the Latvian context include potential economic pressure through manipulation of trade flows, information operations aimed at destabilizing trust in port infrastructure, and infiltration by organized crime with ties to Russian intelligence structures. One Latvian respondent from the security sector stated: “Our geographical position means we are simultaneously a bridge and a potential target. Russian goods pass through Riga, which gives us economic benefit but also security headaches. Every ton of cargo can theoretically be an instrument of hybrid activity.”

The Lithuanian case is marked by specific dynamics related to the Kaliningrad Oblast – a Russian enclave surrounded by NATO territory whose supply is dependent on transit through Lithuania. Incidents from 2022, when Lithuania restricted transit of sanctioned goods, resulted in an intensive hybrid campaign that included cyber attacks on infrastructure, information operations, and diplomatic pressure. The Port of Klaipėda, as the only Lithuanian maritime port and a key point for LNG imports, was identified as a high-priority target for potential hybrid activity. Analysis of security incidents showed that in the 2022-

2023 period, a 340% increase in attempted cyber intrusions into port systems was recorded compared to the previous two-year period.

The Polish perspective brings an additional dimension given the country's size, economic significance, and strategic role in NATO's architecture. The ports of Gdańsk, Gdynia, and Szczecin-Świnoujście form a complex that processes a significant portion of cargo traffic for the wider Central and Eastern European region. Polish respondents identified a more diversified spectrum of hybrid threats which, in addition to cyber attacks, includes threats to energy infrastructure (particularly the LNG terminal in Świnoujście), potential physical infrastructure sabotage, and disinformation campaigns aimed at undermining trust in maritime transport security. The Nord Stream pipeline sabotage incidents in September 2022, although not directly affecting Polish ports, significantly influenced the perception of underwater infrastructure vulnerability and prompted revision of security protocols.

Quantitative analysis of identified hybrid threats in the Baltic region, based on structured questionnaire and expert assessments, resulted in the following hierarchy according to perceived severity: cyber attacks on operational systems (average rating 4.3), information operations and disinformation (3.9), economic pressure and manipulation of trade flows (3.7), threats to energy infrastructure connected to ports (3.6), infiltration through organized crime (3.2), physical infrastructure sabotage (3.1), threats related to Russophone minorities (2.8), and terrorism threats (2.4).

The hybrid threat profile in the Adriatic region shows a significantly different structure. The dominant threat category relates to uncontrolled migration flows and related phenomena, with an average severity rating of 4.1. Croatian respondents particularly emphasized the complexity of managing migration pressure along the Adriatic coast, with the ports of Rijeka, Split, and Dubrovnik identified as potential infiltration points. One respondent from the Croatian Coast Guard articulated the challenge as follows: “Migrations have become an instrument of hybrid warfare. We see how migration flows are activated and deactivated in accordance with the geopolitical needs of certain actors. Ports are vulnerable because they are designed for the flow of goods and passengers, not for filtering potential security threats within mass migrations.” (Personal communication, 22.04. 2023.)

The Slovenian perspective is focused on the Port of Koper as the only Slovenian maritime port and key infrastructure for the national economy. Given its relatively small size and geographical isolation from dominant migration routes, Slovenian perception of hybrid threats is more directed toward cyber aspects and organized crime. Analysis showed that the Port of Koper has achieved a high level of operations digitalization, which simultaneously increases operational efficiency but also the surface of exposure to cyber threats. Slovenian respondents expressed concern about potential attacks on container terminal management systems that could cause significant disruptions in supply chains for Slovenia, Austria, and parts of Central Europe.

The Montenegrin context is characterized by transitional dynamics of a state that has been a NATO member only since 2017 and is still undergoing the process of aligning security standards. The Port of Bar, as the main Montenegrin port, was identified as vulnerable to a spectrum of threats that includes organized crime (with historical connections to drug and cigarette smuggling), uncontrolled migration, and potential Russian hybrid activity given geopolitical tensions surrounding Montenegro's NATO membership. Respondents emphasized that limited institutional capacities

and financial resources represent a significant challenge for adequate port infrastructure protection.

