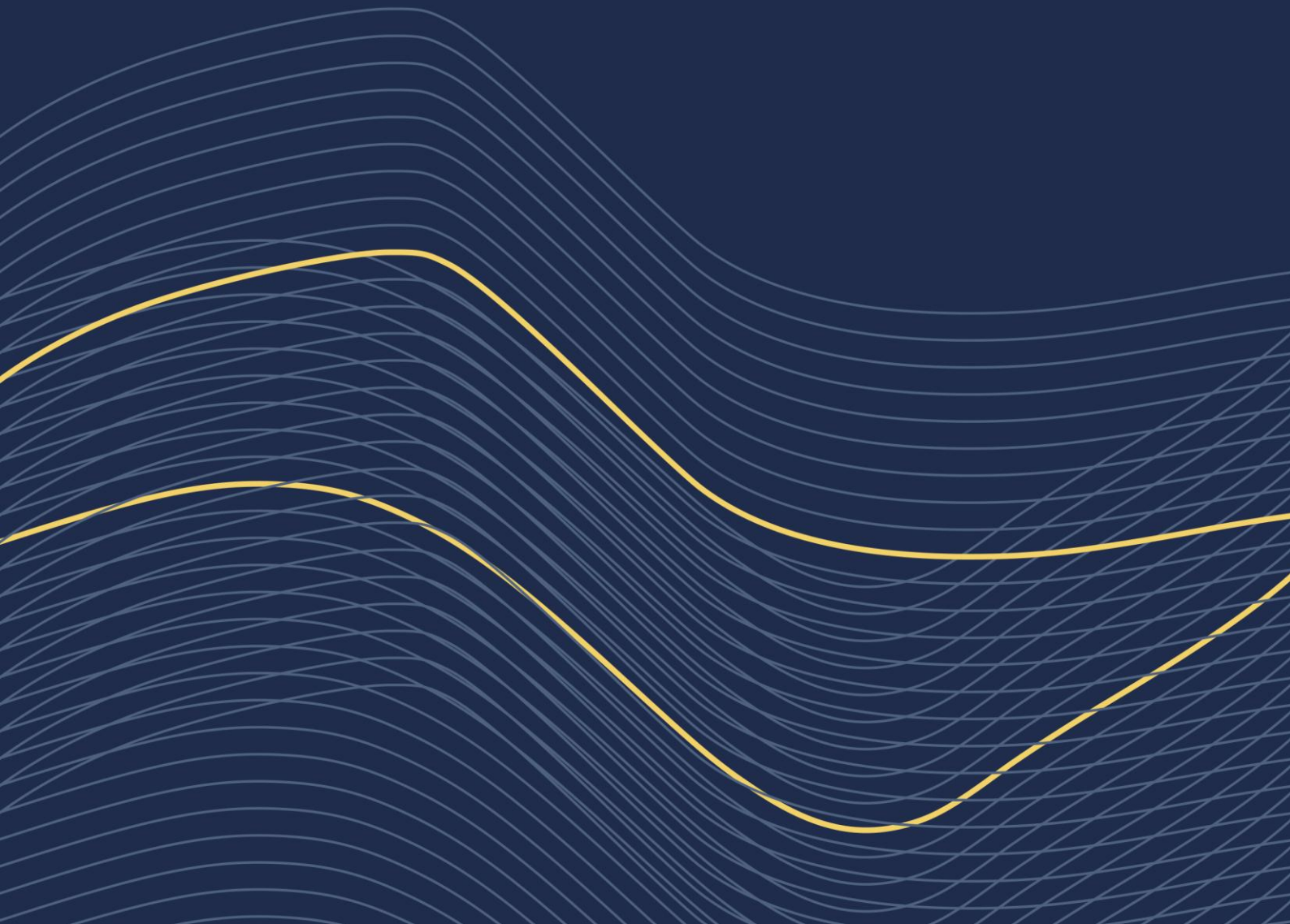
YoPeNET
BALTICNESS

GDAŃSK 2026

YoPeNET Futures

Futures of the Safe & Secure Baltic Sea Region



Authors of the report: Michał Stokowski, Małgorzata Piskórz, Magdalena Muszel

How to cite: Stokowski M., Piskórz M., Muszel M., 2026, YoPeNET Futures. Future of the safe & secure Baltic Sea Region. Fundacja Zatoka – Busola Trends.

The CBSS Summer University 2026 in Gdańsk, Poland is organised by Council of the Baltic Sea States, Zatoka Foundation, Interdisciplinary Centre for Baltic Sea Region Research (IFZO) at the University of Greifswald, University of Gdańsk, Centre for Landscape and Culture at Tallinn University, Busola Trends, European Solidarity Centre, Södertörn University in cooperation with other YoPeNET-Futures project partners.

This publication has been funded by the Council of the Baltic Sea States (CBSS) Project Support Facility (PSF).

The CBSS does not make any warranties with respect to the accuracy or completeness of the information in this publication. The views, findings, interpretations and conclusions expressed in the publication are those of the author(s) and do not necessarily represent the official position of the CBSS.

Copyright: © 2026 Fundacja Zatoka, Busola Trends, Michał Stokowski, Małgorzata Piskórz, Magdalena Muszel

Copyright: © 2026 The Authors

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License (CC BY-NC-ND 4.0). To view a copy of this license, visit https://creativecommons.org/licenses/by-nc-nd/4.0/

ISBN 978-83-975539-0-3

Security is often understood as protection from danger. But in the Baltic Sea Region (BSR), security means much more than the absence of military threat. It is the ability of societies, institutions and communities to remain stable, resilient and connected in a changing world.

Today, security has many dimensions. It is military security, but also energy security, cyber security, economic security, environmental security and social security. It concerns critical infrastructure, supply chains, access to information, trust in public institutions and the health of the sea itself.

The Baltic Sea connects countries, economies and people, but it also connects risks. A disruption in one place can quickly affect the whole region. That is why security should not be seen only as defence, but as a shared capacity to anticipate, cooperate and respond.

For the BSR, the future of security will depend not only on strength, but also on resilience, solidarity and long-term thinking.

LIST OF ABBREVIATIONS 6

HOW TO USE THIS REPORT 7

THEORETICAL FRAMEWORK: SAFETY & SECURITY & RESILIENCE 9

METHODOLOGY 12

Desk research 12

Delphi method 14

Workshops 15

Scenario planning 15

DIRECTIONS OF CHANGE IN SAFETY, SECURITY AND RESILIENCE IN THE BALTIC SEA REGION 17

P. New order of allied and regional coordination 18

M. Militarisation of the Baltic space 20

E. The economy as a tool of security and autonomy 22

S. Rising salience of identity and border control as an axis of domestic and foreign policy 25

I1. Grey-zone operations and infrastructure security in the Baltic Sea Region 28

I2. Information as a tool of pressure and destabilisation 31

FUTURE SCENARIOS 33

Scenario 1: Relying on distant friends 37

Scenario 2: Safety is a business 42

Scenario 3: Pragmatic Resilience 47

Scenario 4: The Baltic Fortress 52

STUDENTS PROJECTS TO ADDRESS CHALLENGES OF THE FUTURE 57

RECOMMENDATIONS & STRATEGIC DILEMMAS 60

LIST OF ABBREVIATIONS

AI – Artificial Intelligence

BRELL – power grid of Belarus, Russia, Estonia, Latvia, and Lithuania

BSR – Baltic Sea Region

CAWI – Computer-Assisted Web Interviewing

CBSS – the Council of the Baltic Sea States

CIS RAM – the Center for Internet Security Risk Assessment Method

EDF – European Defence Fund

EDIP – European Defence Industry Programme

eFP – enhanced Forward Presence

EU – the European Union

EUDIS – European Union Defence Innovation Scheme

EuroHPC – The European High Performance Computing Joint Undertaking

GDP – Gross Domestic Product

GNSS – Global Navigation Satellite System

GPS – Global Positioning System

HELCOM – Helsinki Commission, The Baltic Marine Environment Protection Commission

HPC – high-performance computing

IT – Information Technology

JEF – the Joint Expeditionary Force

LNG – liquefied natural gas

LUMI – Large Unified Modern Infrastructure

NATO – the North Atlantic Treaty Organization

NB8 – Nordic-Baltic Eight

NIST – the National Institute of Standards and Technology

OSW – the Centre of Eastern Studies (Ośrodek Studiów Wschodnich)

PMESII – Political, Military, Economic, Social, Information, Infrastructure

PTS – Swedish Post and Telecom Authority

RCB – Rządowe Centrum Bezpieczeństwa (The Government Centre for Security)

SAFE – Security Action for Europe

SME – Small and Medium-sized Enterprise

DHS – the Department of Homeland Security of the United States

DIANA – Defence Innovation Accelerator for the North Atlantic

UN – the United Nations

US – the United States of America

VUCA – Volatility, Uncertainty, Complexity, and Ambiguity

WTO – The World Trade Organization

HOW TO USE THIS REPORT

The four scenarios describe different conditions in which the Baltic Sea Region may operate by 2035. They are intended to support decisions made today, rather than to identify one future as the most likely. Institutions can use them to examine the assumptions behind their plans, prepare for changes in their operating environment and discuss choices that affect different parts of the region. Three approaches are particularly useful.

The value of these scenarios lies in the decisions they help clarify. Working with them should lead to a clearer understanding of which capabilities the BSR needs under different conditions, which dependencies require attention now and which choices can remain open. The scenarios should be revisited as new events, policies and partnerships change the region's path towards 2035.

1. TEST A STRATEGY AGAINST ALL FOUR SCENARIOS

-Select an institution, policy, investment or area of activity. For each scenario, examine how its responsibilities, resources, partners and operating conditions change.

-Identify which elements of the current strategy remain effective, which require adjustment and which depend on conditions that may no longer hold.

-A port authority, for example, could test its plans against changes in allied military presence, maritime traffic controls, energy infrastructure and access to digital systems.

The result should be a short list of actions that remain useful across several scenarios, alongside decisions that require a different response depending on how the region develops.

2. WORK BACKWARDS FROM 2035

Choose a specific challenge or desired capability, such as the ability to restore a damaged interconnector, maintain essential digital services or coordinate a regional response to an oil spill. Describe what would need to be in place in 2035 for that capability to exist. Then work backwards to identify the investments, agreements, skills and decisions required at earlier stages.

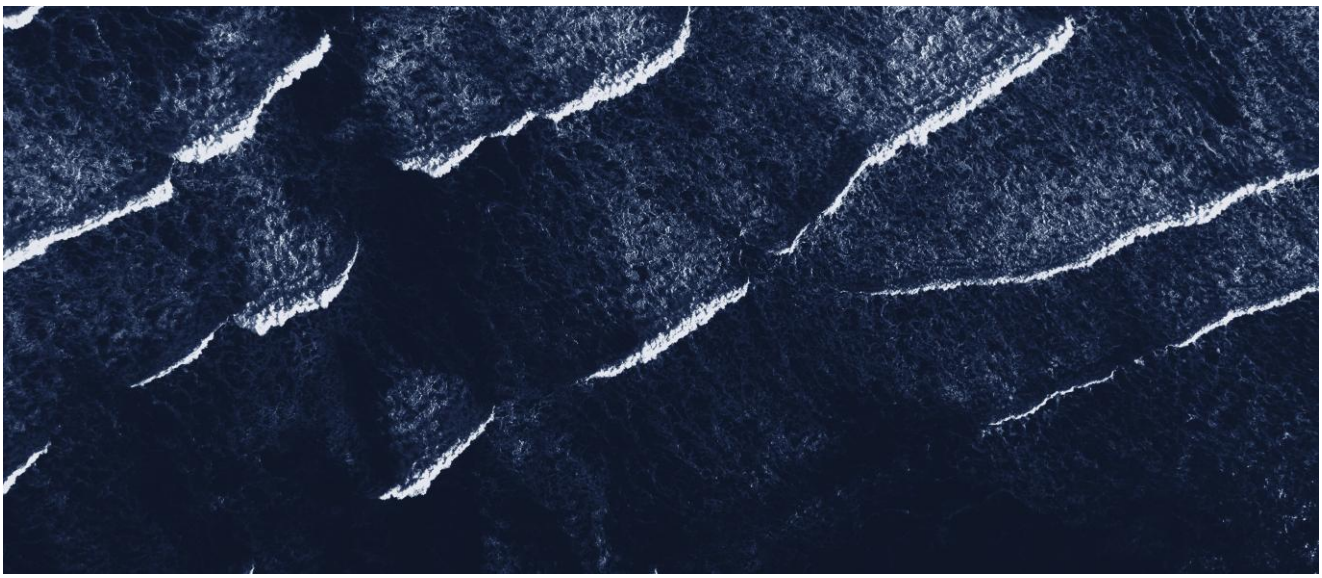
This process helps distinguish actions that can be taken quickly from those that require years of preparation. It is particularly relevant to infrastructure, industrial capacity and institutional cooperation, where delays cannot easily be recovered during a crisis.

3. EXPLORE THE SCENARIOS THROUGH PARTICIPATION

Bring together people affected by a shared challenge: public authorities, infrastructure operators, researchers, businesses, civil society organisations and local communities. Working with one scenario at a time, ask participants how everyday activities and responsibilities change, who gains or loses access to protection, and which consequences are missing from an institutional perspective. Use their findings to develop responses to the opportunities and risks identified.

This approach is valuable when security measures create different consequences for strategic hubs, border areas and peripheral communities. It allows participants to examine whose experience is reflected in a proposed response and whose may have been overlooked.

The three approaches can be combined. Participatory exploration reveals consequences, strategy testing shows where existing plans are vulnerable, and working backwards clarifies what must be started early. The findings can then inform decisions and be revisited as new developments in the region emerge.



THEORETICAL FRAMEWORK: SAFETY & SECURITY & RESILENCE

The Council of the Baltic Sea States defines the "Safe & Secure Region" as one of its three priorities, with three key areas: anti-trafficking, child protection, and civil security:

"Our goal is to make everyone feel safe and secure and at home in every corner of our region. We strive to improve the well-being of our communities, build networks and trust to jointly respond to unexpected hazards and emergencies"[1].

It is no coincidence that the Baltic states, but also Central, Eastern, and Northern European countries in general, are increasingly looking towards strengthening security. With Russia's full-scale war against Ukraine, now several years old, as well as the hybrid war against the EU, the development priorities of EU countries have changed significantly. Other factors and circumstances in recent years, such as the COVID pandemic, the distancing of the alliance with the US, social polarisation, economic turbulence and increasing economic dependence on China, as well as extreme weather events, have not helped either. In a world of VUCA, multicrisis and information chaos, we often ask ourselves: are we safe and what really threatens us?

[1] CBSS. (2025). *Safe & secure region*. https://cbss.org/priorities/safe-secure-region/

For the purposes of this report, it is necessary to clarify the meaning of key terms. According to Selcuk Nas, these terms differ in terms of the hazard sources to which we are exposed, and the definitions are as follows:

- "Safety: The state of being away from hazards caused by natural forces or human errors randomly. The source of hazard is formed by natural forces and/or human errors.
- Security: The state of being away from hazards caused by deliberate intention of human to cause harm. The source of hazard is posed by humans deliberately"[2].

However, in the context of long-term development decisions at the territorial level, it is also important to mention the concept of resilience. Originally, this term was used in relation to the natural environment (coined by Holling in 1973[3]), and later evolved to cover society, the economy, and geographical areas, broadly. In simple terms, resilience is the ability to function effectively in the face of crises. It is often associated with processes of transformation, adaptation, regeneration, and sometimes anticipation[4].

