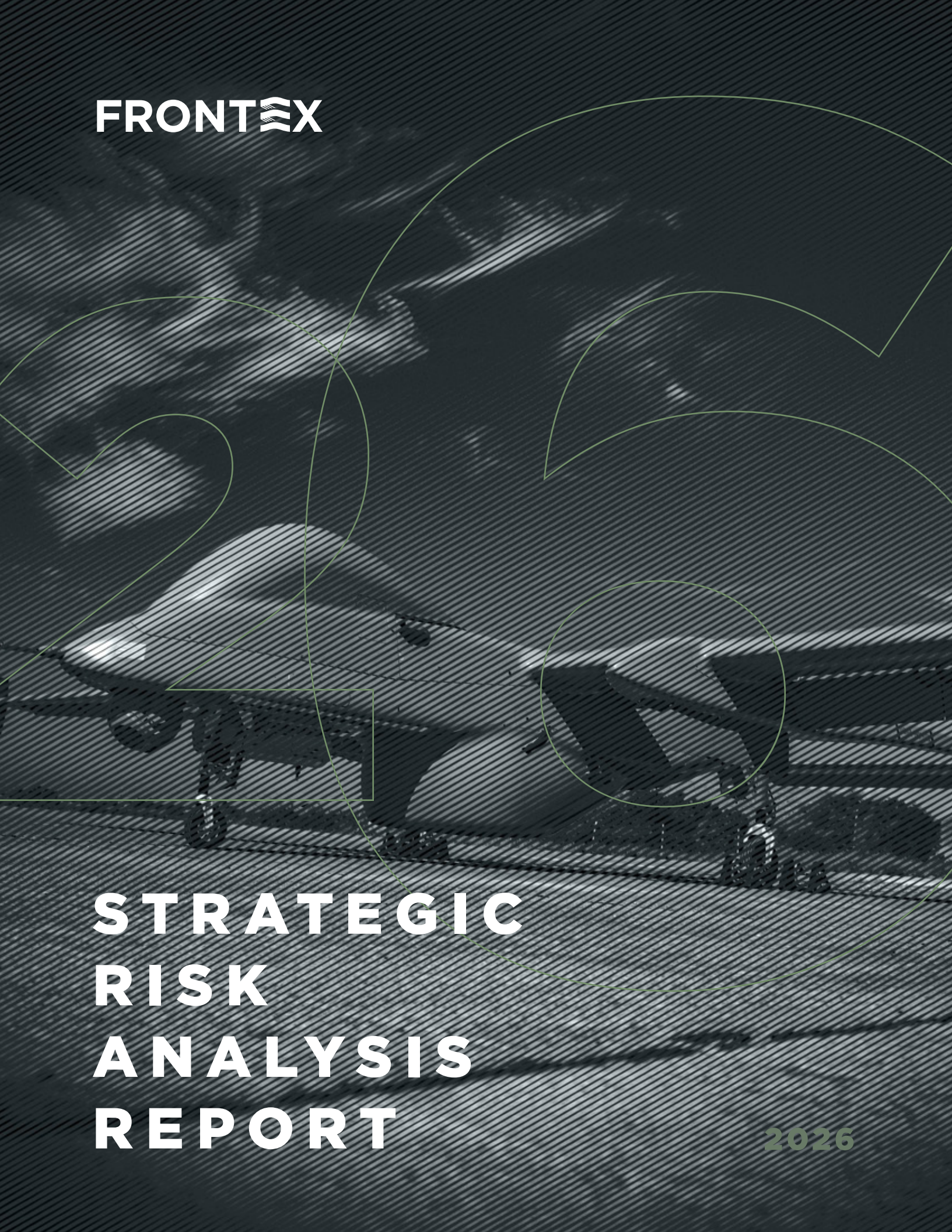
FRONTEX



STRATEGIC RISK ANALYSIS REPORT

2026

THE STRATEGIC RISK ANALYSIS 2026 REPORT was drafted with the support of the dedicated analytical network and benefited from the active involvement of the External Expert Group established for this purpose. The report also draws on valuable contributions from the Joint Research Centre (JRC), European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (EU-LISA), European Union Agency for Asylum (EUAA) and other relevant EU Agencies whose expertise and input were instrumental in shaping and the analysis presented in this report.

For the very first time the history Frontex's foresight report, high-ranking EU officials, Executive Directors as well as Frontex's Executive and Deputy Executive Directors were interviewed for the purposes of this report. This was of tremendous value and enabled reaching the conclusions and recommendations presented. Their involvement was anonymous, but the acknowledgement for their contribution is hereby hearty expressed.

Table of Contents

List of abbreviations 4

Foreword by the Executive Director 6

Executive summary 8

1. Megatrends implications assessment / Strategic Hexagon 11

1.1 The Strategic Hexagon 11
1.2 Megatrends — Strategic Hexagon components 12
1.2.1 Understanding Megatrends 12
1.2.2 Climate 12
1.2.3 Demography 14
1.2.4 Society 16
1.2.5 Economy 18
1.2.6 Technology 22
1.2.7 Geopolitics 24
1.3 Recommendations and areas requiring further exploration 27

2. Strategic Interviews 29

2.1 Methodological and conceptual framework 29
2.2 Analytical relationship between the strategic-interview conceptual themes and EIBM 30
2.3 Critical concerns-Institutional and governance constraints 31
2.4 Integration of the strategic-interview themes with the EIBM components 32
2.5 Positive and dystopic futures 36
2.6 Strategic priorities and stakeholder responsibilities 36
2.7 Key findings 37
3.1 Extreme geopolitical fragmentation and extreme individualism 39
3.2 High fragmentation and cohesive communities 41
3.3 Regional blocks (low fragmentation) and the sovereign individual 45
3.4 Low or no fragmentation and high communitarianism 49

4. Thematic Areas 52

4.1 Migration 52
4.1.1 Recommendations 53
4.2 Return Activities 53
4.3 Internal Security 58
4.3.1 Recommendations 58
4.4 Cross-Border Crime (CBC) 58
4.4.1 Recommendations 67
4.5 Terrorism 67
4.6 Hybrid Threats 69
4.6.1 Recommendations 72

5. Technological development. 74

5.1 Terrestrial and maritime autonomous Systems and Robotics 74
5.2 Air and Space-Based Surveillance 75
5.3 Artificial Intelligence — a Strategic Capability for Border Security 76
5.4 Quantum Technologies 78
5.5 Counter-Unmanned Aircraft Systems (C-UAS) 78
5.6 Secure and Resilient Communications 79
5.7 Digital Twins and Simulation Environments 79
5.8 Advanced Biometrics and Identity Intelligence 80
5.9 Cloud Sovereignty and Sovereign Computing Infrastructure 80

6. Conclusions 82

6.1 Strategic Environment and Megatrends 82
6.2 Key Findings from Strategic Interviews 82
6.3 Thematic Areas 83
6.3.1 Migration 83
6.3.2 Return Activities 83
6.3.3 Internal Security 84
6.3.4 Cross-Border Crime 84
6.3.5 Terrorism 84
6.3.6 Hybrid Threats 84
6.3.7 Cross-cutting pattern 85
6.4 Technology Foresight 85
6.5 Cross-Cutting Recommendations 85
6.6 Areas Identified for Further Exploration 86
6.7 final remarks 86

7. Recommendations 87

7.1 Border control 87
7.2 Search and rescue 87
7.3 Risk analysis 87
7.4 Cooperation between Member States supported and coordinated by the Agency 87
7.5 Inter-agency cooperation 88
7.6 Cooperation with third countries 88
7.7 Technical and operational measures within the Schengen area 88
7.8 Return 88
7.9 Use of state-of-the-art technology, including large-scale IT systems 89
7.10 Quality control mechanism 89
7.11 Solidarity mechanisms, in particular EU funding instruments 89
7.13 Fundamental rights 90
7.14 Education and training 90
7.15 Research and innovation 90

Endnotes 92

List of abbreviations

AI	Artificial Intelligence
AGI	Artificial General Intelligence
AMIF	Asylum, Migration and Integration Fund
ANI	Narrow Artificial Intelligence
ASEAN	Association of Southeast Asian Nations
ASV	Autonomous Service Vessels
AU	African Union
BCP	Border-Crossing Point
BIS	Bank for International Settlements
BMVI	Border Management and Visa Instrument
BRI	China's Belt and Road Initiative
BRICS	Brazil, Russia, India, China and South Africa
BVLOS	Beyond Visual Line Of Sight
CBC	Cross-Border Crime
CBC-RAN	Frontex's Cross-Border Crime Risk Analysis Network
CCTV	Closed-Circuit Television
CJTF-OIR	Combined Joint Task Force — Operation Inherent Resolve
CPU	Central Processing Units
C-UAS	Counter-Unmanned Aircraft Systems
DDoS	Distributed Denial Of Service
EBCG	European Border and Coast Guard
eBL	Electronic Bill Of Lading
ECRIS-TCN	European Criminal Records Information System — Third Country Nationals
EES	Entry/Exit System
EIBM	European Integrated Border Management
EO	Earth observation
ETIAS	European Travel Information and Authorisation System
EU	European Union
EUAA	European Union Agency for Asylum
EUCA	EU Customs Authority
EUISS	European Union Institute for Security Studies
eu-LISA	European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice
EUR	Euro
EURODAC	European Dactyloscopy (the EU's biometric database)
EuroHPC	European High-Performance Computing
Europol	European Union Agency for Law Enforcement Cooperation
EuroQCI	European Quantum Communication Infrastructure
Frontex	European Border and Coast Guard Agency
GCC	Gulf Cooperation Council

GDP	Gross Domestic Product
GDPR	General Data Protection Regulation
GNSS	Global Navigation Satellite Systems
GOVSATCOM	Governmental Satellite Communications
GPS	Global Positioning System
GPU	Graphics Processing Units
HAPS	High-Altitude Pseudo-Satellites
HPC	High-Performance Computing
IBM	Integrated Border Management
ICT	Information And Communication Technology
ID	Identity
IRIS²	Infrastructure for Resilience, Interconnectivity and Security by Satellite
IS	Islamic State
'Islamic NATO'	Trilateral security arrangement signed by Saudi Arabia, Pakistan and Turkey
IT	Information Technology
IEA	International Energy Agency
IMEC	India-Middle East-Europe Economic Corridor
JIT-CP	Joint Investigation Teams Collaboration Platform
LLM	Large Language Model
LNG	Liquified Natural Gas
MDMA	3,4-methylenedioxymethamphetamine (ecstasy)
MS	Member State of the European Union
NATO	North Atlantic Treaty Organization
NGO	Non-governmental organisation
NPS	New Psychoactive Substances
OCG	Organised Criminal Group
OSNMA	Open Service Navigation Message Authentication
PQC	Post-Quantum Cryptography
QKD	Quantum Key Distribution
R&D	Research and Development
SaaS	Smuggling as a Service
SAR	Search and Rescue
SCO	Shanghai Cooperation Organisation
SIS	Schengen Information System
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TEN-T	Trans-European Transport Network
THB	Trafficking in Human Beings
UAS	Unmanned Aircraft System
UAV	Unmanned Aerial Vehicle
UCDP	Uppsala Conflict Data Program
UGV	Unmanned Ground Vehicle
UNODC	UN Office on Drugs and Crime
US	United States of America
USD	US dollar
UUV	Unmanned Underwater Vehicle
VAT	Value-Added Tax
VHR	Very High Resolution
VIS	Visa Information System
VUCA	Volatility, Uncertainty, Complexity and Ambiguity

Foreword by the Executive Director



Ten years ago, this autumn, Frontex became the European Border and Coast Guard Agency. If you had asked anyone in the Agency then to describe the external borders of the EU in 2026, I doubt they would have predicted weather balloons used to smuggle cigarettes across a land border, low-flying drones carrying drugs across a sea border to evade radar, or a pandemic that brought free movement in Europe to a halt within days. Nor, I suspect, a full-scale war a few hours' drive from this office.

The lesson is not that the past decade was unusually turbulent, although it was. It is that the next decade will not resemble the present either, and that the threats we have already seen are a poor guide to the ones we have yet to encounter.

That is why Frontex produces this report. Our Annual Risk Analysis looks a year ahead: it is a forecast, built on what we see at the borders today. The Strategic Risk Analysis, published every other year, is an exercise in foresight. It asks what European Integrated Border Management will be facing a decade from now, and it is where the Union's multiannual strategic policy cycle for border management begins. Foresight is not prediction. The report takes the forces already at work, in the climate, in demography, in our economies and societies, in technology, and in geopolitics, examines how they interact, and describes the plausible futures they could produce.

A word on how to read it: Because it looks so far ahead, and because the academic and research community was involved in producing it by design, the report ranges further than Frontex usually does: into social policy, into migration management more broadly, and into political and economic dynamics that shape the border environment without themselves being border management. That breadth is deliberate, and it is not a claim to any of it as the Agency's business. The scenarios deserve a similar caution. Some of them are uncomfortable, which is the point: a scenario is neither a prediction nor a preference, but a way of testing whether a decision taken today still holds up in a future we would rather not see. In the same spirit, the recommendations are options for those who decide, not prescriptions from Frontex.

Three findings stand out for me.

First, pressure at the external borders will not ease over the coming decade; it will diversify. More people will be on the move, for more reasons, along more routes. Migration, cross-border crime, terrorism, and hybrid threats will increasingly overlap, interact, and amplify each other's impact. The Columbia University historian Adam Tooze has a word for this: polycrisis, meaning not simply several crises at once, but crises that interact until the whole is worse than the sum of its parts. Hostile actors understand this well. They have learned to combine instrumentalised migration, cyberattacks, disinformation, sabotage, and criminal groups acting as proxies, and we should expect them to keep doing so: in the Western Balkans, in Africa, and before long in the Arctic. The question for border management is not which of these will arrive but what, together, they will add up to.

Second, technology will change border work profoundly. Surveillance from the air and from space, artificial intelligence, and cloud infrastructure under European control are identified here as the investments with the greatest leverage, and I agree. But let me be precise about what technology can and cannot do. It can give an officer a better picture, earlier. It cannot take the decision, and it must not be allowed to. Every new technology described in this report comes with the same condition: people who understand it, can check it, and can work without it when it fails. Nor will it replace people. Europe will need more border guards in 2036 than it has today, and, as the report notes, an ageing continent will find it harder to recruit them. Training is not an add-on to the technology. It is what makes the technology worth having.

Third, and this is the finding I would ask every reader to take seriously, one of the most consequential risks to European Integrated Border Management over the coming decade is not external at all. It is the risk that Europe fragments: that Member States' systems fail to talk to one another, that national policies diverge until common operations become difficult, and that the cooperation on which everything else rests erodes from within. The report's answer, and I share it, is to spend the next decade integrating what Europe already has rather than simply adding to it: a system of systems, connected through shared planning, shared data, and interoperable tools, rather than a single command. European added value has to be demonstrated, not assumed.

That bears on the discussions now under way about the future of this Agency: its mandate, the size of its Standing Corps, and its resources. Those decisions are for the Commission to propose and for the Member States and the European Parliament to decide, and I will not pre-empt them here. But this report offers a useful test for whatever is decided. A larger Agency will be a stronger one only if it is also better connected: to the national authorities it supports, to its partner agencies, and to the information that turns a picture into a decision. It will also need to keep the standards, on fundamental rights and on data, that make that cooperation possible. Growth alone is not a strategy.

Foresight, finally, does not end with a report. Unless it reaches budgets, recruitment, procurement, and training, it changes nothing. We cannot be ready for everything. But we can be ready for the futures we judge most plausible, and we can make sure that the choices we take today do not close doors we may need open in 2036. I would rather prepare for a future that never arrives than be surprised by one that does.

HANS LEIJTENS
EXECUTIVE DIRECTOR
FRONTEX

Executive summary

The Strategic Risk Analysis (SRA) 2026 report envisages the challenges that the European Integrated Border Management (EIBM) might face over the next decade and formulates recommendations to optimise EIBM across its four tiers. It draws on a foresight assessment of the interacting megatrends (in line with the Strategic Hexagon approach), tvelve strategic interviews with senior EU stakeholders, six thematic risk areas, and a foresight review of the technological domain with impact on border management. The SRA 2026 constitutes the foundation for the policy document the EU Commission shall prepare developing a multiannual strategic policy for European integrated border management[1].

THE EXTERNAL ENVIRONMENT IN WHICH MIGRATION AND BORDER MANAGEMENT ARE TO BE MANAGED IS BECOMING MORE COMPLEX,

not so much because of new factors but due to the strong interplay of climate, demographic, economic, societal, technological and geopolitical pressures. A more competitive and less predictable geopolitical and security environment is increasing shifting operational responsibility for managing migration and border-related crisis to the EU and its Member States directly. **Internal EU fragmentation is one of the most consequential risks for EIBM in the coming period**: divergent national migration policies and competing interests might hinder an effective, Frontex-driven operational cooperation (including intelligence exchange) and resource sharing across the Schengen area.

The set of 12 **strategic interviews** performed at the highest level of border management for the benefit of the current report, indicate that **EIBM must be governed as a system of systems during the next decade** and integration of the existing systems and capabilities will matter more than organisational expansion. An anticipatory governance should be part of the policy cycle for EIBM and enhanced cooperation is needed between border, police, intelligence, cyber and defence actors to counter forthcoming hybrid threats.

Migration pressure is expected to diversify rather than stabilise with direct impact on staffing and the capacity of national authorities responsible for border control at Member State level. Structural drivers — population growth, urbanisation, climate change and military conflicts — are diversifying migration corridors, *modi operandi* and destination countries. Climate change further complicates capacity planning, as it might change the existing and open new unexpected routes (e.g. in the Arctic area). It also carries direct operational risks as climate emergencies might cause disruptions to logistics, supply chains and IT systems.

Importantly, these complex multifaceted pressures evolve in a strict funding ecosystem. The budgets allocated for border management both at EU (Frontex) and national level are limited by the structural weaknesses of the EU economy — external resource dependency, weak productivity growth, high public debt, an EU-wide investment gap in innovation and reduced strategic autonomy. **The increasing demand for border control, driven by the security megatrend**, might not be sufficiently matched by proportional funding increases, triggering an EIBM which is expected to do more with similar or reduced resources. This makes budget allocation for EU actors such as Frontex a priority for matching the operational capacity needed to face the forthcoming challenges.

RETURN IS AN OPERATIONALLY CHALLENGING PART OF EIBM, BUT IT WILL LIKELY IMPROVE IN THE COMING YEARS.

Return efficiency is currently limited by two operational bottlenecks: identification of individuals to be

returned and securing third-country cooperation on readmission, particularly with states whose nationals make up a large share of the irregular migration flows. Divergent national procedures, limited case-management interoperability and a growing number of unenforceable return decisions add up to the coordination burden. The new EU Return Regulation will reduce the fragmentation of the process if it is backed up by operational convergence and enforcement across the Member States.

CROSS-BORDER CRIME WILL BECOME MORE PROFESSIONALISED AND HARDER TO DETECT WITH THE CURRENT CAPACITY.

As the legal context tightens, the smuggling networks absorbing nearly all the irregular crossings will turn to more complex and professional modi operandi, using encrypted communication, cryptocurrency and possibly artificial intelligence to identify gaps and opportunities in the legal and physical systems deployed. **Firearms trafficking** is shifting toward smuggled components and 3D-prinded parts, undermining existing detection mechanisms which are built for complete weapons. The maritime trade is a known structural gap, which might deepen in the future as the volume of traffic increases. While containers account for an estimated 80—85% of drug seizures at EU ports, only 2—10% are physically inspected.

The threat stemming from terrorism remains primarily linked to conflict areas - with Africa remaining the epicentre of terrorist violence. Undetected crossings of individuals with terrorist ties at the EU's external borders will remain of concern for the internal security of the Union.

This requires the EU to ensure robust border protection and security, including systematic checks of all travellers against relevant databases at the external borders of the European Union, leveraging biometric data and other available technologies to prevent individuals posing a terrorist threat from entering and leaving EU territory undetected and thus enhance the overall security of the Union.

HYBRID ACTIVITY IS EXPECTED TO INTENSIFY AND WILL INCREASINGLY TEST THE EBCG MANDATE, NOT MERELY ITS CAPACITY.

Hostile actors will try to achieve their goals using tools such as instrumentalised migration, propaganda and disinformation, cyberattacks, sabotage and organised crime in a coordinated manner rather than in isolation. The pressure on the eastern borders is expected to continue, irrespective of how the current conflict in Ukraine unfolds. From this perspective, there are three areas that call for particular operational attention over the next decade: **the Western Balkans**, where crime groups could be used as proxies; **Africa**, where instability is linked to renewed migration pressure on the EU; and **the Arctic**, where melting ice is opening new maritime routes and exposing a new theatre of rivalry. Hybrid operations deliberately exploit a legal grey zone and EBCG needs clearer mandates, stronger inter-agency contingency planning for this area and regular joint exercises with EU and NATO structures built on better situational awareness and early warning indicators than crisis management responses.

TECHNOLOGY OFFERS THE EASIEST ROUTE TO CLOSING THE COMING CAPACITY GAP BUT ONLY IF IT IS DEPLOYED WITH RELIABLE HUMAN OVERSIGHT.

Nine technology domains were assessed as the highest-impact investments to be made in the coming decade, with air and space-based surveillance, artificial intelligence and cloud sovereignty carrying the most strategic leverage. Air and space-based surveillance is the most immediate operational priority for the next 10 years, since most other capabilities examined in this report, including autonomous systems, biometric checks and risk analysis, depend on the situational picture it provides. Artificial intelligence may help change EBCG's approach from reactive crisis management to proactive anticipatory action. However, every application considered here, ranging from surveillance procession to biometric matching and counter-drone classification, carries the same operational condition: it requires staff able to understand, verify and override the system's

output. Large scale IT systems, biometric databases and communications links are prime targets for cyberattacks, GNSS jamming and future decryption of currently encrypted data, making the forthcoming migration to post-quantum cryptography an operational priority for the next few years rather than a long-term one. None of this is deliverable in the border guarding environment without EU-controlled cloud and computing infrastructure, since every other technology investment ultimately depends on it.

THREE OPERATIONAL GAPS WERE IDENTIFIED ACROSS EVERY RISK AREA.

First, **cooperation with third countries** works reasonably well with willing partners but leaves hostile and uncooperative states outside meaningful operational engagement, thus weakening both return and anti-smuggling efforts. Second, **the Member State systems and data which are at present insufficiently interoperable** might become an obstacle to running EU-wide risk analysis and interpretation of the data for shared operational, EU-wide decisions in the future. Third, **legal and procedural frameworks continue to remain vulnerable to hybrid, digital and AI-enabled threats**, leaving operational grey areas, which hostile and criminal actors might at some point exploit.

THE 15 COMPONENTS OF EIBM[2] ARE OFTEN SEEN AND REFERRED TO AS A SINGLE INTERDEPENDENT SYSTEM AND SHOULD NOT BE SEEN INDIVIDUALLY IN THE FUTURE.

Likewise, the enforcement of each component is to be seen as a system of systems with perfect interoperability. The additional staff, assets or even legal mandate will have high operational impact only when connected through shared planning, logistics and information systems. The foreseen expansion of Frontex's Standing Corps to 30 000 staff will require a matching investment in the command structure and the data/information/intelligence component. Over the next decade, an anticipatory governance — foresight, risk analysis, horizon scanning — will bring operational value only if backed up by budgeting, recruitment, procurement and continuous training. While EIBM is likely to become more European-wide in day-to-day information sharing and operational efforts, the operational legal and political authority largely remains at national level. Thus, in the years to come, **the best strategy would be to strive for maximum interoperability rather than institutional convergence**." Five priorities for the next decade:

- Maximise the interoperability of SIS, EES, VIS and ETIAS so that information sharing keeps pace with the abovementioned fragmentation risk
- Prioritise investment in air and space-based surveillance, artificial intelligence and cloud sovereignty
- Consistent and full implementation of the EU Return Regulation, which embeds reintegration and interoperable case management
- Develop a coordinated 'Team Europe' approach to third countries, combining migration, development, trade and visa-policy levers instead of fragmented bilateral engagement
- Institutionalise anticipatory governance, stress-testing the resilience of border management against cyberattacks, infrastructure outages, migration surges or climate shocks, and making use of foresight, horizon scanning, data science, artificial intelligence and cyber-security expertise.

Taken together, these findings picture a decade in which EIBM will be less challenged by known and emerging threats. However, the existing VUCA context can generate challenges the EBCG community might face during the next decade but can successfully overcome integrating efficiently the fifteen EIBM components with the updated IT systems.

In the forthcoming period, the pressure of irregular migration, cross-border crime, terrorism and hybrid threats will increase or stay at similar levels at best. EIBM would be able to absorb these pressures while preserving both operational cohesion and public legitimacy only in a context of European unity and high interoperability of law-enforcement authorities responsible for border control.

1. Megatrends implications assessment / Strategic Hexagon

In a world marked by accelerating changes and major transformations, traditional frameworks and tools are becoming increasingly obsolete. The intensity, variety and velocity of changes in all the relevant sectors — from climate to society, from technology to geopolitics — suggests that the world is in a phase of transition, without much clarity on the end result.

This is where the Strategic Hexagon framework comes into play as a way to select and coordinate the main variables based on six dimensions — climate, demography, society, economy, technology and geopolitics — which can be subdivided into as many variables as are needed according to the topic under discussion[3].

1.1 THE STRATEGIC HEXAGON

According to the Strategic Hexagon concept, the combined effect of well-known megatrends is not linear or manageable through classic methods. To effectively apply the model and create scenarios that will deliver reliable and sustainable outputs, the institutions engaged in this exercise should understand how each megatrend and their interactions will affect European Integrated Border Management (EIBM) and how the scenario outputs can produce potential compound risks and feedback loops.

The Strategic Hexagon framework provides a structured way to understand and analyse the complex environment in which the European Border and Coast Guard (EBCG) operates. EIBM and the six interconnected dimensions under the Strategic Hexagon were analysed in the scenarios and various distinct challenges and opportunities were advanced: the rise of competitive and hostile multipolarity and large geopolitical blocs, the push towards strategic autonomy, the fragmentation of the international order, and the proliferation of hybrid threats such as the instrumentalisation of migration.

The global risk environment is characterised by a high degree of volatility, uncertainty, complexity and ambiguity (VUCA) that will most likely intensify in the context of potential future polycrises across all fields of human activity.

The current geopolitical shifts towards prioritising national interests in the Western Hemisphere and reducing its involvement in multilateral affairs increases the likelihood that the European Union (EU) will be expected to assume more responsibility, particularly in managing crises which impact the EU.

Internal political fragmentation within the EU due to competing national interests, differing migration policies and vulnerability to external manipulation was identified as a **major strategic risk, challenging the EU's ability to act cohesively**. This fragmentation might also negatively impact NATO unity and reduce the deterrent effect of the alliance.

In an emerging multipolar world, the growing world population and the growing middle class, urbanisation, influence of the Global South, climate change and environmental degradation, the changing nature of work, consumerism, socioeconomic inequalities, health issues, educational challenges, resource scarcity and geopolitical conflicts[4] will have a cumulative — and perhaps multiplicative — effect, **increasing the number of people on the move**. Over the next decade **advanced economies will continue to be popular destinations for economic migrants and asylum seekers**, especially from low-income countries in Africa and Asia. Emerging market economies will rapidly develop and gradually close the gap with advanced economies. Hence, they will also attract

international economic migration. The number of destination countries for international migrants will therefore increase and migration corridors will diversify. A side-effect of the global transformations will be the rising incidence of humanitarian and migration crises. This will require well-planned operational responses and protective measures.

The instrumentalisation of migration will be increasingly used as a tool for attaining political goals. Key components of it are hybrid threats to border and migration management, such as disinformation, misinformation, destabilisation campaigns and online propaganda, which polarise societies, undermine trust in border policies, and influence conflict dynamics.

1.2 MEGATRENDS—STRATEGIC HEXAGON COMPONENTS

Megatrends[5] are large-scale political, environmental, social, technological and economic trends and key drivers of change at the global level that are observable now, have been in progress for many years, and will most likely have a significant influence on the future. They are slow to form, but once in place are likely to last for a long time — typically for decades — and to profoundly influence a wide range of changes, activities, processes and perceptions in the economic, social, political, and natural environments.

1.2.1 UNDERSTANDING MEGATRENDS

To avoid strategic mistakes, it is necessary to make a distinction between the two main types of megatrends: 'closed' and 'open'. The fundamental variables of closed megatrends are fixed, while those of open megatrends can be changed. One of the most serious mistakes that scenario-builders can make is that of confusing the two — e.g. considering trends that can still be influenced as trends that are impossible to deflect.

Closed megatrends are so deeply embedded in the overall functioning of the world that the possibility of deflecting one of them is close to nil, although there occasionally are some rare possibilities of intervention.

On the other hand, open megatrends give room for manoeuvre: the decisions we make and the actions we take can divert the underlying processes in different directions.

Megatrends are often accompanied by secondary trends that move in the opposite direction. For example, the constant global growth of cities is accompanied by an opposite movement of flight from cities back to the countryside. While paying attention to countertrends can be valuable, what really matters is not to confuse one with the other, the dominant megatrends with the secondary countertrends that counteract the former's effects.

1.2.2 CLIMATE

Climate change has emerged as a structural global megatrend that intensifies resource competition, governance pressures and environmental stress, with cascading effects across demographic, economic and security domains. As extreme weather events, water scarcity[6] and sea level rise increasingly threaten urban and coastal regions[7], climate driven disruptions are projected to displace people, reshaping global mobility and placing sustained pressure on border management systems[8].

Divergent policy trajectories — exemplified by the EU's binding commitments under the Green Deal and the current US administration's expansion of fossil fuel extraction — further fragment international climate governance and weaken multilateral coordination. This widening regulatory asymmetry limits the effectiveness of global mitigation frameworks and heightens the operational, legal and humanitarian challenges associated with climate induced migration. Within the context of EIBM, climate change therefore constitutes a cross cutting driver of instability that demands coherent, forward looking strategies and strengthened international cooperation, as its impacts will increasingly shape migration patterns, border pressures and the broader security environment.

Climate change is an amplifier of existing migration pressures. Extreme weather events, such as floods and droughts, will increase the frequency and complexity of migratory movements which will impact EIBM in numerous ways.

Operational risks, including the degradation of logistics, supply chains and IT systems during climate emergencies must be taken into account. The possibility that new migration routes may open as conditions change in the Mediterranean or other border areas is high. Border management authorities will need to prepare for these shifts with flexible strategies and updated training, as operational impacts include pressure on border infrastructure, SAR and returns.