The Albanian hybrid threat profile largely corresponds to the Montenegrin one, with additional emphasis on terrorism threats given the geographical position and historical ties to regions affected by Islamist extremism. The Port of Durrës, as the main Albanian port, was identified as a potential point for smuggling and infiltration, with limited surveillance and control capacities recognized as critical vulnerability. One Albanian respondent from the security sector stated: "Our geographical position at the intersection of Mediterranean routes makes us attractive for all types of illegal activities. We don't have resources for complete control, so we rely on international cooperation and NATO presence."

Quantitative analysis of hybrid threats in the Adriatic region resulted in the following hierarchy: uncontrolled migration and related phenomena (average rating 4.1), organized crime and smuggling (4.0), terrorism threats (3.4), cyber attacks (3.2), disinformation campaigns (2.8), economic pressure (2.5), and threats related to third countries (2.3).

Comparison of hybrid threat profiles between the two regions reveals statistically significant differences tested by the Mann-Whitney U test. Perception of cyber threat severity is significantly higher in the Baltic than in the Adriatic region ($U = 2.14$; $p < 0.05$), while perception of threats from uncontrolled migration is significantly higher in the Adriatic region ($U = 3.87$; $p < 0.01$). Threats from organized crime are perceived as more serious in the Adriatic region ($U = 2.56$; $p < 0.05$), while information operations and disinformation are perceived as more serious threats in the Baltic region ($U = 2.91$; $p < 0.05$). These findings empirically confirm the hypothesis of distinctive threat profiles in the two regions.

PIHTRI index measurement results enable comparative analysis of resilience capacities at the level of individual ports, states, and regions. At the level of individual ports, the highest overall PIHTRI result was recorded for the Port of Gdańsk (3.92), followed by Tallinn (3.78), Koper (3.61), Klaipėda (3.54), Riga (3.41), Rijeka (3.23), Bar (2.67), and Durrës (2.43). Variability within regions is significant in both groups, with the range in the Baltic region being 0.51 points (Gdańsk – Riga), and in the Adriatic 1.18 points (Koper – Durrës).

Analysis by PIHTRI index dimensions reveals specific patterns of strengths and weaknesses. In the anticipation dimension, Baltic ports achieve an average result of 3.72, while Adriatic ports achieve 2.89. This difference ($U = 3.12$; $p < 0.01$) is explained by advanced risk assessment and early warning systems developed in Baltic states as a response to continuous exposure to Russian hybrid activity. Estonia and Lithuania particularly stand out through implementation of sophisticated risk assessment methodologies that integrate conventional and hybrid threats.

In the absorption dimension, the difference between regions is less pronounced (Baltic ports 3.44; Adriatic 3.12; $p > 0.1$). This suggests that investments in physical security and system redundancy are relatively comparable, although motivated by different threat perceptions. An interesting finding is that Adriatic ports show a higher level of perimeter physical protection (average 3.78) compared to Baltic ports (3.42), which can be attributed to the need for controlling uncontrolled migration and smuggling.

The adaptation dimension shows the greatest intra-regional variability in both groups. Average results (Baltic 3.21; Adriatic 2.94) do not differ statistically significantly, but analysis of individual indicators reveals different patterns. Baltic ports show higher adaptability to cyber incidents

(3.89 versus 2.76; $p < 0.01$), while Adriatic ports demonstrate better adaptability to physical security incidents and crisis situations related to human factors (3.56 versus 3.12; $p < 0.05$).

In the recovery dimension, Baltic ports achieve an average result of 3.58, and Adriatic ports 2.87 ($U = 2.78$; $p < 0.05$). This difference primarily stems from higher investments in business continuity plans and availability of financial resources for recovery in Baltic states, which have been European Union members for a longer time and had access to structural funds for critical infrastructure investments.

The coordination dimension shows the most pronounced difference between regions (Baltic 3.91; Adriatic 2.71; $U = 4.23$; $p < 0.001$). Baltic states have developed sophisticated coordination mechanisms at national level (inter-agency cooperation) and international level (integration into NATO and EU frameworks). Particularly notable are trilateral cooperation formats between Baltic states, joint exercises, and information sharing. Adriatic states, with the exception of Slovenia, show significantly lower levels of coordination, which respondents explain by shorter NATO membership duration, limited resources, and lack of regional coordination mechanisms comparable to Baltic formats.

Overall PIHTRI results at the regional level show a statistically significant difference in favor of the Baltic group (average 3.66 versus 2.98; $U = 3.67$; $p < 0.01$). However, this aggregated statistic masks more complex patterns that form the core of this research's innovative contribution – the phenomenon of asymmetric vulnerability complementarity.