The subjects of analysis in safety, security, and resilience fields are very diverse. Although for many decades the concept of security in a military and civil context dominated, in recent years a holistic approach has become the main discourse. This is more justified in the context of development policies, but it also leads to methodological difficulties.When it comes to building safety, security and resilience, what lies on the other side is also important. The opposite of security is a state of threat or danger, and vulnerability is often cited as the opposite of resilience. The elements that shape the perception of safety in a systemic approach are:

- Risks – "the possibility that the occurrence of an event will adversely affect the achievement of the organization's objectives"[5].
- Hazards – a source of danger that may cause harm to an asset, e.g. a property, a situation, or a state[6].
- Threats – "statement or action indicating an intention to harm or cause damage"[7] or other hostile actions.

---

[2] Nas, S. (2015). The definitions of safety and security. *Journal of ETA Maritime Science, 3*(2), 53–54.

[3] Holling, C. S. (1973). Resilience and stability of ecological systems. *Annual Review of Ecology and Systematics, 4*, 1–23.

[4] Stokowski, M. (2025). Czym jest odporność w ujęciu przestrzennym? O odporności terytorialnej. In W. Jarczewski & B. Sroka (Eds.), *Rola gospodarki przestrzennej w budowaniu rezyliencji i bezpieczeństwa Polski*. IRMiR

[5] Stanford University, Office of the Chief Risk Officer. (n.d.). *Definition of risk*. https://ocro.stanford.edu/enterprise-risk-management-erm/key-definitions/definition-risk

[6] Rausand, M. (2011). *Risk assessment: Theory, methods, and applications*. Wiley.

[7] Federal Protective Service. (n.d.). *Personal safety & security: What is a threat?*

- Crisis – a prolonged, adverse situation resulting in a breach of security in one or more dimensions of life.
- Shock – an event, a point on the timeline, which is a negative surprise and may mark the beginning of a crisis.
- Stress – prolonged pressure, conflict, or disagreement in relations between actors, which may cause a crisis.

Various frameworks are used to collect, evaluate, and rank external and internal distribution factors, as well as to develop preventive or remedial measures. These include general approaches to analysis and planning, such as the Sendai Framework[8], Comprehensive Security Framework[9], UN-Habitat "City Resilience Profiling Tool"[10], DHS Resilience Framework[11], NIST[12] (for cybersecurity), CIS RAM[13], and others, each of which has a specific application.

However, this study focuses on identifying key factors for the future security of the BSR and developing four scenarios for the future, differentiated in terms of the configuration of factors and the level of uncertainty affecting long-term developments. Therefore, it was necessary to make a conscious choice of the method of delimiting factors. The most popular classification of factors is the PEST method and its derivatives. PEST is a division of external factors affecting the operation of an entity/territory by thematic field. The basis is political, economic, social, and technological areas. The division is often expanded, e.g. including environmental, legal, and sometimes demographic, spatial, and other factors, so it creates STEEP, PESTEL, DESTEP, etc.

For military applications, this division evolved into PMESII. It covers factors from the following areas: political, military, economic, social, information, infrastructure. The extended version (PMESII-PT) uses two cross-cutting dimensions – physical environment and time[14]. For the purposes of this project, we have chosen the PMESII delimitation, which, in our opinion, most fully encompasses the phenomena identified in desk research and responds to the conclusions of the development and security policies of the Baltic Sea states and the challenges they face.

---

[8] UNISDR. (2015). *Sendai Framework for Disaster Risk Reduction 2015–2030*.

[9] Espinosa García, J., Hernández Encinas, L., & Peinado Domínguez, A. (2021). A comprehensive security framework proposal to contribute to sustainability. *Sustainability, 13*, 6901.

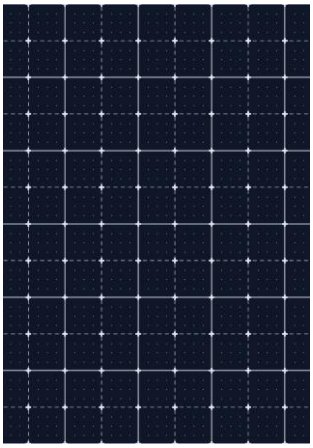
[10] UN-Habitat. (2018). *Guide to the City Resilience Profiling Tool*.

[11] U.S. Department of Homeland Security. (2018). *DHS resilience framework*.

[12] National Institute of Standards and Technology. (n.d.). *Cybersecurity framework*. https://www.nist.gov/cyberframework

[13] Center for Internet Security. (2025). *CIS RAM (Risk Assessment Method)*.

[14] Jurevicius, O. (2025). *PMESII-PT explained*. Strategic Management Insight. https://strategicmanagementinsight.com/tools/pmesii-pt/



METHODOLOGY

DESK RESEARCH

The purpose of the desk research was to establish an analytical foundation for the Delphi survey by identifying, structuring, and preliminarily interpreting the key directions of change and related factors affecting safety, security, and resilience in the BSR. The desk research in this project is intended to fulfill the following objectives:

1. Identify a preliminary list of factors influencing the safety, security and resilience of the BSR, to be used in the Delphi study.
2. Provide context for the research by structuring the security, safety, and resilience landscape of the region, which will be used to supplement future scenarios.

Due to the broad scope of the "Safe & Secure" priority, under which the project falls, and the multitude of security and resilience topics, it was decided to narrow down the selection. Initially, based on a preliminary review of sources, a list of 14 security and resilience topics was created:

01 CIVIL SECURITY	02 CROSS-BORDER SECURITY	03 SOCIAL RESILIENCE	04 MILITARY SECURITY
05 ENERGY SECURITY	06 ECONOMIC & FINANCIAL RESILIENCE	07 ENVIRONMENTAL SECURITY	08 PUBLIC HEALTH SECURITY
09 DIGITAL SECURITY	10 FOOD SECURITY	11 GOVERNANCE RESILIENCE	12 INFRASTRUCTURE & TECH SECURITY
13 CULTURAL & IDENTITY RESILIENCE	14 FINANCIAL SECURITY		

This list became the basis for expert discussion, and it was then decided to limit the focus to priority areas:

- Civil defence,
- Resilient governance (multi-level governance),
- Resilient infrastructure (including environment-as-infrastructure),

- Horizontal themes are "culture and identity" and "collaboration" (cross-border security - alliances).

Based on the focus topics as the key to desk research, the following sources were analysed:

- Documents concerning the security of all Baltic Sea countries.
- Documents concerning the security and development of the BSR at the EU level.
- Agendas and plans of alliances and other formal forms of cooperation between the Baltic countries.
- Scientific articles on the security and resilience of the BSR.
- Publications by think tanks, international organizations, and reports and research findings from other organizations on the international events and developments affecting the BSR.

Documents concerning the security of all Baltic Sea countries were analyzed, as were the agendas and plans of alliances and other formal forms of cooperation between the Baltic states, in order to identify key threats and uncertainties indicated in the documents. In the case of documents from large countries whose BSRs constitute a smaller part, attention was paid to ensure that the listed threats and uncertainties were relevant to the BSR.

Documents concerning the security and development of the BSR at the EU level were reviewed in terms of plans and guidelines specific to the countries of the BSR region, particularly in terms of objectives, priorities, and threats/uncertainties.

Scientific articles on the security and resilience of the BSR were analysed according to focus topics. Mainly publications from the last 10 years were taken into account, which concerned civil security, infrastructure and the natural environment, management, culture, and cooperation.

Publications by think tanks, international organizations, and reports and research findings from other organizations on region were specific sources during the review. Analysis was focused on major international events and developments affecting the BSR, based on official communications and statements from international institutions (including EU institutions, NATO and affiliated bodies), as well as a systematic review of international media sources such as Reuters, The Guardian, and other reputable outlets.

In total, 112 sources relevant to the research in the project were included in the review which highlighted a very strong presence of military-related topics that were directly linked to civil and infrastructure security. Therefore, it was decided to group the specific information according to PMESII criteria, which took military issues into account separately and

allowed for clear delimitation in other areas. This is also suitable due to its roots in the field of security.

The division of security factors resulting from the review in the PMESII delimitation allowed for the grouping of factors affecting the security and resilience of the region. The factors contribute to the Delphi study, and their descriptions are presented in the next section of the material.

Environmental pressures are treated as persistent conditions rather than scenario-specific uncertainties. All four scenarios therefore assume continued climate warming, eutrophication, biodiversity loss and increasing competition for maritime space. They differ not in whether these pressures occur, but in the capacity, resources and political priorities available to manage their consequences.

DELPHI METHOD

The Delphi method is a structured process of expert consultation designed to gather informed judgements on complex and uncertain issues. The aim of the process was to evaluate the factors identified during desk research for the purpose of creating future scenarios. The study was conducted in the form of a CAWI between February and April 2026 and involved 16 experts representing relevant fields and perspectives.

The study was carried out in two rounds. In the first round, participants assessed 31 factors. Each factor was evaluated in terms of both its impact and the probability of the indicated direction of change persisting.

- Probability was measured on a scale from –5 to +5, where –5 indicated that the identified direction of change would certainly reverse, +5 indicated that it would certainly persist, and 0 represented stabilisation or the absence of a clear directional trend.
- Impact was assessed on a scale from 0 to 5, where 0 represented no significant impact and 5 represented the strongest possible impact, whether positive or negative.

The second round focused on a selected group of 6 factors that generated the greatest divergence in expert assessments during the first round. Participants were presented with a summary of the initial results and invited to reconsider their earlier evaluations in light of aggregated responses of the group.

Experts were also encouraged to provide:

- recommendations – measures the countries of the region should take to strengthen security in the face of the uncertainties under consideration;

- consequences that these uncertainties might entail;
- other comments.

WORKSHOPS

The workshop sessions took place in July 2026, during the CBSS Summer University in Gdańsk. The participants were an international group of 21 young professional students. The workshop methodology consisted of two consecutive stages: future exploration and project development. In the first stage, participants were introduced to futures-oriented thinking and developed their own visions of the BSR up to 2035, reflecting their aspirations and expectations. They then worked with the four scenarios developed in the study, identifying opportunities, threats and broader implications for the region through facilitated activities and group discussion. In the second stage, participants shared and discussed their individual visions and selected problem areas arising from the scenarios that they considered particularly relevant. Working in small groups, they developed project proposals addressing the selected challenges and taking into account the threats and their potential consequences identified in the scenarios.

SCENARIO PLANNING

Scenarios are images of the future that depict the future state of a chosen research subject. They often include key processes, events and general pathways. Their role is to support decision-making processes in various formats. It can be assumed that scenarios, together with the process of their development, can fulfil strategic, cognitive and marketing functions[15]. This means that they support the selection of specific objectives and actions and can be incorporated into national, regional and local strategies.

They also facilitate an understanding of ongoing processes and their possible continuation, as well as an assessment of how changes in the surrounding environment might affect the situation. Finally, they can also contribute to the promotion of regions, strengthen communication with various stakeholders and present a collective vision of the future. In this project, a common scenario-building technique was used – the 2x2 matrix. Its application involves the following steps[16]:

---

[15] Cybulska, M., & Dziemianowicz, W. (2024). *Po prostu foresight! W kierunku dojrzałości strategiczno-foresightowej samorządów*. Instytut Rozwoju Miast i Regionów.

[16] Piskórz, M., & Stokowski, M. (2025). *Foresight Edu. Wprowadzenie do pracy z przyszłością*. Busola Trends.

1. Defining driving forces – carried out as part of desk research and the Delphi method.
2. Matrix axes: Key uncertainties were selected based on the factors showing the greatest statistical variation in the Delphi responses. They were positioned on the x and y axes of a 2x2 matrix, with opposing states at each end, generating four scenario combinations.
3. Scenario development: Each scenario describes the implications of a specific combination of extreme states of the key uncertainties. Scenarios were structured across the four PMESII areas and incorporate high-probability trends and other factors identified as particularly impactful in the Delphi study.
4. Scenario exploration and response design: The consequences of the scenarios, including opportunities and threats for the BSR, were explored during expert work and during workshops held as part of a week-long summer school. Participants subsequently developed projects addressing selected challenges identified in the scenarios.
5. The consequences of each scenario, including the opportunities and threats it creates for the BSR, were explored during workshops with participants in a week-long summer school. The participants were young people interested in education and in shaping the future development of the region. At the end of the programme, they developed projects responding to selected challenges and threats identified in the scenarios.
6. Scenario evaluation. The scenarios were evaluated for internal consistency, mutual distinctiveness, plausibility within the 2035 horizon and coverage of the most significant drivers of change. They were also assessed against current developments, institutional plans and the expected continuation of high-probability trends.



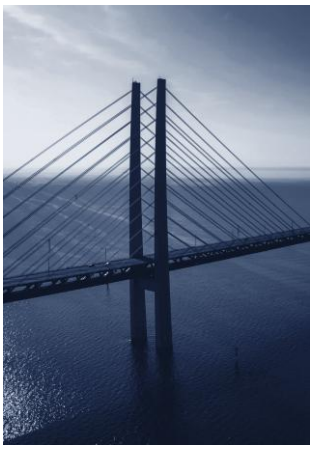
DIRECTIONS OF CHANGE IN SAFETY, SECURITY AND RESILIENCE IN THE BALTIC SEA REGION

Based on desk research and the Delphi method, key directions of change affecting safety, security, and resilience in the BSR were identified, grouped, and synthesised. These directions were organised in accordance with the PMESII delimitation, which allows for the analytical separation and simultaneous integration of political, military, economic, social, information, and infrastructure dimensions. Each direction of change is presented together with the processes and events supporting its identification. The analysis is followed by a set of corresponding factors that operationalise the direction of change and were subsequently assessed by experts in the Delphi study.

> Factors marked in red were reassessed in the second Delphi round because they showed the greatest divergence of expert opinion.

CODE	DIRECTION NAME	MAIN SEMANTIC AXIS
P political	New order of allied and regional coordination	selective regional cooperation; the Eastern Flank; Nordic–Baltic integration; joint response mechanisms; isolation of destabilising actors
M military	Militarisation of the Baltic space	persistent NATO presence; conventional deterrence; armed forces modernisation; conscription; defence infrastructure; militarisation of the maritime domain; escalation of exercises; military interoperability
E economic	The economy as a tool of security and autonomy	systemic resilience; infrastructural autonomy; dependencies as risk; investment screening and control; supply chain security; technological sovereignty; de-risking; high-risk suppliers
S social	Rising salience of identity and border control as an axis of domestic and foreign policy	border control; migration pressure; societal security; national identity; social cohesion; resilience-oriented policy; instrumentalisation of migration; redefinition of integration
I infrastructure	Grey-zone operations and infrastructure security in the BSR	grey-zone activity; infrastructure sabotage; critical infrastructure; subsea cables and pipelines; subsea protection; monitoring and detection; shadow fleet; infrastructure resilience
I information	Information as a tool of pressure and destabilisation	disinformation; societal polarisation; influence operations; information resilience; digital platforms; online radicalisation; platform regulation; cognitive security

TABLE 1 STRUCTURED OVERVIEW OF DIRECTIONS OF CHANGE BY PMESII CATEGORIES.