The long-term outlook for climate change will be full of contradictions: there will be progress in some areas and impediments in others. While green transition and renewable energy sources will gain significant momentum[9] the climate will continue changing, most likely leading overshooting the +1.5C limit set by the Paris Agreement. According to the International Energy Agency (IEA), nuclear energy will regain strategic importance in advanced economies, leading to increased production through 2030[10]. At the same time, the fossil fuel industry — especially in the US — will drive fossil extraction, production and consumption to record highs by 2035.

In the course of the next decade, global climate policy will be fragile, and implementation efforts will be affected by numerous developments (e.g., increased global energy demand by advanced economies, emerging economies and the AI industry, energy competition/security policies, economic crises, trade wars, conflicts)[11].

1.2.3 DEMOGRAPHY

Global demographic trends indicate that the world population will reach 9.7 billion by 2050[12], with growth concentrated in South Asia and sub Saharan Africa. These are regions where rapid population expansion intersects with limited economic opportunities and environmental stressors. This uneven demographic distribution is reshaping global economic power, intensifying resource scarcity and transforming social norms[13].

In the EU, demographic dynamics are marked by population aging, declining fertility, and persistent labour shortages, including in border management services, creating long term structural dependency on migration[14]. At the same time, youth bulges, unemployment, political instability and climate related pressures in origin countries act as strong push factors, while Europe's high living standards and social protections function as pull factors. Although economic development influences mobility patterns, migration flows are also shaped by cultural, political and skills based factors, particularly among highly qualified workers[15].

The estimated number of international migrants worldwide in mid-2024 was 304 million[16]. This figure has grown steadily since the beginning of the century, at more than double the pace (+75%) of the world population (+34%)[17]. EU Member States host about 21% of the total number of international migrants in the world (63 million). At the same time, 10% of the global migrant population originate from the 27 EU Member States.

The decline of export led growth is reshaping development trajectories. The model that enabled many lower income states to narrow income gaps over the past decades is becoming less viable due to the shrinking share of manufacturing in global GDP, declining industrial employment, and a broader retreat from trade globalisation. Simultaneously, productivity gains in agriculture in advanced economies risk further deteriorating the terms of trade for agricultural exporters in developing regions, while climate induced stress is expected to exacerbate vulnerabilities in their domestic agricultural sectors.

Parallel demographic shifts will impose additional structural pressures. Most countries will need to manage growth slowdowns; aging societies will face increasing fiscal demands for pension and healthcare systems; states experiencing youth bulges will confront heightened requirements for education financing and labour market absorption. Together, these dynamics signal a more constrained global development environment, in which traditional pathways to convergence are increasingly limited[18].

For EIBM, this demographic asymmetry generates both operational strain — fewer border guards facing higher migratory pressure — and strategic opportunities, notably through legal pathways, skills based migration frameworks and targeted talent programmes.



Addressing these challenges requires investment in automation, robotics, advanced risk analysis and legislative adaptation, alongside effective integration and reskilling programmes for migrants with the right to stay. Simultaneously, demographic decline in Europe may pressure governments to adjust fiscal policies to sustain pension and health systems, while demographic expansion in low income regions could heighten risks of civil unrest, radicalisation and irregular mobility, generating additional internal and external security pressures.

A comprehensive response will require coordinated measures, including EU wide family support policies, structured legal migration channels, technological innovation to compensate for workforce shortages and long term demographic planning aligned with migration management.

As the population ages, and even shrinks in the West, and the ability to use debt is limited, EU governments may come under pressure to raise taxes to maintain social programmes. Overall, the demography will place stress on labour markets, pension and health systems, and long-term economic viability. By contrast, concomitant growth in the youth populations in emerging markets and low development countries could create large influxes of migrants, increased radicalisation and civil unrest, as well as a greater likelihood for disruptive transnational movements. This could create both internal and external security pressures in the EU that will require greater investment and novel grassroots strategies to combat, including:





- EU-wide programmes that support increases in the birth rates of the European population;
- Targeted legal and talent-based migration programmes in countries of origin of migrants;
- Development and implementation of efficient robotics meant to compensate the work force shortage for basic responsibilities while the influx of workforce from third countries will be enclosed to a qualified labour force;
- Effective integration and reskilling programmes for migrants and refugees who have a right to stay in the EU.

1.2.4 SOCIETY

Societal changes, especially those derived from an aging continent and the collapse of the European welfare model, might affect political stability, social cohesion and the legitimacy of border policy. The societal aspects analysed reflected declining social cohesion, migration politicisation, institutional paralysis, vulnerability to pandemics and perception-driven pressure on EIBM.

IMMIGRATION HAS BECOME A DIVISIVE HOT ISSUE AROUND THE WORLD.

More restrictive immigration policies have been adopted around the world and additional countries characterised by emerging economies, such as Pakistan, India and South Africa are now following suit.

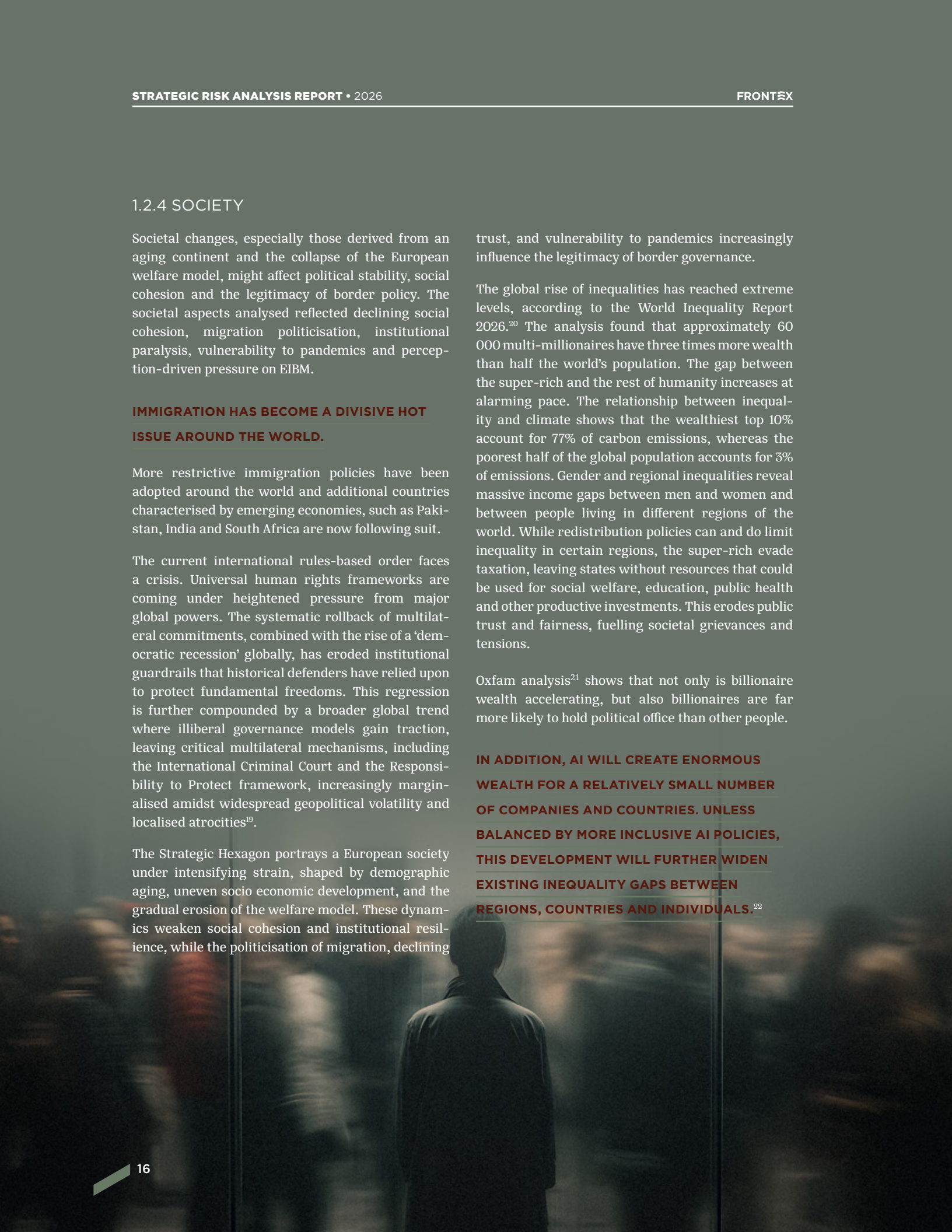
The current international rules-based order faces a crisis. Universal human rights frameworks are coming under heightened pressure from major global powers. The systematic rollback of multilateral commitments, combined with the rise of a 'democratic recession' globally, has eroded institutional guardrails that historical defenders have relied upon to protect fundamental freedoms. This regression is further compounded by a broader global trend where illiberal governance models gain traction, leaving critical multilateral mechanisms, including the International Criminal Court and the Responsibility to Protect framework, increasingly marginalised amidst widespread geopolitical volatility and localised atrocities[19].

The Strategic Hexagon portrays a European society under intensifying strain, shaped by demographic aging, uneven socio economic development, and the gradual erosion of the welfare model. These dynamics weaken social cohesion and institutional resilience, while the politicisation of migration, declining trust, and vulnerability to pandemics increasingly influence the legitimacy of border governance.

The global rise of inequalities has reached extreme levels, according to the World Inequality Report 2026.[20] The analysis found that approximately 60 000 multi-millionaires have three times more wealth than half the world's population. The gap between the super-rich and the rest of humanity increases at alarming pace. The relationship between inequality and climate shows that the wealthiest top 10% account for 77% of carbon emissions, whereas the poorest half of the global population accounts for 3% of emissions. Gender and regional inequalities reveal massive income gaps between men and women and between people living in different regions of the world. While redistribution policies can and do limit inequality in certain regions, the super-rich evade taxation, leaving states without resources that could be used for social welfare, education, public health and other productive investments. This erodes public trust and fairness, fuelling societal grievances and tensions.

Oxfam analysis[21] shows that not only is billionaire wealth accelerating, but also billionaires are far more likely to hold political office than other people.

IN ADDITION, AI WILL CREATE ENORMOUS WEALTH FOR A RELATIVELY SMALL NUMBER OF COMPANIES AND COUNTRIES. UNLESS BALANCED BY MORE INCLUSIVE AI POLICIES, THIS DEVELOPMENT WILL FURTHER WIDEN EXISTING INEQUALITY GAPS BETWEEN REGIONS, COUNTRIES AND INDIVIDUALS.[22]



Primarily a health hazard, pandemics add an additional layer of societal risk, threatening operational continuity at borders and requiring sustained investment in preparedness and health security protocols.

Against this backdrop, immigration politics has become a defining axis of political competition across advanced democracies — central to electoral outcomes in the United States and the United Kingdom, and a persistent source of polarisation within the EU. Restrictive approaches are now also adopted by emerging economies such as Pakistan, India and South Africa, signalling a global diffusion of securitised migration politics.

Within the EU, evolving asylum and protection frameworks reflect a complex geopolitical landscape, particularly regarding the strategic instrumentalisation of migration along the Union's external borders, forcing a delicate calibration between national security imperatives and established international protection norms. Concurrently, internal political discourse, particularly concerning the southern maritime borders, has increasingly integrated these migration challenges into broader debates over identity and governance. This domestic politicisation intersects with a documented narrowing of civic space across parts of Europe, characterised by institutional strains, the contestation of human rights frameworks and the destabilising effects of disinformation and advanced surveillance technologies on public opinion.

Hybrid threat activity increasingly relies on asymmetric warfare — specifically 'parity by subtraction' — where a state actor seeks to elevate its own geopolitical standing by systematically degrading the institutional credibility and moral authority of its counterparts. Rather than relying solely on conventional military capabilities, this approach integrates irregular tactics, psychological operations and cognitive operations to exploit vulnerabilities within democratic societies.[25]

Overall, rising polarisation, ideological fragmentation, and digital information dynamics shape public perceptions of migration and border policy. Disinformation campaigns undermine institutional legitimacy, cultural diversity presents both opportunity and challenge, and pandemics remain a structural vulnerability. For EIBM, integrating societal awareness into communication, training, and operational design is essential to sustaining resilience and public trust. The official communication frames AI governance as a moral imperative grounded in responsibility, transparency and the protection of the humans, calling for international accountability. To mitigate these hybrid threats and prevent internal political polarisation, a comprehensive and coordinated European response is increasingly important.

Addressing the artificial pressures exerted on the EU's external borders requires not only reinforcing localised border management but also expanding the Union's statecraft toolkit. Strengthening response capabilities through targeted diplomatic measures, calibrated economic sanctions, and the strategic adjustment of market access and technical cooperation will be vital to deter external manipulation. Ultimately, safeguarding the integrity of the Union's borders and its democratic institutions depend on establishing robust mechanisms that uphold the rule of law while effectively discouraging the political exploitation of displaced populations.

Rising polarisation, ideological fragmentation and digital information dynamics shape public perceptions of migration and border policy. Disinformation campaigns undermine institutional legitimacy, cultural diversity presents both opportunities and challenges, and pandemics remain a structural vulnerability. For EIBM, integrating societal awareness into communication, training and operational design is essential to sustaining resilience and public trust.

Border management strategies must consider the social context in which they operate and adapt communication, training and procedural frameworks accordingly.

To conclude, rising polarisation, conflicting ideologies and social media dynamics affect public perception of migration, pandemics remain a strategic risk, particularly in border environments, cultural diversity creates both opportunity and challenge for societal cohesion, and disinformation campaigns threaten social trust and institutional legitimacy.

1.2.5 ECONOMY

The global economic megatrend is characterised by **a profound redistribution of macroeconomic and geopolitical authority**. This has included a shift in global economic power from largely Western-led global organisations to regional players such as the E7 countries, mercantilism/protectionism, tax cuts and deficits, monetary pump-priming, more mergers and acquisitions, market distortions and a K-shaped economy where gains concentrate at the top[24].

In this environment, competing versions of capitalism could arise as well as an array of planned economies that could support new global winners in strategically relevant business sectors, including those directly linked to border security and management.

Global economic fragmentation is accelerating the emergence of competing capitalist models and renewed forms of state directed industrial policy, reshaping strategic sectors — including those relevant to border security and management. As states seek to secure economic advantage, increasingly complex supply chains face heightened exposure to cyber enabled espionage, intellectual property theft, and malicious disruption[25].

Complex supply chains seeking to maximise national economic advantages may become increasingly vulnerable to disruption by cyber networks engaged in industrial espionage, theft or terror-based disruptive activities[26]. These pressures are amplified by the emergence of a commodity and critical minerals supercycle, driven by the global energy transition, electrification, and the rapid expansion of clean technology manufacturing. Demand for lithium, cobalt, nickel, rare earth elements and other strategic minerals is projected to outpace supply, intensifying geopolitical competition, resource nationalism and the strategic weaponisation of mineral access.

This supercycle has direct implications for the EU, which remains heavily dependent on external suppliers for critical raw materials essential to its green and digital transitions[27].

Budget deficits, tariffs, immigration restrictions, labour shortages, extreme concentration of wealth in the top 1-5%, and heavy investment concentration in AI are all likely to act as brakes on economic growth[28]. For many developing economies, AI-related productivity gains are highly concentrated in a small professional elite, and the broader economy does not fully benefit from these innovations, which can ultimately limit overall growth.

The EU faces structural constraints including external resource dependency, weak productivity growth, aging demographics, low labour force and elevated public debt. As the relative weight of Western economies declines in a more multipolar system, the rebalancing of the global economy is likely to contribute to a further slowdown in the EU's economic growth.

The strategic role of international trade corridors, gateways and inland infrastructure in the global economy will increase considerably in the future. Huge infrastructural investments in Asia and Europe and large-scale transport projects such as the Trans-European Transport Network (TEN-T) and China's Belt and Road Initiative (BRI)[29], connecting Asia with Africa and Europe via land and maritime infrastructural networks, will not only dramatically change the socioeconomic landscape, but also will have border security implications. Major changes in international and European air, land and maritime mobility, trade and transportation infrastructure networks will most likely increase the pressures on the security of the EU's external borders.



The economic vulnerabilities within the EU have been analysed and it is suggested that there is a need for an annual investment of approximately EUR 750-800 billion to bridge the innovation gap, achieve decarbonisation and reduce strategic dependencies[30]. A 'pragmatic federalism' was proposed to foster deeper EU integration as a solution, though this approach faces notable political resistance. Ultimately, this ongoing political dynamic will significantly influence the EU's global competitive stance[31].

In an asymmetrical multipolar world where international rules are not followed and where the great powers assert their regional spheres of influence, multi-order[32] might also emerge out of necessity. This will influence global economic development and trends. Geoeconomic developments driven by the changing relations between the great powers, middle powers and other countries will likely lead to an intensification of cooperation in the context of international and regional alliances (e.g., SCO, BRICS, AU, ASEAN), parallel financial systems that bypass SWIFT, and a de-dollarisation trend (a possible weakening of the US dollar as the global reserve currency, national central banks increasingly buying gold).

The recent global de-dollarisation trend underscores the strategic need for the EU to pursue a more diversified and resilient monetary framework to safeguard economic stability. The European Central Bank has noted that central banks worldwide are increasing their gold reserves in response to China's accelerated gold accumulation and gradual shift from reliance on the US dollar[33]. This development is attributed to heightened geopolitical uncertainty and aligns with the findings from the Bank for International Settlements (BIS), which emphasises that geopolitical fragmentation is reshaping reserve management strategies and accelerating the search for alternatives to the dollar-dominated system[34].

In the context of increasing global competition between major powers, the EU has devised the India-Middle East-Europe Economic Corridor (IMEC). IMEC is perceived by the EU as a trade initiative to achieve a multipolar connectivity model. It could serve as a key pillar in the EU's pursuit of a strategic economy, fostering a diversified and resilient trade route that mitigates reliance on traditional maritime checkpoints[35]. As noted in a study by the European Union Institute for Security Studies (EUISS), although Saudi Arabia, the UAE, India and Israel recognise IMEC's potential for development and regional stability, they remain cautious about being subsumed into broader great-power rivalries and therefore continue to prioritise diversified strategic partnerships. By contrast, the EU and US view IMEC as a critical instrument for strengthening connectivity with South Asia and the Gulf in support of their wider geopolitical objectives, particularly the effort to counterbalance China's expanding regional influence[36].

Academic and policy analyses underscore that IMEC's European segment relies heavily on efficient Mediterranean entry points. In parallel, the economy can be a primary driver of migration. Migration is linked to economic needs, especially labour shortages. Individuals migrate to improve living standards, gain employment, or escape economic instability. The EU's demand for labour, particularly in care, construction and transport, reinforces these flows, and protection of economic infrastructure and integration of migrant labour are recurring themes. A coherent legal migration framework is needed to align border policy with labour market realities. There is a growing societal demand for clearer justification from states regarding how any resources for border management are deployed. Data-driven risk models offer the promise of greater efficiency and optimal resource allocation. However, these models must be designed to confront and mitigate inherent political and technical biases, requiring transparent audit trails to ensure their legitimacy.

Russia's armed aggression against Ukraine, the tensions in the Indo-Pacific, and the instability in the Middle East are driving a structural increase in defence spending and a reorientation of industrial policy towards dual-use and defence-related sectors. The militarisation of economies and the expansion of defence industries represent a significant economic megatrend with direct implications for EIBM. As global and regional powers increase their defence spending in response to geopolitical tensions, there is a reorientation of industrial policies towards dual use technologies and defence related sectors[37].

This trend influences the prioritisation of border security infrastructure and the deployment of advanced surveillance and monitoring systems. Consequently, EIBM strategies must adapt to incorporate these evolving security landscapes while ensuring that integration with civil and operational needs remains balanced and effective.

Global energy investment is shifting toward diversification as repeated supply shocks reshape risk perceptions, especially in Asia and the Middle East. By 2026, total investment is expected to reach USD 3.4 trillion, with USD 2.2 trillion flowing into clean energy and USD 1.2 trillion into fossil fuels. Oil spending is set to decline for a third year despite high prices, constrained by uncertainty, long project timelines and tight offshore rig markets. In contrast, natural gas investment is projected to rise to its highest level in a decade, driven by a surge of new LNG export projects[38].

Europe's dependence on external markets and resources is seen as a vulnerability. Therefore, protection of the EU single market, strategic sectors and supply chains is essential and strategic investment in key innovation sectors is encouraged. Economic resilience is also linked to technological capacity; therefore, investment in education, research and development, and sustainability supports both economic competitiveness and operational readiness in EIBM.

Economic growth is slowing globally, despite technological advances. Demographic pressures, climate disruptions and monetary policy limitations are contributing factors, so migration policy and EIBM planning should align with economic needs while safeguarding the EU's strategic interests.



THE ECONOMIC DIMENSION INCLUDES THE FOLLOWING PERSPECTIVES

COOPERATION BETWEEN MEMBER STATES

- Unevenly distributed migration pressures interacting with differential demographic and economic trends across the EU can fuel social tensions that challenge cooperation. Nevertheless, the political anchor for collaboration remains the shared benefit of a functioning single market;
- The key to a strong, unified EIBM framework is full-spectrum integration of technology and data standardisation among all Member States.

INTER-AGENCY COOPERATION

- Improved collaboration across agencies with different mandates will yield a direct public-safety dividend. The practical enablers for achieving this are the alignment of economic objectives and the interconnection of ICT systems and best practices.

COOPERATION AT EU LEVEL

- Harmonised legal and administrative procedures at EU level are expected to produce significant economic savings and enhance social cohesion. As with inter-agency cooperation, interoperable technology platforms are viewed as the most critical lever for achieving this harmonisation.

COOPERATION WITH THIRD COUNTRIES

- This cooperation is treated as both a strategic tool and a necessity. Establishing links with partner countries in addition to diaspora communities and pursuing joint projects in different areas addressing root causes of migration can help dampen irregular migration flows. However, this approach also creates risks of asymmetric pressure, where partner countries may 'weaponise' cooperation for political leverage. Current EU efforts to link financial aid and trade policies to secure cooperation from third countries on migration management and returns have yielded mixed results[39].



1.2.6 TECHNOLOGY

The transition from the current narrow artificial intelligence (ANI) to artificial general intelligence (AGI), which is expected to act more like an agent than a tool and will be able to re-write its own code as needed to achieve objectives, is the most significant technological competition between today's superpowers and the most complex challenge humanity has faced since preventing nuclear war.

The systematic development and sustainable use of emerging technologies (such as AI and nanotechnologies) are key to enhancing the competitiveness of the European economy, including sectors directly linked to border security and management. However, there are concerns that AI applications and intelligence automation could lead to enormous job losses, widening the inequality gap and causing a societal backlash, increase the power of governments and profit-driven corporations, potentially leading to abuses of power (e.g. mass surveillance, data misuses, propaganda). AI could also be used to create autonomous weapons, illegal firearms (e.g. 3D-printed) and cybercrime applications.

Excessive surveillance, if not properly governed, may undermine fundamental rights and data protection. Specifically, border management relies on advanced systems, but these systems are also targets for hybrid threats. Cybersecurity, data integrity and technological sovereignty are key areas of concern. Given the role of AI in identity management, risk analysis and surveillance, AI training needs, privacy concerns and the legal and ethical use of technology should be top priorities.

The AI race is fast advancing with massive governmental and private investments in computing power and infrastructure. The US AI Action Plan states that: 'whoever has the largest AI ecosystem will set global AI standards and reap broad economic and military benefits. An industrial revolution, an information revolution, and a renaissance — all at once[40].'

While the US and China remove all barriers on their quest for AI dominance, the EU is lagging behind in investment and development of top AI models, focussing more on regulatory frameworks and applications that will help develop its own AI ecosystem. In this fast-paced domain, the danger is that the top competitors might eventually reap tremendous benefits compared with the AI laggards. So, while AI promises unique opportunities for the EU to assert its geopolitical, technological, economic and military self-reliance, it also poses serious risks of falling behind and increasing its dependencies on these fronts. The EU's regulatory emphasis on quality, explainable and sovereign AI — including the EU AI Act — might have negative as well as positive consequences[41].

There is some scepticism, however, even among those at the frontline of this technological revolution, about the feasibility of actually realising the 'big prize' of AGI. In the course of the next decade, developments will show whether the global hype that drives massive investments and the AI competition was actually real and justified.



BRICS countries demonstrate that the incorporation of AI technologies into criminal investigations is a central factor in improving the effectiveness of investigative activities. This policy is implemented through legislative recognition of electronic data as admissible evidence and through the development of platforms designed to automate investigations and establish unified systems for managing electronic evidence. As information technologies continue to play a central role in criminal activity — especially cybercrime — the importance of digital tools in criminal proceedings will grow, reinforcing the need for expanded international cooperation among law-enforcement agencies.

The modernisation of criminal procedures across the BRICS countries highlights both the practical value and the broader need to adopt advanced digital technologies in criminal justice systems in other countries[42]. The Chinese have developed information networks that are open to government agencies but closed to outside influence. Among the BRICS countries, China is the most advanced in transitioning to a data-driven model of criminal justice, moving away from document-based procedures toward data-oriented investigative and analytical processes. The use of internet platforms and cloud storage systems for exchanging procedural documents between investigative bodies and courts has significantly reduced bureaucratic barriers and streamlined case handling, while enhancing access to information and protecting the procedural rights of participants. However, systemic challenges such as algorithmic discrimination and privacy, remain to be further handled

The EU lags behind other global actors in technological development[43]. Legal frameworks related to privacy and procurement create delays, and there is sometimes reliance on private-sector solutions. Frontex could be used as a test platform for EU-developed technology.

Interoperability is a critical lever for coordination, particularly in joint operations, data sharing and real-time monitoring.

The rapid technological cycles are outpacing public procurement processes, and this emerging AI arms race could have cascading effects across all EIBM pillars unless strong governance is developed from the outset (most advanced technology will under-deliver without deeper legal harmonisation, solidarity in financing and truly integrated databases —foundational governance areas that still lack concrete roadmaps).

Technological advancements, including long-endurance drones, constellation satellites, data analytics and the capability for remote payload drops (e.g., life vests), can significantly extend the coverage and effectiveness of SAR operations. However, criminals will be using the same commercially available tools to engage in illegal activities. As vendors will make new devices 'secure to the user', this will inhibit surveillance and evidence-gathering by intelligence and law enforcement organisations. The challenge for the latter will be to develop and adapt these tools at the speed of business — not the traditional speed of legacy governmental entities.



1.2.7 GEOPOLITICS

THE 21ST-CENTURY INTERNATIONAL SYSTEM IS COMPLEX AND STRUCTURALLY DIFFERENT FROM PREVIOUS ERAS.

It is marked by increasing instability, unpredictability, competition and changing of international perspectives.

The post-World War II model, based on an international order, is eroding and the world is moving towards competitive and hostile multipolarity. Regions and countries are divided in spheres of influence through great powers' diplomatic negotiations (overt and covert) and threats of the use of military force and the actual use of it. States are pursuing their own interests in an anarchic system through more volatile, shifting alliances. In this more overtly transactional order, great powers and middle powers operate within an asymmetric framework, with different capacities and abilities to shape outcomes.

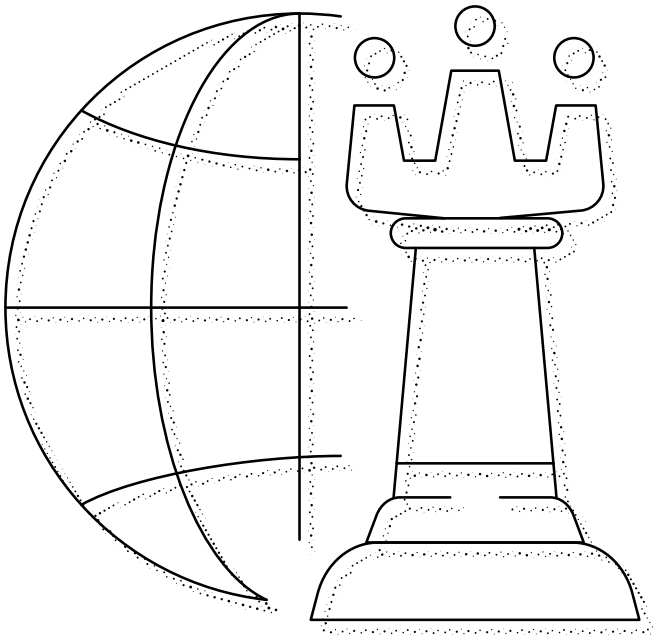
In this security paradigm shift, the methods of confrontation among global players are changing and expanding into all regions and possible theatres of operation (land, sea, space, cyber). These circumstances present serious challenges for EIBM, including the conspicuous one of navigating a world with potentially various border management regimes.

The geopolitical dimension includes increased unpredictability in global affairs, competition between superpowers and major powers, shift of power from the West to the East and from the North to the South, as well as from nation-states to private actors such as multinational/transnational companies, the rise of ad-hoc large geopolitical and geo-economic blocs, fragmentation of alliances, instrumentalisation of migration, and vulnerability to hybrid threats. These developments affect all levels of EIBM, including border control, return cooperation, risk analysis, international engagement and institutional cohesion.

Globally, the number of military conflicts is increasing, whether between states or within states between rival factions.

In 2025, the number of conflicts rose to 64[44], marking it the third consecutive year in which the Uppsala Conflict Data Program (UCDP) recorded a historically high number of conflicts[45]. This has led to the uncontrolled displacement of civilians and increased migration and refugee flows. Europe's security is marked by the ongoing war in Ukraine and hybrid threats to EU borders, leading the EU to take on greater defence responsibilities amid concerns over US commitment.

The Middle East is undergoing geopolitical realignment, with instability in Iran and ongoing conflicts in Iraq, Libya, Syria and Yemen contributing to regional instability despite Israel's military dominance[46]. The Iranian conflict has severely disrupted global energy flows by destabilising the Strait of Hormuz and damaging key extraction and processing facilities. These developments have transformed a previously stable supply environment into one marked by structural vulnerability, with the potential to shift global oil markets from surplus to deficit and intensify competition for LNG. The crisis highlights the systemic risks inherent in concentrated energy corridors and the long-term implications of infrastructure degradation[47].