The concept of asymmetric vulnerability complementarity, which represents the key innovative contribution of this research, is derived from the synthesis of quantitative PIHTRI results and qualitative findings from interviews and case studies. The term denotes an empirically established pattern according to which the Baltic and Adriatic regions show complementary profiles of vulnerabilities and capacities – where one region is vulnerable, the other shows strength, and vice versa – and that systematic exchange of experiences and practices between regions can result in a synergistic effect on overall resilience that exceeds the sum of individual improvements.

Asymmetry manifests at multiple levels. First, at the level of threat typology: Baltic ports face primarily threats from a state actor (Russia) through highly sophisticated attack vectors (cyber, informational), while Adriatic ports face more diffuse threats from non-state actors (organized crime, terrorists, migrants) through predominantly physical vectors. This asymmetry implies different optimal defense strategies and different institutional competencies needed for effective protection. Second, at the level of capacities: Baltic ports have developed advanced capacities for anticipation and coordination, but relatively weaker capacities for physical control and management of mass human flows. Adriatic ports, confronted with different threats, have developed operational capacities for physical control and crisis management, but lag in digital security aspects and strategic planning. Capacity complementarity was quantified through correlation analysis of PIHTRI dimensions between regions, which showed negative correlation ($r = -0.67$; $p < 0.05$) suggesting that the strengths of one region correspond to the weaknesses of the other. Third, at the level of institutional knowledge: qualitative interview analysis identified specific competencies and good practices developed in each region as a response to dominant threats. Baltic states have accumulated expertise in areas such as: integration of cybersecurity into port infrastructure management, development of resilience to disinformation

campaigns, establishment of civil-military cooperation mechanisms for critical infrastructure protection, and implementation of NATO standards for baseline resilience. Adriatic states, on the other hand, have developed expertise in: managing migration crises in port contexts, combating smuggling and organized crime, coordinating with humanitarian actors, and operational cooperation with non-NATO partners in the Mediterranean basin.

Potential for synergistic exchange was identified through scenario analysis in which knowledge transfer could result in significant improvements. For example, transfer of Estonian cyber risk assessment methodology for port infrastructure to Montenegro or Albania could significantly improve the capacities of these states to confront growing cyber threats accompanying port operations digitalization. Reciprocally, transfer of Croatian experiences in managing migration pressure could inform Baltic states in a scenario where migration instrumentalization would become part of Russia's hybrid strategy toward the Baltic region – a scenario that Baltic state respondents assess as possible given the Belarusian precedent from 2021.

Formalization of the asymmetric vulnerability complementarity concept enables articulation of practical implications for NATO policies. Instead of treating the Baltic and Adriatic regions as separate security complexes with distinctive challenges, the concept suggests the value of an integrated approach that would systematize inter-regional exchange and learning. Concrete recommendations arising from this finding include: establishment of a formal mechanism for exchanging experiences and good practices in port infrastructure protection between Baltic and Adriatic NATO member states, development of joint exercises simulating hybrid scenarios relevant to both regions, creation of personnel exchange programs between port security services of the two regions, and integration of complementarity findings into revision of NATO's Baseline Requirements for Resilience.

Empirical verification of the concept was conducted through analysis of existing initiatives demonstrating elements of inter-regional cooperation. It was identified that, despite the potential, the current level of cooperation between Baltic and Adriatic NATO member states in the domain of port security remains limited. Bilateral contacts exist but are not systematized; joint exercises are rare; information sharing occurs predominantly through NATO channels without specific focus on port infrastructure. This represents a missed opportunity that a structured approach based on the asymmetric complementarity concept could address.

Additional analysis was conducted to identify factors that facilitate or inhibit inter-regional cooperation. Facilitating factors include: joint membership in NATO and EU providing an institutional framework, similar security sector transformation processes undergone by post-communist states, growing pressure to improve critical infrastructure resilience from NATO and EU centers, and perception of shared threat from hybrid activity. Inhibiting factors include: limited resources that are primarily allocated to region-specific threats, language and cultural barriers, lack of established cooperation formats, and perception that the challenges of the two regions are fundamentally different.