P. NEW ORDER OF ALLIED AND REGIONAL COORDINATION

Between 2016 and 2026, the BSR underwent a transformation in the field of security cooperation, initiated in the aftermath of Russia's annexation of Crimea. At the NATO Summit in Warsaw in July 2016, member states agreed to deploy four multinational battalion-sized battlegroups under the enhanced Forward Presence (eFP) framework in Poland, Estonia, Latvia, and Lithuania[17]. A decisive turning point for regional security cooperation came in 2022. Following Russia's full-scale invasion of Ukraine on February 24, 2022, states across the region undertook coordinated measures aimed at isolating destabilising actors. In March 2022, the membership of the Russian Federation and the Republic of Belarus in the CBSS was suspended[18]. This decision curtailed channels of regional

[17] *Warsaw Summit Communiqué. (2016). NATO. https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2016/07/09/warsaw-summit-communique*

[18] *Russia/Belarus: Members suspend Russia and Belarus from Council of the Baltic Sea States*. (n.d.). EEAS. https://www.eeas.europa.eu/eeas/russiabelarus-members-suspend-russia-and-belarus-council-baltic-sea-states_en

coordination with aggressor states and initiated a new model of selective political cooperation in the region.

A significant reinforcement of the regional defence architecture was the enlargement of NATO to include two Nordic states. Finland joined the Alliance in April 2023, followed by Sweden in March 2024[19]. As a result, nearly the entire BSR, excluding Belarus and the Kaliningrad Oblast, a Russian exclave, came under a unified defence structure capable of rapid response to both conventional and hybrid threats.

The role of formats complementary to NATO also increased. The Joint Expeditionary Force (JEF), bringing together Nordic and Baltic states alongside the United Kingdom, gained prominence as a framework for responding to threats to subsea infrastructure[20]. A Centre of Eastern Studies (OSW) analysis published in 2025 described the intensification of cooperation among Nordic and Baltic states within the NB8 format, which has increasingly served as a common political platform in relations with global actors, including the United States. The analysis also highlighted the growing role of this format in representing regional interests at the European level[21].

This process reflects a transformation of cooperation into a system based on strategic alignment and coordinated responses to Russia's destabilising actions. As a result, regional security cooperation has become more functional, more responsive, and increasingly oriented toward concrete operational objectives, while simultaneously excluding states that challenge the principles of the international order.

---

19 Palavenis, D. (2024). NATO enhanced forward presence in the Baltics: The nexus between the host and the framework nation. Security and Defence Quarterly. https://doi.org/10.35467/sdq/193734

20 Ministry of Defence. (2023). *Joint statement by Joint Expeditionary Force ministers, November 2023*. GOV.UK. https://www.gov.uk/government/news/joint-statement-by-joint-expeditionary-force-ministers-november-2023

21 Szymański, P. (2025). *Grupa NB8 a inne formaty współpracy na rzecz bezpieczeństwa regionu Morza Bałtyckiego*. OSW Ośrodek Studiów Wschodnich. https://www.osw.waw.pl/pl/publikacje/komentarze-osw/2025-05-29/grupa-nb8-a-inne-formaty-wspolpracy-na-rzecz-bezpieczenstwa

AREA	FACTORS	IMPACT	UNCERTAINTY
P political	Increased importance of cross-border cooperation*	3	1,33
	Decreased importance and effectiveness of global and supra-regional forms of co-operation**	4	2,24
	Fragmentation of multi-level governance in the BSR (tensions between EU, national, regional, and local levels; weak sectoral coordination)*	3	2,68
	Limited legal capacity to respond to cross-border threats (e.g., consequences of sabotage and border pressure, enforcement of sanctions)*	3	3
	Increased political cohesion among countries in the region (differences in interests, different approaches to ecology, national security, Russia, and the role of the state)**	4	1,88
	Declining trust in public institutions as a factor weakening public support for decisions made by public entities**	3,5	1,47

*one round of assessment; **two rounds of assessment

TABLE 2 POLITICAL FACTORS ASSESSED IN THE DELPHI STUDY



M. MILITARISATION OF THE BALTIC SPACE

The decade 2016–2026 brought a systematic militarisation of the BSR, driven by the deteriorating security environment in North-Eastern Europe and the escalation of hybrid, sabotage-related, and conventional threats. The region was transformed from a peripheral maritime area into a strategically significant NATO operational space. A key milestone was the decision taken at the NATO Summit in Warsaw in July 2016 to establish the eFP, involving the deployment of multinational battalion battle groups in Estonia, Latvia, Lithuania, and Poland, which shifted NATO's eastern flank from a buffer zone into an area of permanent allied military presence[22].

In the subsequent years, this process was reinforced by national-level measures aimed at rebuilding and strengthening domestic defence capabilities. In 2017, Sweden reinstated compulsory military service, justifying the decision by the deterioration of the security environment and the increased risk of conventional confrontation[23]. In 2021, Finland decided

[22] *Warsaw Summit Communiqué. (2016). NATO. https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2016/07/09/warsaw-summit-communique*

[23] *Sweden reintroduces conscription, in a changing European security environment.* (2017). IISS. https://www.iiss.org/online-analysis/military-balance/2017/03/sweden/

to procure 64 F-35 fighter aircraft, marking a major investment in the country's combat capabilities[24]. Russia's full-scale invasion of Ukraine in February 2022 gave this process a distinctly escalatory character. In 2023, Latvia adopted the State Defence Service Act, reintroducing mandatory military service from 2024[25]. The Baltic Defence Line represents a joint, long-term defence project of Estonia, Latvia, and Lithuania, involving the construction of permanent counter-mobility infrastructure along the borders with Russia and Belarus. The project includes, inter alia, bunkers, anti-tank ditches, terrain obstacles, engineering barriers, and dedicated storage facilities for fortification elements[26].

The maritime domain gained strategic importance. Poland launched its largest naval modernisation programme since the Cold War, encompassing the construction of three frigates in Gdynia, a submarine programme developed in cooperation with Sweden, the deployment of new mine countermeasure vessels, and the expansion of submarine rescue capabilities. These efforts were accompanied by legal changes strengthening command authorities, an intensification of international exercises, and increased interoperability among the region's naval forces[27].

Between 2018 and 2024, increased Russian military activity was observed in the Baltic airspace, documented by NATO and independent sources as a growing pattern of interception incidents, GPS/GNSS interference, and signalling operations. In 2024, *Reuters* and *Le Monde* reported a significant rise in navigation disruptions in the region, including around Tartu and over the Baltic Sea, resulting in the suspension of civilian flights and operational constraints on maritime traffic and emergency services[28] [29].

This process has been further reinforced by the militarisation of the Arctic domain, including the increase in Denmark's military presence in Greenland from 2026 onwards and

---

24 Lehto, E., & Stone, M. (2021). *Finland orders 64 Lockheed F-35 fighter jets for $9.4 bln*. Reuters. https://www.reuters.com/business/aerospace-defense/lockheed-f-35-jet-wins-finnish-fighter-competition-source-2021-12-10/

25 *Saeima adopts State Defence Service Law*. (2023). Aizsardzības ministrija. https://www.mod.gov.lv/en/news/saeima-adopts-state-defence-service-law

26 Milevski, L. (2024). *The Baltic Defense Line*. Foreign Policy Research Institute. https://www.fpri.org/article/2024/02/the-baltic-defense-line/

27 *As Trump unsettles Europe, Poland begins largest overhaul of its navy to tackle 'Russian threat'*. (2026). Firstpost. https://www.firstpost.com/world/as-trump-unsettles-europe-poland-begins-largest-overhaul-of-its-navy-to-tackle-russian-threat-13971561.html

28 *Finnish carrier suspends Estonia flights after GPS interference prevents 2 landings*. (2024). AP News. https://apnews.com/article/finnair-finland-estonia-gps-interference-flights-c347fe58902b553a936a3efc42e6cc2f

29 Grynszpan, E., & Pietralunga, C. (2024). *Russia's GPS jamming intensifies over the Baltic Sea*. Le Monde.fr. https://www.lemonde.fr/en/international/article/2024/05/02/russia-s-gps-jamming-intensifies-over-the-baltic-sea_6670151_4.html

exercises such as *Operation Arctic Endurance*, which functionally link the Arctic and the Baltic within a single NATO flank[30].

As a result, the BSR has been transformed into an environment of heightened militarisation, both in terms of physical presence and response capabilities. At the same time, the frequency and intensity of hybrid activities have increased, requiring continuous adaptation of doctrines and response scenarios. The Baltic area has ceased to function as a space of neutral maritime cooperation and has become an arena of active deterrence, testing the resilience of military and civilian systems, and demonstrating allied cohesion.

AREA	FACTORS	IMPACT	UNCERTAINTY
M military	Intensification of state-driven hybrid threats in the BSR, including sabotage of critical infrastructure, airspace violations and military pressure below the threshold of open war*	4	1,22
	Acceleration of technical modernisation of the national armed forces of the Baltic states aimed at strengthening self-sufficient deterrence capabilities*	4	1
	Strengthening the security of external borders by expanding physical barrier systems and surveillance measures*	3	1,29
	Increase in the presence of allied forces (e.g., eFR brigade structures) on the territory of the Baltic states**	4	1,47

*one round of assessment; **two rounds of assessment

TABLE 3 MILITARY FACTORS ASSESSED IN THE DELPHI STUDY



E. THE ECONOMY AS A TOOL OF SECURITY AND AUTONOMY

Between 2016 and 2026, a fundamental shift occurred in how the states of the BSR approached economic and investment issues. The previous cost efficiency paradigm, based on the assumption that trade relations were neutral and primarily served to enhance national economic competitiveness, was gradually replaced by a logic of systemic resilience and infrastructural autonomy.

A clear illustration of this shift was provided by the case of Lithuania. Following the opening of a Taiwanese Representative Office in Vilnius in 2021, Lithuania became the target of extensive pressure from the People's Republic of China. As noted in the February 2022

[30] *Exercise Arctic Endurance Continues to Develop*. (2026). Defence Command Denmark. https://www.forsvaret.dk/en/news/2026/exercise-arctic-endurance-continues-to-develop/

OSW analysis *"Lithuania–China: political crisis and economic pressure"*, these measures included Lithuania's removal from China's customs system, the suspension of imports containing Lithuanian components, and indirect pressure on multinational companies to withdraw from cooperation with Lithuanian suppliers[31]. In response, the European Commission filed a complaint with the WTO (DS610) in January 2022, arguing that China's actions violated the principles of multilateral trade[32]. The termination of the DS610 case without a WTO ruling[33], at the request of the EU, indicates that the union's response was primarily political and signalling in nature rather than legal, and highlights the risk of economic interdependencies being used as instruments of geopolitical pressure.

One element of this strategic shift was the securitisation of the telecommunications sector, particularly concerning 5G, understood as a move away from assessing technology itself toward assessing supplier risk and component dependencies within critical network functions. In practice, this translated into the implementation of "high-risk supplier" mechanisms, involving restrictions on or the exclusion of selected vendors from critical infrastructure elements, most notably network cores and management functions, and in some cases requiring the replacement of existing equipment within defined timeframes. The most explicit example in the region was Sweden, where the national regulator PTS linked participation in 5G spectrum auctions to security conditions that resulted in the exclusion of Huawei and ZTE Corporation from specific network deployments and created an obligation to phase out existing components[34]. These decisions became the subject of multi-stage legal disputes and court proceedings. At the EU level, this process was reinforced through regulatory and executive instruments such as the 5G Toolbox[35], the NIS2 Directive[36] and the Critical Entities Resilience Directive[37].

---

31 Płóciennik, S. (2022). *Niemcy a konflikt handlowy między Litwą a Chinami*. OSW Ośrodek Studiów Wschodnich. https://www.osw.waw.pl/pl/publikacje/komentarze-osw/2022-02-04/niemcy-a-konflikt-handlowy-miedzy-litwa-a-chinami

32 *WT/DS610 - China – Measures concerning trade in goods and services*. (2023). Trade and Economic Security. https://policy.trade.ec.europa.eu/enforcement-and-protection/dispute-settlement/wto-dispute-settlement/wto-disputes-cases-involving-eu/wtds610-china-measures-concerning-trade-goods-and-services_en

33 *EU drops complaint against Chinese trade curbs on Lithuania at WTO - document*. (2025). Reuters. https://www.reuters.com/sustainability/eu-drops-complaint-against-chinese-trade-curbs-lithuania-wto-document-2025-12-01/

34 VVGB Law - European law, trade law, corporate law - Lawyers Brussels, Belgium. https://www.vvgb-law.com/media/1119/20201129-hw-swedish-pts-decision.pdf

35 *Unijny zestaw narzędzina rzecz bezpieczeństwa sieci 5G*. (2020). Kształtowanie cyfrowej przyszłości Europy. https://digital-strategy.ec.europa.eu/pl/library/eu-toolbox-5g-security

36 *Dyrektywa NIS 2: zabezpieczenie sieci i systemów informatycznych*. (n.d.). Kształtowanie cyfrowej przyszłości Europy. https://digital-strategy.ec.europa.eu/pl/policies/nis2-directive

37 *Critical infrastructure resilience at EU-level*. (2026). Migration and Home Affairs. https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/protection/critical-infrastructure-resilience-eu-level_en

In the BSR, the development of high-performance computing (HPC) infrastructure and artificial intelligence–based systems began to be framed as part of a broader concept of technological sovereignty. Finland launched the LUMI supercomputer and the LUMI AI Factory under the EuroHPC initiative, positioning itself as one of the core nodes of Europe's computational infrastructure[38]. Sweden expanded its capacity for advanced AI applications, including through the MIMER project and the launch of new cloud regions by global service providers in 2025[39]. Poland attracted investments from hyperscale cloud operators, linking them to the development of national cybersecurity frameworks, cooperation with public administration, and applications for the energy sector[40] [41]. According to the *Digital Decade Country Report 2025*, Estonia achieved one of the highest levels of cloud services adoption in the EU, while simultaneously developing digital resilience policies and competency programmes, including educational initiatives in the field of artificial intelligence[42]. In January 2026, the European Commission announced a draft legislative proposal providing for the gradual phase-out of components and equipment supplied by so-called high-risk vendors from key infrastructure sectors. The proposed revision of the EU cybersecurity framework covers 18 sectors, ranging from telecommunications and energy to water systems and autonomous vehicles, as well as cloud computing, semiconductors, and space technologies. The initiative indicates a reduction of the presence of Chinese suppliers in these sectors. The proposed measures are intended to strengthen cybersecurity and the EU's technological sovereignty. Transitional periods for mobile and fixed network operators are expected to last up to 36 months from the publication of the list of high-risk suppliers[43].

