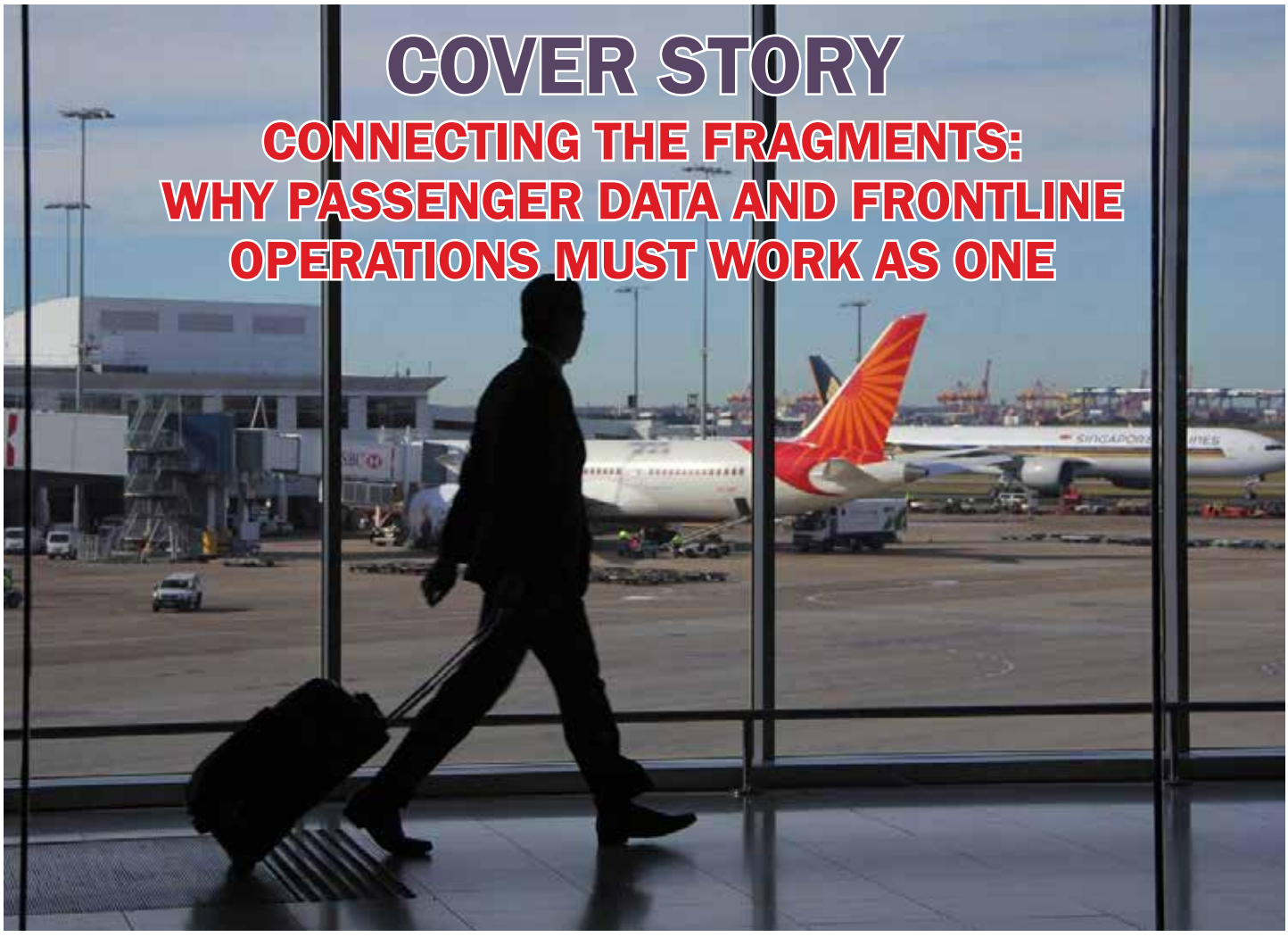
BORDER SECURITY REPORT

VOLUME 50
SEPTEMBER / OCTOBER 2026

THE JOURNAL OF BORDER SECURITY AND TRANSNATIONAL CRIME FOR THE WORLD'S BORDER PROTECTION, MANAGEMENT AND SECURITY INDUSTRY POLICY-MAKERS AND PRACTITIONERS



COVER STORY

CONNECTING THE FRAGMENTS: WHY PASSENGER DATA AND FRONTLINE OPERATIONS MUST WORK AS ONE

SPECIAL REPORT



AI At The Border p.12

AGENCY NEWS



A global review of the latest news and challenges from border agencies and agencies at the border. p.40