At the same time, the Middle East crisis has diverted Western attention and key military assets away from Ukraine, while rising economic pressures have deepened political fragmentation within Europe. Collectively, these dynamics enhance Russia's resilience and reduce incentives for meaningful negotiations, increasing the likelihood of a prolonged conflict, potentially resulting in additional waves of refugees fleeing towards Europe and putting strain on EIBM. A sustained downturn in Gulf economies would adversely affect millions of foreign workers whose livelihoods depend on employment in Gulf Cooperation Council (GCC) states. Reduced remittances would exacerbate economic fragility in key origin countries such as Pakistan, Bangladesh, Egypt and Sudan, nationalities already prominent in irregular migration flows towards the EU.

Such deterioration could intensify outward mobility pressures, increase arrivals along the Central and Eastern Mediterranean routes, and further strain EU border management systems. Moreover, Israeli ground operations in Lebanon have strained the already worsened humanitarian situation there, which has resulted in more than one million people displaced internally and seeking refuge elsewhere, potentially the EU.

In Africa, major power competition for resources and ongoing conflicts are exacerbating humanitarian crises and migration towards Europe. As a result, the EU must navigate increased migration pressures, both external and internal. The African continent is facing large-scale open conflicts and internal and cross-border tensions that could escalate into military conflicts affecting the civilian population. At the same time, fierce competition for mineral resources in African countries is taking place between the US and Western countries on the one hand, and China and the Russian Federation on the other.

In its 2025 National Security Strategy[48] and 2026 National Defence Strategy[49], the current US administration introduced a reorientation of US foreign policy towards asymmetric multipolarity and a more transactional approach to international relations. This policy framework, emphasising US sovereignty, includes a strategic recalibration of arms transfers and a reassessment of US engagement with international organisations that are not aligned with its national interests. In this evolving context, the EU is regarded as a significant geopolitical entity with substantial regulatory influence. However, the US perspective, as outlined in these strategies, calls for a recalibration of the transatlantic relationship. It encourages European allies to enhance their defence capabilities and spending, with an emphasis on nation based cooperation rather than engagement through supranational EU institutions.

In sum, the US is advocating for a 'Europe of Nations' model, prompting the EU to navigate a diplomatic landscape where US bilateral relationships with individual Member States are prioritised. This approach aims to foster a balanced yet redefined partnership while respecting the distinct sovereignty of each nation.

In Asia, there are also tensions that could lead to large-scale conflicts, with East Asia now going through its most dangerous period since the Second World War. Notably, there is tension between China and Taiwan, a state supported by the US, the territorial dispute between China and Japan over Senkaku/Diaoyu Islands, and the rising diplomatic tensions between the two countries with regard to Taiwan, the South China Sea territorial and maritime conflict between China and neighbouring countries of Taiwan, Vietnam, the Philippines, Malaysia, Brunei and Indonesia, as well as the tension between India and Pakistan, which disputes the territory of Kashmir.

The situation in Afghanistan is also tense, with internal factions such as the Taliban — who took political power in 2021 after the withdrawal of US armed forces — and the Islamic State-Khorasan group, which has carried out large-scale attacks inside and outside Afghanistan, seriously undermining the Taliban's dominance and credibility.

In the Arctic region, President Trump's comments on Greenland, the gateway to the Arctic Ocean, have prompted a series of tough questions regarding Arctic security, transatlantic relations, and NATO unity. In the evolving landscape of global megatrends, the 2026 US intervention in Latin America can be assessed as a significant inflection that reconfigures geopolitical norms. It highlights a discernible shift towards a more unilateral and assertive US posture in the Western Hemisphere.

The regional ripple effects of the US's 2026 intervention in Venezuela will likely have long-term repercussions. The likely national, regional and systemic repercussions of the intervention extend beyond Venezuela, generating a constellation of security, migration and geopolitical effects with direct relevance to EIBM. The regional spillovers include heightened infighting among non-state actors, the rerouting of trafficking networks, refugees and asylum seekers from the countries affected by such interventions. It could also have long-term global repercussions for the Chinese-Russian de facto alliance. Russia abstained from criticising Washington's intervention in the hope of getting a better deal from the US on Ukraine, and it could also interpret it as retroactive legitimation of Russia's war of invasion in Ukraine. As for China, it could be tempted to proceed in a more or less similar way with regard to Taiwan.

Competition among the great powers is set to intensify in outer space, which has become a critical arena for strategic, technological, and commercial rivalry.

Space-based infrastructures, particularly large satellite constellations, now constitute essential national and private assets (US, China and Russia). Beyond Earth orbit, the Moon is emerging as a focal point for long term geopolitical competition. Its potential for resource extraction and the establishment of permanent bases positions lunar activity as a future determinant of technological and strategic advantage. States that secure early leadership in this domain will gain leverage in terrestrial power dynamics, given the dual use nature of space technologies and their implications for communications, navigation and military operations.

Great powers are developing advanced anti satellite capabilities — including high energy lasers, electronic warfare and cyber tools — reflecting the expectation that space will be a decisive theatre in any major conflict. This militarisation of space unfolds against a broader backdrop of global instability, marked by proliferating armed conflicts and systemic geopolitical uncertainty. Under these conditions, sustained or intensified population movements from conflict affected or high risk regions toward Europe remain highly likely[50].

International cooperation will be crucial for EU border management. As countries of origin or transit of migrants in the Global South see their GDP rising, they might be less and less inclined to work with the EU. Strained relations with key third countries of origin and transit will contribute to migratory flows as well as impede the return to their own countries of third country nationals who have no legal right to stay and are subject to return in accordance with EU and international law. Cooperation with third countries in the EU neighbourhood and beyond will also depend on how systematically the EU will work on migration and other thematic issues at the political and diplomatic level.

However, the combined effects of the geopolitical challenge of maintaining EU cohesion under external pressure, societal tensions arising from diverse national attitudes to migration, and uneven technological capabilities across EU Member States is identified as a major strategic risk potentially leading to internal political fragmentation within the EU. Competing national interests, differing migration policies and vulnerability to external manipulation may challenge the Union's ability to act cohesively and even lead to a possible de facto split between northern and southern European countries and/or western and eastern European countries. This fragmentation could impact NATO unity and reduce the effectiveness of border and security operations coordinated at EU level.

1.3 RECOMMENDATIONS AND AREAS REQUIRING FURTHER EXPLORATION

The harmonisation of border-related procedures, the interoperability of large-scale IT systems and the integration of advanced technologies are priorities for the EBCG community. This process will be a major consideration requiring adjustments of EU policies, such as promoting better integration of the EBCG within the EU's internal framework in upholding both the internal and external security of the EU.

BASED ON THESE CONSIDERATIONS, THE FOLLOWING RECOMMENDATIONS ARE TO BE CONSIDERED

- **Reinforce EU** unity and institutional cohesion in response to competitive and hostile multipolarity and internal political fragmentation (develop strategies to strengthen EU cohesion).
- **Prepare** for the increased instrumentalisation of migration by third countries (work on robust EU organisations to prevent hybrid destructive intervention).
- **Strengthen** pre-frontier knowledge to contribute to situational awareness and early warning mechanisms shared at EU level.
- **Reinforce** maritime and land border controls.
- **Strengthen** cooperation with third countries of origin and transit to improve migration governance, including on return and readmission while ensuring a balanced approach that combines effective migration management with respect for international law and humanitarian obligations.
- **Promote** capacity-building with origin and transit countries (invest in training and innovation).
- **Strengthen** the EBCG mandate, staffing, and optimizing its role within the overall EU security architecture. Pursue strategic autonomy in border management and reduce vulnerability to external influence, including legal, societal and technological dependencies (invest in innovation and technology).
- **Address** hybrid threats by linking migration, security and diplomatic strategy in a coordinated EU approach (design lean processes in the context of inter-agency cooperation).
- **Given** the stated intention to reinforce the EBCG by up to 30 000 staff over time — this will likely pose challenges for the organisation and operational activities of Standing Corps staff at the borders of the EU and in certain third countries.
- **Develop** adaptive migration policies that account for long-term climate impacts, demographic shifts and resource competition.
- **Align** border management procedures with economic and workforce needs, ensuring that skills and labour migration are integrated into EIBM planning.
- **Invest** in the resilience of border infrastructure, including contingency planning for natural disasters, pandemics and technological disruptions.
- **Promote** interoperable systems and shared standards across EU Member States to reduce operational inequality and increase efficiency.
- **Ensure** cybersecurity, system integrity and risk mitigation across all technology platforms used in border management.
- **Ever greater** integration of policy, operational and legal frameworks building upon the recently implemented Pact on Asylum and Migration, the Return Regulation, Scheval, the Interoperability Package and other legal and policy measures. Increase funding for European research and development in border-related technologies to close innovation gaps and reduce reliance on non-EU systems.
- **Use** technologic solutions to support EIBM, such as Digital Twin and others, including reliable and fundamental rights compliant surveillance tools.
- **Design** and implement a communication strategy tailored to both EU citizens and countries of origin to promote legal migration pathways and counteract misinformation.

- **Reframe** the strategic narrative of European Integrated Border Management (EIBM): The current 15-component framework for EIBM, while technically comprehensive, is ill-suited for high-level political communication. A clearer, more resonant mission statement should be developed to better articulate strategic objectives to policy-makers and the public.
- **Counterbalance** one-sided narratives that portray all international migration as a security threat.
- **Ensure** proportionality in technological deployment: Exercise strategic restraint in the deployment of new technologies. While state-of-the-art systems offer efficiency gains, their use must be critically assessed to prevent disproportionate surveillance ('Big Brother-style' control) and to ensure that 'rights-by-design' principles are embedded from the outset.
- **Develop** robust contingency and resilience plans: Prioritise the development of robust contingency plans and live stress tests for critical failure scenarios
- **Enhance** the resilience of border infrastructure, including contingency planning for natural disasters, pandemics and technological disruptions.
- **Conduct** a strategic review of border militarisation: Initiate a formal strategic reflection on the observable trend towards the militarisation of border control. A conscious and deliberate policy discussion is required to assess the long-term implications of this trend and determine its alignment with the EU's strategic objectives and fundamental values.
- **Further** develop a holistic migration management framework: Move towards a more holistic and integrated approach to migration management. This requires breaking down administrative silos to create a seamless policy framework that effectively connects initial border control procedures with the subsequent reception and successful integration of migrants and refugees.
- **Integrate** futures studies and scenario planning informed by complexity thinking into migratory policy and operational planning.



2. Strategic Interviews

This chapter offers a thematic synthesis of strategic foresight interviews with senior EU agency executives. The strategic interviews, aligned with the European Commission's multiannual policy for EIBM, examine the following domains — critical concerns, positive and dystopic futures, strategic priorities, and anticipatory governance requirements — through the 15 component architecture of Regulation (EU) 2019/1896.

Across a ten year horizon, stakeholders interviewed aim for a coherent integration of legislation and information for EIBM, from crisis driven adaptation to anticipatory governance, from data collection to decision relevant intelligence, from numerical growth to capability based planning, and from isolated border control to end to end migration and security management.

The most plausible future is one of asymmetric integration: technical and operational convergence will advance more rapidly than political or legal development. Sustainable EIBM will therefore depend on interoperable information systems, complementary EU-national capabilities, credible fundamental rights safeguards, institutional trust, and a foresight driven governance cycle linking analysis, resources and operations.

As a collective intelligence exercise, the interviews broaden the assessment of future border management risks. Rather than producing a single scenario, they map plausible, desirable and disruptive futures, expose uncertainties and assumptions, identify relevant stakeholders, and support current decisions oriented towards anticipatory governance.

2.1 METHODOLOGICAL AND CONCEPTUAL FRAMEWORK

Within strategic foresight, strategic interviews examine how decision-makers understand uncertainty, emerging risks, organisational constraints and possible futures. The strategic interviews are designed to alternate among positive and disruptive scenarios, historical data, current objectives and decision-making, revealing assumptions often hidden in conventional planning documents.

The exercise has connected objectives: mapping the operational and institutional environment; detecting weak signals and medium- to long-term drivers; contrasting desirable and dystopic outcomes; and linking those outcomes to stakeholders capable of action.

Two assumptions guide the analysis: first, the EU will continue to support a larger operational role for Frontex while requiring robust national capabilities and clear European-national complementarity. Second, operational readiness should be aligned with strategic foresight so that external-border protection remains consistent with security, fundamental rights, humanitarian principles and regional stability. The desirable condition is anticipatory governance supported by active strategic-risk management and institutional foresight capacity.

EIBM is therefore understood as a system: border control, risk analysis, information exchange, return, technology and fundamental rights cannot be assessed separately because each depends on the others.

2.2 ANALYTICAL RELATIONSHIP BETWEEN THE STRATEGIC-INTERVIEW CONCEPTUAL THEMES AND EIBM

Strategic-interview analytical domain	Central question	Principal EIBM relationship
CRITICAL CONCERNS	Which internal, external and global conditions could weaken strategic-risk management?	Risk analysis; information exchange; cooperation; technology; quality control; funding; skills.
POSITIVE OUTCOME	Which institutional and operational conditions define a desirable future?	All 15 components functioning as one coherent and trusted system.
DYSTOPIC OUTCOME	Which failures would signal loss of relevance, legitimacy and adaptability?	Fragmentation, reactive governance, data failure, capability weakness and rights-related loss of trust.
PRIORITIES AND STAKEHOLDERS	Which decisions are required now, and by whom?	Responsibilities across EU institutions, Member States, agencies, civil society, academia and industry.
ANTICIPATORY GOVERNANCE	How can foresight be embedded in routine management and policy implementation?	Policy-cycle integration, multiannual capability planning, preparedness, evaluation and institutional learning.



2.3 CRITICAL CONCERNS-INSTITUTIONAL AND GOVERNANCE CONSTRAINTS

The focus of the strategic interviews is on what keeps interviewees and EU leaders awake at night. It addresses concerns at three levels: internal institutional constraints, external ecosystem pressures and global strategic drivers. The dominant internal concern is that governance and planning remain better suited to administrative compliance than strategic adaptation.

Political cooperation is uneven. EU agencies and Member States are mutually dependent, yet their assumptions, incentives and planning timelines do not always fully align. European structures may therefore be expected to respond without sufficient knowledge of national capabilities.

The financial framework creates similar constraints. EU agencies have limited influence over the timing and structure of resources even as mandates and expectations change rapidly. Budget-led planning can obscure the effects to be delivered and the capabilities required; the interviews therefore favour value- and effects-based planning tied to strategic risk, operational need, capability gaps and measurable outcomes.

HUMAN RESOURCES, ORGANISATIONAL CULTURE AND INSTITUTIONAL RELEVANCE

Human resource quality is a major concern. Rapid growth can increase numbers without equivalent gains in expertise, coherence or performance. Recruitment that reproduces familiar profiles and assumptions limits adaptability; diversity in the staff background, professional experience and cognitive perspective strengthens it.

The future competence profile includes strategic foresight, intelligence analysis, artificial intelligence, cyber security, engineering, logistics, procurement, legal expertise, fundamental-rights knowledge, stakeholder engagement and leadership under uncertainty. These capabilities must be combined with accumulated experience through knowledge management, succession planning and reskilling, creating a future-ready workforce rather than replacing experience with novelty. EU agencies must convert data into specialised training, operational tools, common standards, analytical products, technology and direct support.

TECHNOLOGY, INFORMATION AND THE SPEED OF ADAPTATION

Technology is simultaneously an opportunity, dependency and threat. The interviews reflect on the importance of artificial intelligence, interoperable systems, and automation, but reject the view that technology constitutes a capability by itself. Staff, processes, data quality, legal authority, cyber resilience and ethical safeguards must develop alongside it. EU institutions need a reliable data-to-decision chain encompassing collection, validation, integration, analysis, dissemination, operational use and feedback. Cyber security is integral to this chain. As EIBM digitalises, the confidentiality, integrity and availability of information become operational requirements.

EXTERNAL AND GLOBAL DRIVERS

The external environment is increasingly volatile. Armed conflict, geopolitical realignment, pressure on the rules-based international order, climate change, poverty and economic instability shape migration, social cohesion and organised crime.

Criminal adaptation is often faster than institutional change. Organised crime exploits new technologies, legitimate commercial infrastructure, corruption and legal gaps, while the same forces that generate displacement and vulnerability can expand smuggling, trafficking and related criminal activity. EIBM must therefore connect directly with internal-security analysis rather than operate as a separate migration-management domain. Although European agencies lack control many root causes, they can improve detection, interpretation and preparedness.

2.4 INTEGRATION OF THE STRATEGIC-INTERVIEW THEMES WITH THE EIBM COMPONENTS

The 15 EIBM components form the legal architecture, but their effectiveness depends on one another. For analysis, they may be viewed through four functional layers: (i) operations and migration management; (ii) information, analysis and technology; (iii) governance, cooperation and solidarity; and (iv) assurance and future readiness. This grouping does not replace the legal components; it clarifies the dependencies required for EIBM to function as one system.

COMPONENT 1
BORDER CONTROL

The European Commission defines border control broadly: checks and surveillance, facilitation of legitimate travel, detection of cross-border crime, screening, identification of vulnerable persons and access to international protection. The interviews particularly **reinforce continuous situational awareness, intelligence-led deployment, rapid reaction, stronger identity and document controls, and closer links between border operations and crime prevention**.

COMPONENT 2
SEARCH AND RESCUE

Search-and-rescue obligations must be explicit in operational planning, training, asset specifications, standard operating procedures, coordination with rescue centres, fundamental-rights safeguards and evaluation. Treating search and rescue as incidental to surveillance would weaken both the legal completeness and legitimacy of EIBM.

COMPONENT 3
RISK ANALYSIS

Risk analysis is closely aligned across the interviews and the European Commission framework. It should combine operational data, strategic intelligence, weak-signal detection, quantitative forecasting, qualitative foresight and scenarios, while exploiting the distinctive European capacity to identify simultaneous developments across Member States and external-border sections.

The main weakness is the incomplete link from analysis to decision. Risk products may describe trends without altering capabilities, budgets, recruitment, deployments or partnerships. Anticipatory governance requires a closed cycle in which analysis identifies risk and effects, reveals capability gaps, triggers an accountable decision and is evaluated against operational results.

Risk analysis must also be end-to-end, integrating asylum outcomes, return, secondary movements, cross-border crime, cyber threats and relevant third-country developments. This would reduce blind spots before arrival and after admission or refusal.

COMPONENT 4
INFORMATION EXCHANGE

Information exchange is essential but remains fragmented across national authorities, EU systems and institutional networks. The main downside is that reporting may be manual, delayed or based on inconsistent definitions.

The objective should be a data-to-decision architecture, not merely technical interoperability. It should define common standards, access conditions, analytical responsibilities, timeliness, cyber-security controls, feedback to providers and operational use. Systems should be connected to improve timely decision-making.

COMPONENT 5

NATIONAL INTER-AGENCY COOPERATION

Centralised national EIBM governance involving border-control, return and other competent authorities. This is operationally important because border authorities, police, customs, asylum services and return bodies often use different planning methods, information systems and risk models, fragmenting the national picture and weakening European planning.

Functional specialisation should therefore operate within one national EIBM strategy, one integrated risk picture and clear interfaces. National coordination should align capability planning, contingencies, information exchange, training, funding and implementation monitoring, with return authorities fully included.

COMPONENT 6

COOPERATION AMONG EU ACTORS

The interviews favour a cooperation-driven European system in which institutions and agencies act as connected information hubs, service providers and centres of specialist expertise. Cooperation should cover joint risk analysis, shared data, common training, complementary operational support, research and technology, and structured links across border management, asylum, law enforcement, justice and information systems.

Clear mandates are required to prevent duplication and gaps, while joint products and operational arrangements should be routine rather than dependent on emergencies or crisis. Centres of excellence can support national delivery within a federated European operating environment.

COMPONENT 7

COOPERATION WITH THIRD COUNTRIES

The external dimension is a crucial aspect. EIBM will increasingly begin in countries of origin and transit through liaison networks, intelligence exchange, capacity building, anti-smuggling cooperation, return and readmission engagement, operational partnerships and cooperation with international organisations. The preventive aim is to understand and, where lawful and feasible, address risks before they reach the external border.

The principal risk is fragmentation between common European priorities and national bilateral relationships. Bilateral cooperation can add value, but competing arrangements may duplicate effort, create inconsistent incentives and reduce European situational awareness.

Return hubs, asylum processing arrangements and cooperation on readmission can foster a more coherent, efficient and effective implementation of EU returns policies. However, key issues in jurisdiction, protection standards, and operational sustainability must be thoroughly assessed and addressed. Also the need for coordination, coherence, complementarity and information-sharing to mitigate the aforementioned risks is essential.

COMPONENT 8

MEASURES WITHIN THE SCHENGEN AREA

External-border performance and Schengen resilience are interdependent. When Member States lack confidence in border management, information systems, asylum procedures, return or the handling of secondary movements, they are more likely to retain or reintroduce internal-border controls.

Stronger police and customs cooperation, more comprehensive utilisation of existing information systems and systematic analysis of secondary movements can provide alternatives. Credible external-border and post-entry management therefore strengthens mutual trust across Schengen.

COMPONENT 9

RETURN

Return is an area that could benefit from deeper integration. The European Commission highlights return as a core EIBM function, one that requires coordinated European and national capacity, effective third-country cooperation, a full suite of voluntary, forced return tools and reintegration implemented with full respect for fundamental rights.

Gaps include weak integration of return data into risk analysis, limited participation of return authorities in EIBM networks, incomplete information on national infrastructure and capability, lack of vulnerability assessment, fragmented return data and lack of return case digitalization. These weaknesses prevent a single operational picture linking entry, status determination, secondary movement and exit.

A mature model would integrate return into risk analysis, information exchange, national coordination, quality control, funding, third-country cooperation and fundamental-rights monitoring. Return is a shared responsibility.

COMPONENT 10

USE OF STATE-OF-THE-ART TECHNOLOGY

The interviews support advanced technology — including artificial intelligence, automated border-control tools, integrated sensors, large-scale information systems and digital administration — to strengthen capacity.

Greater dependency also increases exposure to cyberattack, manipulation and supplier risk. **Innovation must therefore be combined with human oversight**, legal and ethical assessment, fallback capacity, security-by-design, lifecycle maintenance and regular operational validation.

COMPONENT 11

QUALITY-CONTROL MECHANISMS

Quality control combines Schengen evaluation, vulnerability assessment and national mechanisms. The interviews support this architecture but call for performance measures beyond expenditure, staffing and equipment. Evaluation should test whether information was timely, capabilities were ready, European support complemented national structures, objectives were achieved and fundamental rights were respected.

Results from evaluation and preparedness assessment should shape funding, capability planning, training, organisational reform and future risk analysis. Scenario-based stress testing would add evidence on performance under compound crises, not only routine conditions.

COMPONENT 12

SOLIDARITY MECHANISMS AND EU FUNDING

The interviews reject budget-driven planning that designs activity around available resources rather than strategic effects, and they question expenditure that produces no distinctive European added value.

Funding should follow jointly identified risks and gaps, reinforce complementarity between national and European resources, cover enabling functions and lifecycle costs, and avoid duplication. Pooled assets, common technology, intelligence services or in-kind support may sometimes deliver more value than separate national grants.

COMPONENT 13

FUNDAMENTAL RIGHTS

Fundamental rights are an overarching component and a condition of institutional trust. The interviews emphasise legality, proportionality, professional standards, data protection and accountability; their negative scenarios associate misconduct, weak governance, serious data incidents or mandate overreach with loss of confidence.

Rights safeguards are therefore operational capability. Member States are more likely to share sensitive information, accept common assessments and rely on European deployments when authority is exercised lawfully. Safeguards should be embedded by design in risk analysis, technology, operational planning, return, third-country cooperation, training, command and evaluation.

COMPONENT 14
RESEARCH AND INNOVATION

Research and innovation should be linked to horizon scanning and operational need, anticipating technological, criminal and geopolitical change, testing solutions and supporting European technological autonomy.

The interviews favour stronger partnerships with academia, industry, civil society and specialist technology communities, including work on AI-supported analysis, autonomous systems, integrated sensors, advanced identity tools and new organisational models. The key challenge is moving from experimentation to sustainable capability through a pipeline connecting foresight, requirements, research, testing, legal and ethical assessment, procurement, deployment, training, maintenance and evaluation.

COMPONENT 15
EDUCATION AND TRAINING

Education and training are essential to converting organisational growth into professional capability. Common standards, specialised curricula, qualification frameworks and a European professional culture should support a broader profile combining operational border expertise with intelligence, data science, AI, cybersecurity, engineering, logistics, procurement, law, fundamental rights, stakeholder engagement and strategic foresight.

Training must be linked to workforce planning, certification, exercises, careers, succession and knowledge management. Institutions should recruit diverse backgrounds, retain experienced personnel and transfer knowledge systematically. Strategic foresight should form part of the competence framework for leaders and specialists, not remain confined to a small analytical unit.



2.5 POSITIVE AND DYSTOPIC FUTURES

Dimension	Positive future	Dystopic future
GOVERNANCE	Agile, accountable and connected to strategic effects.	Procedurally heavy, reactive and unable to provide direction.
INFORMATION	Common, trusted and decision-relevant operational picture.	Fragmented repositories, uneven data quality and cyber vulnerability.
CAPABILITIES	Specialised, ready, sustainable and complementary to national capacity.	Numerical growth without quality, logistics or operational integration.
COOPERATION	European mechanisms are the natural first source of cross-border support.	Bilateral arrangements and national safeguards replace common action.
RETURN AND MIGRATION CYCLE	Border, asylum, secondary-movement and return information are connected.	Entry is managed, but post-entry outcomes remain fragmented and ineffective.
LEGITIMACY	Fundamental rights and professional standards sustain trust.	Misconduct, opacity or data compromise undermine the licence to operate.

2.6 STRATEGIC PRIORITIES AND STAKEHOLDER RESPONSIBILITIES

The analysis identifies Frontex's core strategic function as generating a European integrated border management intelligence picture (composed of risk analysis, vulnerability assessment, operational data and results of Eurosur Fusion Services), supplying specialised capabilities, and coordinating cross border resources that cannot be efficiently replicated at national level. In genuinely transnational situations, the Agency should serve as the primary source of European operational support, knowledge and technology.

This role requires complementarity rather than substitution. Strong national systems remain indispensable, while the European layer should address collective gaps, simultaneous pressures, specialised technologies and upstream engagement. Effective capability planning must differentiate what is delivered nationally, through pooled EU capacity, or jointly with other EU actors. Budgets must therefore encompass assets, infrastructure, logistics, maintenance and digital systems, and staff frameworks should support field operations, specialist recruitment and mobility across the European Border and Coast Guard community.

Adequate consideration should be given to integrating Returns into the mandate of vulnerability assessment, so to improve capacity and readiness of MS across the whole EIBM spectrum.

The interviews confirm the Commission's EIBM architecture while demonstrating that its 15 components cannot function as isolated workstreams. Border control depends on risk analysis and information exchange; return on coordination, cooperation and rights safeguards; technology on research, training and cyber resilience; and funding on jointly identified capability gaps. **The strategic priority is therefore integration depth, not additional instruments**.

A coherent future model requires data to decision performance, disciplined capability planning, institutional trust and the conversion of foresight into action. The desirable configuration is multi level governance in which European and national actors operate from a shared strategic picture without necessitating full centralisation.

The dystopic alternative is formal comprehensiveness combined with practical fragmentation: bilateral responses, low value information systems, non-integrated return, organisational growth without capability, and governance or rights failures that erode cooperation. EIBM's decisive test is whether it can absorb geopolitical, migratory, technological and security shocks while maintaining coherence and legitimacy.

2.7 KEY FINDINGS

1. **EIBM MUST BE GOVERNED AS A SYSTEM OF SYSTEMS.**

   Its 15 components are mutually dependent and cannot be planned, financed or evaluated effectively in isolation.

2. **INTEGRATION DEPTH MATTERS MORE THAN ORGANISATIONAL EXPANSION.**

   Staff, assets and mandates create value only through common planning, specialist skills, logistics, information and clear operational roles.

3. **ANTICIPATORY GOVERNANCE MUST ENTER THE POLICY CYCLE.**

   Foresight is useful only when it changes budgets, recruitment, procurement, training, external partnerships and contingency planning.

4. **THE CORE INFORMATION CHALLENGE IS DATA-TO-DECISION PERFORMANCE.**

   The EU needs trusted, timely and integrated processes that convert data into shared decisions and operational feedback.

5. **RETURN, AS A CRUCIAL PART OF EIBM, SHOULD BE CONSIDERED UNDER JOINT EIBM GOVERNANCE AND ACTIVITIES WOULD BENEFIT FROM ENHANCED INTEGRATION.**

   It must be embedded in risk analysis, national governance, vulnerability assessment, capability planning, information exchange, funding and third-country strategy.

6. **TECHNICAL INTEGRATION WILL OUTPACE POLITICAL CENTRALISATION.**

   The systems will likely be increasingly European in information and operations while sensitive legal and political authority remains substantially national.

7. **HYBRID THREATS REQUIRE A BROADER SECURITY-RESILIENCE ARCHITECTURE.**

   Border, police, intelligence, cyber-security, civil-protection and defence actors need clearer interfaces for instrumentalised migration, cyber operations, organised crime, state activity and attacks on critical systems.

8. **FUNDAMENTAL RIGHTS AND PROFESSIONAL STANDARDS ARE OPERATIONAL CAPITAL.**

   Legality, data protection, proportionality and accountability sustain the trust needed for information-sharing, deployment, mandate development and Schengen resilience.



9. SEARCH AND RESCUE, LEGITIMATE TRAVEL AND VULNERABILITY SAFEGUARDS REQUIRE GREATER VISIBILITY.

The interviews highlighted that these priorities merit more substantial emphasis in the development of future strategic frameworks.

10. THE NEXT PHASE SHOULD PRIORITISE CONSOLIDATION AND CAPABILITY QUALITY.

Enabling functions, workforce professionalisation, reduced silos and fewer high-impact priorities should follow crisis-driven expansion.

11. EUROPEAN ADDED VALUE MUST BE DEMONSTRATED.

Common institutions are relevant when they deliver knowledge, technology, coordination and operational effects that isolated or bilateral action cannot efficiently produce.

12. THE POSITIVE FUTURE IS A TRUSTED, ANTICIPATORY AND INTEROPERABLE NETWORK.

It requires a common strategic picture, complementary capabilities and adaptive European-national governance, rather than complete centralisation.

3. Future Scenarios

INTRODUCTION

Scenarios are descriptions of possible futures. They are helpful when uncertainty is high and customary extrapolations into the future do not work. Their main purpose is to challenge high-level decision-makers by showing them different, even surprising ways in which things can unfold. Decision-makers thus have a chance to prepare their organisations for otherwise unexpected surprises.