For the BSR, this has meant that trade and technological interdependencies have ceased to be perceived as neutral infrastructures of exchange and have instead come to be treated as assets requiring control and selection. Over the analysed decade, the Nordic – Baltic states adopted a paradigm in which the economy is understood as an integral component of security, a shift reflected both in regulatory frameworks and in institutional

---

38 *The successor for LUMI announced — a new pan-European supercomputer and one of the first European Union's AI Factories to be placed in Finland*. (2024). LUMI. https://lumi-supercomputer.eu/successor-for-lumi-announced/

39 Brady, T., & Wiss, M. (2025). *Google Cloud launches 42nd cloud region in Sweden*. Google Cloud Blog. https://cloud.google.com/blog/products/infrastructure/google-cloud-launches-42nd-cloud-region-in-sweden

40 *Microsoft announces a PLN 2.8 billion investment in cloud and AI infrastructure, skilling and cybersecurity in Poland*. (2025). Microsoft. https://news.microsoft.com/pl-pl/2025/02/17/microsoft-announces-a-pln-2-8-billion-investment-in-cloud-and-ai-infrastructure-skilling-and-cybersecurity-in-poland/

41 *Google hub in Poland to develop AI use in energy and cybersecurity sectors*. (2025). AP News. https://apnews.com/article/google-poland-ai-innovations-investment-475ad8b95cb3f3060e352be8720008bd

42 *Estonia 2025 Digital Decade Country Report*. (2025). Shaping Europe's digital future. https://digital-strategy.ec.europa.eu/en/factpages/estonia-2025-digital-decade-country-report

43 *Yun Chee F.* (2026). EU plan to phase-out high-risk tech draws fire from China's Huawei. https://www.reuters.com/business/media-telecom/eu-phase-out-high-risk-tech-targets-huawei-chinese-companies-2026-01-20

approaches to foreign investment, technology providers, and the configuration of supply chains.

AREA	FACTORS	IMPACT	UNCER-TAINTY
E economic	Increased political control over key economic and technological links at the national and EU level*	3	1,42
	Strengthening strategic autonomy through accelerated energy transition, based on harmonising sustainability-driven and security- and resilience-driven framework**	3,5	1,84
	Escalation of risks to maritime security and navigation in the Baltic Sea (shadow economy activities, shadow fleet, GPS interference, provocative military maneuvers, temporary closure of waters*	3,5	1,34
	Increase in the share of GDP allocated to the technical modernization of the armed forces and the purchase of advanced weapon systems by the Baltic states*	4	1,53
	Increased importance of ports as dual-use infrastructure (Baltic ports serve commercial, energy, military, and logistical functions, which increases their strategic importance)*	4	1,20
	Prioritisation of development policies focused on resilience and security rather than sustainable development*	3	1,82

*one round of assessment; **two rounds of assessment

TABLE 4 ECONOMIC FACTORS ASSESSED IN THE DELPHI STUDY



S. RISING SALIENCE OF IDENTITY AND BORDER CONTROL AS AN AXIS OF DOMESTIC AND FOREIGN POLICY

States of the BSR and Northern Europe gradually transformed their approach to border management and social policy, shifting the centre of gravity from a model of openness and integration towards one based on control, selectivity, and social resilience. A key turning point was the migration crisis on the eastern borders of the EU in 2021, which both the European Union Agency for Asylum (EUAA) and the Polish Institute of International Affairs (PISM) explicitly interpreted as a political instrument used by the Belarusian regime to destabilise Poland, Lithuania, and Latvia[44] [45]. In this context, borders ceased to function

[44] European Union Agency for Asylum. (2022). *Asylum report 2022* (Section 4.1.1, Situation on the eastern borders).

[45] *The Border Crisis as an Example of Hybrid Warfare*. (2022). PISM. https://www.pism.pl/publications/the-border-crisis-as-an-example-of-hybrid-warfare

solely as instruments of migration policy and instead became a physical and symbolic arena of hybrid confrontation.

In the following years, states of the region not only reinforced the physical infrastructure of their borders, including fences, surveillance systems, and control points, but also revised their legislative and operational approaches. The project was officially announced on January 19, 2024. In December 2025, Lithuania declared a state of emergency following a series of incidents involving balloons used for smuggling and for violations of airspace, which were described by the authorities as elements of "hybrid interference"[46]. On October 28, 2025, Lithuania decided to temporarily close its last remaining border crossings with Belarus, resulting in the complete suspension of official cross-border traffic along that section[47]. In September 2025, the Polish authorities temporarily closed all border crossings with Belarus in response to the launch of the Russian–Belarusian Zapad-2025 military exercises[48]. In the following weeks, Poland partially reopened selected road and rail border crossings, declaring readiness for further reopenings. However, unrestricted cross-border movement was not restored along the entire border, and decisions regarding the status of individual crossings remained conditional on ongoing security assessments.

At the same time, the region experienced growing internal tensions related to identity and integration issues. In Estonia and Latvia, reforms of the education system were implemented after 2022, providing for the gradual phasing out of Russian-language schooling. In Estonia, this reform was formalised as a strategic policy framework extending to 2030, implemented under an education reform programme aimed at strengthening social cohesion and equal opportunities[49]. These measures formed part of internal security policies aimed at reducing the vulnerability of national minorities to external pressure and disinformation.

The political trajectory has increasingly shifted towards values centred on order, resilience, and national identity. Across several countries in the region, including Finland, Sweden, Germany, and Poland, political forces with anti-immigration, Eurosceptic, and or nationalist profiles have gained strength. For example, in the German federal elections of February 2025, Alternative für Deutschland (AfD) placed second and emerged as a key force

---

46 Sytas, A. (2025). *Lithuania declares state of emergency over balloons from Belarus*. Reuters. https://www.reuters.com/world/lithuania-declares-state-emergency-over-smuggler-balloons-belarus-2025-12-09/

47 Hivert, A.-F. (2025). *Lithuania closes its border with Belarus*. Le Monde.fr. https://www.lemonde.fr/en/international/article/2025/10/28/lithuania-closes-its-border-with-belarus_6746836_4.html

48 Fedorowicz, K. (2025). *Reakcje strony białoruskiej na zamknięcie (i otwarcie) granicy z Polską*. Instytut Europy Środkowej. https://ies.lublin.pl/komentarze/reakcje-strony-bialoruskiej-na-zamkniecie-i-otwarcie-granicy-z-polska

49 Pettai, V. (2024). Chapter 13: Educational Reform in Estonia and Latvia. *European Yearbook of Minority Issues Online, 21*(1), 313–332. https://doi.org/10.1163/22116117_02101014

shaping the axis of political debate, a development described by *Reuters* as a historic turning point[50]. In Finland, the programme of the new government, formed with the participation of the Finns Party, introduced a paradigmatic shift towards a more restrictive migration policy[51]. In Sweden, the victory of the right-wing bloc in 2022 led to the formal incorporation of the Sweden Democrats (SD), a far-right party, into the governing arrangement as a key political actor[52].

As a result, borders acquired a new function: they no longer serve solely to protect against external threats, but also to define the political community within states. National identity became embedded in the security architecture, while social cohesion was redefined as the capacity to withstand informational, migratory, and normative pressure. The model of "societal resilience" thus replaced the earlier paradigm of the "open society".

AREA	FACTORS	IMPACT	UNCERTAINTY
S social	Growing instrumentalisation of migration, which involves using migration flows as a political tool in the context of domestic politics and geopolitics*	3	2,22
	Increasing societies' willingness to bear the economic and social costs associated with security policies*	3	2,09
	Declining importance of public participation and including local and peripheral voices in security, climate, and infrastructure policies*	3	2,37
	Increased support for nationalist political parties*	3	1,42
	Growing acceptance of democratic restrictions in the name of security*	3	2,05
	Divergence of national migration policies in the BSR following the termination of temporary protection regimes*	2,5	2,22

*one round of assessment; **two rounds of assessment

TABLE 5 SOCIAL FACTORS ASSESSED IN THE DELPHI STUDY

[50] *Results Germany*. (2025). The Federal Returning Officer. https://www.bundeswahlleiterin.de/en/bundestagswahlen/2025/ergebnisse/bund-99.html

[51] *Finland's incoming govemmentto reduce immigration*.(2023). Reuters. https://www.reuters.com/world/europe/finlands-incoming-government-reduce-immigration-2023-06-16

[52] Henley, J. (2022). *Swedish parties agree coalition with backing of far-right*. the Guardian. https://www.theguardian.com/world/2022/oct/14/swedish-parties-agree-coalition-with-backing-of-far-right



I1. GREY-ZONE OPERATIONS AND INFRASTRUCTURE SECURITY IN THE BALTIC SEA REGION

BSR infrastructure was subject to systematic sub-threshold activities, including sabotage, disruptions, incidents of ambiguous attribution, and technological pressure targeting systems of critical importance. As a result, the region became a key arena of confrontation within the so-called "grey zone" between war and peace. The most visible manifestations of these activities concerned subsea infrastructure, both energy and telecommunications, which was repeatedly damaged or disrupted under circumstances requiring international investigations.

An important background factor in the escalation of such incidents was the reconfiguration of the region's infrastructure architecture, involving the gradual reduction of dependencies on systems linked to Russia and Belarus. As early as June 2018, a decision was taken to synchronise the electricity grids of the Baltic states with the continental European system as an alternative to continued operation within the post-Soviet BRELL system, which connected Lithuania, Latvia, and Estonia with Russia and Belarus. This process was not merely technical in nature but explicitly political, serving as a means of reducing systemic energy dependencies on states perceived as security threats[53]. A key milestone was the disconnection of the Baltic states from the BRELL system in February 2025 and the completion of full synchronisation with the EU electricity grid[54]. This process, implemented under the supervision of European and national institutions, was explicitly framed as a component of enhancing resilience against sabotage and destabilisation threats, rather than merely as an infrastructure modernisation effort. In parallel, physical infrastructure enabling independent energy supply routes was expanded. In 2022, the Baltic Pipe (PL–DK) was commissioned, allowing for the transmission of natural gas from Norway to Poland while bypassing Russian infrastructure[55]. The project, co-financed with EU funds, was promoted as a key pillar of supply diversification in the region and as evidence of European energy solidarity.

Against the backdrop of this infrastructural reconfiguration, the BSR experienced a series of incidents involving damage to subsea infrastructure of growing systemic significance. A

---

53 Cook, B. (2025). *BRELL Desynchronisation Assessment*. NATO ENSEC COE. https://www.enseccoe.org/publications/brell-desynchronisation-assessment

54 Ibid.

55 *Launch of the Baltic Pipe*. (2022). European Commission. https://commission.europa.eu/news-and-media/news/launch-baltic-pipe-2022-09-27_en

critical turning point was the explosions on the Nord Stream 1 and 2 pipelines in the Baltic Sea on September 26, 2022, which exposed the vulnerability of energy infrastructure in the region. Investigations conducted by Denmark, Sweden, and Germany did not lead to the identification of a definitive perpetrator, but they confirmed the scale of risks associated with physical attacks on subsea installations[56]. On October 8, 2023, the Balticconnector gas pipeline between Finland and Estonia, along with associated telecommunications cables, was damaged, triggering responses from security services and the initiation of operational measures[57]. In December 2024, a failure of the Estlink 2 subsea electricity interconnector occurred, resulting in a 41% increase in the average wholesale electricity price on the Nord Pool market compared to the previous week[58]. At the strategic level, these incidents led to the recognition of subsea infrastructure as an element of national security. As early as November 2023, the JEF launched the "JEF Response Option", an air and maritime component focused on the protection of underwater infrastructure[59]. At the EU level, the response took the form of the *EU Action Plan on Cable Security*, adopted on February 21, 2025, which for the first time addressed the full cycle of measures related to cables and pipelines, including prevention, detection, response, and recovery[60].

An important related aspect is the phenomenon of the so-called "shadow fleet", that is, a group of vessels used, among other purposes, to circumvent sanctions and conduct concealed oil trade, which has been identified as one of the main sources of risk. Analyses published in December 2024 and January 2025 pointed to links between these vessels, damage to critical infrastructure, and environmental threats. Finland, Denmark, and other countries in the region launched port inspection regimes, tightening insurance and registration requirements for vessels deemed suspicious.

A statement issued by the Finnish Ministry for Foreign Affairs on December 16, 2024 described coordinated measures undertaken by a group of coastal states bordering the Baltic Sea and the North Sea, including the United Kingdom, Denmark, Sweden, Finland, Poland, and Estonia, aimed at countering Russia's shadow fleet of tankers. The core of this

---

56 Braw, E. (2025, November 26). *How the Baltic Sea nations have tackled suspicious cable cuts*. Atlantic Council. https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/how-the-baltic-sea-nations-have-tackled-suspicious-cable-cuts/

57 Hyndle-Hussein, J., & Tarociński, J. (2023, October 11). *The Balticconnector gas pipeline damage*. OSW Centre for Eastern Studies. https://www.osw.waw.pl/en/publikacje/analyses/2023-10-11/balticconnector-gas-pipeline-damage

58 *Damage to EstLink 2 cable raises energy prices in Baltic countries*. (2025, January 3). Baltic Wind. https://balticwind.eu/damage-to-estlink-2-cable-raises-energy-prices-in-baltic-countries/

59 Ministry of Defence. (2023, November 28). *Joint statement by Joint Expeditionary Force ministers, November 2023*. GOV.UK. https://www.gov.uk/government/news/joint-statement-by-joint-expeditionary-force-ministers-november-2023

60 *EU Action Plan on Cable Security, JOIN(2025) 9 final*. (2025, February 21). European Commission. EUR-Lex. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52025JC0009

initiative consists of regular checks of insurance certificates, particularly with regard to coverage for environmental damage following potential oil spills, conducted along key maritime routes such as the English Channel, the Danish Straits, and the Gulf of Finland, combined with announcements of further sanctions targeting vessels associated with this fleet[61]. In January 2025, NATO launched the *Baltic Sentry* initiative, aimed at improving detection capabilities and readiness to respond to acts of infrastructure sabotage[62]. Denmark implemented maritime infrastructure monitoring systems based on artificial intelligence, satellite data, and autonomous unmanned platforms, strengthening early-warning and detection capabilities for threats to subsea infrastructure[63].

As a result, the infrastructural domain, previously treated primarily as a technical and commercial sphere, became fully securitised. Subsea incidents ceased to be interpreted as technical failures and increasingly came to be understood as actions testing state resilience. Responses evolved into complex inter-allied and institutionalised measures, involving NATO, the EU, and bilateral cooperation frameworks. The Baltic Sea has thus been transformed into a space of continuous monitoring, risk management, and counteraction against activities of ambiguous origin, permanently reshaping the governance of infrastructure security in the region.

AREA	FACTORS	IMPACT	UNCERTAINTY
I infrastructure	Growing importance of civil infrastructure as targets for terrorism and sabotage*	3,5	1,50
	Degradation of the Baltic Sea ecosystem combined with climate change*	3,5	1,85
	Growing importance of digital infrastructure and data centers in the context of security*	3,5	1,32
	Development of a supra-regional transport network in the region, connecting BSR countries*	3	2,53

*one round of assessment; **two rounds of assessment

TABLE 6 INFRASTRUCTURE FACTORS ASSESSED IN THE DELPHI STUDY

61 Ministry for Foreign Affairs of Finland. (2024). *Group of coastal states around Baltic Sea and North Sea to take targeted measures against Russian shadow fleet*. https://um.fi/current-affairs/-/asset_publisher/gc654PySnjTX/content/ryhma-itameren-ja-pohjanmeren-rantavaltioita-kohdentaa-toimia-venajan-varjolaivastoon-puuttumiseksi

62 *NATO launches 'Baltic Sentry' to increase critical infrastructure security*. (2025). North Atlantic Treaty Organization (NATO). https://www.nato.int/en/news-and-events/articles/news/2025/01/14/nato-launches-baltic-sentry-to-increase-critical-infrastructure-security

63 Bryant, M. (2025). *Denmark deploys 'saildrones' in Baltic to protect undersea cables from Russia*. the Guardian. https://www.theguardian.com/world/2025/jun/19/denmark-to-deploy-saildrones-in-baltic-to-protect-undersea-cables-from-russian-threat



12. INFORMATION AS A TOOL OF PRESSURE AND DESTABILISATION

The information space within the EU, including the BSR, has been durably integrated into the logic of state and alliance security. EU institutions and regional governments have systematically identified coordinated disinformation campaigns as an element of hybrid activities aimed at undermining NATO's credibility, the legitimacy of the EU, and the political stability of the eastern flank states. The European External Action Service, through its East StratCom Task Force, documented the growing scale and professionalisation of these activities already prior to 2022, highlighting their long-term and strategic nature.[64].