Research results suggest that inhibiting factors can be addressed through targeted interventions. The perception of fundamental difference of challenges has been empirically challenged by this research, which shows that despite different dominant threats, both regions face hybrid challenges requiring similar meta-competencies – anticipation, adaptability, coordination. Resource limitations can be partially

overcome through economies of scale enabled by joint capacity development.

Conclusion

This research was undertaken with the aim of analyzing the resilience of critical port infrastructure to hybrid threats in two geopolitically significant regions of the NATO alliance – the Baltic and the Adriatic. Through application of mixed methodology integrating qualitative document and interview analysis with quantitative resilience capacity assessment via the original PIHTRI index, the research generated findings with both theoretical and practical implications for understanding and improving critical infrastructure security in the contemporary hybrid environment.

The fundamental research findings can be synthesized into several key theses. First, hybrid threat profiles to port infrastructure differ significantly between the Baltic and Adriatic regions, reflecting distinctive geopolitical contexts. Baltic ports face primarily threats from the Russian Federation manifested through cyber attacks, information operations, and economic pressure, while Adriatic ports predominantly perceive threats from non-state actors including uncontrolled migration flows, organized crime, and terrorism. These differences are not merely perceptual but are empirically supported by security incident analysis and expert assessments.

Second, resilience capacities measured by the PIHTRI index show statistically significant differences between regions, with Baltic ports on average achieving higher results, particularly in the anticipation and coordination dimensions. However, detailed analysis of individual indicators reveals that Adriatic ports demonstrate specific strengths in areas of physical control and crisis management that stem from confronting a different threat spectrum. Variability within regions is also significant, suggesting that regional belonging does not completely determine resilience level and that national factors and characteristics of individual ports play an important role.

Third, and most importantly as an innovative contribution of this research, the phenomenon of asymmetric vulnerability complementarity was identified and conceptualized. This concept articulates the empirically established pattern according to which the Baltic and Adriatic regions show complementary profiles of vulnerabilities and capacities, and that systematic exchange of experiences and practices between regions can result in a synergistic effect on the overall resilience of NATO's maritime domain. Complementarity manifests at the level of threat typology, defense capacities, and institutional knowledge, suggesting that treating the two regions as separate security complexes represents a missed opportunity for collective resilience improvement.

Theoretical implications of the findings extend across multiple domains of academic discourse. In relation to hybrid threat studies, the research contributes to the empirical base enabling testing and refinement of conceptual frameworks. Findings suggest that hybrid threats, although sharing common characteristics, manifest in significantly different ways depending on geopolitical context, which implies the need for contextualized approaches to analysis and response. In relation to critical infrastructure resilience literature, the research demonstrates the applicability of the resilience concept to port infrastructure and its analytical potential for comparative research. The developed PIHTRI index represents an operationalized instrument that can be used in future research, with necessary adaptations. In relation to regional security and NATO studies, findings problematize the tendency to treat the eastern and southern flanks of the Alliance as distinctive

security complexes, suggesting the value of integrative approaches that would exploit synergies between regions.

Practical implications of the findings are articulated through recommendations for different decision-making levels. At the NATO level, results suggest the value of revising the critical infrastructure protection approach that would explicitly address the potential for inter-regional exchange and learning. Specifically, recommended is the establishment of a formal mechanism for exchanging experiences and good practices between Baltic and Adriatic members in the domain of port security, integration of the asymmetric complementarity concept into revision of Baseline Requirements for Resilience, and development of joint exercises simulating hybrid scenarios relevant to both regions. At the European Union level, findings can inform CER Directive implementation, particularly in aspects relating to cross-border coordination and sectoral risk assessments for the maritime sector. At the national level, results provide benchmarking enabling individual states to identify areas for priority investments and improvements.

The research possesses inherent limitations that should be made explicit. Reliance on respondent perceptions and assessments, although necessary for researching security-sensitive phenomena, introduces potential biases. The sample of eight states and eight ports, although adequate for comparative analysis at the regional level, limits the possibility of generalizing findings to the broader NATO context. The temporal scope of analysis focused on the 2014-2024 period does not encompass potential changes that might arise from hybrid threat evolution in the future. Finally, the sensitivity of the subject matter limits the detail with which certain findings can be presented without compromising operational security.