The field of Futures Studies (Strategic Foresight) has developed quite a few ways of scenario-building, known by a variety of denominations such as Shell, Manoa, Houston, La Prospective, Four Archetypes, and Morphological Analysis, among others. We have chosen the Shell method (aka Intuitive Logic), for the simple reason that it is the method most widely used in the corporate sector.

The scenarios envisage four different sets of circumstances in which the EU could find itself in 2035. Some aspects of these circumstances are considered through the prism of the four-tier access control model, which forms the core of EIBM.

3.1 EXTREME GEOPOLITICAL FRAGMENTATION AND EXTREME INDIVIDUALISM

This scenario describes a future in which international cooperation, European solidarity and collective responsibility progressively deteriorate. States pursue narrowly defined national interests, while individuals privilege personal autonomy, consumption and short-term advantage over social cohesion, institutional trust and collective action. These mutually reinforcing dynamics weaken EIBM across the entire four-tier access control model.

STRATEGIC CONTEXT

Geopolitical fragmentation reduces cooperation among EU Member States, neighbouring third countries, countries of transit and countries of origin. Information exchange becomes less systematic, common standards are applied unevenly, and governments are increasingly reluctant to share responsibilities, financial resources and operational capacities. At the same time, extreme individualism weakens confidence in public institutions and reduces acceptance of collective obligations, potentially affecting the recruitment, motivation and integrity of border-management personnel.

The combined effect is a shift from coordinated European border management towards unilateral national responses. Member States may reintroduce internal border controls, disregard common procedures or transfer responsibility for migration and security challenges to other states. In its most severe form, this behaviour could undermine mutual trust and threaten the operational sustainability of the Schengen area.

IMPLICATIONS FOR THE FOUR-TIER ACCESS CONTROL MODEL

At the first tier, measures in countries of origin and transit are constrained by declining diplomatic and operational cooperation. Information exchange, visa-related consular activities, training, capacity-building and measures addressing the drivers of irregular migration become more difficult to coordinate. Climate change, demographic growth, resource scarcity and political instability increase displacement, while the absence of a common international regime for climate-related displacement contributes

to irregular migration. Return and readmission cooperation may be negatively impacted, particularly where countries of origin depend increasingly on remittances.

At the second tier, cooperation with neighbouring non-EU countries becomes less reliable. Reduced trust and geopolitical competition limit joint surveillance, intelligence exchange, anti-smuggling operations and coordinated responses to emerging routes. Environmental degradation, regional conflicts and changing economic conditions may generate new migration and criminal pathways, reducing the EU's ability to address risks before they reach its external borders.

At the third tier, external border authorities face larger and more complex migration flows, increased applications for international protection, sanctions-related controls, greater volumes of goods and more sophisticated cross-border crime. Smugglers and other malign actors use drones, artificial intelligence, and encrypted communications to observe, evade or disrupt controls.

At the fourth tier, reduced police cooperation, weaker information exchange and declining solidarity restrict the detection of secondary movements, supplementary checks, joint risk analysis and return processes. Member States most exposed to hybrid threats, weapons trafficking, terrorism or irregular migration may receive insufficient assistance. Free-riding, unilateral action and attempts to transfer responsibility consequently weaken common Schengen governance.

INTERACTION OF THE PRINCIPAL MEGATRENDS

Climate change functions as a major threat multiplier. Resistance to collective environmental measures and the absence of coordinated international action accelerate environmental degradation, extreme weather events and the loss of livelihoods. Migration increases towards and within the Schengen area, while emigration from Europe may also intensify its demographic difficulties. New routes, including in the Arctic, emerge without an agreed legal and operational framework for climate-related displacement.

Demographic developments reinforce these pressures. Low European birth rates, population ageing, labour shortages and fiscal pressure on welfare systems make migration economically necessary, particularly in care-related sectors, while remaining politically contested. Simultaneously, population growth in parts of the Global South, combined with insufficient educational and employment opportunities, increases migration pressure. Border authorities may therefore face recruitment and budgetary constraints precisely when their responsibilities expand.

At the societal level, declining trust in public institutions makes border-control measures more difficult to implement. Challenges to official authority, corruption, bribery and insider threats become more significant as shared norms weaken. Urbanisation and the depopulation of border regions reduce local situational awareness, while the circulation of weapons and the return of foreign fighters increase internal-security risks. During a future pandemic, individual resistance to restrictions could also undermine health-related border measures.

Economic stagnation compounds these problems. Resource scarcity and higher commodity prices reduce the capacity and willingness of Member States to finance national border authorities and common EU instruments, including Frontex. At the same time, demand for inexpensive imported goods increases the volume of goods requiring checks, obliging border services to perform broader functions with fewer resources.

Technology has a dual role. Artificial intelligence, drones, sensors, cameras, automated vehicles and large-scale information systems can improve surveillance, information processing and risk analysis. However, private companies increasingly dominate innovation, while weaker public investment and interstate cooperation reduce European technological autonomy. Cyberattacks, system outages, encrypted communications and insider threats may compromise critical systems, including the Schengen Information System. Technology can mitigate staff shortages, but cannot replace institutional cooperation, professional integrity or common governance.

Geopolitical tensions further expand the border-management mandate. Border guards may assume hybrid civilian and military functions, monitor sanctions compliance and manage increased traffic across conflict-affected borders, particularly the Ukrainian border. Continued displacement or large-scale return movements linked to post-conflict reconstruction would both increase operational demands.

CHALLENGES AND OPPORTUNITIES

The principal challenges are reduced information exchange, the erosion of international and intra-EU cooperation, declining staff and financial resources, greater exposure to corruption and insider threats, and increasingly sophisticated criminal and hybrid activity. Together, these factors create implementation gaps across all four tiers of EIBM.

Technological development nevertheless provides a limited but important opportunity. Properly governed artificial intelligence and large-scale information systems could strengthen surveillance, automate the processing of extensive reporting and improve risk analysis and information exchange. If the EU preserves institutional cohesion in a fragmenting environment, it may also reinforce its strategic role and demonstrate the value of coordinated European action.

STRATEGIC ORIENTATION

This scenario requires greater investment in research, technological development and large-scale IT systems, supported by stronger safeguards against cyber vulnerabilities and insider threats. Frontex could assume a more prominent role in identifying, developing and providing common technological solutions, while Member States expand training in information-led border management and high-quality risk analysis.

Resources should be deployed flexibly across the Schengen area according to assessed risks rather than predominantly national considerations. Above all, EIBM resilience depends on preserving information exchange, solidarity and operational cooperation throughout the four-tier model. Technological improvements alone would not prevent fragmentation from undermining border security, migration management and the functioning of Schengen.

3.2 HIGH FRAGMENTATION AND COHESIVE COMMUNITIES

This scenario envisages Europe in 2035 operating within a hostile and asymmetrical multipolar order. Global governance is divided among competing political, military, technological and financial blocs, while strategic autonomy increasingly displaces interdependence. States align with stronger geopolitical poles and reduce dependencies perceived as vulnerabilities. Social cohesion persists, but becomes concentrated within national, political, ethnic, religious or alliance-based communities, strengthening internal solidarity while sharpening the distinction between insiders and outsiders.

For EIBM, this creates a fundamental tension. The external environment becomes more competitive and coercive, whereas the protection of Schengen requires sustained integration, information exchange and solidarity among Member States. The four-tier access control model therefore remains the principal framework for addressing migration, mobility and security risks across countries of origin and transit, neighbouring third countries, the external borders and the EU/Schengen area.

STRATEGIC CONTEXT

The international system is characterised by geopolitical rivalry, protectionism, tariffs, trade disputes, hybrid interference, information warfare and recurrent armed or proxy conflicts. Emerging powers across the global east and south increase their influence through large markets, demographic growth, access to strategic resources, technological innovation and investment in fossil-fuel and nuclear-energy capacity. Additional nuclear-armed mid-

dle powers further alter deterrence relationships and accelerate military and influence competition among major alliances and blocs.

Borders acquire greater strategic significance as points at which sanctions, mobility restrictions, commercial competition and hybrid pressure are exercised. The EU remains functional because Member States recognise the costs of acting alone, yet this integration is fragile. Nationalist parties increasingly attribute domestic crises to European institutions, other Member States or external groups, while non-EU powers use funding, technology, influence operations and political or economic pressure to test European cohesion.

INTERACTION OF THE PRINCIPAL MEGATRENDS

GEOPOLITICAL DEVELOPMENTS

Geopolitical fragmentation increases the strategic importance of border management. Migration may be instrumentalised for political coercion, while sabotage, disinformation, cyber operations and state-supported criminal activity test external-border resilience. Border authorities must therefore manage irregular migration and cross-border crime alongside sanctions enforcement, strategic infrastructure protection, foreign interference and hybrid threats.

Deteriorating international cooperation also affects return and readmission. While closer cooperation within the European Border and Coast Guard can support effective returns, some third countries become uncooperative or adopt a transactional stance. In this context readmission arrangements need to be tailored to specific incentives, interests and political conditions of each partner.

CLIMATE CHANGE

Climate change drives mobility and instability through environmental emergencies, resource scarcity and deteriorating livelihoods. Sudden events may redirect established routes with limited warning, while long-term degradation increases displacement from vulnerable regions. In a fragmented geopolitical environment, comprehensive international responses become less likely.

EU border management must therefore anticipate climate-related movements through horizon-scanning, pre-frontier intelligence and contingency planning. Climate emergencies must be understood as interconnected humanitarian, migration and security developments affecting surveillance, international protection, search and rescue, reception capacity and return policy.

SOCIETY AND DEMOGRAPHY

European societies experience demographic decline, ageing populations and the erosion of established cultural reference points. Communities and communitarian identities may support resilience, voluntary assistance and institutional legitimacy, but can also reinforce ethnic, religious and political boundaries. Patriotic 'us versus them' narratives strengthen cohesion within particular groups while weakening solidarity with migrants, neighbouring countries or other Member States.

Mixed migration flows become increasingly politicised, and nationalist actors portray asylum or European solidarity mechanisms as threats to national identity. Nevertheless, political authorities and the public continue to rely on Frontex and national border and coast-guard authorities to protect Schengen. Their credibility depends on combining operational effectiveness with legal certainty, transparency and respect for fundamental rights.

ECONOMIC DEVELOPMENTS

Tariffs, trade disputes, competition for rare earths and other strategic resources, increased defence expenditure and changing energy dependencies create sustained economic pressure. Artificial intelligence and automation disrupt labour markets and conventional career pathways, contributing to insecurity and political polarisation. Customs restrictions, sanctions and controls on strategic or dual-use goods expand the workload at border-crossing points.

Border authorities must facilitate legitimate travel and trade while detecting sanctions evasion, illicit financial activity and smuggling. At the same time, constrained national budgets limit investment in personnel, infrastructure and technology, increasing the value of pooled European capabilities, common procurement, shared technological services and risk-based resource allocation.

TECHNOLOGY

Artificial intelligence, automated border-control systems, biometrics, interoperable databases, satellite surveillance, unmanned aerial vehicles and advanced analytics improve situational awareness and operational efficiency. They enable authorities to process larger volumes of travellers and data, identify suspicious patterns and deploy resources more rapidly.

Digital dependence nevertheless creates systemic vulnerabilities. Cyberattacks, data manipulation, hostile intelligence activity and disinformation may interrupt operations or compromise biometric and identity data. Technology must therefore be supported by cyber resilience, human oversight, data-quality controls, legal safeguards, fallback procedures and redundant power supplies, and communications.

IMPLICATIONS FOR THE FOUR-TIER ACCESS CONTROL MODEL

At the first tier, measures in countries of origin and transit become central to anticipating climate-related displacement, demographic pressure, instability and route changes. A common pre-frontier risk picture should combine horizon-scanning, strategic intelligence and operational indicators. External engagement should include liaison networks, capacity-building, anti-smuggling cooperation, visa measures, humanitarian pathways, resettlement and skills partnerships. Return and readmission arrangements should be adapted to partner incentives while remaining consistent with international protection and fundamental-rights obligations.

At the second tier, cooperation with neighbouring non-EU countries becomes variable and politically conditional. Some partners remain reliable, while others align with competing blocs or use migration pressure strategically. Cooperation should combine joint surveillance, intelligence exchange, coast-guard coordination, contingency planning and monitoring of abrupt changes in visa policies or routes. The EU must cooperate pragmatically without becoming excessively dependent on partners whose strategic interests may change.

At the third tier, external-border authorities confront increased irregular migration, cross-border crime, terrorism, hybrid pressure and sanctions-related controls. Interoperable systems must translate data into timely decisions through reliable hit management, biometric quality and effective identity resolution, with safeguards for data protection. The Frontex Standing Corps provides tiered surge capacity through defined deployment standards and modular assets such as UAVs, satellite maritime surveillance, mobile screening laboratories and deployable command posts. Coast-guard cooperation must integrate law enforcement with search-and-rescue obligations, while border-crossing points require cyber-hardened infrastructure and continuity arrangements.

At the fourth tier, police cooperation, information exchange, joint risk analysis, supplementary checks and the monitoring of secondary movements become decisive for mutual trust. A more effective asylum system and functioning solidarity mechanisms can distribute pressure, but their legitimacy depends on implementation. Return should connect entry, registration, status determination, secondary movement and departure through coordinated case management and rights-compliant joint operations. Counter-disinformation measures are also necessary to prevent hostile actors from exploiting migration-related incidents.

OPERATIONAL AND INSTITUTIONAL RESPONSE

In this scenario, EIBM must operate as a living, anticipatory, interoperable, resilient and rights-anchored system. Strategic triggers, including sudden route shifts, sanctions cycles, commodity shocks, climate

emergencies and abrupt visa-policy changes, should activate predefined operational postures. Risk analysis must therefore influence staffing, deployment, procurement, training and external partnerships rather than merely describe developments.

Fundamental rights remain integral to operational legitimacy. Independent monitoring, a functioning complaints mechanism, mandatory rights training and transparent accountability protect democratic standards and institutional trust. Performance should be assessed through a limited set of decision-relevant indicators, including screening time, hit accuracy, false-positive rates, absconding and non-attendance ratios, return-to-decision rates, Standing Corps deployment times and public-trust measures.

CHALLENGES AND OPPORTUNITIES

The principal challenges are intensifying geopolitical rivalry, the politicisation of migration, deteriorating third-country cooperation, cyber vulnerability, disinformation and the persistent gap between return decisions and actual returns. Cohesive communities may reinforce resilience and collective responsibility within groups, but may also deepen exclusion, nationalist competition and resistance to common European solutions.

The principal opportunity lies in the EU's capacity to maintain disciplined integration despite external fragmentation. Frontex and national border and coast-guard authorities remain functional and retain public and political relevance. Interoperable systems, pooled resources, common risk analysis and measurable solidarity offer a strategic advantage over isolated national responses.

STRATEGIC ORIENTATION

Schengen resilience depends on selective but deep integration where fragmented action would create collective vulnerability. Priorities include a common pre-frontier intelligence picture, interoperable border systems, rapid European surge capacity, cyber-resilient infrastructure, effective and lawful returns, structured third-country partnerships and regulated alternatives to irregular mobility.

Cohesive communities can contribute to European resilience only when solidarity extends beyond narrow national or political boundaries. By integrating technology, operational capacity, cooperation and fundamental rights within a single EIBM architecture, the Union can protect Schengen while preserving the confidence of travellers, border personnel and European societies.



3.3 REGIONAL BLOCKS (LOW FRAGMENTATION) AND THE SOVEREIGN INDIVIDUAL

This scenario envisages a future in which Europe reinforces its internal political and institutional cohesion while reorganising governance around individual autonomy, personal accountability and utilitarian assessments of collective benefit. 'Low fragmentation' refers primarily to consolidation within major regional blocs rather than to a cooperative global order. Relations between blocs remain competitive, and the EU is regarded either as a successful model of regional integration or as a geopolitical, economic and ideological competitor.

The scenario is defined by a structural paradox. EU-level authority becomes stronger and more centralised, but its legitimacy is increasingly grounded in individual sovereignty rather than in traditional Member State prerogatives or broad social solidarity. EIBM therefore evolves towards a more centralised, technology-intensive and selective system.

This may increase consistency and efficiency while creating significant risks concerning equality, privacy, accountability, fundamental rights and access to international protection.

STRATEGIC CONTEXT

The consolidation of the EU follows a recognition that individual Member States cannot adequately protect European citizens' interests in an environment shaped by competition among the United States, China, Russia and other emerging powers. A substantial reform of the acquis communautaire transfers important powers from Member States to EU institutions and strengthens a citizen-centred model of governance.

The European Parliament becomes more responsive to individual constituencies, while artificial intelligence supports institutional accountability, administrative monitoring and evidence-based decision-making. Political cohesion is maintained less through conventional state sovereignty than through a libertarian and utilitarian conception of European citizenship.

This model generates contrasting international reactions. Parts of Africa and South America may regard European integration as a model to replicate, while other regions perceive it as unviable, threatening or strategically competitive. Within the EU, migration becomes an instrument of economic and demographic management: entry is favoured for persons recruited for particular occupations, individuals with valued skills and, in some cases, persons whose wealth may generate substantial local benefit. Mobility is therefore increasingly determined by measurable economic utility.

INTERACTION OF THE PRINCIPAL MEGATRENDS

GEOPOLITICAL DEVELOPMENTS

Regional, proxy and localised conflicts remain major drivers of forced displacement and irregular migration. In response, EIBM is increasingly centralised under EU institutions, with border surveillance, threat detection, resource deployment and rapid-response mechanisms governed through a common framework. This model seeks to standardise enforcement and strengthen responses to migration-based hybrid threats, cyber operations, transnational crime and instability in neighbouring regions.

Severe crises may require a wider security response combining law-enforcement functions, advanced surveillance, rapid deployment forces and, where necessary, military assistance. Although this increases coordinated capacity, it also accelerates the militarisation of border management and may privilege efficiency and collective security over Member State autonomy or individual safeguards. Centralised authority must therefore remain subject to democratic, judicial and fundamental-rights control.

CLIMATE CHANGE

Libertarian and utilitarian governance weakens global climate cooperation as states and regional blocs prioritise immediate efficiency, competitiveness and individual interests over coordinated environmental obligations. Mitigation efforts stagnate and climate-related displacement rises substantially in countries of origin. Because selective EU admission policies favour skills, employment or wealth, many displaced persons remain trapped in their regions or in neighbouring transit countries, creating prolonged humanitarian vulnerability.

Neighbouring states may become unstable transit or absorption zones, while environmental degradation changes the physical geography of the EU's external borders. Drying wetlands, water scarcity, changing coastlines and other forms of collapse may transform historically porous areas and prompt new physical or technological barriers. Within the EU, resistance to common climate policies, integrated energy systems and burden-sharing may contribute to de facto internal controls. EIBM must therefore incorporate extreme-weather forecasting, displacement-corridor analysis and assessments of climate impacts on border infrastructure into strategic risk analysis.

DEMOGRAPHY

Europe's ageing population and persistent labour shortages create an objective demand for migration. The EU develops a managed migration system designed to attract economically productive individuals while restricting access for those who do not satisfy predefined criteria. Although this may support productivity in selected sectors, it deepens regional inequality, reinforces brain drain from countries of origin and encourages persons excluded from regular channels to use irregular routes.

Demographic needs also differ within Europe. Wealthier and northern Member States may seek more skilled migrants, while economically weaker and southern regions resist further labour loss and the concentration of investment in already prosperous areas. These differences may generate de facto internal borders intended to protect labour markets. The ageing workforce also affects border authorities, increasing reliance on automation, outsourced services and private operators and raising questions about the delegation of coercive functions, democratic accountability and the commercial use of biometric data.

SOCIETY

Social divisions deepen between economic classes, regions and competing global blocs. Although the EU remains politically integrated, unequal wealth, cultural differences, labour-market conditions and attitudes towards migration create internal fragmentation. Wealthier regions attract skilled migrants and investment, while poorer areas experience depopulation, labour loss and resentment, weakening support for common policies and encouraging additional controls within Schengen.

Externally, mobility becomes increasingly transactional. Tourism, business travel and residence are facilitated for those with financial resources, qualifications or access to private networks, while persons displaced by drought, flooding, conflict or state failure face physical barriers, detention and restricted lawful entry. This 'borders-as-market' dynamic makes mobility dependent on economic capital and perceived utility. Selective admission may also prioritise productivity without adequate integration, cultural orientation or long-term social participation. The coexistence of national and Schengen citizenship frameworks consequently complicates the development of a coherent European identity and common standards for integration and public services.

ECONOMIC DEVELOPMENTS

The libertarian economic model favours lower taxation, reduced public expenditure and private-sector innovation. These policies may widen the divide between affluent and marginalised groups and diminish resources for social protection, migration management and public border infrastructure. Labour shortages, disrupted supply chains and weak public investment may contribute to recession or stagnation, while fiscal pressure and declining trust increase corruption risks, particularly where public

functions are transferred to private actors without adequate oversight.

The economic logic of selective migration may become self-defeating. Restrictive admission can prevent the EU from filling essential labour shortages, while unequal access to mobility and public services intensifies social tensions and undermines the fairness claimed by citizen-centred governance. EIBM therefore relies increasingly on automation, risk-based allocation and private technological services, but efficiency gains must be weighed against dependency, inequality and reduced democratic control.

TECHNOLOGY

Artificial intelligence, facial recognition, predictive analytics, automated identity verification and advanced surveillance become central to border management. They enable authorities to process large data volumes, optimise deployment, identify suspicious patterns and respond rapidly to threats. However, third countries, criminal organisations and competing blocs may develop equal or superior capabilities. Encrypted communications, cyber intrusions, identity manipulation and AI-supported evasion techniques facilitate smuggling, infiltration and transnational crime, requiring continuous European investment and anticipation of adversarial innovation.

The scenario also places greater emphasis on privacy and individual data rights. Public resistance to extensive cross-border data sharing may restrict timely access to information for police and border authorities. The operational dilemma is therefore to reconcile interoperability with personal sovereignty. AI-driven systems require clear legal mandates, human oversight, transparent decision-making, data-quality safeguards and accessible mechanisms for contesting automated decisions; otherwise, the technology intended to strengthen cohesion may deepen inequality and erode trust.

IMPLICATIONS FOR THE FOUR-TIER ACCESS CONTROL MODEL

At the first tier, visa policy, consular procedures and pre-departure screening implement the EU's selective migration strategy. Admission decisions focus on occupational needs, qualifications, economic contribution and, in some cases, financial capacity. A unified European visa regime would improve consistency, but legal channels would remain concentrated on persons considered economically beneficial, potentially increasing brain drain and leaving vulnerable groups without realistic regular alternatives.

Climate monitoring, early-warning systems and strategic risk analysis become essential for anticipating environmental emergencies, demographic pressure and conflict-driven displacement. The legitimacy of this tier depends on whether external measures merely restrict movement or also support resilience, lawful mobility and access to protection.

At the second tier, neighbouring states become critical buffer, transit and absorption zones as climate displacement, regional conflicts and exclusion from selective EU pathways increase pressure on their institutions. Cooperation includes information exchange, surveillance, migration management, anti-smuggling measures and contingency planning, but relations become increasingly transactional. Partners may seek financial, technological or political concessions in exchange for controlling migration or accepting returnees.

Instability may require rapid EU intervention or hybrid civilian-security capabilities. The EU must maintain practical cooperation while avoiding excessive dependence on governments whose strategic interests or political orientation may change.

At the third tier, the external borders, admission becomes highly differentiated. Travellers, workers and investors who satisfy economic or security criteria may use streamlined digital procedures, while other categories face extensive screening and restrictive controls. AI-supported surveillance, automated border-control systems, biometric identification and predictive risk assessment improve efficiency and may be complemented by physical barriers, autonomous systems and rapid-response capacities.

The principal risks are discriminatory profiling, unequal treatment, privacy violations and excessive reliance on private technologies. Effective control therefore requires legal clarity, human oversight, transparent accountability and reliable remedies in addition to technological sophistication.

The fourth tier is shaped by tension between centralised European governance and persistent de facto internal fragmentation. EU institutions may exercise greater authority over information systems, border policy and operational deployment, while Member States or regions introduce practical restrictions to protect employment, welfare systems or internal security. Stricter privacy expectations complicate police cooperation and cross-border data exchange, although fragmented access to information also creates vulnerabilities for criminal and hostile actors.

A coherent response requires common standards for integration, citizenship, access to welfare and the treatment of persons moving between Member States. Without such standards, selective migration may intensify competition among regions and undermine the freedom of movement on which Schengen depends.

TRANSFORMATION OF EIBM

In this scenario, EIBM develops from a system coordinated mainly among national authorities into a more centralised European structure. EU institutions increasingly direct border surveillance, operational standards, information systems, technological development and rapid-response mechanisms. The potential benefits are greater procedural standardisation, more efficient allocation of personnel and assets, improved interoperability and threat detection, faster crisis response, reduced duplication and a more coherent European position towards other regional blocs.

Centralisation nevertheless concentrates power and may weaken national accountability without automatically ensuring effective European democratic control. The expanding role of private technology providers and military capabilities further complicates institutional responsibility. The legitimacy of the transformed EIBM therefore depends on a clear division of responsibilities, parliamentary and judicial scrutiny, effective data protection and mechanisms through which individuals can challenge border-management decisions.



CHALLENGES AND OPPORTUNITIES

The central challenge is reconciling the sovereign individual with a centralised and technologically intrusive border-management system. A model founded on autonomy and privacy may conflict with the extensive collection, exchange and automated analysis of personal data required for contemporary border security. A related challenge is the discriminatory effect of skill- and wealth-based admission, which risks creating a stratified mobility regime in which opportunities depend on market value.

The scenario also raises a politically and legally sensitive debate concerning irregular entry, access to asylum and the fundamental-rights framework. Any reconsideration must remain compatible with applicable European and international protection obligations; the scenario identifies the issue as a challenge rather than providing a resolved legal model.

The principal opportunity lies in combining EU political cohesion, technological innovation and standardised operational action. A centralised EIBM could enhance preparedness, reduce duplication and ensure more consistent management of regional crises. It may also provide a model for other regional organisations seeking to reconcile integration with individual sovereignty.

STRATEGIC ORIENTATION

Strategic priorities include establishing a unified European visa regime; developing common integration standards; clarifying consistent criteria for national and European citizenship; designing systems to anticipate and mitigate extreme weather and associated displacement; strengthening European research in artificial intelligence, cybersecurity, autonomous surveillance and border technology; preserving human oversight, privacy and democratic accountability; limiting excessive dependence on private providers for coercive or rights-sensitive functions; and balancing labour-market needs with social cohesion, international protection and the development interests of countries of origin.

OVERALL ASSESSMENT

The regional blocs and sovereign individual scenario presents an EU that is institutionally cohesive, technologically advanced and capable of exercising more centralised control over its external borders. Its strength derives from regional integration, citizen-centred governance and the use of artificial intelligence to improve efficiency and accountability.

Its principal vulnerability arises from the individualistic and utilitarian principles on which it is constructed. Selective mobility, weakened climate cooperation, market-based access to borders, technological surveillance and reduced solidarity may deepen inequality within Europe and between regional blocs. Schengen resilience therefore depends on combining centralised operational capacity with genuine protection of individual rights. A technologically advanced EIBM remains sustainable only when admission, surveillance, asylum, integration and citizenship policies are transparent, legally grounded and subject to effective democratic control

3.4 LOW OR NO FRAGMENTATION AND HIGH COMMUNITARIANISM

In this scenario, Europe in 2035 operates through a highly integrated and communitarian model of EIBM. Border management is no longer understood primarily as control exercised at the physical external border, but as a continuous system of measures applied across the entire international mobility and migration continuum.



IMPLICATIONS FOR THE FOUR-TIER ACCESS CONTROL MODEL

The four-tier access control model provides the operational structure for this system, while a central European coordination and foresight network connects the tiers through shared data, predictive analysis, common standards and coordinated decision-making. The Brussels-based 'horizon layer' should therefore be understood as an overarching

governance mechanism rather than as a separate operational tier.

At the first tier, measures in countries of origin and transit increasingly rely on technological anticipation rather than a substantial permanent EU presence. Reduced European political leverage and stronger competition from other global powers encourage the use of environmental, economic and social early-warning systems, digital preregistration, pre-travel screening and automated mobility forecasting. Cooperation with international partners, including technologically dominant states, has become necessary for monitoring migration drivers and anticipating displacement caused by climate change, food insecurity, conflict, cyber disruption and economic instability. At the same time, greater dependence on external technological partners creates risks relating to strategic autonomy, data governance and political influence. Return cooperation is organised more consistently at European level, although in this scenario, permanent external returns centres function to relative degrees of success depending on operational, financial and political variables both within the EU and in host countries.

The second tier, which covers neighbouring non-EU countries, is characterised by technologically advanced but increasingly transactional cooperation. Joint coordination structures combine satellite information, drones, predictive analytics, social-media monitoring and local reporting to identify emerging movements before they reach the external border. Cooperation packages are no longer based mainly on financial incentives, but increasingly include access to surveillance technology, climate-adaptation resources, water management, green infrastructure and specialised technical assistance. Liaison officers, local organisations and community networks become important operational partners because they provide contextual information that remote technological systems cannot generate independently. This tier therefore combines technological monitoring with locally embedded knowledge and new forms of resource-based partnership.

At the third tier, which corresponds to the EU's external borders, border control is highly automated, integrated and risk driven. Drones, sensors, biometric systems and real-time analytical tools support the detection, identification and registration of persons and vessels, while dynamic operational corridors allow resources to be adjusted according to predicted pressure. Human personnel remain essential for command decisions, complex identity assessments, search-and-rescue coordination, vulnerability identification and interaction with individuals and communities. Certain technical and specialist services may be provided by private-sector or external experts, transforming the traditional concept of a unified border-guard structure into a broader network of public and specialised service providers. Nevertheless, automation and externalisation require strong public oversight, common professional standards, cyber resilience and clear accountability.

The scenario also envisages selective community-based admission and sponsorship arrangements, supported by diaspora organisations and local communities. Such mechanisms could facilitate integration and provide structured support to new arrivals, but they would require transparent eligibility criteria and safeguards against unequal access, preferential treatment or the emergence of hierarchies among migrant communities. Similarly, highly regulated admission and return procedures would need to remain compatible with search-and-rescue obligations, access to international protection, data-protection requirements and fundamental-rights safeguards. These elements are essential to the legitimacy and operational credibility of EIBM, particularly in a system that depends heavily on automated screening and information exchange.