At the same time, institutional data pointed to growing social polarisation across EU member states, particularly in relation to the war, sanctions, migration, and relations with NATO and the EU. Eurobarometer surveys and reports by the European Union Agency for Fundamental Rights from 2022–2024 documented a decline in trust in media information alongside the rise of emotionally driven and identity-based narratives. This dynamic was further reinforced by the architecture of digital platforms, which became one of the key justifications for the adoption of the Digital Services Act as a regulatory instrument addressing systemic security risks.

Europol data for 2024 indicate that 58 terrorist attacks were recorded across EU member states, including 34 carried out attacks, five failed attempts, and 19 foiled plots, alongside 449 arrests related to terrorist activities in 20 member states. A particularly notable feature of the 2024 threat landscape was the low age of a significant share of perpetrators and suspects. A total of 133 detained individuals were aged between 12 and 20, accounting for nearly 29 per cent of all arrests, including 70 minors.

Europol emphasises that processes of radicalisation and mobilisation are increasingly taking place online, within decentralised networks and micro-communities operating outside formal organisational structures. These environments often display a hybrid ideological profile, combining elements of jihadist terrorism, right-wing violence, accelerationism, and anti-system narratives. Digital platforms have thus ceased to function merely as channels of communication and have increasingly become environments for attitude formation, the normalisation of violence, and recruitment, particularly among young people vulnerable to social isolation, mental health challenges, and algorithmic amplification[65].

---

64 *EEAS Strategic Communication Task Forces*. (2025). EEAS. https://www.eeas.europa.eu/eeas/eeas-strategic-communication-task-forces_en?s=2803

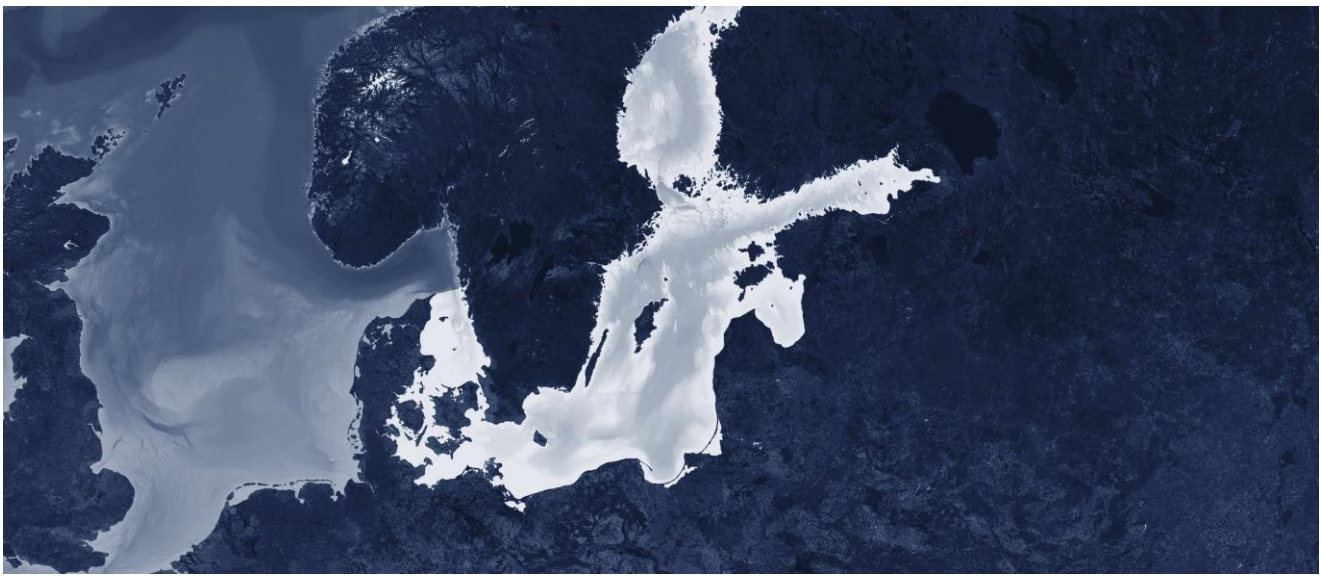
65 Europol. (2025). *European Union terrorism situation and trend report*. Publications Office of the European Union.

In response, BSR states, particularly Finland and Estonia, incorporated information resilience, media literacy, and strategic communication into their national comprehensive security frameworks. In these documents, polarisation and disinformation were defined as factors directly affecting social cohesion, crisis response capacity, and the long-term resilience of the state.

AREA	FACTORS	IMPACT	UNCERTAINTY
I information	Growing polarisation of media coverage*	3	1,42
	Rising social polarisation*	4	1,81
	Growing influence of generative technologies (deepfakes, synthetic content)*	3,5	0,91
	Declining security of communication channels and digital tools (dependence on two key providers with differing interests – China and the US)**	4	2,19
	Declining public trust in the media*	3	2

*one round of assessment; **two rounds of assessment

TABLE 7 INFORMATION FACTORS ASSESSED IN THE DELPHI STUDY



FUTURE SCENARIOS

The research work led to the selection of the following axes and their opposing end states:

X-axis: The significance of supra-regional forms of cooperation relating to security:

1. Global cooperation: A return to prioritising supra-regional forms of cooperation.
2. Regional cooperation: Priority given to regional organisations and cross-border cooperation, as a result of the reduced importance of supra-regional forms of co-operation.

Y-axis: Technological dependence on global leaders:

1. Dependence: Increased technological dependence on global leaders (the US and China), caused by the ineffectiveness of measures/attempts to achieve independence at the EU and national level.
2. Sovereignty: Increased technological independence from global leaders (the US and China), manifested in the wider use of European and national tools.



PICTURE 1 SCENARIOS OF BSR FRAMEWORK

In developing the scenarios, particular attention was paid to describing the PMESII areas and to taking into account other key factors, which included both certain factors (on which experts had reached a relative consensus regarding their future trajectory) and factors subject to uncertainty (factors that are significant but for which there are significant differences in the assessment of their trajectories). These are listed in the table below.

SIGNIFICANT AND CERTAIN FACTORS:

1. Intensification of state-driven hybrid threats in the BSR, including sabotage of critical infrastructure, airspace violations and military pressure below the threshold of open war
2. Escalation of risks to maritime security and navigation in the Baltic Sea (shadow economy activities, shadow fleet, GPS interference, provocative military maneuvers, temporary closure of waters.
3. Growing influence of generative technologies (deepfakes, synthetic content)
4. Acceleration of technical modernisation of the national armed forces of the Baltic states aimed at self-sufficient deterrence capabilities.

5. Increased importance of ports as dual-use infrastructure (Baltic ports serve commercial, energy, military, and logistical functions, which increases their strategic importance).
6. Growing importance of digital infrastructure and data centers in the context of security
7. Increase in the share of GDP allocated to the technical modernisation of the armed forces and the purchase of advanced weapon systems by the Baltic states.

SIGNIFICANT BUT UNCERTAIN FACTORS:

1. Declining trust in public institutions as a factor weakening public support for decisions made by public entities
2. Increased political cohesion among countries in the BSR (greater alignment of interests in security, energy, ecological and Russia-related policies)
3. Strengthening strategic autonomy through accelerated energy transition, based on harmonising sustainability-driven and security- and resilience-driven framework
4. Increase in the presence of allied forces (e.g., eFP brigade structures) on the territory of the Baltic states.

TABLE 8 KEY FACTORS FOR THE REGION.

A red line in the margin marks a wild card: a sudden, high-impact event that could abruptly change the course of a scenario.

The four scenarios differ not only in the configuration of the main axes, but also in the source of security, the trajectory of the war in Ukraine, the organisation of technological systems, the dominant model of societal resilience and the principal costs borne by the region.

AREA	SCENARIO 1: RELYING ON DISTANT FRIENDS	SCENARIO 2: SAFETY IS A BUSINESS	SCENARIO 3: PRAGMATIC RESILIENCE	SCENARIO 4: THE BALTIC FORTRESS
Primary source of security	US and NATO security guarantees	Regional arrangements supported by external suppliers	NATO–EU cooperation and growing European capabilities	Permanent regional defence mechanism
Ukraine's situation in the face of the full-scale Russian-led war	US-backed armistice	Strategic defeat	Strategic success	Sovereignty preserved through regional support and deterrence
Technology	Dependence on global providers	Dependence combined with regional procurement and commercial services	European control within NATO–EU frameworks	Regional control over critical technological systems
Societal model	Uneven resilience and differing levels of institutional trust	Commercialised and territorially unequal protection	Democratically governed and coordinated resilience	Universal culture of total defence and preparedness

TABLE 9 DIFFERENTIATION OF SCENARIOS BY MAIN THEMATIC AREAS.

SCENARIO

1

RELYING ON DISTANT FRIENDS

a world with a strong allied umbrella, but weak control over its own technological backbone

THIS IS AN IMAGE OF A REGION IN WHICH:

- security is based on a strong transatlantic NATO presence, rather than on the independent defence capabilities of the Baltic Sea states.
- the attempt to build technological sovereignty has failed, leaving the region dependent and forced to buy ready-made systemic and military solutions from the US and Asian countries.
- Baltic ports gain critical military and logistical importance, yet their key assets are owned by American and Chinese companies, giving external powers significant leverage over critical regional infrastructure.
- the region is divided into two speeds of trust: strong institutions and high trust in the north, growing polarisation and vulnerability to disinformation in the south and south-east.



PMESII SCENARIO DIMENSIONS

POLITICAL DIMENSION

By 2035, the BSR remains embedded in strengthened global security structures, with NATO and broader transatlantic cooperation regaining strategic relevance in response to persistent hybrid pressure from Russia and instability in the maritime domain. Following a renewed Russian offensive, the United States and NATO substantially increased their military support for Ukraine, preventing its defeat and eventually securing an armistice. By then, large-scale combat has ended, but no durable political settlement has been reached. Ukraine remains sovereign, while the stability of the armistice depends on continued American military assistance, intelligence and security guarantees. Russia continues its confrontation with the West through hybrid operations, including sabotage, cyberattacks, GPS interference, disinformation and shadow-fleet activity in the Baltic Sea. This outcome reinforces confidence in the transatlantic alliance but also demonstrates that European states remain unable to provide comparable security guarantees and critical military technologies without US support. Allied military presence in the BSR states remains high, while accelerated defence modernisation becomes both a security necessity and a political instrument used to maintain public legitimacy amid declining trust in public institutions.

Political cohesion across the region improves only selectively, as states differ in their approaches to energy security, industrial policy and relations with external powers. The growing influence of generative technologies deepens information manipulation, weakens public trust and increases pressure on governments to tighten regulations on digital platforms and strengthen cyber resilience, a move that meets resistance from influential political and business groups. Legal disputes intensify around maritime security, sanctions enforcement, shadow-fleet operations and the ownership of strategic port infrastructure. However, the region's ability to resolve these disputes independently remains constrained by its technological and economic dependence on the US and China. Expanding hybrid threats and sabotage incidents contribute to the securitisation of governance, strengthening actors advocating greater executive powers, military preparedness and broader surveillance capabilities.

ECONOMIC DIMENSION

The regional economy becomes increasingly shaped by security imperatives and technological dependence on external providers, particularly from the United States and China. Russia's growing isolation from Western markets further strengthens its strategic and economic alignment with China, deepening Russian dependence on Chinese finance and technology and increasing China's leverage

over supply chains and infrastructure relevant to the BSR. Despite ambitions for strategic autonomy, the slowdown of the energy transformation increases reliance on imported technologies, fuels and digital infrastructure. European efforts to develop sovereign AI, cloud and semiconductor ecosystems fail to achieve strategic scale. Defence spending and the modernisation of the armed forces are boosting certain sectors of the economy, particularly logistics, cybersecurity and the defence industry, thereby supporting GDP growth; however, most of the solutions are sourced from outside Europe. EU decision-making and regulatory processes remain relatively slow compared with the speed of technological change, limiting the ability of European institutions to respond rapidly to emerging dependencies.

The armistice in Ukraine opens a gradual reconstruction market for Baltic logistics, energy and digital companies, but the largest contracts and critical technological systems remain dominated by American and other non-European providers. At the same time, rising security expenditures limit investments in social policy and the green transition. Baltic ports are gaining strategic importance as dual-use infrastructure, linking trade, energy and military mobility, which means that assets owned by Chinese and American companies provide a rationale for the superpowers to pursue efforts to maintain security in the region. The absence of effective implementation of European preference mechanisms in public procurement limits the competitiveness of European suppliers in critical sectors and technologies. Businesses and public institutions significantly expand investment in cybersecurity and data protection, while border and coastal regions near Russia and Belarus face declining investment attractiveness due to heightened risk. Environmental monitoring benefits from EU and international cooperation, but restoration measures are implemented unevenly as rising defence expenditure constrains national investment and key monitoring technologies remain dependent on external providers. Offshore energy, military mobility and infrastructure protection intensify competition for maritime space. The Baltic Sea Action Plan is only partially implemented, and the overall ecological status of the sea remains poor.

MILITARY DIMENSION

High defence spending remains a long-term feature of the region, supported by public perceptions of persistent threats and the need to sustain NATO interoperability. The presence of allied forces, including brigade-level eFP structures, remains the foundation of deterrence in the BSR, building on NATO's post-2016 adaptation and the accession of Finland and Sweden. Continued support for Ukraine and the enforcement of the armistice further strengthen the role of US intelligence, air defence, logistics and command systems across the region. NATO programmes such as DIANA and the NATO Innovation Fund expand access to innovation, while the EU promotes strategic autonomy and European suppliers. Military modernisation accelerates, but capability gaps are closed mainly through acquisitions from the US and other non-European suppliers such as South Korea. Software, upgrades, spare parts and integration remain largely outside regional control. Tensions emerge between NATO interoperability and EU industrial preferences. States face a choice between rapidly acquiring proven non-European systems or investing in European alternatives that offer funding and industrial benefits but require longer implementation. The commands of the region's states retain formal agency, but their capacity to act depends on NATO standards, intelligence data, command systems, and allied service and logistics infrastructure. Military modernisation outpaces the development of industrial and maintenance capacity. The region's military security rests more on an external umbrella than on a full capacity to sustain a long conflict independently.

INFRASTRUCTURE DIMENSION

Baltic ports become critical dual-use infrastructure, combining military mobility, trade, energy transmission and crisis-response functions. Their strategic importance increases further as they become key nodes for military mobility, energy flows, reconstruction-related trade and global supply chains. Their protection, together with subsea cables and energy infrastructure, is increasingly coordinated through mechanisms such as Baltic Sentry, the EU Action Plan on Cable Security and the JEF. However, key technological components remain dependent on external providers, including American cloud services and non-European hardware. The implementation of directives such as NIS2 and tools limiting supplier-related risk improves cybersecurity, but the lack of an effective European preference in public procurement means that regulations strengthen procedural resilience without taking control over the technological core of the system. The successful synchronisation of Estonia, Latvia and Lithuania with the continental European electricity system in February 2025 ended the dependence of their electricity systems on the Russian-controlled IPS/UPS network. However, it did not eliminate vulnerabilities related to cross-border interconnectors, imported technologies, system balancing and the protection of critical energy infrastructure.