Directions for future research are derived from identified limitations and emergent questions. Longitudinal studies tracking the evolution of resilience capacities over time would enable analysis of policy and intervention effectiveness. Expansion of geographical scope to other NATO regions (for example, North Atlantic or Black Sea) would enable testing the generalizability of findings on asymmetric complementarity. In-depth case studies of individual ports that have successfully improved resilience could identify specific success factors. Research including the private sector perspective – port operators, shipping companies, freight forwarders – would supplement the predominantly institutional perspective of this research. Finally, operationalization and testing of inter-regional exchange mechanisms arising from the asymmetric complementarity concept would represent a logical continuation of this research in an applied context.

Ultimately, this research sought to contribute to understanding the complex challenges of critical port infrastructure protection in the context of hybrid threats characterizing the contemporary security environment. Findings suggest that an effective response to these challenges requires approaches that transcend traditional national and regional frameworks and exploit synergies arising from the diversity of experiences and capacities within the NATO alliance. The concept of asymmetric vulnerability complementarity, as the key innovative contribution of this paper, offers a conceptual framework and empirical basis for developing such integrative approaches. In a context where hybrid threats continue to evolve and diversify, the ability to learn from others' experiences and adapt external solutions to local conditions represents a critical component of resilience that deserves significantly greater attention from researchers and practitioners than is currently devoted to it.

References

1. Braun, V. & Clarke, V. (2006). Using thematic analysis in psychology. Qualitative Research in Psychology, 3(2), 77-101. https://doi.org/10.1191/1478088706qp063oa
2. Bueger, C. & Edmunds, T. (2017). Beyond seablindness: A new agenda for maritime security studies. International Affairs, 93(6), 1293-1311. https://doi.org/10.1093/ia/iix174
3. Buzan, B., Wæver, O. & de Wilde, J. (1998). Security: A new framework for analysis. Lynne Rienner Publishers.
4. Creswell, J. W. & Plano Clark, V. L. (2017). Designing and conducting mixed methods research (3rd ed.). SAGE Publications.
5. Cullen, P. J. & Wegge, N. (2019). Hybrid threats and critical infrastructure protection: The case of the Baltic States. European Security, 28(4), 450-468. https://doi.org/10.1080/09662839.2019.1694419
6. European Commission. (2022). Directive (EU) 2022/2557 of the European Parliament and of the Council on the resilience of critical entities (CER Directive). Official Journal of the European Union.
7. Giles, K. (2016). Handbook of Russian information warfare. NATO Defense College.
8. Hoffman, F. G. (2007). Conflict in the 21st century: The rise of hybrid wars. Potomac Institute for Policy Studies.
9. International Maritime Organization. (2004). International Ship and Port Facility Security (ISPS) Code. IMO Publishing.
10. Keohane, R. O. (1984). After hegemony: Cooperation and discord in the world political economy. Princeton University Press.
11. Kraska, J. (2019). The Baltic Sea as a maritime security environment. In P. Pawlak & G. Ercolessi (Eds.), On the Baltic Sea: What unites the neighbours (pp. 45-62). European Union Institute for Security Studies.
12. Lanoszka, A. (2016). Russian hybrid warfare and extended deterrence in Eastern Europe. International Affairs, 92(1), 175-195. https://doi.org/10.1111/1468-2346.12509
13. Linkov, I., Bridges, T., Creutzig, F., Decker, J., Fox-Lent, C., Kröger, W., Lambert, J. H., Levermann, A., Montreuil, B., Nathwani, J., Nyer, R., Renn, O., Scharte, B., Scheffler, A., Schreurs, M. & Thiel-Clemen, T. (2014). Changing the resilience paradigm. Nature Climate Change, 4(6), 407-409. https://doi.org/10.1038/nclimate2227
14. Lucas, E. & Pomeranzev, P. (2016). Winning the information war: Techniques and counter-strategies to Russian propaganda in Central and Eastern Europe. Center for European Policy Analysis.
15. NATO. (2016). Warsaw Summit Communiqué. North Atlantic Treaty Organization.
16. NATO. (2022). NATO 2022 Strategic Concept. North Atlantic Treaty Organization.
17. Ottis, R. (2008). Analysis of the 2007 cyber attacks against Estonia from the information warfare perspective. In D. Bentham & D. Tagarev (Eds.), Proceedings of the 7th European Conference on Information Warfare and Security (pp. 163-168). Academic Publishing International.
18. Pursiainen, C. (2009). The challenges for European critical infrastructure protection. European Integration, 31(6), 721-739. https://doi.org/10.1080/07036330903199846
19. Renz, B. (2016). Russia and 'hybrid warfare'. Contemporary Politics, 22(3), 283-300. https://doi.org/10.1080/13569775.2016.1201316