At the fourth tier, inside the EU and the Schengen area, information from the preceding tiers is integrated with data on labour-market needs, secondary movements, social cohesion, welfare capacity, return and internal security. Digital identity systems facilitate access to services, while local integration hubs, community organisations and mediators address cultural tensions and support social stability. Police cooperation, internal risk analysis and the monitoring of disinformation contribute to the preservation of public trust. High communitarianism strengthens the role of local communities and diaspora net-

works, but it may also produce social stratification between highly connected groups and communities with limited access to digital, economic or political resources. Pervasive virtual checks and automated access controls therefore create continuing risks of excessive surveillance, exclusion and algorithmic discrimination.

Overall, the low fragmentation and high communitarianism scenario presents EIBM as a coordinated European network in which common information systems, shared technological capabilities, community participation and integrated return arrangements connect action in third countries, neighbouring states, the external borders and the Schengen area. Environmental pressures become a permanent element of risk analysis and operational planning, while preparedness increasingly depends on the capacity to transform global indicators into timely operational decisions.

The model does not necessarily require complete political centralisation. Its effectiveness depends instead on common strategic awareness, interoperable systems, complementary European and national capabilities, structured cooperation with external partners and clearly defined responsibilities across all four tiers. Its sustainability would ultimately depend on maintaining human oversight, equitable treatment, fundamental-rights compliance, cyber security and institutional accountability. In this sense, the scenario reflects a positive EIBM future based on a trusted, anticipatory and interoperable network, rather than on isolated border-control measures or fragmented national responses.



4. Thematic Areas

4.1 MIGRATION

Migration in its different forms (internal, cross-border, regional and international/intercontinental) is usually sustained by geopolitical instability and economic downturns. Wars, such as those in Ukraine, Gaza and the Sahel, are currently among the most significant drivers of displacement, with the potential to trigger sudden refugee crises.

To address the structural drivers of migration, including systemic poverty, protracted conflicts and climate-induced instability, implementation of systematically informed policy frameworks grounded in interdisciplinary analyses is needed.

The EU should balance human rights commitments with pragmatic measures, such as aligning labour market needs with skills-based migration. This requires agile governance. Such an approach must prioritise the integration of socioeconomic, political and environmental dimensions, rather than adhering to reductive securitisation paradigms that prioritise short-term risk mitigation over the holistic understanding of systemic interdependencies.

Ultimately, migration policy must prioritise resilience and adaptability. Strengthening international cooperation, leveraging technology for border security and building societal trust against anti-migrant narratives are vital. By fostering solidarity, the EU can navigate migration challenges while upholding its values of human dignity and solidarity.

International cooperation on migration is complex and politically charged, constrained by structural, ideological and geopolitical barriers. This underscores the EU's imperative to address root causes in border and migration policy, given the systemic challenges of interconnected megatrends that demand proactive, forward-thinking strategies.

Multicausality complicates identifying critical variables, creating cascading effects on EIBM. While root-cause solutions are ideal for sustainability, their implementation is often limited, necessitating pragmatic, outcome-oriented goals to strengthen crisis preparedness. Effective EIBM requires balancing long-term root-cause mitigation with adaptive, collaborative frameworks to navigate migration's evolving complexities.

EU's Status Agreements and Working Arrangements primarily engage cooperative third countries, but uncooperative or hostile states remain outside meaningful collaboration, leaving gaps in addressing migration drivers and enabling smuggling networks to operate unchecked.

Cooperation with top migration-source countries (Africa, Middle East) relies heavily on transactional incentives (financial aid, legitimisation), which risk undermining long-term sustainability.

Global political and security shifts, coupled with unpredictable third-country policies, threaten EU border management initiatives, necessitating adaptive, resilient strategies.

On the other hand, operational constraints, such as the inability to conduct police, judicial or border cooperation with uncooperative states, further weaken efforts to combat transnational crime and irregular migration.

The EU faces a broader policy dilemma: balancing normative imperatives (human rights, rule of law) with geopolitical pragmatism, especially as external actors like the US[51] influence global priorities. To address these challenges, the EU must diversify engagement strategies, combining incentives with capacity-building in origin/transit countries, strengthen diplomatic and intelligence capabilities, and adopt forward-looking frameworks to navigate the interplay of values, geopolitical realities, and the volatility of international migration dynamics.

Key recommendations emphasize enhancing pre-frontier intelligence, institutionalizing standing border corps, and refining strategic governance models. Long-term success depends critically on sustained international collaboration, highlighting the necessity of adaptive, collaborative governance mechanisms to navigate EIBM's dynamic and evolving complexities.

The EU should adopt a tech-enabled and cooperative strategy to address migration, cross-border crime, and hybrid threats. Priorities include long-term foresight to anticipate crises and root causes, strengthening institutional and digital resilience against external and internal vulnerabilities and balancing security imperatives with ethical and global responsibilities in an interconnected world.

The geopolitical and economic situation are the megatrends with the highest impact on irregular migration in the present and this might maintain during the forthcoming period. To address these challenges, the good road undertaken with the European migration strategy should be further explored and implemented, with a view to a progressive harmonization of national and EU level policies.

This includes strengthening legal migration pathways, investing in development and conflict resolution in origin countries, and creating return hubs in stable regions to facilitate voluntary return.

4.1.1 RECOMMENDATIONS

- Migration must be seen through long time horizons to distinguish structural trends from short-term fluctuations and short-term indicators to avoid risk misinterpretation.[52] Data collection and analysis must move beyond quantitative metrics to incorporate mixed methods approaches that capture the socio-political and economic dimensions of migration.[53]
- Call for a cohesive, unified, forward-looking migration strategy that harmonises national and EU-level actions to ensure resilience and adaptability. This year saw already the adoption of the European Migration Strategy and the entry into application of the Pact on Migration and Asylum, an huge step fulfilling the aforementioned need.
- Whilst ackowledging MS competencies in legal migration and labor matters, adequate consideration should be given to fostering legal migration pathways. Strengthen shared early warning and preparedness through EUROSUR and existing migration-monitoring arrangements, including lawful use of open-source intelligence and social-media monitoring. Establish clear arrangements for timely reporting, validation, sharing and escalation of alerts, and link warnings to contingency planning and exercises involving the relevant authorities.

4.2 RETURN ACTIVITIES

Returns act as a strong deterrent to irregular migration and their effectiveness depends on a combination of internal and external factors.

Internally, the degree of harmonisation of MS` procedures towards a common EU return system, the efficiency of national administrative and judicial procedures all play a role. As return is often a shared responsibility between different Institutions in Member States, there is scope for improved coordination mechanisms to ensure prioritisation and the efficient use of available tools and resources.

The disparity of the efficacy rate of returns to different countries underscores systemic challenges in aligning operational capacity with geopolitical and demographic dynamics. In the external dimension, cooperation with the countries of origin is decisive for nationality verification, documentation and effective admission of the returnees to their territory. A policy investing in the conclusion of partnerships, readmission agreements, return arrangements and in using strategic incentives with third countries, play a pivotal role in strengthening international cooperation towards more effective returns. This also underlines the importance of a coordinated EU approach ('Team Europe') to the external dimension of return, based on a coherent common use of leverage and incentives, rather than fragmented or predominantly bilateral engagement.

MAIN CHALLENGES

The effectiveness of the EU return and readmission policy is strongly dependant on the level of efficiency of each Member State`s return systems and on their overall coherence with EU policy and tools. The persistence of **divergent national approaches** to return procedures is a structural challenge. Return processes in Member States differ in legal frameworks, administrative practices, procedural timelines, and enforcement measures, including detention and related alternatives. Adequate investments are necessary to timely process readmission procedures, prevent absconding of returnees, and to implement return and reintegration counselling in line with the EU voluntary return and reintegration strategy.

Beyond this, **cooperation with third countries** remains a critical factor as it can strongly impact the effective identification and documentation of the returnees, essential to enforce most of returns.

Lack of investments and poor coordination on both, national and EU level, impact the return procedures at multiple stages, leading to delays, increased administrative burden, and reduced overall effectiveness of return systems. This is more evident in forced returns, where the implementation of the return decision is hindered by the absence of voluntary compliance and lack of cooperation of the returnee. Different political sensitivities, administrative capacity constraints, economic factors and uneven level of cooperation of the countries of return limit the coherence and effectiveness of EU efforts and the implementation of existing policies.

Situations in which return decisions cannot be effectively implemented may arise for a number of reasons, often in combination, including limited cooperation from countries of origin, difficulties in establishing identity or obtaining travel documents, and protracted legal and procedural pathways. In this context, fundamental rights are not the obstacle; rather, the challenge lies in ensuring that safeguards are applied through efficient procedures and effective oversight, so that return obligations can be enforced where legally possible while avoiding situations of prolonged legal limbo. This points to the need for structured cooperation with judicial authorities and independent fundamental-rights monitoring actors, including non-governmental organisations, to support timely appeal processes and credible compliance monitoring.

Individuals affected by such impediments may remain in a state of prolonged unresolved status, with limited prospects for return and without a clear pathway to regular stay. This can generate sustained pressure on national administrations and services and increase exposure to exploitation and marginalisation. Importantly, the accumulation of unenforced return decisions may also undermine the credibility of the EU return system and wider migration governance.

From a strategic perspective, return-impediment cases highlight a persistent gap between policy objectives and what can be delivered in practice under existing legal and operational constraints. They raise fundamental questions for the EU migration framework about how to manage long-term unresolved cases in a manner that is legally robust, administratively workable and consistent across Member States — without assuming that a single, comprehensive solution is available.

Absconding or evading return processes and migrants moving between Member States remains a significant challenge for implementing return decisions. These movements may be driven by perceived differences in national systems, including access to services, enforcement practices, or legal opportunities.

Such movements may undermine the effectiveness of return decisions by enabling individuals to evade enforcement measures. They may also result in duplication of administrative procedures, increasing the burden on national authorities.

Limitations in system interoperability and information-sharing facilitate these movements, highlighting the need for a common system that allows identifying absconded returnees across the EU, based on common identification methods and aligned with Member States' return case management.

Digitalisation is widely recognised as a key enabler of more efficient and coordinated return systems.

However, interoperability between national and EU-level systems remains limited, which continues to constrain effectiveness.

Continued investment in interoperable systems and common standards is likely to be essential for addressing these challenges. Interoperability must be developed within the applicable legal framework, with clear responsibilities, access controls and data protection safeguards.

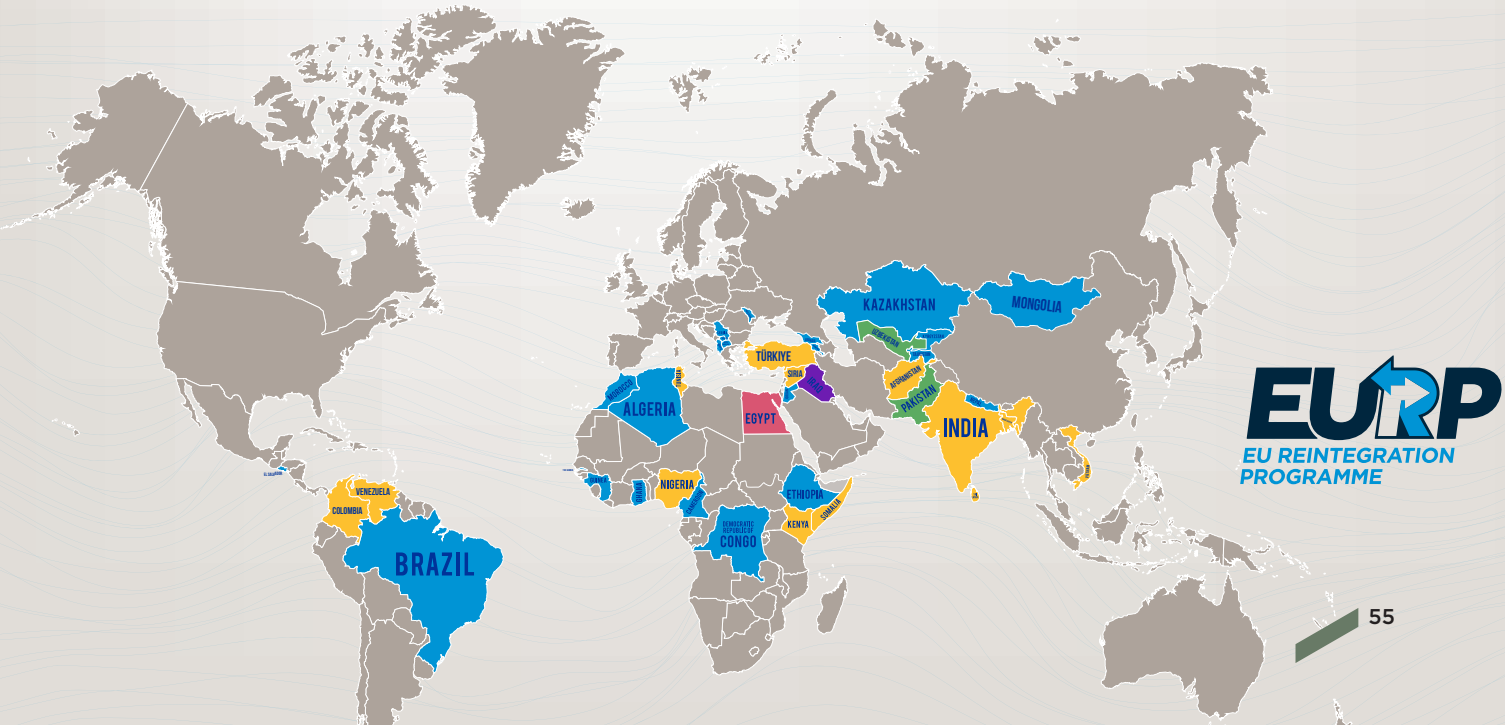
Return procedures are subject to a robust legal framework that includes fundamental rights obligations. Beyond the existence of these safeguards, a key differentiator for return outcomes is whether procedures provide timely legal certainty. Where appeal pathways are lengthy or fragmented, return cases can remain unresolved for extended periods, contributing to legal limbo and undermining the credibility of return decisions. Deepening and streamlining existing cooperation with judicial authorities can support faster, predictable review, thereby reducing uncertainty while enabling enforcement where legally possible.

The strategic environment for **reintegration support** is expected to evolve in light of the upcoming new Return Regulation and the announced review of Regulation (EU) 2019/1896 on the European Border and Coast Guard. These developments are likely to influence the scale, structure and governance of reintegration assistance, as well as the expectations placed on Frontex with regard to coordination, implementation support and management of Union-funded reintegration programmes. It is to note that the new Return regulation clearly position the reintegration assistance as a tool — not a right — in the return system and should be avoided that it is misused and would act as a pull factor.

The new Return Regulation aims to establish a more uniform and effective EU system covering return, readmission and reintegration. Within this framework, reintegration assistance is increasingly treated as a component of the overall migration management cycle, including through provisions allowing the exchange of personal data with actors competent for reintegration assistance and through the envisaged development of digital case-management systems covering return, readmission and reintegration in an integrated manner.

These elements indicate a policy direction towards greater continuity between procedures in Member States and post-arrival/post-return support in countries of origin.

Forward planning for reintegration should take into account the likelihood of increased demand for EU-coordinated assistance, stronger legal expectations regarding continuity of support after return, and the need for systems that are scalable, financially sustainable and adaptable to evolving policy and regulatory requirements.



ROLE OF FRONTEX

Frontex's role in returns in the coming years will be defined by the new legislative framework, the new Frontex mandate and aligning the obligations foreseen under the future Return Regulation and return digitalisation regulation. These legislative tools will determine how the Agency will position itself in the EU return system and what responsibilities and obligations it will seek to fulfil.

Over the next year, Frontex is expected to further consolidate its role as a central operational and coordination actor in EU return management. A rapid expansion has been observed in recent years, where the Agency supported approximately 42-44% of all effective returns in 2024-2025 compared to around 12% in 2021.

Frontex will continue providing operational support to Member States. This includes the provision of logistical support, coordination of return flights and deployment of specialised personnel. The Agency's role in pooling resources and standardising operational practices is expected to contribute to increased efficiency and consistency.

In parallel, Frontex is expected to further strengthen its coordination function, supporting the alignment of return procedures across Member States. By promoting common operational standards and facilitating information exchange, the Agency may contribute to reducing fragmentation and addressing challenges linked to uneven enforcement and secondary movements.

The external dimension of return is also likely to remain a key area of engagement. Frontex will continue to support Member States in their interaction with third countries, particularly in relation to nationality verification, documentation and readmission processes. This may include technical assistance, facilitation of communication channels, and capacity-building activities. Such support is likely to be increasingly relevant in contexts where cooperation with third countries remains limited or inconsistent.

In the area of reintegration, Frontex is expected to continue playing a key operational role in supporting the implementation of the EU's reintegration programme, with potential for further evolution depending on policy and legislative developments. Ensuring continuity and quality of post-return support is likely to remain a key priority, with increasing emphasis on its integration into the broader return framework. This may require more structured cooperation with implementing partners, as well as enhanced monitoring and quality assurance mechanisms.

SCENARIOS OR POSSIBLE FUTURE DEVELOPMENTS

A plausible Pact-driven trajectory is that faster status resolution becomes the organising principle: asylum and return operate increasingly as one pipeline. In this respect, the Screening Regulation, the Asylum Border Procedure and the Return Border Procedure form a continuum — with a single fast track procedural chain — intended to strengthen the EU's external borders.

A second likely development is the deeper embedding of return preparedness inside asylum procedures, including earlier nationality screening and more systematic return counselling. In parallel, detention and alternatives to detention may be used more strategically as acceleration increases incentives for short, targeted detention (identity verification, preventing absconding, pre-removal) alongside scaled alternatives where capacity or legal risk is high.

In terms of migrant behaviour, absconding and secondary movements may shift from 'after rejection' to before the system locks in (post-arrival / screening or upon early negative signals), with greater use of false identities, document destruction, and deliberate non-cooperation, and with smuggling services adapting to provide 'packages' focused on timing, asylum-lodging advice, and evasion of screening rather than border-crossing alone. Swift uploads of SIS return alerts with biometrics data enables MS to mitigate the risk of (early) absconding also supporting the mutual recognition of return decisions.

Interoperability and digital case management creates continuity between asylum and return files and supports risk-flagging (repeat applications, identity matches, absconding indicators), while remaining

exposed to litigation and data-protection that can slow implementation and sustain fragmentation. Challenges related to timely uploads of SIS alerts will be resolved by increased interoperability of national and EU IT systems. Even if internal coupling between asylum and return improves, due to limited cooperation of partner countries, the number of returnees keeps growing unless third-country cooperation on documentation / readmission materially strengthens, which may also shape route choices and claimed-nationality strategies.

Digitalisation is expected to play a central role in shaping the Agency's future contribution to return. Frontex continues to promote digitalisation of national return case management systems, striving for interoperability and providing additional digital solutions to support return processes and seek digital convergence with other migration processes.

CONCLUSION

The effectiveness of the EU's return systems in the coming years is expected to remain shaped by a complex interaction of structural, operational, legal and external challenges. While recent and forthcoming policy developments aim to enhance harmonisation, efficiency and coordination, a number of persistent constraints are likely to continue limiting overall returns.

Addressing these challenges will require sustained and coordinated efforts across multiple policy domains, including migration, external relations, judicial cooperation and fundamental-rights oversight, digital governance, and reintegration. Operationally, the contribution of Frontex — within the evolving legislative framework — is likely to remain important for pooling capacity, supporting coordination among Member States, and enabling more consistent implementation.

At the core of these challenges lies the uneven level of cooperation with third countries, which remains decisive for nationality verification, and documentation — and therefore for the feasibility and timeliness of effective returns.

Divergences among Member States in administrative practices, judicial timelines and operational capacities continue to argue for a more common system. In most EU MS, return related responsibility lies between different authorities, lacking solid coordination mechanisms. These differences — combined with limitations in digital interoperability and cross-border data sharing — may continue to constrain the ability to monitor cases end-to-end, reduce duplication, and enforce decisions, including by contributing to absconding and secondary movements within the EU.

The number of individuals who cannot be effectively returned reflects practical impediments and protracted procedures rather than fundamental rights as such. Where review and appeal pathways do not provide timely legal certainty, cases may remain in prolonged legal limbo, sustaining pressure on national systems and undermining credibility. Reintegration assistance is expected to remain increasingly relevant — especially for voluntary return — but will raise questions around scalability, partner capacity, monitoring of outcomes and prevention of abuse.

KEY JUDGEMENTS

- Persistent disparities in effective return figures across Member States are expected, linked to differences in return caseloads, nationality composition, procedural approaches and cooperation with third countries.
- Cooperation on readmission and returns with third countries is an essential element and may be influenced by broader political and economic dynamics.
- The introduction of new EU-level legal instruments binding for all (regulation not directives) will determine the return system of the EU as well as Frontex's role in it within the next five to ten years.
- The number of individuals who cannot be effectively returned could grow in the absence of more workable and timely pathways to enforce return decisions.
- The demand for digitalisation of return processes will continue to grow, including interoperability at national and EU scale.

Further digitalisation and AI use must preserve data protection, data quality and effective human oversight.

- Legal and fundamental rights considerations will continue to shape return procedures. If these safeguards are not ensured systematically, they can hamper return outcomes and undermine the credibility of fair and transparent return policies.
- Demand for reintegration support is likely to increase, raising questions regarding sustainability, scalability and funding.

4.3 INTERNAL SECURITY

Addressing the security and systemic risks of migration requires a balance between proactive, scenario-driven governance and pragmatic, multilateral cooperation. By integrating complexity-aware strategies, technological innovation and reflexive policy design, the EU can enhance its resilience to evolving threats while fostering sustainable, inclusive solutions. The impact of internal security on border management and migration is a topic to be further analysed looking also at the diasporas and the pull factors.

4.3.1 RECOMMENDATIONS

- **Wider focus of border control:** Strengthen partnerships with countries of origin to manage migration flows and reduce the influence of criminal networks.
- **Enhance countering irregular migration:** Increase operational support to Member States' law enforcement authorities and information-sharing to disrupt irregular migration pathways.
- **EU-coordinated support:** Prioritise EUMS collaboration to harmonise responses, share resources and ensure consistency in addressing security and migration challenges.

4.4 CROSS- BORDER CRIME (CBC)

The EU faces escalating cross-border crime risks, driven by increasingly sophisticated criminal networks that exploit both physical and virtual borders.

However, cooperation to prevent irregular migration between the EU and countries of origin, transit and departure, combined with new technologies in border management, have made it much harder to reach the EU.

This may have resulted in an increased reliance on **migrant-smuggling services**, incentivising criminal networks and smugglers to intensify their activities for financial profit and other objectives. Networks now offer package services (including forged documents, transportation, safe houses, etc). Crossing the external border without the use of smuggling services has become and will continue to be a rare occurrence.

Migrant smugglers have also come to play a key role in the instrumentalisation of migration, as hostile actors attempt to leverage global crises stemming from geopolitics and other megatrends like climate change, demographic imbalances and regional conflicts to exert pressure on the EU to achieve strategic objectives. Migrant smugglers are likely to continue to benefit from these crises and remain important political tools for hostile actors.

Migrant smuggling is also becoming increasingly digitalised, with technology facilitating the smuggling process, from marketing of services via social media (increasingly tailored to the client's background and needs, also with the use of AI), encrypted and self-deleting messaging apps for coordination, navigation applications to avoid law enforcement during the journey, and cryptocurrencies / digital

currencies to make covert transactions. Technological features such as unmanned vehicles (e.g. drones) may be increasingly used by migrant smugglers.

We can also expect smugglers to use technology to more easily circumvent border-control systems. This includes further expanding their use of encrypted communications, online marketplaces and crime-as-a-service providers to rapidly source and distribute fraudulent identities across multiple jurisdictions. Increased digitalisation will thus continue to lower risks of detection for migrant smugglers while increasing their profit margins.

Trafficking in human beings (THB) is also likely to pose an increasing threat to EIBM and internal security in the future. As climate change accelerates, droughts and flooding will increase resource scarcity, particularly in Africa. Climate change is thus expected to further exacerbate income inequality, pushing people to migrate and creating more vulnerable populations for traffickers to exploit. Geopolitical challenges and insecurity in key countries of origin and transit are likely to persist, resulting in opportunities for exploitation.

Apart from the predominant sexual or labour exploitation, another form could be exploitation for engagement in conflict zones in the vicinity of the EU, which could impact the EU's internal security and border management. Such victims could later seek protection in the EU and may pose a threat due to psychological trauma, military experience or even involvement in war crimes.

The EU is set to face a labour shortage in the coming years, driven by an aging population and diminishing workforce. The impacted sectors will include construction, manufacturing and transportation, which may attract THB, as the European THB market offers one of the highest profits per victim. Recent years have seen an upward trend in detected cases of trafficking for labour exploitation, and this trend is likely to continue.

Digitalisation is increasingly acting as a global bridge for traffickers. Traffickers can recruit geographically distant victims on social media, connect them to clients in the EU via online platforms, 'control' them using digital methods (camera surveillance, blackmail via sextortion, etc.), and make discrete transactions using cryptocurrency. Digitalisation has made THB more difficult to prevent and detect while increasing profit margins by expanding potential victim and client bases. As the world becomes increasingly interconnected and more vulnerable populations obtain internet access, digitalisation is likely to drive THB in the EU. Countering the increasing use of digital means for trafficking flags the need to enhance the capacity in third countries of origin or transit to identify malicious use, harmonising procedures and good practices in these regards with the EUMS.

Firearms smuggling remains closely linked to ongoing and frozen conflicts. The close cooperation and intensive efforts by the EU and Ukraine have contributed substantially to the firearms smuggling threat thus far not having had a significant impact. The long-term risk remains in the shape of gradual leakage of weapons and the diversion of illicit stockpiles when the fighting stops.

Experience from the Western Balkans in the 1990s shows that post-conflict arms proliferation can affect EU internal security for decades. Over the next ten years, the persistence or freezing of regional conflicts may create grey zones where weapons are stockpiled, resold or trafficked through land corridors into the EU. Instability in Africa and the Middle East further compounds this dynamic. In this context, anticipating post-conflict arms diversion and emerging trafficking routes is essential to mitigate potential long-term security risks.

Firearms trafficking has evolved into a hybrid model combining physical smuggling with digital facilitation. Encrypted communication platforms, darknet marketplaces and anonymous payment systems enable brokers to coordinate cross-border deliveries with reduced exposure. Instead of trafficking complete firearms, networks increasingly ship modular components — slides, barrels, trigger assemblies — via postal and parcel services. These smaller consignments are harder to detect and are often mixed with legitimate e-commerce flows. Simultaneously, the spread of affordable 3D printing allows for partial domestic production of untraceable firearms. If 3D printing lowers the barrier to decentralised physical

production, AI may be used for discovering, synthetising or optimising design knowledge to modify everyday objects into weapons, which will create a risk environment where both production and knowledge become more widely accessible. While fully printed weapons remain technically limited, hybrid weapons — combining printed frames with trafficked essential components — will continue to pose a growing threat. The smuggling focus therefore is likely to shift in the future from complete weapons to critical parts and manufacturing tools.

The proliferation of firearms has broader societal implications beyond organised crime. Socioeconomic disparities, polarisation and radicalisation trends across parts of the EU increase the motivation of individuals and extremist actors to acquire weapons. Instability in neighbouring regions continues to provide supply channels.

In the next ten years, the key risk is not only the mass inflows of military-grade arms from past conflict zones, but also the steady accumulation of illegal firearms within criminal and extremist environments. Even moderate increases in availability can significantly amplify violent crime rates, gang conflicts and terrorist capabilities. An influx of weapons erodes public trust in state authority and places sustained pressure on internal security systems. The interaction of these trends could evolve into a structural security driver, increasing the likelihood of more frequent and violent incidents across the EU in the next decade.

In the **drug smuggling** domain, Europe remains one of the world's largest and most lucrative markets. Key source regions include Latin America (primarily for cocaine), Central-West Asia (notably for heroin), and North Africa (for cannabis resin), while some Asian countries play a major role in supplying new psychoactive substances (NPS), precursor chemicals and related equipment. As international trade continues to expand (particularly maritime container traffic, which is expected to triple by 2050) the increasing complexity of global supply chains are creating new vulnerabilities that smuggling networks can exploit.

Shipping containers account for an estimated 80-85% of drug seizures in European ports[54]. The proportion of maritime containers physically inspected across



EU ports remains very low, estimated at between 2% and 10%, making it a preferred means of transport for drug traffickers[55]. Criminal networks are therefore very likely to continue concealing drugs within legitimate shipments, especially in imported foodstuffs, which present inspection challenges for border guard and custom authorities[56].

Efforts are being made to enhance maritime trade security. Innovative detection technologies will continue to be used and developed by EU authorities and law enforcement involved in tackling drug trafficking. Several international trade organisations are promoting the digitalisation of trade documentation, including the adoption of electronic bills of lading (eBLs), with commitments to fully transition to digital documents by 2030[57]. In addition to container-based maritime smuggling, air cargo and courier services are expected to remain preferred methods for direct shipments and the anonymous distribution of illicit drugs to consumers.

Cannabis remains the most widely consumed drug in the EU, with the European market worth around EUR 12 billion, followed by cocaine. European seizures of cocaine exceed 300 tonnes annually, with European ports being the main entry points. Although heroin seizures in Europe have declined, over 60% of the heroin reaching Western Europe still passes through south-eastern Europe. Meanwhile, the European opioid market is undergoing a rapid transformation. There has been a marked increase in new, highly potent synthetic opioids, which are likely to pose serious public health risks in the coming years due to their high potency, low production costs and ease of concealment and transport.

Coca cultivation in Colombia and Bolivia continues to increase[58] suggesting that the supply of cocaine to the EU is unlikely to decline, driven by strong domestic demand and the significant profits generated for traffickers. Although maritime cocaine seizures have decreased at some major EU entry points, this does not necessarily indicate reduced supply. Rather, it may reflect adaptive trafficking strategies, including route diversification or displacement effects. Overall volume entering the EU, whether in the form of finished cocaine or cocaine base destined for processing in clandestine laboratories in Europe, is not expected to decrease.

Drug trafficking networks, particularly those in the Balkans and South American cartels, rely on the corruption of port personnel and the use of stolen container codes ('pin code fraud'). Another aspect is the resurgence of violence, with record numbers of armed incidents and explosions related to territorial control of drug markets. Profits are quickly laundered through cryptocurrencies and informal money brokers (hawala systems).