In 2028, a coordinated cyberattack combined with physical damage to key interconnectors causes temporary electricity shortages and a sharp increase in energy prices in the eastern part of the region. The crisis demonstrates that integration with the continental European electricity system is not sufficient without redundant connections, rapid repair capabilities, secure control systems and adequate generation reserves. Its consequences deepen dependence on supra-regional support mechanisms and external technology providers, while rising energy costs and uneven infrastructure investment exacerbate disparities along the eastern flank. Climate-related flooding and extreme weather add a further layer of physical risk, but adaptation remains uneven and concentrated around the most strategically important nodes.

SOCIAL DIMENSION

The prolonged confrontation between Russia and the West continues to shape public perceptions of security throughout the region. Continued hybrid attacks, cyber incidents, sabotage and maritime disruptions maintain a persistent sense of insecurity. Public support grows for collective defence, civil preparedness and critical infrastructure protection, inspired by approaches such as Finland's Comprehensive Security and Sweden's Total Defence concepts. Security becomes a central element of public policy and everyday life. At the same time, persistent security pressures strengthen a shared Baltic regional identity, including a growing perception of Poland as an integral part of the Baltic security community. However, societal resilience develops unevenly. Countries on the northern shores of the Baltic Sea generally maintain higher levels of institutional trust, stronger traditions of civic participation and greater confidence in public authorities. In contrast, parts of the southern and south-eastern BSR remain more exposed to political polarisation, distrust towards institutions and identity-based conflicts. Migration continues to address labour shortages and demographic decline. Following the armistice, some Ukrainians return to participate in reconstruction, while many remain permanently in BSR states, making Ukrainian communities a structural part of the region's societies and labour markets. Civil society remains active and internationally connected, particularly in areas such as humanitarian support, democratic participation and local resilience-building.

INFORMATION DIMENSION

Information issues become one of the most strategically significant domains in the BSR. Governments, international

organisations and private actors invest heavily in cybersecurity, information security and strategic communication. Despite these efforts, the region remains dependent on external technological ecosystems, as most advanced AI systems, cloud services, social media platforms and digital infrastructures are controlled by global providers outside the region. This provides access to innovation but limits strategic autonomy. Russia continues to treat the information domain as an important arena of competition. Influence operations increasingly focus on generating uncertainty, weakening trust, amplifying social tensions and exploiting existing political disagreements. Campaigns are increasingly synchronised with cyberattacks, GPS disruptions and incidents affecting critical infrastructure. The rapid spread of generative AI further transforms the information landscape. Deepfakes, synthetic audio, AI-generated local-language content and highly personalised influence campaigns become increasingly common. Although societies become more aware of information threats, awareness does not automatically translate into control. Information resilience improves gradually through media literacy initiatives, strategic communication efforts and regulatory frameworks such as the Digital Services Act and the AI Act, while NIS2 strengthens the cybersecurity of critical systems. However, these measures primarily strengthen the capacity to respond to threats rather than eliminate the structural dependence on external technological providers.

SCENARIO

2

SAFETY IS A BUSINESS

a world of regional mobilisation, in which security becomes a growth sector while protection becomes more transactional and unequal

THIS IS AN IMAGE OF A REGION IN WHICH:

- the region has come to rely more heavily on Nordic–Baltic formats such as NB8 and the JEF, while NATO remains an important but less cohesive and more transactional security umbrella and regional self-confidence hardens into security-driven, populist politics.
- two Baltics exist side by side: port metropolises booming with defence investment, while the borderland with Russia and Belarus turns into a shadow zone that no one wants to invest in.
- Denmark, Sweden and Norway are increasingly willing to use direct coercive measures against Russia's "shadow fleet": vessels are physically blocked, turned back and towed.
- the region builds one of the world's most advanced systems of information resilience, yet remains dependent on foreign AI systems, cloud infrastructure, and platforms, a strategic paradox: it can defend itself against hostile narratives, but does not fully control the technology through which they spread.



PMESII SCENARIO DIMENSIONS

POLITICAL DIMENSION

By 2035, weakening confidence in global institutions pushes the BSR towards stronger regional cooperation frameworks focused on pragmatic security coordination and the protection of shared strategic interests. The erosion of NATO's cohesion and the declining predictability of its allies are accompanied by a negative turn of events in Ukraine. The country is suffering a strategic defeat and is being forced to accept an agreement which leaves further territories under Russian control, curtails its military capabilities and fails to provide credible protection against renewed aggression. Ukraine remains formally sovereign; however, its process of accession to the EU and integration with countries of the region is being stalled. This increases the threat to the BSR due to Russia's growing political influence and the release of its financial and military resources. The possibility of a direct military confrontation with Russia becomes a central planning assumption, even if full-scale war is avoided. Across the BSR, this outcome further weakens confidence in global institutions and accelerates regional defence cooperation. Formats such as NB8 and the JEF assume greater roles in defence coordination and crisis management, while the CBSS focuses increasingly on civil security and infrastructure resilience. This produces a layered regional architecture rather than a single substitute for NATO: NB8 and the JEF form the Nordic–Baltic core, while Poland, Germany and other BSR actors participate through bilateral, mini-lateral and functional arrangements.

NATO remains important but becomes less politically cohesive and increasingly transactional. Stronger regional coordination gives the BSR states a more influential and coherent voice within the EU and, where possible, within NATO. Continued dependence on foreign defence systems, AI, cloud infrastructure and intelligence technologies turns security into one of the region's main areas of investment and economic growth. Public trust in national institutions stabilises at a relatively low level, creating fertile ground for populist and security-oriented political movements that build legitimacy through defence spending and promises of protection against hybrid threats. Persistent sabotage incidents, maritime provocations and disinformation campaigns fuel a gradual securitisation of politics and law, including expanded surveillance powers and stricter regulation of critical infrastructure ownership. The spread of generative technologies weakens the credibility of public communication and legal systems, forcing governments to introduce emergency mechanisms for digital authentication and information control. Regional states increasingly coordinate legal responses to sanctions circumvention, shadow-fleet activities and cyberattacks, even

when such actions stretch existing norms of international law.

ECONOMIC DIMENSION

The economy of the BSR becomes more regionally integrated but remains technologically dependent on external suppliers from the US and China, particularly in digital systems, AI tools, defence technologies and energy infrastructure. At the same time, the intensifying US–China rivalry contributes to the fragmentation of global supply chains. Traditional allies, such as the US, can impose economic and legal measures on individual countries by leveraging trade relations. Efforts to strengthen strategic autonomy through energy transformation continue, but progress remains uneven due to high costs, fragmented regulations and dependence on imported technologies. Defence modernisation and the expansion of dual-use infrastructure stimulate industrial growth in sectors such as shipbuilding, cybersecurity, logistics and ammunition production, creating new jobs and strengthening selected regional supply chains. Regional supply-chain policies stimulate industrial production, particularly in Poland and Sweden, strengthening their roles as regional production and defence-industrial hubs. Baltic ports evolve into heavily securitised strategic hubs combining military, energy and trade functions, increasing state involvement in ownership and investment decisions. At the same time, recurrent disruptions in maritime navigation, cyberattacks and hybrid incidents raise insurance, transport and infrastructure protection costs across the region. Ukraine's strategic defeat further increases the regional risk premium, as businesses expect continued Russian pressure and no longer assume that allied intervention will be automatic or sufficient. Economic development becomes increasingly uneven – metropolitan and coastal hubs linked to defence and logistics benefit from new investments, while border regions near Russia and Belarus experience declining attractiveness for foreign capital and advanced digital industries due to persistent geopolitical risk. Defence-related innovation increasingly spills over into civilian sectors, particularly through technologies developed for cybersecurity, maritime surveillance, autonomous systems and logistics.

MILITARY

The number of allied forces in the BSR stabilises and no longer grows in proportion to the scale of threats. Military preparedness expands through broader conscription and reserve systems across the region. Ukraine's strategic defeat allows Russia to redirect part of its military capacity towards the Baltic and increases pressure on the region's airspace, borders and maritime infrastructure. As global conflicts compete for attention and resources, regional states increasingly rely on pragmatic bilateral and regional defence arrangements. Military modernisation continues but remains uneven and driven by national priorities. Poland, Sweden and Finland strengthen deterrence, air defence, naval and logistical capabilities, while other states focus on territorial defence, cybersecurity, reconnaissance and critical infrastructure protection. Regional defence cooperation increasingly focuses on developing naval capabilities, maritime surveillance technologies and unmanned systems within the region. This reduces selected operational dependencies in surveillance, integration and maintenance, but core platforms, software and critical components remain largely externally sourced.

In 2029, an ageing and inadequately insured tanker linked to Russia's shadow fleet suffers a steering failure during severe GPS interference and runs aground near the Danish Straits, causing a major oil spill. The incident demonstrates that legal tools, inspections and diplomatic pressure are insufficient. Following the adoption of joint regional emergency rules, the coastguards and navies of

Denmark, Sweden and Norway begin to move from document checks to more direct measures: armed escort, turning high-risk vessels back and, where permitted under maritime law, detaining or towing them. By 2035, active control of maritime traffic has become a normal security practice. AI-based detection systems and unmanned platforms, previously developed within the framework of Baltic Sentry, are redirected towards tracking uninsured and high-risk vessels before they approach straits, ports, cables or energy infrastructure. This raises freight and insurance costs but gives the states of the region a greater sense of agency in their own waters, even though these actions trigger disputes over freedom of navigation and the limits of international law. NB8 cooperation becomes more structured and routinised, while the JEF takes on a larger operational role. Together, these formats perform some functions that had previously depended on a more cohesive NATO, but they do not replace NATO's collective-defence framework.

INFRASTRUCTURE DIMENSION

Repeated sabotage incidents, GPS disruptions, cyberattacks and shadow fleet activity make infrastructure protection a central regional priority. Following an adverse outcome for Ukraine, infrastructure along the eastern flank is treated as more exposed to military pressure, sabotage and deliberate disruption. Ports, straits, energy infrastructure and cable routes are increasingly monitored not only for military threats but also for environmental, financial and insurance-related risks. Following synchronisation with the European electricity grid, dependence on Russia declines, yet reliance on imported technologies, digital energy systems and interconnectors creates new vulnerabilities. States pursue different energy pathways, including offshore energy, LNG, nuclear power and storage solutions, reflecting national priorities rather than regional integration. Infrastructure therefore becomes more resilient physically but remains technologically dependent on external providers. Competition for ports, railways, terminals, grids and maintenance facilities intensifies as these assets must simultaneously support trade, energy, military mobility and crisis response. With dispersed responsibility and the relocation of new assets away from borderlands, areas along the borders with Russia and Belarus are the most exposed and, at the same time, the least protected. The lack of sovereign computing capacity and common cloud standards limits the ability of the region's states to create a single analytical layer for ports, cables, energy systems and shipping. Data is collected increasingly intensively, but processed through different systems, providers and procedures. The region sees more but does not always see together. Climate-related flooding and extreme weather reinforce the same territorial divide: major ports and wealthier municipalities can finance adaptation and redundancy, while peripheral areas face higher exposure and increasingly expensive protection.

SOCIAL DIMENSION

The BSR increasingly functions as a regional resilience community. While global institutions remain important, governments and societies place growing trust in Nordic–Baltic cooperation as the most effective framework for addressing security challenges. Trust therefore shifts away from global and some national institutions towards regional networks, municipalities, security agencies and organisations that provide visible protection. Influenced by Finnish, Swedish and Baltic resilience models, preparedness becomes a whole-of-society responsibility. Civil preparedness, volunteerism, media literacy, crisis response and infrastructure protection become mainstream public policy priorities. Municipalities, schools, NGOs and local communities are integrated into preparedness systems and cross-border networks, strengthening social resilience. Nevertheless, growing securitisation also increases

tensions between social groups and raises concerns about the distribution of responsibilities. Migration remains economically necessary but is managed through a security-oriented approach that prioritises integration, civic participation and resilience. Expanding military and reserve structures create additional pressure on labour markets, particularly in countries already experiencing demographic decline and labour shortages. Access to advanced preparedness services increasingly depends on the resources of municipalities, employers and households, producing strong protection in strategic hubs but weaker capabilities in peripheral regions. A stronger regional identity emerges, rooted in democratic values, preparedness and collective responsibility. A new wave of displacement from Ukraine increases pressure on housing, education and public services, while populist actors use disputes over the distribution of support to deepen social and political divisions. Large-scale demobilisation in Ukraine and Russia creates long-term challenges related to veterans' health, employment and social reintegration, as well as the cross-border circulation of weapons and military expertise. However, increasing securitisation generates concerns about surveillance, individual freedoms and growing inequalities between well-protected strategic hubs and more peripheral regions.

INFORMATION DIMENSION

By 2035, the BSR develops one of the world's most advanced systems of regional information resilience. Governments, cybersecurity agencies, universities, media regulators and civil society organisations cooperate closely to detect and counter disinformation and influence operations. Information resilience becomes an institutionalised component of regional security governance. An unfavourable outcome of the war for Ukraine becomes a central subject of influence operations portraying Western institutions as unreliable, further polarising debates over NATO, migration, defence expenditure and relations with Russia. Despite this progress, the region remains dependent on foreign AI systems, cloud infrastructures, digital platforms and cybersecurity tools, creating a strategic paradox: it can defend itself against hostile narratives but does not fully control the technological environment in which they spread. Generative AI accelerates the use of deepfakes, automated influence campaigns and synthetic content, yet common authentication standards, digital identity systems and coordinated fact-checking significantly reduce their effectiveness. Trust increasingly shifts from platforms towards verified institutions, experts and local information networks. Information literacy becomes a core educational priority across the region. Schools increasingly treat critical thinking, source verification, digital citizenship and AI literacy as fundamental civic competencies. The objective is to build long-term societal resilience against manipulation and cognitive warfare.

SCENARIO

3

PRAGMATIC RESILIENCE

a world of coordinated resilience, in which global cooperation is combined with growing European control over technology

THIS IS AN IMAGE OF A REGION IN WHICH:

- NATO and the EU act in a coordinated and complementary way, although frictions emerge between the EU and the US when Washington's interests collide with Europe's drive for self-sufficiency.
- EU regulations procurement and investment policies have driven the development of European technological ecosystems, substantially reducing exposure to external "kill switch" risks.
- the Baltic Sea becomes one of the first maritime areas in the world covered by an integrated, multi-layered network of autonomous monitoring: drones, sensors and satellites supported by AI.
- spending on defence and technological sovereignty stimulates modern industry but generates fiscal pressure and sparks social debates about territorial justice and the location of burdensome infrastructure.