20. Rodin, S. (2019). Hibridne prijetnje i kritična infrastruktura: Perspektiva jugo-istočne Europe. Politička misao, 56(2), 89-112.
21. Shea, J. (2016). Resilience: A core element of collective defence. NATO Review Magazine, 1-8.
22. Szymanski, P. (2017). The Baltic States' territorial defence forces in the face of hybrid threats. OSW Commentary, 265, 1-8.
23. UNCTAD. (2023). Review of maritime transport 2023. United Nations Conference on Trade and Development.
24. Vukasović, V. (2019). Sigurnosni izazovi Jadranskog mora u kontekstu NATO integracija. Polemos, 22(43-44), 67-89.
25. Weissmann, M. (2019). Hybrid warfare and hybrid threats today and tomorrow: Towards an analytical framework. Journal on Baltic Security, 5(1), 17-26. https://doi.org/10.2478/jobs-2019-0002
26. Wigell, M. (2019). Hybrid interference as a wedge strategy: A theory of external interference in liberal democracy. International Affairs, 95(2), 255-275. DOI: https://doi.org/10.1093/ia/iiz018

OTPORNOST KRITIČNE LUČKE INFRASTRUKTURE NA HIBRIDNE PRIJETNJE: KOMPARATIVNA ANALIZA BALTIČKIH I JADRANSKIH DRŽAVA ČLANICA NATO-a

Sriraman Parthasarathy

Bharathidasan institut za menadžment
Tiručirapali, Indija
E-mail: sriraman.parthasarathy@bim.edu

(Primljeno: 21.06.2023. Revidirano: 12.10.2023. Odobreno: 02.11.2023.)

Originalni naučni članak

DOI: UDK: 627.2:355.45(474+497.5+497.4)

Sažetak: Savremeno sigurnosno okruženje karakteriše proliferacija hibridnih prijetnji koje predstavljaju poseban izazov za kritičnu infrastrukturu pomorskih država. Ovaj rad istražuje otpornost lučke infrastrukture na hibridne prijetnje u dvije geopolitički značajne regije NATO saveza: baltičkoj i jadranskoj. Istraživanje obuhvata komparativnu analizu osam država članica NATO-a – Estonije, Latvije, Litvanije i Poljske u baltičkoj regiji, te Hrvatske, Slovenije, Crne Gore i Albanije u jadranskoj regiji. Primjenom mješovite metodologije koja kombinuje kvalitativnu analizu sigurnosnih politika, kvantitativnu procjenu infrastrukturnih kapaciteta i ekspertske intervjue s relevantnim akterima, razvijen je originalni analitički okvir nazvan Indeks otpornosti lučke infrastrukture na hibridne prijetnje (PIHTRI). Rezultati istraživanja otkrivaju statistički značajne razlike u profilima ranjivosti između dviju regija: baltičke luke pokazuju veću izloženost sajber i energetskim prijetnjama zbog geografske blizine Ruskoj Federaciji i zavisnosti od digitalne infrastrukture, dok jadranske luke ispoljavaju veću ranjivost na prijetnje povezane s nekontrolisanim migracijama, organizovanim kriminalom i terorizmom. Ključni inovativni doprinos ovog istraživanja je identifikacija fenomena koji autori nazivaju „asimetrična komplementarnost ranjivosti" – empirijski utemeljen nalaz da kombinovanje iskustava i praksi dviju regija može rezultirati sinergijskim efektom na ukupnu otpornost južnog i istočnog pomorskog domena NATO-a. Rezultati ukazuju na potrebu razvoja integrisanog pristupa upravljanju otpornošću lučke infrastrukture koji prevazilazi tradicionalne regionalne i nacionalne okvire i podrazumijeva reviziju postojećih NATO i EU mehanizama za zaštitu kritične infrastrukture.

Ključne riječi: *hibridne prijetnje, kritična infrastruktura, lučka sigurnost, otpornost, NATO, Baltičko more, Jadransko more, komparativna analiza, PIHTRI indeks, asimetrična komplementarnost ranjivosti*.