The Western Balkans are expected to remain a key transit region for various drug types, including heroin transported through the region and cannabis or synthetic drugs locally produced. Despite intensified law enforcement, the countries are likely to continue being the largest producers of outdoor-grown cannabis in Europe, taking advantage of the legal cultivation of medicinal cannabis to fuel the illegal market[59].

The sustained availability of cocaine and other high-value drugs, combined with the criminal exploitation of legitimate business structures, poses increasing risks to European transport and logistics infrastructure. Airports with regular connections to Latin America and Africa — including major passenger and cargo hubs — are expected to continue reporting frequent seizures of cocaine, heroin and synthetic drugs such as MDMA, nitazenes, ketamine, and fentanyl. Although consumption remains low compared to the US, methamphetamine has become a major component of the Balkan route, trafficked from laboratories in Afghanistan and Iran to European markets, often concealed in legitimate goods.

The growing number of dismantled synthetic drug production laboratories within the EU[60] points towards intensified domestic production, leading to potential increased competition for imported precursor chemicals. Methamphetamine production in European laboratories has increased for export to global markets. Online drug markets and direct partnerships between European traffickers and criminal networks in source countries are likely to further intensify smuggling activities.

Criminal networks are expected to continue adapting their trafficking strategies by shifting routes towards smaller or less scrutinised ports, diversifying their operational methods. Emerging methods include drop-off techniques, unmanned vessels, drones, AI-assisted logistics, and blockchain-based payment systems.

The use of digital assets has become mainstream among cartels, offering anonymity and speed in international settlements. Illegal wallets received assets worth approximately USD 158 billion in 2025, a massive increase over previous years. Drug sales via cryptocurrencies increased by 19% between 2024 and 2025. There is a noticeable migration from traditional Darknet markets to encrypted messaging apps (Telegram, Signal) for direct transactions. Nearly half of the new drug markets launched in 2024 use the cryptocurrency Monero (XMR) exclusively, given its strong focus on privacy. Traffickers are increasingly using AI to automate the mixing of funds and create transactions that mimic the behaviour of legitimate users, making their transactions more difficult for law enforcement authorities in the EU to detect.

Though, money laundering through cash smuggling remains one of the challenges faced by the EU as it still relies on the physical movement of banknotes across the borders, rather than traceable electronic transfers. Within the area of free movement this is hard to detect, OC introducing the money intro legitimate economy through cash-intensive businesses, property purchases or bank deposits under the reporting threshold. Detection of cash smuggling at the EU External borders, relying on a mix of legal declaration requirements, physical inspection and risk-based profiling is and will remain during the next decade an endeavour.

Excise goods smuggling represents a persistent challenge for the EU. Smuggling of tobacco, alcohol and energy products constitutes a significant and evolving threat to the economic security and public health policies of EU Member States. The primary drivers are substantial disparities in taxation across the EU Member States and the erosion of purchasing power due to high inflation and broader economic pressure. These conditions allow criminal organisations to exploit economic vulnerabilities, resulting in significant lost tax revenue for EU governments. The complexity of the issue necessitates a multi-faceted approach, moving from reactive border interdictions to proactive, intelligence-driven strategies and enhanced international cooperation to disrupt these sophisticated transnational networks.

The allure of high profit margins and sustained domestic demand will very likely continue to drive the illicit trade in excise products, particularly tobacco (including emerging products such as e-liquids and e-cigarettes). Criminal networks remain agile, exploiting regulatory tightening and increasing taxation of these products across various EU Member States, particularly those in the western part of the EU, where high tax rates correlate with the highest levels of illicit tobacco consumption, leading to billions in lost potential revenue.

Fraud in the fuel sector often involves 'washing' marked diesel (subsidised for agriculture) and reselling it as standard diesel. Energy products are often part of complex 'carousel' schemes, where goods are fictitiously moved between Member States to generate illegal tax refunds.

The proliferation of global supply chains and the vast scale of international trade facilitate smuggling operations. With over 500 million containers shipped worldwide each year, with a forecast of three times that amount by 2050, and only an estimated 2% to 10% being inspected[61], criminals often conceal illicit goods within legitimate shipments or in hidden compartments.

Criminal networks constantly adapt their methodology. They import machinery to produce contraband cigarettes and establish manufacturing facilities within EU territory. Smuggling routes exploit different domains, including maritime routes (accounting for 90% of intercontinental trade), land borders and increasingly, digital platforms and e-commerce for anonymised deliveries. Geopolitical instability on the EU's eastern borders may further contribute to shifts in smuggling routes in the medium term, given the role of certain regional third countries in producing illicit cigarettes.

EU Member States' authorities will face a significant challenge in keeping pace with the sheer volume of trade and technological innovation of criminal networks, which have begun using advanced AI devices, drones and unmanned aircraft or weather balloons to evade detection. While innovative detection technologies such as improved X-ray systems and photofission techniques might enhance control capabilities, their effectiveness could be outpaced by exponential growth in trade volumes if adequate resources and coordination mechanisms are not deployed at both national and EU levels.

Regarding **smuggling of stolen vehicles**, the rapid expansion of electric mobility across the EU has fundamentally reshaped the vehicle crime landscape. High-value EV components have become targets for organised crime groups (OCGs). Criminal networks now combine traditional vehicle theft with cyber-enabled techniques such as keyless relay attacks and remote immobiliser bypassing. The profitability of dismantling EVs for parts has increased, and trafficking routes increasingly link EU to eastern Europe, while maritime container shipments via the North Sea and Mediterranean ports conceal dismantled components.

Over the next decade, this development implies a need for enhanced technological border controls, as vehicle theft investigations should exploit digital evidence. The convergence of cybercrime and property crime represents a structural shift that will define border security priorities through 2036.

The reconstruction of conflict-affected regions, including Ukraine, will significantly increase demand for vehicles, agricultural machinery and construction equipment. In the next ten years, this demand is likely to remain high, creating structural incentives for organised property crime. Criminal groups exploit urgent procurement needs and weak oversight in post-conflict or economically fragile regions to supply stolen goods that are re-registered using falsified documentation.

Rather than exporting whole vehicles, criminal groups increasingly dismantle cars and distribute parts via online marketplaces and parcel services. This fragmented model reduces detection risk and allows anonymous cross-border sales. Smaller, high-value components — control units, airbags, infotainment systems, batteries — are shipped within legitimate e-commerce flows. For EIBM, the challenge lies in detecting low-volume, high-frequency shipments blended into legal trade. Over the next decade, AI-supported cargo profiling and enhanced parcel screening will be essential to counter evolving stolen vehicle trafficking models.

Document fraud is and will remain a cross-cutting crime area. Over the next decade, document and identity fraud will remain a structural enabler of various forms of cross-border crime and a permanent challenge to be addressed by EIBM. Organised crime is becoming more networked, more digital and more closely intertwined with geopolitical tensions. Within this evolving landscape, fraudulent identities are not merely tools for movement; they are multipliers of criminal opportunity. They enable the facilitation of irregular migration, trafficking in human beings, drug and firearms smuggling, excise and VAT fraud, sanctions evasion and elements of the crime-terror nexus. Fraudulent documentation will also continue to reinforce the interdependence between migration-related crime and broader internal security threats by enabling labour exploitation, infiltration of legal business structures, financial crime and other forms of cross-border criminality. In a context marked by hostile multipolarity, hybrid interference and the instrumentalisation of migration, the manipulation of identity documents and systems can also serve broader destabilisation objectives.

The deployment of large-scale IT systems such as ETIAS, EES and VIS and the digitalisation of visa procedures represents a transformative shift in border governance and contributes to a progressive digitalisation and interoperability of EU border systems that will significantly strengthen identity verification and information exchange. However, enhanced controls in legal travel channels are likely to produce displacement effects. Individuals denied visas or travel authorisation may increasingly resort to impostor fraud, fraudulently obtained identity travel and breeder documents or high-quality counterfeits. OCGs which facilitate irregular migratory movements to, from and within the EU, will continue

integrating document fraud services into comprehensive smuggling packages.

Artificial intelligence will act as a decisive factor multiplier. Generative AI tools already enable the production of highly realistic synthetic identity documents, automated facial morphing and deepfake-supported impostor scenarios, capable of challenging first-line border checks and automated border-control gates. AI-assisted biometric threats may undermine confidence in biometric verification across the entire identity chain. At the same time, AI can optimise travel routes, match stolen genuine documents to 'look-alike' impostors and adapt risk profiles dynamically to evade non-biometric detection systems (e.g. ETIAS). As digital identity ecosystems expand, vulnerabilities are likely to shift from traditional physical forgery towards attacks targeting enrolment procedures, remote identity verification processes and backend databases.

For EIBM, the strategic challenge will be to ensure resilience across the entire identity chain — from document issuance and biometric enrolment to border verification and post-entry controls. This requires not only advanced technological safeguards, such as multimodal biometrics and enhanced enrolment and detection, but also sustained investment in first-line capabilities, specialised training, digital forensics and intelligence-led cooperation with third countries. Without continuous adaptation and systemic protection of digital and biometric infrastructures, document and identity fraud will evolve faster than the mechanisms designed to contain it, directly affecting the security, credibility and operational sustainability of the EU's external borders.

In the field of **waste trafficking** and the illegal transport of hazardous waste (illegal export to/through third countries, dumping in unauthorised areas), there has been a noticeable increase in the illegal activity of OCGs that specialise in this type of crime, exploiting legislative loopholes and corrupting public officials in EU Member States. This leads to the creation and/or consolidation of intra-EU flows between Member States with weak controls, clandestine exports to third countries, and transit through large ports and areas with low surveillance.

GENERAL CONSIDERATIONS

Effectively combating cross-border crime requires a strategic shift towards coordinated, proactive measures. Key actions include strengthening international cooperation and intelligence-sharing between EU Member States, third countries, EU and international law enforcement actors. Shifting to intelligence-driven strategies is crucial for disrupting transnational criminal networks.

Legislative and technological measures must complement law enforcement efforts. Reducing incentives for smuggling through, inter alia, balanced taxation policies, enhanced supply chain security through advanced tracking and tracing systems, and proportionate and dissuasive penalties are key elements of a targeted approach against smuggling. Cooperation between border guard and customs authorities is crucial in this regard. The new EU Customs Authority to be established could prove a significant counterpart, which would facilitate real-time information-sharing and intelligence exchange, leading in comprehensive operational measures against cross-border crime and other security threats.

Technological advancements also facilitate collaboration among criminal groups, allowing them to divide tasks more efficiently across jurisdictions. The modus operandi and sophistication of criminal operations will increasingly blur the distinction between legal and illegal activities. The growth in international trade and the security weaknesses of global supply chains, transportation / logistics systems and especially the shipping industry and seaports will be exploited to facilitate all types of illicit trade. To counter these trends, the EU must prioritise the use of technology (AI-driven analytics, biometric systems) to strengthen border checks.

Member States should prioritise countermeasures to cross-border crime, treating it as a critical societal threat. To build on this, deepening cooperation with third countries to address root causes and intercept transnational operations is essential, alongside empowering EU agencies to lead coordinated responses.

Recent developments, such as the Joint Investigation Team (JIT-CP) platform for cross-border investigations, the ECRIS-TCN system for accessing criminal records of third-country nationals, and the revamping of EURODAC to record additional biometric and identity data for a broadened scope of usecases, represent critical steps toward improving police-judicial cooperation and asylum system integrity.

Frontex's Cross-Border Crime — Risk Analysis Network (CBC-RAN), which produces annual threat assessments, represents a promising initiative in systematically addressing cross-border crime, with significant potential for expansion, enhanced collaboration, and deeper integration with global and regional partners. To enhance effectiveness, the EU must expand data collection, deepen collaboration with agencies like Europol, Eurojust, the future EU Customs Authority (EUCA), Interpol, and the UN Office on Drugs and Crime (UNODC), as well as leverage open-source data and academic research on criminal dynamics, including money laundering, smuggling routes and emerging technologies.

Cross-border crime in Europe has evolved into highly flexible networks by adopting a modular, professionalised, and digitised business model similar to on-demand service platforms, and referred to as 'smuggling-as-a-service' (SaaS). The SaaS model often offers different 'packages' or levels of service, reflecting varying costs and risks for migrants. Thus, more expensive 'service packages' may include better transport conditions or routes considered safer, while cheaper options often involve considerably higher risks.

In this context, large, organised crime groups no longer control the entire route, but act as service integrators. These groups subcontract specific segments to local 'providers' who specialise in certain stages of the route or certain types of services. This allows for greater flexibility and increased resilience of the network if an operational cell is compromised or dismantled.



Migrant trafficking is also increasingly managed through digital technology (the Digital Journey concept). Online platforms and messaging apps are used for recruitment, communication with migrants, providing route information and managing logistics. Digitisation makes operations faster and more difficult to monitor using traditional methods, complicating the activities of law enforcement authorities in EU Member States and European organisations like Europol and Frontex.

To facilitate transactions and avoid detection, networks use sophisticated payment systems, often involving intermediaries and non-banking methods (e.g., Hawala). These systems are designed to ensure that payments are made securely for traffickers, often once the service has been confirmed as delivered.

Organised crime groups involved in migrant smuggling are characterised by a multinational structure and advanced digitisation of the entire recruitment and transport process. Frontex analysis estimates that almost 90% of migrants entering the EU illegally use the services of these networks.

The groups offer 'full package' services, i.e., packages that include transportation, experienced guides who know border areas very well, secure accommodation in transit hubs, as well as local facilitators in EU Member States. In this context, there has been a major paradigm shift, in the sense that the crime bosses are in the countries of origin and they hire local facilitators in EU Member States to make the network as flexible as possible. If a cell is dismantled by law enforcement in EU Member States, the network continues to operate and the dismantled cell is eventually replaced by another one, without compromising the bosses. Organised crime groups involved in migrant smuggling also frequently use violence to maintain discipline among migrants or to fight rival groups for control of routes.

Another feature is the recent use of speedboats by OCGs in the Mediterranean Sea. Previously, criminal groups used boats in poor technical condition to transport illegal migrants, as the boats might well be seized by EU law enforcement. This change in the modus operandi confirms that large sums of money are generated by migrant smuggling and highlights the profitability of the operations.

Digitalisation has radically transformed OCGs' business model, with illegal migration becoming a 'cyber-facilitated' activity. Traffickers use social networks (e.g., Facebook, TikTok, Instagram) as advertising platforms and for online recruitment and marketing. Social media is used to carry out disinformation campaigns, in particular by posting videos showing successful illegal journeys to create a false narrative about the safety of the routes. Sophisticated algorithms are sometimes used to identify people in financial difficulty, offering them 'all-inclusive' packages.

Technology allows traffickers to manage operations without being physically present at the border, reducing the risk of being caught by law enforcement authorities. To this end, they use end-to-end encrypted communications (such as WhatsApp, Telegram, Signal or dedicated platforms) to guide migrants in real time via GPS and digital maps. Smuggling networks also produce and transmit counterfeit visas, passports and work permits online through specialised digital networks.

Another major change that makes it difficult for law enforcement authorities to monitor cash flows is the use of anonymous financial transactions, particularly through the use of cryptocurrencies. In 2025, the volume of crypto-asset transactions related to human trafficking increased by 85%, reaching hundreds of millions of euros. At the same time, digital payment systems (Hawala 2.0) are being used, integrating traditional money transfer methods with digital wallets and online banking applications to launder profits under the radar of the formal financial system. The dark web and e-commerce platforms are used to anonymise financial transactions.

Advanced OCGs use technology to monitor the activities of law enforcement agencies by integrating facial recognition programs into CCTV camera networks in controlled areas to identify undercover agents, as well as creating false identities or manipulating evidence in the digital environment to mislead judicial investigations.

AI has become a game changer in migrant smuggling since 2025-2026, but its impact is a double-edged sword, as it serves both criminal networks and the authorities combating them.

Migrant smugglers and human trafficking networks have quickly adopted advanced tools to streamline their operations, such as using machine learning to analyse and monitor social networks and identify vulnerable people in disadvantaged areas, tailoring fake job offers to attract victims, while generative technology is used to create compromising content (deepfakes) used in sextortion schemes or to manipulate victims' identities online. The use of large language models (LLMs) also allows traffickers to generate communication scripts in multiple languages to mislead authorities or manage victims globally without language barriers.

Border authorities and law enforcement agencies use AI to counter these risks, namely predictive analysis of migrant flows by integrating certain specialised systems that collaboratively analyse data from various sources (financial, transport, public records) to predict traffic routes and identify critical points where law enforcement agencies can effectively intervene. Since October 2025, advanced biometric identification has also been used through systems such as the EU's Entry/Exit System (EES), which collects fingerprints and live facial images to prevent criminals from using false identities. Another important area is maritime and land surveillance using drones equipped with AI sensors and specialised systems that enable real-time detection of suspicious activity in isolated areas or at sea, highlighting nocturnal anomalies.

4.4.1 RECOMMENDATIONS

- Implement a systemic, integrated approach to address the interdependencies between CBC and hybrid threats, as their interactions generate second- and third-order effects requiring coordinated policy responses.
- Enhance the role of EU Agencies responsible for countering CBC.
- Strengthen international cooperation mechanisms against CBC, leveraging partnerships with third countries and global institutions to enhance collective capacity.
- Conduct systematic analysis of global and EU criminal markets, including demand-supply dynamics and the evolving landscape of serious and organised crime, in conjunction with mapping and assessing EU-based and international transnational networks and their systemic enablers.
- Evaluate the effectiveness of regulatory frameworks and policy mechanisms in mitigating CBC, with a focus on identifying systemic gaps and operational shortcomings, while exploring opportunities for enhancement and innovation through ongoing, evidence-based evaluations.
- Use AI and other new technologies to enhance border checks.
- Prioritise virtual-domain operations to address borderless digital threats (cybercrime, encrypted communications) by leveraging AI-driven tools for detection, prediction and disruption of cross-border crime.
- Develop and deploy advanced analytical tools (AI-driven systems) to detect, predict and disrupt CBC.

4.5 TERRORISM

The threat of terrorism continues to be primarily, but not exclusively, linked with conflict and post conflict areas. From the perspective of the EU's external border, undetected crossings of individuals that represent a security threat will remain a cause of concern. Their travel patterns will likely be shaped by opportunity, intent and constraints. Further developments in digital technologies and AI may favour these individuals' mobility, with cyberspace increasingly representing a predominant operational battlefield providing avenues for recruitment, planning and propaganda.

The EBCG plays a critical role in supporting Member States in combatting the terrorist threat, contributing to resilience and facilitating safe travel by securing the borders and screening the flow of people. Due to the fluid nature of the terrorist threat, it is necessary to expand the scope of information exchange beyond the EU law-enforcement boundaries. Despite advancing integration efforts, interoperability concerns persist, and more time may be needed to achieve a fully operational integrated information systems. Until then, the efficiency of border procedures can be improved by performing systematic checks of all travellers against relevant databases, leveraging biometric data and integrating other available technologies.

IMPACT ON EIBM[62]

WEST AFRICA IS SET TO REMAIN THE MAIN HUB OF TERRORIST ACTIVITY IN THE COMING YEARS[63]

Although regional military and political reconfigurations appear to have enabled the broader jihadist milieu to consolidate territorial footholds, expand operational reach and intensify recruitment, their operational impact seems to remain largely regional. At the same time, they have sought to strengthen financial sustainability and military capabilities — including through the acquisition of weapons and other assets — by exploiting regional and local conflicts, intersecting with the interests of criminal rings, and diversifying their networks and alliances.

More broadly, Africa's security landscape is increasingly shaped by Russia's expanding footprint, including the growing role of its armed proxies. This fuels violence and insecurity, enabling jihadist recruitment, and erodes past regional counterterrorism efforts.

Concurrently, uncertainty surrounding the future of US military and financial engagement in the region — amid a broader strategic shift towards the Indo-Pacific and the Arctic — risks further weakening regional stability, providing jihadist networks and other actors with opportunities to expand territorial gains and project influence.

The risks linked to EIBM can be most immediately related to travelling terrorists or subjects susceptible to radicalization once in the EU. The links between organized crime and terrorism, given the vast network of drugs trafficking, THB and migrant smuggling originate from the African continent.

DEVELOPMENTS IN THE BROADER MIDDLE EAST WILL CONTINUE INFLUENCING THE TERRORIST THREAT

Since its territorial defeat, IS has sought resurgence in the broader region. It is maintaining a low-level operational posture, exploiting security vacuums to rebuild and expand.

The mass escape and untracked dispersal of thousands of individuals from Al-HOI in February 2026 -ranging from radicalized adherents to victims of trafficking - alongside the heightened institutional fragility surrounding Al-Roj camp — the last remaining main detention camp in Syria - have contributed to raise concerns in the broader region.

The security vacuum surrounding these camps raises the risk that former ISIS fighters and their dependents will attempt to return to the EU, or migrate to active global conflict zones, directly reinforcing the operational and combat capabilities of other terrorist networks.

The Syrian government is facing growing pressure (both internal and international) to address the presence of foreign terrorist fighters and other armed factions to mitigate the risk of these people infiltrating security forces and to implement robust security governance across the country.

The regional security environment is likely to be further complicated by the US and Iraq's decision to set a timeline for ending the operations of the US-led Combined Joint Task Force — Operation Inherent Resolve (CJTF-OIR) in Syria and Iraq. The planned drawdown could create security gaps that may enable a resurgence of IS activity, with potential spillover effects for the wider region.

A prolonged military confrontation against Iran threatens to further undermine the security and

political equilibrium in the region. These hostilities are exacerbating an already dire humanitarian situation inside Iran and beyond, and risk triggering cascading instability e.g., weakening or fragmentation of the Iranian state. This may lead to an increasing number of Iranians seeking refuge in neighbouring countries, particularly Turkey, and may provide opportunities for elements close to the Iranian establishment who represent a security threat to the EU to relocate themselves abroad to preserve influence, assets or personal security.

Yet, in the long term hostilities may also play in favour of the Iranian regime in its attempt to rally Iranian society. With a fragmented and largely leaderless opposition and an unclear US/Israel plan for what follows the campaigns of airstrikes, the regime may utilise the attacks to bridge domestic divides and consolidate support behind the new leadership.

THE THREAT OF TERRORISM WITHIN HYBRID ACTIVITIES ON THE EU'S EASTERN BORDERS

Russia is already engaged in unconventional offensive activities targeting European infrastructure. This may expand to include the covert deployment or infiltration of irregular operatives inside the EU with the aim of conducting deniable operations.

Migration pressures along the EU's eastern borders will remain a powerful tool for neighbouring states to advance political and strategic objectives vis-à-vis the Union. Such dynamics — often accompanied by serious human rights violations — may create conditions that could be exploited for the deliberate infiltration of members of terrorist organisations or individuals vulnerable to radicalisation once inside Europe.

4.6 HYBRID THREATS

Hybrid threats are projected to intensify over the coming decade, driven by technological advances and the exploitation of systemic vulnerabilities across physical, digital and societal domains. Their defining feature — the instrumentalisation of all available levers — enables hostile state and non state actors to weaponise migration, promote disinformation, endanger critical infrastructure and instrumentalise criminal networks to destabilise societies, erode institutional trust and fragment political cohesion.

At the EU's external borders, hybrid activities manifest through orchestrated migration flows, influence operations, cyberattacks, physical sabotage, malicious use of drones, corruption and the co option of organised crime. These actors exploit disparities in legislation, gaps in IT interoperability, resource constraints, social polarisation and vulnerabilities in commercial and maritime networks. When activated, such threats can overwhelm border control, increase trafficking and security risks, generate political and economic costs, and undermine public confidence.

Instrumentalised migration might involve directing large groups of persons towards the border, facilitating crossings, creating artificial pressure through blockages or staged incidents, and manipulating asylum systems to delay procedures. Disinformation campaigns — amplified through social media, bots, deepfakes and proxy organisations — seek to delegitimise border authorities, polarise public opinion and justify hybrid actions by portraying borders as insecure or institutions as complicit.

Cyber operations target border management systems, surveillance networks, biometric databases and logistics platforms through phishing, zero day exploitation, ransomware, DDoS attacks, supply chain intrusions and data manipulation. Physical sabotage and paramilitary actions focus on degrading border infrastructure and exploiting remote terrain, outdated systems and coordination gaps. Organised crime groups further weaken border security through trafficking, corruption, document fraud and cyber enabled smuggling.

Hybrid threats will remain central to strategic competition. In the context of the war in Ukraine, Russia is expected to intensify asymmetric tactics to generate insecurity, influence negotiations and maintain geopolitical leverage. Even after hostilities cease,

Moscow may recalibrate rather than reduce hybrid operations, using proxies to preserve plausible deniability and operational flexibility. Russia will continue pursuing real or perceived military successes on the battlefield to shape and frame the negotiation process from a position of advantage. This is aimed at ensuring an uncompromising goal: maintaining geopolitical predominance on the eastern flank of the EU. Negotiation for Russia is a tool rather than an end point. There is a rationale behind it. War and peace have rather blurred boundaries for Russia. Regardless of the outcome of the conflict, confrontation with the broader West will/should continue by other means. Chaos and uncertainty allow for great opportunities to destabilise, create and exploit frictions and — as a result — shape the strategic environment.[64]

Beyond Europe, Russia's expanding presence in Africa may enable the manipulation of migration dynamics there to exert political pressure on the EU. In the Western Balkans, organised crime and potential proxy actors may exploit migration routes to overwhelm border systems. The Arctic is also becoming a strategic frontier, where climate driven accessibility intersects with military build up, intelligence activity and risks to critical infrastructure.

North Korea, also constitutes a hybrid threat to the EU's internal security, notably through its cyberattacks, its illicit financing activities, notably in order to circumvent international sanctions and generate revenue for the regime.

To respond effectively, the EBCG must enhance and support situational awareness, early warning mechanisms and resilience of critical infrastructure. Hybrid operations often unfold in legal grey zones. This requires clearer mandates, stronger inter agency contingency planning and regular joint exercises with EU and NATO structures. Intelligence led risk analysis and robust information exchange across EIBM and internal security domains are essential for anticipation, coordination and strategic decision making.

HYBRID THREATS WILL REMAIN A TOOL OF STRATEGIC COMPETITION

When reflecting on the future implications of hybrid threats for the EU, developments surrounding the conflict in Ukraine are key. As the war continues, it is expected that the Russian Federation will intensify asymmetric tactics aimed at feeding a deep sense of insecurity among EU citizens to foster frictions within the EU and with NATO allies on the conditions to end the conflict.

Once the war ends, one of the main questions for Russia will be whether to demobilise or relocate military assets from Ukraine. Relocation would allow for a sort of strategic continuity in exercising pressure on the EU as well as mitigating the risk of a drastic structural shift at home, and avoiding — or (more likely) postponing — frictions in domestic politics.

IMPACT ON EIBM[65]

As long as the war in Ukraine endures, Moscow will likely maintain sustained pressure on the eastern borders of the EU to strengthen its leverage at the negotiating table. From a border perspective, orchestrated multi-domain hybrid operations will continue evolving to adapt to the operational environment and exploit EU Member States' vulnerabilities. As demonstrated by the growing tempo and complexity of hybrid activities in 2025, cyberspace will likely stand as the predominant battlefield, with attacks ranging from critical digital infrastructure to communication / information systems. Advancements in AI will keep shaping malicious state / non-state actors' opportunities to operate below the threshold of open confrontation. Yet, territorial proximity to the EU's external borders — direct or via aligned partners — will keep offering viable options to instrumentalise migration to deepen unhealthy polarisation and challenge core EU values.

At the operational level, state actors will likely continue outsourcing hybrid activities to non-state actors following the logic of benefiting from proxies' knowledge of the context / resources while maintaining plausible deniability. But it would be wrong to consider the non-state actors only as passive executors of hybrid action. Regardless of the nature of the non-state actor, this relationship has often represented a mutually beneficial trade-off. Criminal networks play a preponderant role in e.g., facilitating

the movement / transport and accumulation of people near the EU's external borders.

In this context, the concept of instrumentalisation of migration can be understood as an umbrella term encompassing actions that extend beyond the mere accumulation or redirection of people to generate political leverage. While the scale of migratory flows remains a primary indicator of potential shifts in the security landscape, such dynamics may also create direct and indirect opportunities for malicious actors. These include the infiltration of non-attributable assets to conduct covert actions, as well as the facilitation of weapons and drug smuggling aimed at destabilising the EU's internal security architecture.

AFRICA WILL CONTINUE OFFERING AVENUES TO INSTRUMENTALISE MIGRATION

Russia is likely to continue pursuing military and political expansion in Africa — particularly through state-controlled armed groups — to manipulate geopolitical dynamics, access resources and project power in a region that may become instrumental in pressuring Europe. A potential strategic refocus of US foreign policy towards other theatres, coupled with reduced investment in the region could enable Moscow to deepen its foothold in African countries whose governments perceive western commitment to be waning. Here, growing insecurity, unemployment, weak governance, organised crime and terrorism are powerful tools to stir migration across and beyond the region to pursue hybrid campaigns with significant strategic ramifications. Coupled with a young local population ripe for recruitment, Russian state-linked security forces have all the resources they need to strengthen regional presence and project power.

WESTERN BALKANS

The broader Western Balkans region will continue offering migrants opportunities both overland and by air to reach the EU's external borders. OCGs are expected to keep exploiting migration routes in the Balkans, turning irregular migratory flows into a lucrative source of revenue and influence. Due to the strategic importance of this region, the exploitation / co-option of those groups as non-state proxies by a hostile state actor cannot be ruled out. Regimes dissatisfied with the present international system or concerned about real / perceived foreign threats to their internal stability may be willing to challenge the international equilibrium through a hybrid threat campaign aimed, for example, at rapidly overwhelming EU Member States' border controls and migration management capacities.



THE ARCTIC AS AN EMERGING STRATEGIC BATTLEGROUND

Over the next decade, the Arctic is likely to emerge as a critical strategic battleground for the EU. Climate change is accelerating the melting of sea ice, opening new maritime routes such as the Northern Sea Route and potentially trans-Arctic passages that could reshape global trade flows. For the EU, this creates both opportunities and vulnerabilities: opportunities — by expanding shipping traffic near EU Arctic territories and fostering avenues for economic development and cooperation; vulnerabilities — by increasing the role of the region as a theatre of strategic rivalry, particularly involving Russia, China and the US.