PMESII SCENARIO DIMENSIONS

POLITICAL DIMENSION

By 2035, the BSR operates within a renewed framework of effective global cooperation, in which NATO, the EU and regional institutions act in a more coordinated and mutually complementary manner. Sustained coordination between NATO and the EU, combined with growing European defence production and continued transatlantic support, enabled Ukraine to achieve strategic success in its conflict with Russia. Large-scale warfare ended on terms that preserved Ukraine's sovereignty, military capabilities and freedom to pursue European integration, while preventing Russia from achieving its strategic objectives. This outcome strengthened confidence across the BSR in coordinated NATO–EU action and reduced the immediate risk of conventional military escalation. Countries in the region are now able to draw more freely on Ukrainian expertise and procure certain defence technologies. As anti-establishment populist forces remain electorally constrained, political cohesion among BSR states gradually strengthens around shared approaches to deterrence, energy security, digital resilience and policy towards Russia. Public trust in institutions stabilises or increases moderately as a result of greater transparency and visible improvements in security. The presence of allied troops in the Baltic states remains generally high, accompanied by major investments in European defence capabilities and interoperable regional security systems. The expansion of military and surveillance capabilities remains balanced by relatively strong democratic oversight and legal safeguards. Governments respond to generative technologies, cyber manipulation and economic fraud through coordinated international regulations and common authentication standards. Common European data infrastructures and interoperable databases become increasingly important for public services, including secure systems for medical information, professional qualifications and public administration. Persistent hybrid threats and disruptions to maritime traffic accelerate legal harmonisation within NATO and the EU concerning sanctions enforcement, critical infrastructure protection and the management of strategic assets such as ports, telecommunications and data infrastructure. Nevertheless, frictions persist when US strategic and industrial interests diverge from EU policies concerning defence procurement, technological sovereignty and digital regulation.

ECONOMIC DIMENSION

The BSR combines deep integration in global trade networks with a coordinated strategy for technological and energy sovereignty. However, continued integration with global trade networks leaves the region exposed to disruptions in global supply chains, particularly in sectors

where critical components and raw materials remain sourced outside Europe. Effective implementation of NIS2, the Cyber Resilience Act and AI-related regulations strengthen digital governance and resilience. EU Competitiveness Compass actions, including public procurement policies, increasingly strengthen European suppliers in strategic sectors. An accelerated energy transition and coordinated industrial policy support the development of European and regional technology ecosystems in the fields of cybersecurity, artificial intelligence (within a strictly defined scope), defence manufacturing and digital infrastructure. Ukraine's reconstruction and preliminary accession process expand the European market for energy, transport, digital and defence infrastructure, while Ukrainian companies become increasingly integrated into European industrial and technological consortia. Although cooperation with the US and Asian partners remain important from an economic perspective, dependence on external digital and defence technologies is decreasing as public and private investment strengthens local innovation capacity. Increased defence spending and military modernisation are stimulating economic growth, particularly in advanced manufacturing, the maritime industry and secure digital infrastructure, whilst placing pressure on public finances and competition for a skilled workforce. These pressures generate renewed disagreements over public spending priorities, particularly between defence, social policy, climate action and technological investment. Baltic ports are transforming into heavily protected dual-use centres, crucial for trade, energy distribution and military logistics, whilst oversight remains fragmented amongst various actors, including external military units. Persistent maritime and cyber threats continue to generate additional operational costs, yet improved regional coordination and resilient infrastructure mitigate the economic impact of disruptions and enhance the region's attractiveness for long-term strategic investment.

MILITARY DIMENSION

European defence capabilities increasingly form a stronger European pillar within NATO. At the same time, uncertainty over the long-term scope of US engagement encourages European states to prepare for a wider range of security responsibilities. The presence of allied forces on the eastern flank remains at a high level or increases periodically, accompanied by major investments in European defence capabilities and interoperable regional systems. The region gradually gains control over critical technological layers, including software, integration, data and updates, while remaining embedded in NATO and EU frameworks. The region benefits from allied presence, joint exercises and intelligence data, while at the same time, developing European and national capabilities intended to reduce the risk of an external technological "kill switch". Armed forces modernisation increasingly relies on European programmes, joint procurement and industrial consortia, covering air defence, artillery, unmanned systems and cyber defence. Ukrainian defence companies and military institutions participate in selected European programmes, while battlefield experience in drones, electronic warfare and distributed command systems is incorporated into regional doctrine and procurement. Autonomous technologies evolve from experimental deployments into a permanent layer of surveillance, infrastructure protection and command support. Following a series of incidents affecting maritime security and critical infrastructure, the Baltic Sea becomes one of Europe's first maritime areas covered by integrated autonomous monitoring networks. Defence spending stimulates advanced manufacturing and innovation but also creates fiscal pressure and competition for highly skilled personnel.

INFRASTRUCTURE DIMENSION

By 2035, stronger implementation of EU industrial and cybersecurity policies supports the development of

sovereign digital infrastructure, trusted cloud services and autonomous technologies. The Baltic Sea is covered by a multilayered early-warning system integrating drones, sensors, satellites and AI-supported traffic analysis. Ports evolve into highly protected dual-use hubs combining military mobility, trade and energy functions, although governance remains complex due to overlapping national, regional, EU and NATO responsibilities. Growing demand for computing power accelerates investment in data centres, which become recognised as critical infrastructure supporting administration, defence and cybersecurity. Interoperable European databases and trusted digital identities become increasingly common in public services, combining high standards of data protection with greater reliability and cross-border usability. Energy policy increasingly serves technological sovereignty: offshore energy, nuclear power, storage systems and transmission networks provide the foundation for digital infrastructure and autonomous systems. Accelerated investment in energy reduces dependence on external energy suppliers and strengthens the region's capacity to provide reliable energy for increasingly electricity-intensive digital infrastructure. The region develops capabilities not only to acquire technologies but also to maintain, repair, certify and integrate them within trusted European and transatlantic frameworks.

Repeated maritime incidents, including pollution events associated with high-risk shipping, bring environmental security into the same coordinated resilience framework as infrastructure protection. The 2029 oil spill turns environmental security into a major area of commercial activity. Governments and ports expand expand shared surveillance, spill-response and remediation capacity through HELCOM and EU mechanisms, increasingly using European sensing, satellite and autonomous systems. Regional risk mapping and mutual-assistance arrangements extend protection beyond high-value ports, shipping corridors to coastal communities, fisheries and vulnerable ecosystems. Environmental monitoring and restoration become more closely integrated with infrastructure planning, although tensions remain over costs, data governance and the territorial distribution of protection. Climate adaptation is incorporated into common infrastructure standards, so resilience planning addresses extreme weather alongside sabotage, cyber disruption and maritime accidents.

SOCIAL DIMENSION

The BSR benefits from a combination of renewed global cooperation and growing technological sovereignty. NATO, the EU and regional cooperation frameworks continue to provide security and stability, while stronger control over critical infrastructures increases societal confidence and a sense of agency. Public trust in institutions increases moderately, especially where citizens see visible improvements in crisis preparedness, digital security, energy resilience and protection of critical infrastructure. However, the expansion of AI-supported surveillance and border-management systems generates new societal debates over privacy, proportionality and democratic control. This leads civil society organisations and citizen movements to scrutinise the use of AI in border management, policing and public administration, creating pressure for stronger democratic oversight. The northern part of the region continues to benefit from higher levels of institutional trust and established whole-of-society security models. In the southern and south-eastern parts of the region political polarisation does not disappear, but stronger EU-level frameworks, more transparent digital governance and visible security investments reduce some of the vulnerabilities associated with distrust and fragmented or polarised public debate. As institutional trust and the visibility of effective public action improve, the electoral appeal of anti-establishment and populist forces

gradually weakens in parts of the region.. Migration remains important for demographic and economic stability, while Ukraine's reconstruction encourages partial returns and growing circular mobility between Ukraine and the BSR states. These movements are managed through coordinated systems supported by secure digital identities and increasingly interoperable public services. Civil society becomes more deeply integrated into resilience-building through education, preparedness, media literacy and democratic participation. Where these systems are transparent and accountable, visible improvements in digital and security services reinforce institutional confidence. Stronger European investment frameworks and more coordinated public procurement reduce the risk that technological transformation will benefit only the most advanced parts of the region. At the same time, debates emerge around the location of data centres, energy-intensive digital infrastructure and critical facilities, which create tensions between economic development, environmental sustainability and territorial equity.

INFORMATION DIMENSION

The BSR develops a more secure, regulated and democratically accountable information environment. Continued cooperation within NATO and the EU is complemented by greater technological sovereignty through European cloud services, cybersecurity tools, authentication systems and selected AI applications. While dependence on global technology providers does not disappear, public authorities gain greater control over the infrastructures supporting elections, administration, critical infrastructure and crisis communication. Russia and other hostile actors continue to use disinformation, cyber operations and synthetic media as tools of pressure. Narratives targeting Ukraine, NATO presence, migration, sanctions, energy policy and trust in democratic institutions remain persistent. However, the effectiveness of these operations is reduced by stronger institutional coordination, secure communication channels and more reliable authentication systems. Across the region, institutions and organisations increasingly benefit from the exchange of operational experience and intelligence, including knowledge gained whilst responding to persistent hybrid operations targeting critical infrastructure, public institutions and IT systems. The exchange of knowledge and experience involves both the BSR countries, which are particularly affected by hybrid pressure, and Ukraine. Common European standards for AI transparency, digital identity and platform accountability improve the ability to detect manipulation and verify information. Media literacy, AI literacy and digital citizenship become mainstream educational priorities, strengthening long-term societal resilience and contributing to a gradual improvement in trust towards institutions and information sources across the region.

SCENARIO

4

THE BALTIC FORTRESS

a world of regional self-sufficiency, in which control, resilience and security prevail over efficiency

THIS IS AN IMAGE OF A REGION IN WHICH:

- faced with a sharp reduction in US military presence in Europe and persistent limits on the EU's capacity to act quickly on hard security, the Baltic Sea states create their own permanent defence mechanism and a common military capabilities fund, with Poland and Sweden as industrial pillars.
- the green transition slows dramatically, as resources and funding are redirected towards power-supply resilience, reserves and local emergency sources, subordinating the market and climate to security requirements.
- the states of the region possess a high degree of information sovereignty — their own clouds and identity systems — which allows them, in moments of crisis, to introduce drastic emergency restrictions and force foreign platforms to identify the sources of synthetic content, botnets and coordinated influence operations.
- a strong, transnational Nordic–Baltic identity emerges, based on a culture of "total defence", where self-sufficiency, volunteerism, and resilience are embedded in the everyday life of every citizen.



PMESII SCENARIO DIMENSIONS

POLITICAL DIMENSION

By 2035, the BSR increasingly relies on tightly coordinated regional cooperation as confidence in the long-term reliability of broader transatlantic guarantees weakens. NATO cohesion weakens further and the US military presence in Europe declines. This shift builds on defence-industrial, technological and military capabilities developed by the states of the region while transatlantic support was still available. As broader allied assistance to Ukraine becomes less predictable, the Nordic and Baltic states, Poland and other regional partners use these existing capabilities to sustain Ukraine's defence. Ukraine remains sovereign and large-scale combat eventually ends, but neither side achieves a decisive victory and no durable political settlement is reached. A fragile armistice is maintained primarily through Ukrainian and regional deterrence rather than extensive US security guarantees. The outcome demonstrates that regional sovereignty can prevent Ukraine's defeat, but cannot fully replace the political, military and financial scale of broader transatlantic cooperation.

A number of serious hybrid incidents in the Baltic Sea increases public support for further strengthening regional self-sufficiency. The limited capacity and presence of allied forces push BSR states towards deeper political integration in defence planning, border security, cyber resilience and protection of critical infrastructure. At the same time, public trust in national institutions gradually improves as governments become more locally responsive and visibly focused on regional security and economic resilience. Regional political cohesion strengthens around a shared perception of threat from Russia and the need for strategic self-reliance, although this also contributes to the growing influence of security-oriented political actors and narratives centred on resilience and preparedness. The spread of generative technologies intensifies information warfare and economic fraud, leading governments to introduce stricter regional regulations concerning digital identity, online platforms and data sovereignty. Hybrid attacks, sabotage and maritime disruptions further accelerate the expansion of dual-use infrastructure and emergency governance mechanisms, while regional legal frameworks increasingly prioritise security and resilience over liberal market openness or environmental considerations. The growing prioritisation of security also creates tensions with established principles of international law and freedom of navigation, particularly in the Baltic Sea. Despite greater regional self-reliance, the BSR remains exposed to pressure from actors with substantially greater political, military and economic capabilities, particularly Russia, China and, increasingly, the United States.

ECONOMIC DIMENSION

The BSR pursues a strategy of regional technological sovereignty built on local industrial capacity, coordinated procurement and reduced dependence on external suppliers from the US and China. Although the pace of the energy transition slows down due to financial and technological constraints, regional states continue investing in resilient energy systems, defence industries, cybersecurity and sovereign digital infrastructure. Reduced allied military presence is partially offset by intensive national rearmament programmes and the development of regional defence production chains, supporting employment and industrial growth but increasing pressure on public budgets. Sustaining Ukraine and supplying the capabilities required to uphold the armistice place additional pressure on these production chains, making ammunition, repair facilities, air defence and unmanned systems permanent priorities of regional industrial policy.

The defence economy is supported by sustained public procurement, joint production programmes and demand for dual-use technologies, but this growth increasingly competes with civilian investment and contributes to a reallocation of public resources away from welfare and other policy areas. Baltic ports become central strategic assets controlled more directly by states and regional consortia, serving military logistics, energy security and trade continuity functions. Persistent hybrid threats, cyberattacks and maritime instability raise operating costs and weaken investment attractiveness in border areas near Russia and Belarus, while simultaneously driving demand for secure infrastructure and domestic technological solutions. Recurring supply crises linked to US–China rivalry disrupt access to technologies and critical components. Trade relations become more regionalised and selective, with a stronger preference for trusted political and economic partners, even at the cost of reduced efficiency and slower economic growth compared to globally integrated models.

MILITARY DIMENSION

The importance of supra-regional security structures declines as uncertainty surrounding US commitments and slow EU decision-making encourage BSR states to strengthen regional defence cooperation. The region compensates through intensive military modernisation and the development of regional defence production chains linking Nordic and Baltic states with Poland and other partners. Between 2027 and 2029, formats such as NB8 and the JEF expand cooperation in planning, exercises, infrastructure protection and crisis response. Growing Nordic–Baltic strategic capabilities also increase the region's influence over emerging Arctic transport routes and associated trade and security dynamics. By 2030, a permanent regional defence mechanism emerges, supported by a common capabilities fund focused on ammunition, cyber defence, unmanned systems, military mobility and the protection of subsea infrastructure. The growing emphasis on mobilisation and preparedness also contributes to the militarisation of public life, particularly through expanded reserve systems, civil-defence responsibilities and security-oriented education. By 2035, it coordinates long-term military assistance to Ukraine and supports the regional deterrence required to maintain the fragile armistice. Poland and Sweden become key industrial pillars. Regional mechanisms allow faster and more decisive responses than broader European decision-making structures. The region gains greater strategic agency and faster decision-making, but building sovereign capabilities remains costly and resource-intensive, requiring long-term investments in maintenance, production capacity, secure supply chains and specialised personnel. The weakening of US extended deterrence also stimulates renewed regional debate over how British and French nuclear forces might

contribute to a more European deterrence posture. Discussions focus on consultation mechanisms, conventional support, burden-sharing and the role of states such as Poland in wider European deterrence arrangements, rather than on creating an independent regional nuclear arsenal. The issue remains politically divisive and institutionally unresolved by 2035.

INFRASTRUCTURE DIMENSION

The BSR prioritises technological sovereignty and resilience over efficiency. Regional investment funds support the development of sovereign cloud services, cybersecurity systems, autonomous technologies and digital infrastructure. This path provides greater control but is more expensive and slower than using ready-made technologies from global leaders. The pace of the energy transition slows significantly, because resources are directed towards power-supply resilience rather than sustainable development. Priorities become supply stability, reserves, redundancy, grid protection, local emergency sources and infrastructure that enables the state to continue operating in a crisis. Market rules and environmental conditions are subordinated to security and the continuity of state functioning. Infrastructure projects are assessed primarily through the lens of resilience, control and the ability to sustain operations, and only then in terms of cost efficiency or environmental impact. Strategic infrastructure is increasingly located according to security needs rather than market logic, including in areas near the eastern border. Transport corridors, repair facilities, energy connections and logistics hubs supporting Ukraine are incorporated into this security-oriented infrastructure network. This reduces territorial vulnerabilities but increases costs and slows implementation, creating a visible "innovation tax" on public finances and other policy priorities. Environmental policy is increasingly subordinated to energy security, military infrastructure and continuity of essential services. Regional monitoring capacity is strong, although it is used primarily to protect strategic assets and detect spills, sabotage and maritime disruptions. Marine spatial planning gives priority to ports, cables, domestic energy generation and defence infrastructure, delaying some restoration measures and protected-area commitments. Adaptation focuses on hardening strategic assets against flooding and extreme weather, while ecosystem-based measures receive less funding where they conflict with military or energy priorities. Environmental degradation is increasingly tolerated as a cost of regional sovereignty and security.

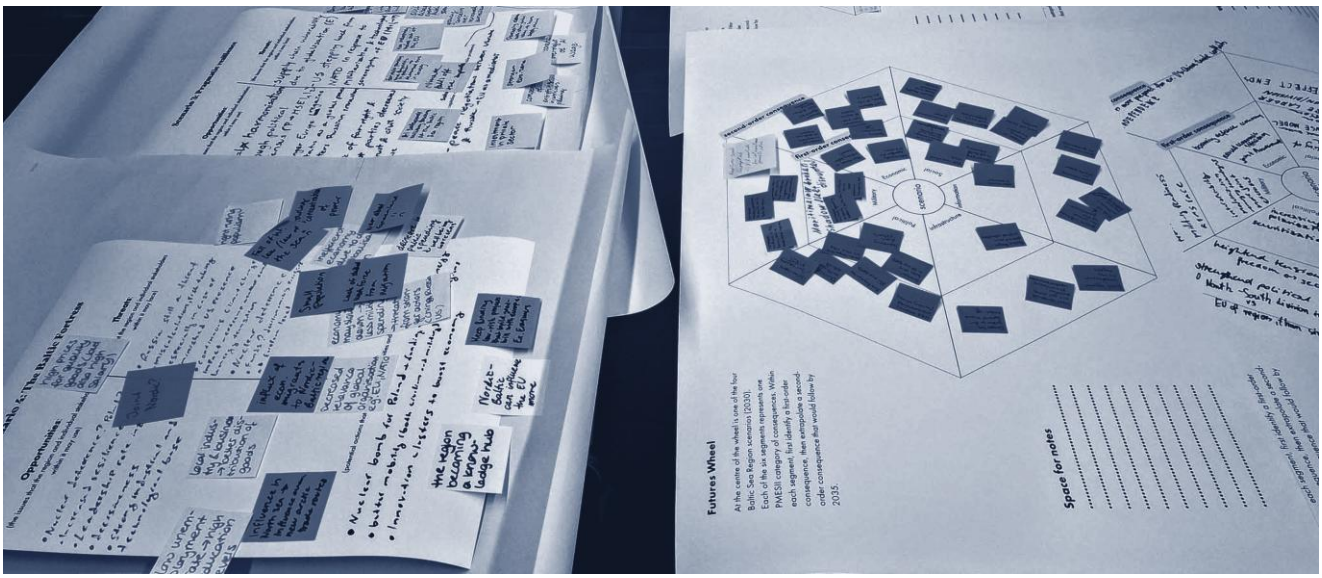
SOCIAL DIMENSION

Societies across the BSR increasingly organise around self-reliance, regional solidarity and preparedness. While cooperating with NATO and EU continues, governments place greater emphasis on strengthening local and regional capacities in energy, infrastructure, digital systems and civil protection. A distinct Nordic–Baltic identity emerges as a more important complement to national identities than before. Shared experiences of hybrid threats, infrastructure incidents, climate-related disruptions and geopolitical pressures strengthen social cohesion across the region. The expansion of state control over security, infrastructure, energy and strategic industries concentrates political and economic power in the hands of the executive and security institutions. Parliamentary scrutiny, independent oversight and institutional checks and balances are increasingly subordinated to the demand for rapid and coordinated action. Support for Ukraine becomes embedded in these systems through volunteer networks, training, medical assistance and long-term integration of Ukrainian communities, although the financial burden increasingly generates public debate. Growing labour shortages in defence, technology, infrastructure and manufacturing increase demand for skilled economic

migration, making migration policy an increasingly important component of regional economic security. Migration remains economically important but is managed through a more selective approach focused on integration, skills and social cohesion. The emphasis on resilience and self-sufficiency also generates new tensions. Debates increasingly focus on the environmental, social and financial costs of sovereignty, as well as on how its benefits should be distributed across societies and generations. Sustained defence and resilience spending increasingly competes with expenditure on healthcare, welfare and other public services, contributing to a gradual deterioration in some aspects of social provision.

INFORMATION DIMENSION

Information sovereignty becomes a defining feature of the BSR. Governments invest heavily in regional cloud systems, trusted AI, secure data centres and independent digital infrastructures, reducing dependence on external technology providers. Common regional standards for AI governance, cybersecurity and information security support closer cooperation between public institutions, researchers, media organisations and civil society. Polish and other BSR institutions form regional cybersecurity and threat-intelligence networks and cooperate with Ukrainian institutions to draw on relevant operational experience from the war. Information resilience becomes embedded throughout education and public policy. Following a major cyber and disinformation attack, governments introduce new crisis protocols and strengthen digital identity systems to secure critical services. In response, emergency restrictions on foreign social media platforms are introduced during crisis situations. Platforms are required to rapidly identify the sources of synthetic content, botnets and coordinated influence operations. Existing European Digital Identity Wallet standards provide part of the technical foundations for trusted connectivity in critical services and are supplemented by regional identity infrastructure. By 2035, trusted connectivity becomes a core principle of public administration and financial infrastructure, although debates intensify over privacy and digital freedoms. The Baltic Sea increasingly functions as a digitally monitored strategic space, with integrated situational-awareness systems supporting responses to hybrid threats, infrastructure incidents and environmental risks. Strong authentication systems, trusted digital infrastructures and coordinated responses reduce the effectiveness of external disinformation campaigns. However, growing control over data and digital systems creates new dilemmas concerning privacy, democratic oversight and the balance between security and civil liberties. The key challenge shifts from external technological dependence towards governing increasingly powerful sovereign information systems responsibly.



STUDENTS PROJECTS TO ADDRESS CHALLENGES OF THE FUTURE

During the YoPeNet Summer University, young professionals – students who had explored the scenarios further examined the opportunities and threats arising from them and sought to identify their potential implications. They also developed their own responses to the emerging challenges facing the region. Through group work, they developed seven projects that addressed identified problems and sought to capitalise on emerging opportunities, either directly or through more creative approaches.

One example of the solutions developed is the SafeObywatel app[66]. The objective of the project is to build and test a trusted municipal crisis-communication model that improves civil resilience and preparedness and can be replicated across the BSR. SafeObywatel is a metropolitan communication and preparedness system for the northern Poland's Tricity Metropolitan Area, addressing a gap in public security infrastructure, while complementing already existing systems: Alert RCB, 112, sirens, radio and municipal websites. Residents receive one coherent local picture: verified alerts, clear instructions, offline preparedness guidance and maps of shelters, hospitals and aid points. The system

[66] Authors: Aleksandra Kwiatkowska (aleksandra.kwiatkowska@sciencespo.fr); Alina Mingalieva (mingalieva.alina@wp.pl); Artur Oliinyk (a.oliinyk@outlook.com).

operates before, during and after a crisis, thus supporting preparation, real-time communication and recovery. Municipalities and responsible services jointly define authorised sources, publication procedures and response times. Citizen reports act as signals for verification, not as automatic public alerts to keep disinformation from spreading. The pilot starts small with essential local updates, offline content and maps, and multi-channel distribution, while more advanced features - location-sharing in emergencies, family check-ins and a guided information assistant - follow only after evaluation. Every non-essential function remains optional and user-configured to avoid overwhelming users with information. Success is measured through delivery time, reach, preparedness and public trust. Over time, developing common alert templates, terminology, and multilingual communication in the app allows different BSR municipalities to adopt the same model, and creates a transferable standard for stronger civil resilience and cooperation across the region.

Another example is The Baltic Maritime Defence Accelerator[67]. The objective of the accelerator would be to convert scattered BSR defence SMEs into bid-ready consortia via a challenge sprint and standing cluster for undersea infrastructure protection. It turns the BSR into the seabed-to-surface protection layer for NATO's eastern maritime flank. Repeated sabotage of subsea cables and pipelines (e.g Balticconnector, C-Lion1, Estlink 2) has exposed a capability gap in persistent maritime autonomous systems while the region's defence SMEs develop exactly this technology yet rarely scale. Barely 0.9% ever reach medium size, scattered across nine national markets. It links the threat to the talent through two mechanisms. A twice-yearly challenge sprint invites end-users (navies, coastguards, cable operators) to publish actual undersea-infrastructure problems; SMEs, start-ups and university labs compete, and winners receive a seed grant, a guaranteed test slot and a path to procurement. A standing industrial cluster then pools these firms into bid-ready consortia large enough to win EU and NATO contracts, aggregating demand so small states buy together. One regional "front door" replaces the maze of nine national systems and four EU programmes. The model needs no new fund because it stacks DIANA, EDF/EUDIS, EDIP and SAFE onto existing test infrastructure and proven regional firms. Defending the cables and pipelines that are the region's connective tissue makes Balticness a lived-in identity and resilience a common project.

Further projects addressed a range of issues, including migration, energy, cross-border cooperation, heritage, regional promotion, civil society development, crisis management, and residents' access to information:

---

[67] Authors: Simona Petrzilkova, Leonie Kristina Trebeljahr, Michal Tamerlan Bilinski.

- **Forging Balticness through Common Heritage** - a grant programme designed to make Balticness more visible and tangible by supporting mobile initiatives connecting communities across the BSR and beyond. The programme would focus on three pillars – 1) Youth, 2) Science and Literature, 3) Civil Society. It would support exchanges, joint cultural and educational activities, heritage research, media and literature, and other initiatives exploring the region's shared experiences and connections.
- **Anti-weaponisation of Migration** - a regional mechanism addressing the humanitarian and security consequences of the instrumentalisation of irregular migration as part of hybrid pressure on the EU by Belarus and Russia. The proposal combines mobile humanitarian teams and formal access and referral mechanisms with a Baltic Human Rights Observatory, which would independently monitor border conditions, maintain a shared evidence base and support transparent reporting, accountability and dialogue.
- **AMBER** - a regional application designed to strengthen individual, household and community preparedness across the whole BSR. It would provide emergency notifications, incident tracking, shelter and safe-route information, preparedness checklists and courses, with core functions available offline and a common interface across national systems. Beyond crisis response, it would promote everyday preparedness and contribute to a shared regional approach to civil resilience.
- **Powering Sovereignty** - a proposal for an integrated regional network of nuclear power plants, complemented by educational, social and environmental initiatives extending to 2045. The project approaches energy security as a component of regional resilience and sovereignty.
- **Baltic Security Transparency Initiative** - an initiative aimed at improving transparency, access to information and public understanding of security-related developments in the BSR.

The ideas behind the above solutions could form the basis for discussions on plans for the region. At the same time, the approach itself could serve as a starting point for other student and expert groups when working with the report.



RECOMMENDATIONS & STRATEGIC DILEMMAS

This report, based on a foresight approach, is not intended to provide ready-made solutions. Its purpose is to encourage reflection on the current and future position of the region's states and the relations between them within a changing geopolitical, economic, social and environmental landscape. Drawing on the experts' insights, we can highlight several key recommendations to be taken into account when formulating and implementing new policies:

- Time is a crucial resource. Rebuilding industrial capacity (e.g. shipyard repair facilities or a skilled workforce) takes considerably longer than increasing the presence of allied forces. Developing in-house technologies can take years, and without institutions with a clearly defined strategy, they may never be implemented for public use. There is never a good time for a crisis to strike, but it is always worth being prepared.
- The transition from strategy to practice is crucial if operational capabilities are to be tested (whether intentionally or not). The region's security will depend on tangible assets – such as dry docks or resilient digital systems – rather than merely on abstract strategic documents. At the same time, without consensus on strategy and political direction, actions may become so fragmented that they squander resources rather than building resilience.

- Cooperation driven by the threat should be harnessed. Although the current situation is undesirable for all countries in the region, the shared threat to critical infrastructure could act as a catalyst for deeper institutionalisation of cooperation and joint defence funding within the EU.
- The response to the restoration of relations with Russia needs to be considered. The prevailing view is that Russia (and Belarus as its extension) poses the main threat to the region. However, there is a possibility that other EU countries and those in the global West/North will seek to normalise trade and political relations if the war prolongs. In the long term, once the war in Ukraine has ended, it will be necessary to develop a new security framework, drawing lessons from the current situation.

However, the most important recommendation is to ensure that the following dilemmas are included on the agenda of forthcoming regional, cross-border, national and local strategic discussions:

01 **SECURITY GUARANTEES** or **STRATEGIC AUTONOMY**

How far should the region continue to rely on the US and NATO, and which capabilities must it be able to maintain independently?

02 **EUROPEAN INTEGRATION** or **REGIONAL SELF-RELIANCE**

Should security, energy and infrastructure resilience be developed primarily through NATO and the EU, or through permanent Baltic–Nordic–Polish mechanisms capable of operating when broader institutions lose cohesion?

03 **EFFICIENCY** or **REDUNDANCY**

How much economic efficiency should be sacrificed to create reserve generation, backup connections, repair capacity, strategic stocks and alternative technological systems?

04 **OPEN MARKETS** or **CONTROL OVER CRITICAL SYSTEMS**

Where should states limit foreign ownership, external cloud services and non-European technologies to retain control over ports, energy networks, data and defence systems?

05 MARITIME SECURITY or FREEDOM OF NAVIGATION

How far can the region go in intercepting, detaining or redirecting high-risk vessels without undermining international maritime law?

06 PREPAREDNESS or CIVIL LIBERTIES

How much surveillance, information control and emergency authority is acceptable when responding to sabotage, cyberattacks and generative disinformation?

07 PROTECTION FOR EVERYONE or PROTECTION OF STRATEGIC HUBS

Should scarce resources first secure ports, capitals, military corridors and energy systems, or provide comparable resilience to peripheral regions and vulnerable communities?

08 SECURITY or ENVIRONMENTAL RECOVERY

How should the region resolve conflicts between defence infrastructure, offshore energy, shipping, economic continuity and the ecological recovery of the Baltic Sea?

The scenarios do not identify a single expected or preferred future. Together, they show that the central challenge for the BSR is not simply to choose between global cooperation and regional sovereignty, but to decide which dependencies remain acceptable, which capabilities must be secured within the region, and which social, economic, democratic and environmental costs its states are prepared to bear. These decisions are already shaping the region's capacity to respond to the different futures described in this report.


YoPeNET
BALTICNESS