As Russia militarises its Arctic infrastructure and China advances its 'Polar Silk Road' ambitions, the EU's external northern borders could face increasing hybrid challenges (increased military activity, intelligence operations, disinformation and pressure on critical infrastructure, e.g., undersea cables and other installations), forcing a northward shift of EU/NATO security concerns.

EIBM SHOULD CONTINUE DEVELOPING ITS CAPABILITY TO ADAPT AND RESPOND TO GROWING SECURITY CHALLENGES AT THE EXTERNAL BORDERS

The EBCG will remain a key frontline actor in addressing hybrid threats at the EU's external borders, particularly in situations where migration may be deliberately instrumentalised. In such contexts, border authorities strengthen the Union's resilience by maintaining border security while screening incoming flows to identify individuals who may pose security risks.

Effective border protection depends on a solid understanding of emerging threats and the ability to anticipate hybrid campaigns targeting border management systems. These risks can be mitigated through early-warning mechanisms based on the systematic monitoring of key indicators, including unusual migration patterns and other tactics potentially orchestrated by hostile state actors to overwhelm border management capacities.

As hybrid threats grow more complex, EBCG functions must evolve accordingly. Hybrid operations often fall into legal and operational grey zones, where a border authority's mandate may prove inadequate. A careful assessment of the EBCG's opportunities and limitations is therefore essential.

As orchestrated multi-domain hybrid operations grow in scope and intensity, the EU will need to move from defensive adaptation to effective countermeasures. From the border perspective, this will entail primarily boosting situational awareness and preparedness capacities. As for the latter, efforts should be made to enhance the resilience of key border infrastructure (e.g., information systems), develop and maintain inter-agency contingency planning at national and EU level to ensure a timely and effective response, as well as regularly conduct joint exercises with EU/NATO structures to maintain a flexible operational posture.

As regards situational awareness, risk analysis and intelligence activities will continue playing a pivotal role in EBCG integrated planning and strategic decision-making. Only by ensuring effective information exchange across relevant EU stakeholders will the EBCG community be in the position to effectively anticipate challenges and coordinate operational response.

4.6.1 RECOMMENDATIONS

Understanding Context and Networks:

- Adopt a relational, network-based approach to map adversarial and criminal networks, anticipate strategic changes and enhance crisis preparedness.
- Analyse geopolitical dynamics through both deterministic (structural) and constructivist (narrative) lenses, recognising that hybrid threats will follow deterministic pathways even after temporary settlements.

Countering misinformation and building resilience

- Further enhance a coordinated EU strategy to combat propaganda and disinformation, particularly in border security contexts (false narratives about migration or border breaches)[66].
- Strengthen collective societal resilience by prioritising training and educational initiatives, institutionalised fact-checking mechanisms, and the cultivation of critical literacy to mitigate hybrid disinformation campaigns.
- Reliable Channels: Promote verified platforms (EU Agency for cybersecurity, national border agencies) as trusted sources of information to counter false narratives.
- Prioritise responses based on disinformation impact levels (public safety risks, policy manipulation) using metrics like reach, emotional impact and geographic spread.

Knowledge sharing and Innovation

- Develop technologies to safeguard critical systems against hybrid interference, including disruptions to communication and navigation in contested domains like outer space and the subsea environment.
- Strengthen strategic autonomy by reducing overreliance on third countries and enhancing EU-wide coordination to address hybrid threats that exploit interdependencies.
- Digital Repository: Create a centralised, secure platform to identify and disseminate Member States' best practices and lessons learned.
- Model Zones: Designate Member States with advanced capabilities as 'innovation hubs' to pilot EU-wide solutions and share expertise.
- Run Tech Demonstrations and use the results to refine tools and standardise protocols for cross-border threat detection.
- Strengthen NATO-EU cooperation on hybrid threats and critical infrastructure protection.

Anticipating adversarial strategies

- Recognise that rivals (state and non-state actors) actively seek to exploit weaknesses by crafting narratives, subverting institutions and weaponising societal divisions.
- Prioritise real-time information exchange and adaptive policy responses to counter evolving tactics, such as the instrumentalisation of migration or digital disinformation campaigns.



5. Technological development.

The next decade will bring significant technological change to border security. Emerging capabilities, some already maturing, others still in early development, have the potential to transform how the EU monitors and manages its external borders. Nine technology areas are likely to have the highest impact on border security operations and capability planning over the next decade.

These areas were selected based on an assessment combining horizon scanning, expert consultation and operational relevance analysis. Each technology was evaluated based on its alignment with the priorities identified in the EBCG's Capability Roadmap.

This foresight will be regularly reviewed and updated as technologies evolve, new capabilities emerge and operational needs shift — ensuring that European border security remains adaptive and future-ready.

5.1 TERRESTRIAL AND MARITIME AUTONOMOUS SYSTEMS AND ROBOTICS

Autonomous systems encompass uncrewed platforms operating on land, at sea and underwater with increasing levels of independence from human operators. This includes autonomous surface vessels (ASV), unmanned ground vehicles (UGV), and unmanned underwater vehicles (UUV) for subsea inspection and surveillance. Advances in sensors, edge computing and AI will enable most platform types to better understand their operating environment, make decisions and execute tasks with progressively less human direction.

WHY IT MATTERS FOR BORDER SECURITY

Autonomous surface and ground systems extend surveillance coverage, reduce risk to personnel and maintain a persistent presence at scale in remote or dangerous environments. In the maritime domain, ASVs and UUVs have the potential to increase patrol duration and recovery of survivors and to detect threats invisible to surface surveillance, including semi-submersible drug platforms and attacks on subsea infrastructures. At land borders, UGVs are expected to support patrolling and cargo scanning at border-crossing points. AI-based coordination of mixed autonomous fleets should by 2030 enable persistent coverage of high-risk areas at a significantly lower cost than fully crewed operations. Still, the value of autonomous systems is entirely dependent on the quality of human oversight governing them: operators must be able to understand what an autonomous platform is doing, intervene when its behaviour diverges from intent, and hold clear accountability for the outcomes of its actions. This is a legal and operational requirement. Autonomous systems that operators cannot trust, understand or reliably correct will not be deployed at scale regardless of their technical capability.

TEN-YEAR OUTLOOK

By 2036, autonomous surface and subsurface systems will be part of EBCG maritime operations, with human operators supervising mixed fleets rather than controlling individual assets. Ground-based autonomous systems will be deployed in complex terrain. AI-driven coordination will dynamically allocate surveillance resources against emerging risk patterns. The frameworks governing these systems will be built on a single underlying principle: at every level of the command chain, a human must be able to understand what the system is doing and be able to stop it if necessary.

5.2 AIR AND SPACE-BASED SURVEILLANCE

Airborne capabilities span the full spectrum of platforms: fixed-wing manned aircraft for long-range maritime and land surveillance, rotary-wing aircraft for SAR and rapid deployment, unmanned aircraft systems (UAS) from tactical mini-UAS to large strategic systems, and high-altitude pseudo-satellites (HAPS) operating in the stratosphere.

These platforms carry sensor payloads including electro-optical and infrared cameras, synthetic aperture radar, maritime radar, electronic intelligence sensors and acoustic systems. Space-based capabilities comprise Earth observation (EO) satellites, satellite communications (SATCOM), and global navigation satellite systems (GNSS), anchored in the EU's flagship programmes — Copernicus, Galileo and GOVSATCOM / IRIS². The two layers are operationally inseparable: space provides the persistent wide-area context and secure connectivity backbone; airborne platforms provide the tactical and operational resolution, responsiveness and intelligence precision that satellites cannot deliver.

WHY IT MATTERS FOR BORDER SECURITY

No other sensor domain offers the combination of reach, persistence, resolution and responsiveness that airborne and space-based surveillance together provide. For the EBCG, this integrated layer is the foundation on which all other operational capabilities rest: without persistent awareness of what is happening across Europe's external borders, every other capability, autonomous systems, biometric checks, return operations, is reactive rather than anticipatory.

AIRBORNE CAPABILITIES

The coming decade will transform the airborne layer through three convergent developments.

First, AI-powered on-board sensor fusion will convert airborne platforms from passive data collectors into intelligent edge nodes capable of classifying vessels, detecting persons, generating tracks and correlating intelligence against watchlists at the point of collection, without waiting for data to reach a ground station. This dramatically shortens the sensor-to-decision cycle and reduces the volume of raw data requiring transmission over constrained satellite links.

Second, HAPS operating in the stratosphere at 18-25 km altitude will provide continuous wide-area surveillance of entire migration corridors with endurance measured in weeks rather than hours, at a lower lifecycle cost than satellite constellations. HAPS uniquely bridge airborne and space layers, offering the responsiveness and sensor flexibility of an aircraft with the persistence and coverage of a satellite.

Third, the proliferation of hostile UAS by criminal networks, used for surveillance of EBCG operations, smuggling payload delivery and disruption of surveillance systems, will require airborne counter-UAS (C-UAS) capability to be integrated into patrol aircraft and UAS as a standard mission element, not an optional addition.

SPACE SURVEILLANCE AND SERVICES

Space assets provide wide-area, persistent, weather-independent, secure communications links and authenticated positioning that airborne platforms depend on for effective operations. Copernicus supports change detection, vessel tracking, migration route monitoring and environmental surveillance. Copernicus-Next and a possible EU border security space constellation would provide dedicated, prioritised Earth observation capacity for border-security missions, reducing dependence on shared civil capacity. Commercially, the rapid growth of very high resolution (VHR) commercial EO constellations with sub-metre resolution optical and SAR imagery, is transforming space from a strategic to a near-operational intelligence layer, with sub-daily revisit times over priority areas. AI-powered processing of this imagery at cloud scale will reduce the satellite-to-intelligence timeline from hours to minutes.

Galileo's Open Service Navigation Message Authentication (OSNMA) is increasingly critical as GNSS spoofing and jamming, documented extensively along the EU's eastern borders, degrades the positioning

integrity on which UAS operations, maritime surveillance and autonomous system coordination depend. GOVSATCOM and IRIS² provide secure, jam-resistant satellite connectivity to keep airborne assets operational when terrestrial networks are absent or degraded. Satellite Quantum Key Distribution (QKD), developed through the European Quantum Communication Infrastructure (EuroQCI) programme, may by 2036 provide the most sensitive Frontex intelligence channels with cryptographic protection.

TEN-YEAR OUTLOOK

By 2036, airborne and space-based surveillance will function as a seamlessly integrated, AI-orchestrated multi-layer architecture. Large strategic UAS will handle most routine maritime patrol missions. HAPS will maintain persistent stratospheric coverage of critical border sections. Crewed aircraft will concentrate on complex, multi-sensor intelligence-gathering operations and escalating situations that require human judgment and adaptability. Space assets will provide persistent wide-area context and secure connectivity to amplify the effectiveness of the airborne layer. AI will fuse multi-layer data (airborne, stratospheric and satellite) into a unified operational picture updated in near-real time and accessible across the EBCG community through the European Situational Picture. The regulatory environment will have matured to enable large-scale beyond visual line of sight (BVLOS) UAS operations, removing current constraints on aerial deployment range and altitude.

5.3 ARTIFICIAL INTELLIGENCE — A STRATEGIC CAPABILITY FOR BORDER SECURITY

Artificial intelligence is not a single technology but a family of capabilities — machine learning, computer vision, natural language processing, predictive analytics and the emerging generation of agentic systems — that together constitute a consequential technological shift in border management. AI is the enabling architecture through which every other capability described in this report reaches its potential: it converts data from UAS, satellites and ground systems into actionable intelligence; it coordinates autonomous platform fleets; it detects fraudulent identities in biometric data; it predicts migration pressures before they materialise at the border; and it compresses the cycle from threat detection to operational response.

Federated learning, training shared AI models across distributed datasets without centralising raw data, makes it possible to build pan-European intelligence capabilities without requiring Member States to cede control over their national data. Generative AI will add capabilities in document analysis, automated intelligence reporting and multilingual operational support.

THE STRATEGIC ROLE OF AI IN BORDER CAPABILITY DEVELOPMENT

In the situational awareness and risk analysis domain, AI will enable the EBCG to shift from a posture of reactive response to genuine anticipatory awareness, identifying the indicators of an impending pressure pattern days or weeks before it reaches the external border. AI models drawing on migration data, geopolitical indicators, climate signals and open-source intelligence are expected to generate probabilistic forecasts of emerging pressure on specific border sections, enabling Frontex and Member State authorities to reallocate human resources and technical equipment, intensify aerial surveillance and engage third-country partners before a situation escalates.

In the operational domain, AI will transform the human-machine relationship across the entire EBCG capability stack. In the airborne layer, AI on-board processing converts UAS and patrol aircraft from data collection platforms into intelligent surveillance nodes that generate actionable intelligence at the

edge, drastically reducing the bandwidth required for satellite downlinks and the latency of the intelligence cycle. In maritime operations, AI will enable autonomous surface vessels to maintain persistent patrol coverage, identify and monitor vessels of interest, and dynamically reposition in response to emerging situations. Across all these domains, AI will not replace human judgment in decisions, it will amplify the quality and speed of the information available to human decision-makers and will reduce the cognitive burden of monitoring tasks that might exceed human capacity.

In the longer term, AI will transform capability development itself. The EBCG research and innovation agenda will increasingly be shaped by AI-supported analysis of operational performance data, identifying the capability gaps, sensor limitations and procedural bottlenecks that have the greatest impact on border security outcomes. AI-powered simulation environments, drawing on Frontex's Digital Twin of the EU External Borders, will allow new capabilities to be tested, evaluated, and refined in virtual operational scenarios before development and procurement decisions are made. This will dramatically reduce the cost and time of capability development cycles and improve the probability that new investments deliver their intended operational effect.

WHY IT MATTERS FOR BORDER SECURITY

The high volume of data generated by UAS, satellites, sensors, cameras and information systems across the EBCG is close to exceeding the analytical capacity of the human workforce managing it. This gap will widen significantly over the coming decade as UAS fleets expand, HAPS provide continuous wide-area imagery, commercial satellite constellations increase revisit frequency, and biometric systems process growing traveller volumes. Without AI, the expansion of surveillance infrastructure will produce diminishing returns: more sensors generating more data that cannot be converted into timely intelligence at the pace operational decisions require. With AI, each new sensor and platform added to the EBCG capability stack will generate compounding returns, because AI can integrate the new data streams into a continuously improving operational picture without proportional growth in the human analytical workforce.

The strategic and operational primacy of AI comes with an equally significant responsibility: to ensure that AI systems always remain under meaningful human control. This is not a constraint on AI's effectiveness, it is the condition that makes AI deployment politically sustainable, legally defensible and operationally reliable. An AI system whose outputs operators cannot understand, whose errors they cannot detect and whose behaviour they cannot correct is not a capability, it is a high-risk liability. The history of technology adoption in security and law enforcement contexts demonstrates clearly that public and institutional trust in new capabilities depends entirely on the confidence that humans are directing them, not the other way around.

TEN-YEAR OUTLOOK

By 2036, AI will be embedded across the entire border management chain, from on-board UAS edge processing and satellite imagery analysis to operational planning and capability development. Agentic AI systems will manage routine operational tasks like airborne patrol tasking and alert generation, with human oversight concentrated on exception management and decisions with significant consequences for individuals. The establishment of a Frontex-coordinated federated learning infrastructure would enable shared predictive intelligence across all Member States. AI will have become the primary engine of capability development: operational data will continuously feed AI-driven analysis of performance gaps and investment priorities, and virtual simulation environments will allow new capabilities to be evaluated before procurement. The EBCG's AI governance architecture, built on explainability, continuous monitoring, adversarial testing and dependency management, will ensure that as AI systems become more capable and more deeply embedded in operations, the human capacity to understand, direct and correct them keeps pace.

5.4 QUANTUM TECHNOLOGIES

Quantum technologies are expected to deliver advanced capabilities in sensing, communication and computing. Quantum sensors will offer unprecedented sensitivity for detecting magnetic, gravitational or electromagnetic signals, enabling detection of concealed objects, tunnels and submerged vessels beyond classical physical limits. QKD will enable higher security cryptographic key exchange — physically impossible to intercept without detection.

WHY IT MATTERS FOR BORDER SECURITY

Quantum sensing could detect concealed smuggling tunnels, submerged vessels and concealed weapons with sensitivity unavailable to classical systems. Satellite-based QKD through EuroQCI may within the decade provide Frontex's most sensitive channels with advanced cryptographic security.

TEN-YEAR OUTLOOK

By 2036, early quantum sensing and QKD will be entering operational use for high-value missions. All EBCG encrypted solutions will have completed migration to post-quantum cryptography (PQC) — resistant cryptography on sovereign infrastructure — establishing the non-negotiable cryptographic baseline from which all other technology investments proceed.

5.5 COUNTER-UNMANNED AIRCRAFT SYSTEMS (C-UAS)

C-UAS technologies detect, track, identify and, where authorised, neutralise non-cooperative or hostile drones. Detection methods include radar, radio-frequency scanning, acoustic sensors and electro-optical systems. Neutralisation encompasses electronic jamming, signal spoofing and directed-energy systems. The proliferation of advanced commercial UAS, long-range FPV drones, swarm-capable platforms and AI-guided systems is rapidly expanding the airspace threat at borders. The EU Drone and Counter-Drone Action Plan provides the policy framework, but operational implementation and legal harmonisation across Member States remain uneven.

WHY IT MATTERS FOR BORDER SECURITY

Criminal networks use drones for hostile surveillance, smuggling payload delivery and coordination of irregular crossings. Hostile state actors might achieve the capacity to use drone swarms to overwhelm or deceive border surveillance systems. AI-driven swarm behaviour, multiple cooperating drones adapting collectively to countermeasures, requires layered architectural responses rather than single point-defence systems. C-UAS must be integrated into the Frontex surveillance architecture: UAS and patrol aircraft operating along EU external border areas increasingly face the risk of hostile drone interference, requiring on-board detection and countermeasure capability. Control over C-UAS AI systems, particularly automated classification and discrimination, is critical: operators must be able to understand and verify the basis for any neutralisation recommendation before authorising action, and must retain the ability to override AI outputs at any stage of the engagement cycle.

TEN-YEAR OUTLOOK

By 2036, integrated multi-layer C-UAS systems will be standard at high-risk border sections and embedded in the EBCG aerial fleet. AI classification will have substantially reduced false alarm rates. Directed-energy systems will complement electronic countermeasures. EU harmonised legal frameworks for airspace neutralisation will have matured, enabling consistent and proportionate operational responses across Member States.

5.6 SECURE AND RESILIENT COMMUNICATIONS

Next-generation communication technologies include 5G/6G networks, software-defined radios, mesh networking and satellite-terrestrial hybrid systems. Combined with Post-Quantum Cryptography (PQC and GOVSATCOM / IRIS², these technologies enable secure, high-bandwidth, low-latency connectivity for deployed assets and command centres. For the EBCG airborne domain, secure and resilient GOVSATCOM is the critical link enabling real-time data transmission from UAS and surveillance aircraft and will evolve to support AI-enabled on-board processing with selective downlink of processed intelligence rather than raw sensor data streams.

WHY IT MATTERS FOR BORDER SECURITY

EEffective border operations depend on reliable, secure and interoperable communications in remote and contested environments. Airborne platforms, UAS and crewed aircraft are particularly dependent on resilient communications for mission control and sensor data transmission. Loss or degradation of command links for UAS in BVLOS operations represents both an operational and safety risk. All EIBM communication infrastructure must meet three sovereignty objectives under the EU Cloud Sovereignty Framework: Legal and jurisdictional sovereignty; operational sovereignty and security and compliance sovereignty including PQC-compliant encryption.

TEN-YEAR OUTLOOK

By 2036, EBCG communications will be hybrid, combining terrestrial, airborne and satellite links with automatic failover and AI-managed spectrum optimisation. PQC encryption will protect all sensitive operational data. IRIS² and GOVSATCOM will underpin secure connectivity for deployed aerial and maritime assets. AI-driven network management will maintain communications continuity for UAS in BVLOS operations and crewed aircraft on extended surveillance missions.

5.7 DIGITAL TWINS AND SIMULATION ENVIRONMENTS

A digital twin is a dynamic virtual representation of a physical system or environment, continuously updated with live operational data. For border security, this extends from individual BCPs to the EU's external borders as a whole, integrating open sources, satellite imagery, airborne sensor feeds and ground surveillance inputs into a unified operational model. The Frontex Digital Twin of the EU External Borders is expected to be the most significant investment in this domain.

WHY IT MATTERS FOR BORDER SECURITY

The digital twin supports operational planning and contingency management by enabling planners to simulate migration pressure scenarios, capability deployments and policy responses before committing resources. At the tactical level, it allows commanders to rehearse responses to specific scenarios in safe virtual environments. AI systems driving digital twin scenario generation must meet the same controllability and transparency standards applied to operational AI: planners must be able to understand the assumptions underlying simulated outcomes and challenge them when they appear inconsistent with operational judgment.

TEN-YEAR OUTLOOK

By 2036, the Digital Twin of the EU External Borders will be an operational planning tool updated continuously by satellite, airborne and ground sensor feeds. AI-driven scenario generation will enable planners to identify optimal asset pre-positioning across the EBCG. Training scenarios derived from the twin will be accessible across Member States, reducing the cost of large-scale exercises while maintaining standardised quality.

5.8 ADVANCED BIOMETRICS AND IDENTITY INTELLIGENCE

Advanced biometric technologies encompass next-generation facial recognition, multimodal biometrics combining face, iris and fingerprint, AI-driven document authentication, and synthetic identity detection. The EU's large-scale information systems, EES, VIS and EURODAC, provide the biometric reference infrastructure for pre-departure screening through visa procedures and border checks, managed through the eu-LISA interoperability framework.

WHY IT MATTERS FOR BORDER SECURITY

Biometric accuracy and resilience directly determine the effectiveness of border control. AI-generated synthetic identities, deepfake facial imagery and adversarial biometric inputs represent a growing and technically sophisticated threat requiring dedicated counter-AI testing programmes. Biometric AI systems carry the highest requirement for human oversight and explainability of any AI application in border management: a biometric match or non-match can determine the outcome of an individual's border-crossing, and border guards must be able to understand the confidence level, the factors contributing to a decision and the circumstances under which the AI output should be challenged.

TEN-YEAR OUTLOOK

By 2036, AI-enhanced multimodal biometric systems will be standard at major EU BCPs. Automated processing will handle most low-risk travellers, concentrating officer attention on complex and ambiguous cases. Quantum-proof encryption might be required to protect biometric data repositories. Continuous adversarial testing programmes will maintain accuracy against evolving attack techniques.

5.9 CLOUD SOVEREIGNTY AND SOVEREIGN COMPUTING INFRASTRUCTURE

Cloud sovereignty refers to the degree to which digital services, data and AI systems remain under EU legal, operational and technological control. The European Commission Cloud Sovereignty Framework (DG DIGIT October 2025) establishes Sovereignty Objectives and Sovereignty Effectiveness Assurance Levels. The European High-Performance Computing (EuroHPC) Joint Undertaking provides the sovereign high-performance computing layer, EU-jurisdiction graphics processing units (GPU) and central processing units (CPU) clusters with no non-EU third-party control, for the most demanding EIBM workloads: AI model training, surveillance and satellite data analytics, biometric processing and digital twin simulation.

WHY IT MATTERS FOR BORDER SECURITY

Every technology mentioned in this report runs on cloud infrastructure. The sovereignty of that infrastructure determines whether advanced capabilities are operationally resilient and legally defensible or exposed to the legal reach of non-EU jurisdictions. For airborne surveillance specifically, real-time UAS sensor feeds, vessel tracks, biometric records and migration intelligence all require processing on infrastructure that excludes legal access from countries outside the EU.

TEN-YEAR OUTLOOK

By 2036, all EIBM-critical infrastructure will have been assessed and procured against the Sovereignty Objectives and Sovereignty Effectiveness Assurance Levels. EuroHPC nodes will serve as the primary HPC substrate for AI training, surveillance and satellite analytics, and biometric processing. Infrastructure with the highest Sovereignty Effectiveness will host all quantum-safe key management and biometric repositories.

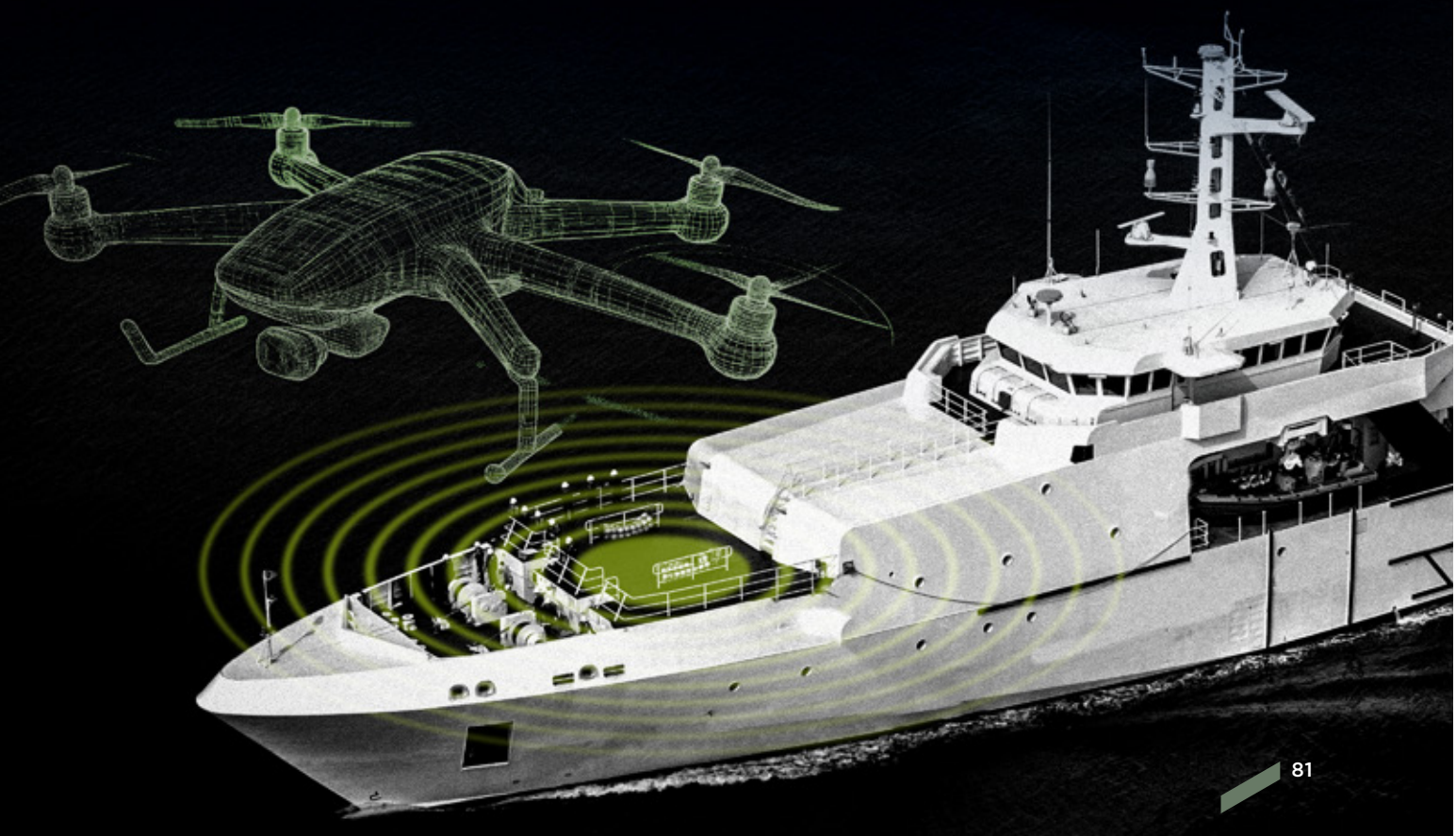
5.9.1 CONCLUSION

The nine technology areas: autonomous systems, airborne and space-based surveillance, AI, quantum technologies, counter-UAS, secure communications, digital twins, advanced biometrics and cloud sovereignty, represent the most significant drivers of change for European border security over the next decade. Three strategic priorities emerge above all others.

Airborne and space-based surveillance is the most operationally immediate priority. The EBCG's aerial capability, UAS, HAPS, crewed patrol aircraft, integrated with satellite EO and communications, is the main surveillance and intelligence source on which most capabilities depend. The transition from predominantly crewed aircraft to a mixed layered architecture of strategic UAS, HAPS and crewed platforms for complex missions is underway and must be accelerated, with space and airborne assets operated as a unified integrated architecture optimised by AI.

Artificial intelligence is the defining strategic technology of the decade. It is not simply a tool that improves individual tasks, it is the capability that enables the EBCG to shift from reactive response to anticipatory awareness, from data overload to actionable intelligence at operational speed, and from linear capability development to AI-driven continuous improvement. The condition for realising this potential is maintaining human control over AI systems at every level: understanding what they are doing, being able to correct them when they are wrong, and preserving the human proficiency to operate without them when necessary.

Cloud sovereignty is the infrastructure foundation that determines whether all other investments are effectively utilised and operationally resilient. The EU Cloud Sovereignty Framework and EuroHPC provide the tools to ensure that the technology on which EBCG decisions depend remains under EU control. Post-quantum cryptography migration must begin in the coming years, before the cyber threat of harvest-now-decrypt-later materialises on current sensitive EBCG communications.



6. Conclusions

6.1 STRATEGIC ENVIRONMENT AND MEGATRENDS

EIBM is implemented in a highly volatile, uncertain, complex and ambiguous (VUCA) global environment, shaped by six interacting dimensions: climate, demography, society, economy, technology and geopolitics (the 'Strategic Hexagon').

KEY CONCLUSIONS

- Internal EU political fragmentation — driven by competing national interests, divergent migration policies and vulnerability to external manipulation — is a major strategic risk to the EU's ability to act cohesively on border issues.
- A more competitive, hostile, multipolar geopolitical order is expected to push the EU toward assuming greater responsibility for managing its own crises, including migration.
- Structural forces (population growth, urbanisation, climate change, resource scarcity, socioeconomic inequality) are expected to cumulatively increase the number of people on the move over the next decade, diversifying migration corridors beyond current patterns.
- The instrumentalisation of migration — often paired with disinformation campaigns — is expected to grow as a hybrid-threat vector aimed at destabilising EU border policy and public trust.
- Demographic aging in Europe creates a dual pressure: fewer people available to recruit as border guards, while economic demand for migrant labour rises — a tension that EIBM planning must reconcile rather than treat as a side issue.

6.2 KEY FINDINGS FROM STRATEGIC INTERVIEWS

Based on ten anonymised strategic interviews with senior EU stakeholders, analysed against the EIBM's 15-component framework, the following should be taken into account:

- **EIBM must be governed as a system of systems.** The 15 components are interdependent; managing them in isolation leaves implementation structurally incomplete.
- **Integration depth matters more than organisational expansion.** Additional staff, assets or mandate only create value when connected through shared planning, logistics and information systems.
- **Anticipatory governance must enter the policy cycle.** Foresight only has operational value when it actually reshapes budgets, recruitment, procurement and contingency planning.
- **The core information problem is data-to-decision performance, not data scarcity.** The EU has enough data; it lacks integrated, trusted and timely processes to convert it into shared decisions.
- **Return is the most under-integrated EIBM component.** It needs systematic inclusion in risk analysis, governance, vulnerability assessment and third-country strategy.
- **Technical integration will outpace political centralisation.** By 2036-2040, the likely outcome is a system more European in information and operations, but still largely national in legal / political authority.

- **Hybrid threats require a wider security-resilience architecture.** Instrumentalised migration, cyber operations and organised crime demand clearer interfaces between border, police, intelligence, cyber and defence actors.
- **Fundamental rights and professional standards are operational capital.** Legality, data protection and accountability sustain the trust needed for information-sharing and mandate growth — they are not merely legal constraints on operations.
- **Search and rescue, legitimate travel and vulnerability safeguards need more visibility.** These are well covered in the Commission's formal framework but under-represented in stakeholder discourse.
- **The next phase should prioritise consolidation over expansion.** After a period of crisis-driven growth, the strategic need is to professionalise, reduce silos and focus on fewer high-impact priorities.
- **European added value must be demonstrated, not assumed.** EU-level institutions remain relevant only where they provide capabilities that Member States cannot efficiently produce alone.
- **The positive future is a trusted, interoperable network — not full centralisation.** Success requires a common strategic picture and complementary capabilities, not a single unified command.

6.3 THEMATIC AREAS

6.3.1 MIGRATION

- Geopolitical instability and economic downturns (Ukraine, Gaza, Sahel) are identified as the leading drivers of displacement towards the EU, with geopolitics and economics rated the two highest-impact megatrends on irregular migration.
- A purely security-driven ('securitised') approach is discouraged in favour of addressing structural drivers — poverty, conflict, climate — while pursuing pragmatic, outcome-oriented crisis management given the slow pace of root-cause solutions.
- Frontex international cooperation frameworks (status agreements, working arrangements) function well with cooperative third countries but leave uncooperative states outside meaningful collaboration, creating space for smuggling networks.
- Transactional cooperation incentives (aid, legitimisation) with major source countries are flagged as a long-term sustainability risk rather than a durable solution.

6.3.2 RETURN ACTIVITIES

- Return effectiveness across the EU should be further increased in close alignment with other EIBM elements.
- The effectiveness of the EU's return systems in the coming years is expected to remain shaped by a complex interaction of structural, operational, legal and external challenges. At the core of these challenges lies the uneven level of cooperation with third countries.
- The harmonisation of divergent national approaches to return procedures is expected by changes in the EU legal framework, in particular by the new Return Regulation.
- Challenges related to timely uploads of SIS alerts will be resolved by increased interoperability of national and EU IT systems.
- Digitalisation and AI use in return-case management are expected to keep expanding, Further digitalisation and AI use must preserve data protection, data quality and effective human oversight.

6.3.3 INTERNAL SECURITY

- The definition of border control itself should be widened to include partnerships with origin countries and disruption of criminal networks. These should not be treated as separate from border security.
- EU-coordinated (rather than bilateral) responses are essential for consistency across Member States.

6.3.4 CROSS-BORDER CRIME

- Migrant smuggling is expected to keep growing structurally. As legal routes tighten, crossing the external border without a smuggler is becoming a rare occurrence, pushing nearly all irregular migration through criminal networks.
- Smuggling and trafficking are increasingly digitalised (AI-tailored marketing, encrypted apps, cryptocurrency), lowering smugglers' risk of detection while raising profit margins.
- Labour trafficking is expected to rise alongside the EU's aging workforce and labour shortages, particularly in construction, manufacturing and transport.
- Firearms trafficking is shifting from complete weapons to smuggled components via ordinary parcel services, compounded by 3D-printing enabling partial domestic weapon production. This undermines detection strategies built around whole firearms.
- Maritime containers account for an estimated 80-85% of drug seizures at EU ports, yet only 2-10% of containers are physically inspected — a major structural vulnerability.
- Cocaine supply into the EU is not expected to decline even if seizures fall at some entry points, since this likely reflects route displacement rather than reduced trafficking.
- Cross-border crime and hybrid threats should be treated as interconnected problems requiring one coordinated policy response, with heavier use of AI-driven detection tools.

6.3.5 TERRORISM

- The terrorist threat to the EU remains linked mainly to conflict zones; undetected border crossings by individuals who pose a security risk are the primary border-relevant concern.
- Africa is expected to remain the main global hub of terrorist activity in the coming years, with Russia's expanding regional footprint seen as indirectly fuelling instability and jihadist recruitment.
- US drawdown from Syria / Iraq could open security gaps enabling an ISIS resurgence, with a risk of spillover towards the EU.
- Weapons proliferation from the war in Ukraine is expected to feed trafficking networks and extremist ecosystems on the EU's eastern border for years, regardless of whether the conflict ends.
- As EU security-database interoperability remains incomplete, in the near-term systematic checks of all travellers against existing databases should be ensured, along with better use of biometrics.

6.3.6 HYBRID THREATS

- Hybrid threats are expected to intensify, defined by adversaries instrumentalising multiple levers simultaneously — migration, disinformation, cyberattacks, sabotage and organised crime — rather than any single-vector attack.
- Russia is expected to continue or recalibrate (not necessarily reduce) hybrid operations against the EU's eastern border even after a Ukraine ceasefire, treating the ambiguity between war and peace as a deliberate strategic tool.
- Three flashpoints are highlighted for the next decade: The Western Balkans (organised crime groups as potential state proxies), Africa (Russian-enabled migration pressure), and the Arctic (an emerging strategic frontier as melting ice opens new routes and rivalry intensifies over infrastructure).

- Hybrid operations deliberately exploit 'legal grey zones' where current EBCG mandates may be inadequate. This implies existing legal / operational frameworks already lag behind the threat.
- Recommended countermeasures: Network-based mapping of adversarial and criminal actors, a coordinated EU anti-disinformation strategy, deeper NATO-EU cooperation, and designated 'innovation hub' Member States to pilot and standardise cross-border detection tools.

6.3.7 CROSS-CUTTING PATTERN

Across all six thematic areas, three structural gaps recur: (1) uneven cooperation with third countries, (2) fragmented, non-interoperable Member State systems and data, and (3) a widening gap between legal frameworks and the operational reality of hybrid and digital threats. This mirrors the strategic-interview findings above, suggesting the report's thematic and interview-based analyses reinforce each other.

6.4 TECHNOLOGY FORESIGHT

Nine technology domains were assessed as the most significant drivers of change for European border security over the next decade: autonomous systems, air and space-based surveillance, AI, quantum technologies, counter-UAS, secure communications, digital twins, advanced biometrics and cloud sovereignty. Three stand out as top strategic priorities:

AIR AND SPACE-BASED SURVEILLANCE

- the most operationally immediate priority. The EBCG's aerial capability (UAS, HAPS, crewed aircraft) integrated with satellite EO and communications is the primary surveillance and intelligence source most other capabilities depend on. A shift toward a mixed, AI-optimised layered architecture is underway and should be accelerated.

ARTIFICIAL INTELLIGENCE

- described as the defining strategic technology of the decade, enabling a shift from reactive response to anticipatory awareness. Its benefits depend on maintaining human control at every level: understanding, correcting, and being able to operate without AI systems when necessary.

CLOUD SOVEREIGNTY

- the infrastructure foundation determining whether other technology investments are effectively usable and resilient. The EU Cloud Sovereignty Framework and EuroHPC are cited as key enablers, alongside an urgent need to begin post-quantum cryptography migration before 'harvest-now-decrypt-later' cyber threats materialise against current sensitive communications.

6.5 CROSS-CUTTING RECOMMENDATIONS

Recommendations drawn from across the report's megatrends, thematic and technology sections:

- Harmonise border-related procedures and ensure interoperability of large-scale IT systems across the EBCG community.
- Strengthen pre-frontier intelligence and land / maritime border controls.
- Pursue strategic autonomy in border-relevant technology to reduce dependency on

non-EU systems; use Frontex as a testbed for EU-developed technology.

- Reframe the migration narrative from a pure security threat towards an economic / demographic opportunity, while guarding against disproportionate surveillance through 'rights-by-design' principles.
- Conduct a formal strategic review of the trend towards border militarisation and assess its compatibility with EU values.
- Build robust contingency and resilience plans covering cyberattacks, infrastructure failure, climate shocks and migration surges.
- Move towards a holistic framework connecting border control with reception and integration, rather than treating them as separate administrative silos.
- Establish clear, transparent legal frameworks and migration governance mechanisms to prevent fragmentation and ensure consistent application of rights and responsibilities.
- Increase EU research and development funding in border-related technologies to close innovation gaps.
- Design a tailored communication strategy for both EU citizens and countries of origin to promote legal migration pathways and counter misinformation.

6.6 AREAS IDENTIFIED FOR FURTHER EXPLORATION

- Long-term implications of geopolitical fragmentation for EU strategic autonomy and return-cooperation mechanisms.
- The role of legal migration in addressing demographic decline and workforce shortages, including possible expansion of the EBCG's mandate.
- Concrete contingency plans for climate-related disruption and migration surges, including legal frameworks for climate-displaced populations.
- Governance, ethics and operational integration of AI, surveillance technologies and large-scale IT systems in border management.
- A formal review of the militarisation trend in border control and its compatibility with the EU's strategic identity.
- Scalable models for inter-agency and inter-Member-State cooperation under conditions of asymmetric pressure or systemic crisis.

6.7 FINAL REMARKS

EIBM is entering a decade that will be defined less by adding capacity and more by integrating what already exists — across the 15 EIBM components[67], across Member States' IT and legal systems, and across the border, security and technology domains. Migration, cross-border crime, terrorism and hybrid threats are increasingly treated as interconnected rather than separate risk categories, all converging on the same structural weak points: uneven third-country cooperation, fragmented data and legal systems, and a legal / operational framework that lags behind hybrid and digital threats. Air and space-based surveillance, AI and cloud sovereignty are identified as the technology investments with the highest strategic leverage for closing these gaps over the next decade.

7. Recommendations

7.1 BORDER CONTROL

LEGISLATIVE · Adopt an enhanced Frontex regulation and the pending **amendment to the Schengen Borders Code** defining instrumentalisation of migrants and the applicable response rules. Enforce the adopted **screening Regulation** linking border checks to return and asylum procedures.

OPERATIONAL · Complete SIS/EES/VIS/ETIAS interoperability and pair the statistical information from these systems (where allowed by legislation) with AI-optimised, layered air and space-based surveillance (UAS, HAPS, satellite EO) – this report's top-priority technology investment – so situational awareness and physical BCP controls advance together.

POLICY · Develop a formal strategic review to enhance border control and border surveillance to keep pre-frontier capability growth aligned with EU values; develop an anticipatory policy based on foresight and horizon scanning.

7.2 SEARCH AND RESCUE

OPERATIONAL · Extend the maritime autonomous systems and satellite Earth-observation investment identified in the technology foresight explicitly to **SAR detection coverage**, not only enforcement surveillance, so persistent patrol assets serve both functions.

POLICY · Treat SAR capacity as a named line in the ten-year EBCG technology roadmap rather than an implicit by-product of border-surveillance procurement, given how directly the two depend on the same aerial and maritime assets.

7.3 RISK ANALYSIS

OPERATIONAL · Build the **Frontex-coordinated learning infrastructure** described in this report, in order to generate probabilistic pressure forecasts from migration, geopolitical, climate and open-source data without requiring Member States to centralise raw national data.

POLICY · Shift risk-analysis products from a reporting function to a **decision-triggering** one: Require that strategic risk analysis and vulnerability assessment findings feed directly into budget, procurement and deployment decisions for each planning cycle, closing the 'data-to-decision' gap that this report identifies as the central information problem.

7.4 COOPERATION BETWEEN MEMBER STATES SUPPORTED AND COORDINATED BY THE AGENCY

LEGISLATIVE · Use the pending review of Regulation (EU) 2019/1896 to give the **30 000-strong Standing Corps** an explicit legal and command basis — deployment conditions, legal status on Member State and third-country territory — rather than scaling headcount ahead of the governance framework required to absorb it.

POLICY · Position Frontex as the Member States' **default first call** for cross-border knowledge, technology and operational support — complementarity, not substitution — and require Member States to align national border-management strategies to the EU's strategic policy.

7.5 INTER-AGENCY COOPERATION

OPERATIONAL · Formalise joint risk products and shared services between Frontex, Europol, EUAA and eu-LISA on a fixed cycle, and extend functional cooperation structures with **customs authorities** at national level so goods and passenger flows are managed through one coordinated picture rather than parallel systems.

POLICY · Build standing interfaces — not case-by-case arrangements — linking border authorities with law enforcement, intelligence, cyber-security, civil protection and, where relevant, defence actors for **hybrid-threat response**, as the foresight report's strategic interviews call for without endorsing militarisation.

7.6 COOPERATION WITH THIRD COUNTRIES

LEGISLATIVE · Conclude the **remaining status agreements** under the existing Council mandate so that third-country has a stable, harmonised legal counterpart on the EU side.

OPERATIONAL · Expand the **liaison-officer network** and complete the working arrangements already in negotiation, prioritising the main migratory-route countries.

POLICY · Adopt a coordinated **'Team Europe'** approach to third countries — combining migration, development, trade and visa-policy leverage — replacing the fragmented, largely bilateral engagement that this report identifies as a structural weakness, particularly with currently uncooperative countries of origin.

7.7 TECHNICAL AND OPERATIONAL MEASURES WITHIN THE SCHENGEN AREA

LEGISLATIVE · Ensure the new Return Regulation and its digitalisation instrument explicitly require Member States to feed **absconding and secondary-movement data** into shared Schengen-area case management, closing the interoperability gap that this report ties directly to secondary movements.

OPERATIONAL · Build a **common EU system for identifying absconded returnees**, on top of the new SIS return-decision alert feature.

7.8 RETURN

LEGISLATIVE · Enforce the new **Return Regulation as a directly applicable regulation, not a directive**, which will determine the EU return system's coherence over the next five to ten years. Write reintegration into the legal architecture of return rather than leaving it grant-funded: Define Frontex's **Joint Reintegration Services** role, data-sharing basis, and minimum continuity-of-support standards directly in the Return Regulation and the EBCG Regulation review.

OPERATIONAL · Consolidate the **Return Coordinator / High-Level Network for Returns** operational strategy. Change reintegration-support contracting from **annual grant agreements** to flexible, scalable, multiannual partnerships, and complete digitalisation of national return case-management systems on the Frontex-built model to support interoperable, case-level oversight.

POLICY · Ensure judicial review and appeal pathways operate through timely procedures, deepening structured cooperation with judicial authorities and independent fundamental-rights monitors including NGOs — this report stresses that **prolonged legal challenges**, not fundamental-rights safeguards themselves, are what undermines return credibility.

7.9 USE OF STATE-OF-THE-ART TECHNOLOGY, INCLUDING LARGE-SCALE IT SYSTEMS

LEGISLATIVE · Set a **binding EU-wide deadline for post-quantum cryptography migration** across EBCG and Member State systems ahead of 'harvest-now-decrypt-later' exposure and codify 'rights-by-design' and proportionality requirements as a condition of procurement, not a post-hoc review, for AI and surveillance deployment.

OPERATIONAL · Enhance the **Central repository for reporting and statistics** online on the EU-LISA timeline so that the repository can, under well-defined purposes and safeguards, feed into decision making more effectively. Further development the existing toolbox of vulnerability assessment simulation exercises. Use the findings to strengthen preparedness and address identified capability gaps.

POLICY · Rank **air/space-based surveillance, AI, and cloud sovereignty** as the three top-priority technology investments for the decade, per the foresight report's own technology ranking, rather than distributing funding evenly across all nine assessed domains; adopt an EIBM-wide AI governance policy built on explainability, continuous monitoring, adversarial testing and non-negotiable human oversight.

7.10 QUALITY CONTROL MECHANISM

OPERATIONAL · Convert Schengen evaluations and vulnerability assessments from **periodic compliance exercises** into live stress tests — this report calls specifically for stress-testing border-management resilience against cyberattacks, power-grid or database outages, migration surges and climate shocks, rather than only paper-based reviews.

POLICY · Feed vulnerability-assessment findings directly into the effects-based capability planning so quality-control results change resourcing decisions rather than only producing recommendations to national authorities.

7.11 SOLIDARITY MECHANISMS, IN PARTICULAR EU FUNDING INSTRUMENTS

LEGISLATIVE · Require, through the EBCG Regulation review, that BMVI/AMIF allocations to Member States are **conditional on alignment** with the EIBM strategic policy's stated goals.

OPERATIONAL · Use the **Technical Support Instrument** proactively to help lower-capacity Member States implement specific EIBM components rather than leaving uptake to individual national requests, 7.12 Crisis prevention and preparedness.

POLICY · Increase the share of BMVI/Frontex budget devoted to **European R&D in border technology**, using Frontex as a test agency for EU-developed solutions, to reduce dependency on non-EU systems as a deliberate strategic-autonomy objective.

7.12 CRISIS PREVENTION AND PREPAREDNESS

OPERATIONAL · Build and **live-test** contingency and resilience plans for critical failure scenarios (a major economic downturn, widespread cyberattacks, power-grid or database outages) as explicit, scheduled exercises rather than static documents held in reserve

POLICY · Institutionalise anticipatory governance as a standing part of the policy cycle: Weak-signal monitoring, scenario planning and capability-gap review feeding directly into the Schengen cycle's budget, recruitment, procurement and training decisions, not published as a separate foresight exercise.

7.13 FUNDAMENTAL RIGHTS

OPERATIONAL · Ensure effective implementation of the Screening Regulation's fundamental-rights safeguards, including independent monitoring under Article 10, appropriate resources, follow-up to findings and referral of alleged violations to the competent authorities.

POLICY · Treat fundamental rights, legality and proportionality as **operational capital** rather than a compliance constraint: This report is explicit that trust built on rights compliance is what sustains information-sharing, mandate growth and Schengen resilience — a reputational and functional asset, not only a legal obligation.

7.14 EDUCATION AND TRAINING

OPERATIONAL · **Embed fundamental-rights content** in every basic and specialist training track, not as a separate module, so the 'common border guards' culture is built into initial training rather than added afterwards.

POLICY · Widen recruitment and training beyond traditional operational profiles to encompass **foresight, data science, AI, cyber-security and fundamental-rights expertise**, with structured reskilling and succession planning — the strategic-interview evidence treats this diversification as a precondition for organisational adaptability, not an optional add-on.

7.15 RESEARCH AND INNOVATION

OPERATIONAL · Enhance the **Digital Twin of the EU External Borders** to test and refine new capabilities in simulation before procurement, and expand structured public-private-academic cooperation on technology and skills, with data-protection and independence safeguards built into the cooperation agreements.

POLICY · Adopt the **ten-year EBCG technology roadmap**, covering operational needs, dependencies, lifecycle costs, cyber-security requirements and the skills needed to operate and maintain each system. This roadmap should be congruent with the seven priorities set in the Capability Roadmap of the European Border and Coast Guard.


EUROPEAN BORDER AND COAST GUARD AGENCY
FRONTEX

Endnotes

1 As outlined in Article 8(4) and 29 (2) of the REGULATION (EU) 2019/1896 of the European Parliament and the Council of 12 November 2019

2 as outlined in Article 3(1) and (2) of Regulation (EU) 2019/1896

3 The Strategic Hexagon clusters the 14 Megatrends, long-term driving forces that are observable now and will most likely have significant influence on the future. *https://knowledge4policy.ec.europa.eu/foresight/tool/megatrends-hub_en*

4 The 14th edition of Global Megatrends

5 As defined and described by the Joint Research Centre

6 Department of Water Supply and Sewerage Systems, Faculty of Environmental Engineering, Wroclaw University of Science and Technology, 50-370

7 Sea level rise is a global threat — here's why | World Economic Forum *https://www.weforum.org/stories/2025/03/rising-sea-levels-global-threat/*

8 The Global Water Crisis: Stress, Scarcity, and Conflict — Council on Foreign Relations. *https://www.cfr.org/backgrounders/water-stress-global-problem-thats-getting-worse*

9 *https://www.iea.org/reports/world-energy-outlook-2025*

10 *https://www.iea.org/reports/electricity-2026*

11 *https://www.iea.org/reports/electricity-2026*

12 New United Nations Population Estimates and Projections *https://populationconnection.org/article/new-united-nations-population-estimates-and-projections/*

13 G20 Extraordinary Committee of Independent Experts on Global Inequalit

14 Demographic Trends and Regional Disparities in the EU https://www.mdpi.com/2076-0760/14/9/556

15 Demographic Trends and Regional Disparities in the EU https://www.mdpi.com/2076-0760/14/9/556

16 UNDESA — International Migrant Stock 2024

17 UNDESA — 2024 Revision of World Population Prospect

18 Demographic Trends and Regional Disparities in the EU https://www.mdpi.com/2076-0760/14/9/556

19 Human Rights Watch — World Report 2026

20 *https://www.oxfam.org.uk/get-involved/campaign-with-oxfam/fight-inequality/oxfams-global-inequality-report/#:~:text=In%202025%2C%20billionaire%20wealth%20increased,political%20office%20than%20ordinary%20people.*

21 *https://www.undp.org/asia-pacific/publications/next-great-divergence*

22 Belarus-as-a-hybrid-threat-actor-Hybrid-CoE-Paper-30

23 Pope Leo's 'Magnifica humanitas': AI must serve humanity not concentrate power — Vatican News

24 Kelecha, M. (2026). Polycrisis and global inequality. Global Sustainability, 9, e5, 1—13. *https://doi.org/10.1017/sus.2025.10040*

25 ENISA Threat Landscape 2025_v1.2.pdf *https://www.enisa.europa.eu/sites/default/files/2026-01/ENISA Threat Landscape 2025_v1.2.pdf*

26 ENISA Threat Landscape 2025_v1.2.pdf *https://www.enisa.europa.eu/sites/default/files/2026-01/ENISA Threat Landscape 2025_v1.2.pdf*

27 Resource curse in the age of critical minerals: Geopolitical forces and market maturity — ScienceDirect https://www.sciencedirect.com/science/article/pii/S2214629625003287

28 World Economic Outlook Update, January 2026: Global Economy: Steady amid Divergent Forces; World Economic Outlook 2026/003 *https://financing.desa.un.org/sites/default/files/2026-01/IMF World Economic outlook update 2026JAN.pdf*

29 How the EU's Global Gateway Can Compete in the Global South | Carnegie Endowment for International Peace *https://carnegieendowment.org/europe/strategic-europe/2025/10/how-the-eus-global-gateway-can-compete-in-the-global-south*

30 The Draghi report on EU competitiveness *https://commission.europa.eu/topics/competitiveness/draghi-report_en*

31 *https://thediplomatin spain.com/en/2025/10/24/draghi-defends-a-pragmatic-federalism-for-europe-to-counteract-the-slowness-of-eu-decision-making/ and https://www.politico.eu/article/mario-draghi-push-pragmatic-federalism-get-europe-out-predicament/*

32 See e.g., *https://www.jpmorganchase.com/content/dam/jpmorganchase/documents/center-for-geopolitics/jpmc-world-rewired.pdf*

33 ECB (2023). Gold demand: the role of the official sector and geopolitics *https://www.ecb.europa.eu/press/other-publications/ire/focus/html/ecb.irebox202506_01~f93400a4aa.en.html*

34 BIS (2025). BIS Quarterly Reviews *https://www.bis.org/quarterlyreviews/index.htm*

35 Digital Europe (2024). Overcoming Europe's connectivity challenges to reclaim global leadership

36 Brief_2024-10_IMEC.pdf *https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief_2024-10_IMEC.pdf*

37 Global defence spending continues to grow amid geopolitical uncertainty *https://www.iiss.org/online-analysis/military-balance/2026/02/global-defence-spending-continues-to-grow-amid-geopolitical-uncertainty/*

38 World Energy Investment 2026 — Analysis — IEA *https://www.iea.org/reports/world-energy-investment-2026*

39 For instance, under the 2023 MoU, Tunisia was assured up to about €1 billion funding for migration control. This was €105 million from the EU budget, €150 million for migration, and up to €900 million in macro-financial loans, in exchange for border surveillance, accepting returns of its nationals, and anti-smuggling work. On departures it worked: departures from Tunisia fell by 75% in 2025, but unfortunately those from Libya and Algeria rose by 40% and 43%. That suggests the flow moved rather than disappeared. Returns of Tunisians are a separate problem: according to Eurostat data, Tunisia was still among the top five nationalities ordered to leave in late 2025.
Egypt and Morocco a case of partners bargaining: Egypt received a €7.4 billion package in 2024, yet Egypt considered it is not enough and requested Europe to share more of the cost of hosting refugees. Scholars called this "reversed conditionality": third countries leverage the EU's dependency to further their own interests. Also, after the Ceuta crisis at the end of July 2026, the EU is set to increase funding for Morocco's border control and migration management as part of a partnership deal. Exclusive: EU to boost funding for Morocco's migration management after Ceuta crisis - Yahoo News Canada +2. *https://ca.news.yahoo.com/exclusive-eu-boost-funding-morocco-150008919.html*
DGAP's June 2026 review of the Tunisia, Mauritania, Egypt, Lebanon and Jordan deals concludes that their effectiveness and broader consequences remain contested. *https://dgap.org/en/research/publications/effects-eus-migration-diplomacy*
The EU's Generalised Scheme of Preferences (GSP) / Trade preferences (GSP) were just signed on the 18th of June 2026. This introduces for the first time a link between trade preferences and readmission cooperation. It is expected to apply from 1 January 2027. There is a general risk that this may have limited effect, because return is often not in the interest of sending countries that depend on remittances

40 *https://www.whitehouse.gov/wp-content/uploads/2025/07/Americas-AI-Action-Plan.pdf*

41 *https://www.magazynrekruter.pl/the-sovereign-ai-race-the-eus-fight-for-tech-independence/*

42 Dimitreva et all (2023). The features of the use of Information Technologies in criminal proceedings in the BRICS countries

43 *https://commission.europa.eu/document/download/fcbc7ada-213b-4679-83f7-69a4c2127a25_en?filename=Address%20by%20Mario%20Draghi%20at%20the%20Presentation%20of%20the%20report%20on%20the%20future%20of%20European%20competitiveness.pdf*

44 *https://ucdp.uu.se/downloads/charts/*

45 Organized violence 1989 — 2024, and the challenges of identifying civilian victims — Shawn Davies, Therése Pettersson, Margareta Sollenberg, Magnus Öberg, 2025 *https://journals.sagepub.com/doi/10.1177/00223433251345636*

46 *https://www.theguardian.com/world/2026/mar/22/iran-says-destroy-middle-east-infrastructure-us-energy-sites*

47 *https://www.theguardian.com/world/2026/mar/22/iran-says-destroy-middle-east-infrastructure-us-energy-sites*

48 *https://media.defense.gov/2026/Jan/23/2003864773/-1/-1/0/2026-NATIONAL-DEFENSE-STRATEGY.PDF*

49 *https://www.whitehouse.gov/wp-content/uploads/2025/12/2025-National-Security-Strategy.pdf*

50 Government AI Readiness Index 2025

51 the 2025 National Security Strategy

52 Hein de Haas's seminal work reinforced this approach by emphasizing that migration trends are best understood through long-term historical analysis

53 For instance, understanding the role of transnational criminal networks in exploiting migration routes requires integrating qualitative insights with statistical trends

54 *https://worldtradescanner.com/wco-report_infiltration-of-maritime-cargo-supply-chains_june-2025.pdf*

55 *https://www.europol.europa.eu/cms/sites/default/files/documents/Europol_Joint-report_Criminal%20networks%20in%20EU%20ports_Public_version.pdf#:~:text=%E2%96%BA%20EU%20ports%20are%20critical%20infrastructure%20that,makes%20detection%20of%20illicit%20goods%20extremely%20challenging*

56 *https://insightcrime.org/news/5-new-creative-ways-traffickers-tried-smuggle-cocaine/*

57 *https://www.intracen.org/file/20250423itcexpediting-tradewebpagespdf*

58 *https://www.unodc.org/documents/data-and-analysis/WDR_2025/WDR25_B1_Key_findings.pdf*

59 *https://www.euda.europa.eu/publications/eu-drug-markets/cannabis/criminal-networks_en*

60 24 industrial-scale labs dismantled in the largest-ever operation against synthetic drugs - Over the course of the investigation, authorities seized 1 000 tonnes of chemicals, potentially removing 300 tonnes of synthetic drugs from the EU drug market | Europol

61 *https://www.europol.europa.eu/cms/sites/default/files/documents/Europol_Joint-report_Criminal%20networks%20in%20EU%20ports_Public_version.pdf#:~:text=%E2%96%BA%20EU%20ports%20are%20critical%20infrastructure%20that,makes%20detection%20of%20illicit%20goods%20extremely%20challenging*

62 FPI.25.5011 Common Risk indicators (CRIs) v.2025

63 *https://docs.un.org/en/S/2026/44*

64 *https://www.marshallcenter.org/en/publications/clock-tower-series/strategic-competition-seminar-series-fy25*

65 25.0291 EU Integrated Border Management in an era of hybrid threats

66 *https://commission.europa.eu/publications/european-democracy-shield-documents_en*

67 As outlined in Article 20 of the REGULATION (EU) 2019/1896 of the European Parliament and the Council of 12 November 2019

FRONTEX
EUROPEAN BORDER AND COAST GUARD AGENCY

Plac Europejski 6 • 00-844 Warsaw • Poland
frontex@frontex.europa.eu • www.frontex.europa.eu
©2026 European Border and Coast Guard Agency (Frontex) • FPI-26.0159
PRINT ISBN 978-92-9411-828-8 DOI 10.2819/9626013 TT-01-26-034-EN-C
PDF ISBN 978-92-9411-827-1 DOI 10.2819/3817204 TT-01-26-034-EN-N

Publications Office of the European Union