SHORT REPORT

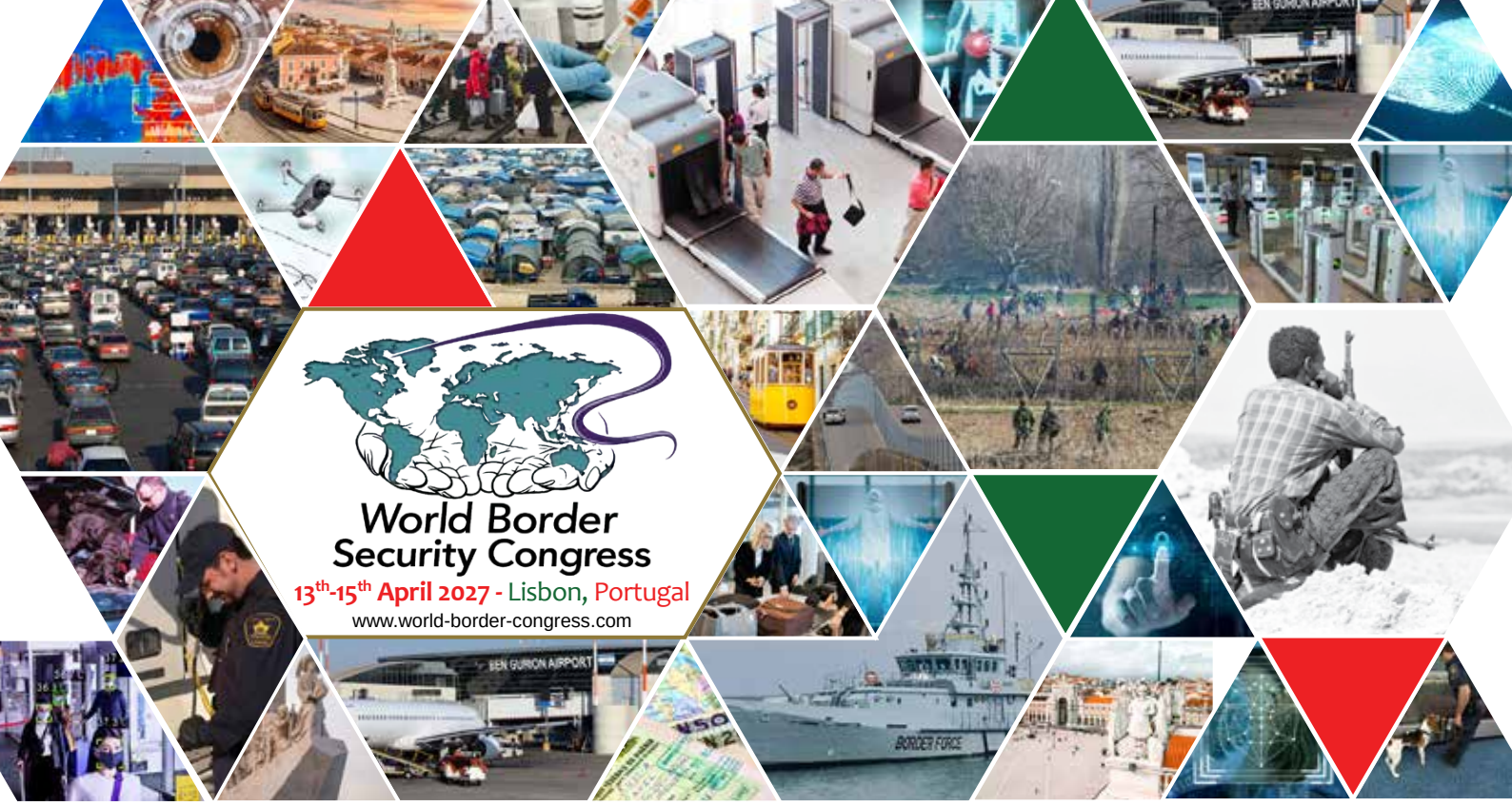


WCO builds freight forwarders capacity to manage rules of origin p.5

INDUSTRY NEWS



Latest news, views and innovations from the industry. p.66d



Transforming Border Management Strategies Through Co-operation and Technology

SAVE THE DATES

Portugal's border security is shaped by its geography and role within the Schengen Area, placing responsibility on protecting the EU's external frontier. Since the dissolution of the SEF, the border security function is coordinated by the Sistema de Seguranca Interna (Internal Security System) and implemented by the Polícia de Segurança Pública (PSP) and Guarda Nacional Republicana (GNR).

Administrative overload and legal migration pressure remains Portugal's main challenges, but the country relies on maritime and airport surveillance rather than land borders. Its Atlantic coastline presents monitoring challenges, particularly for irregular migration routes and drug trafficking. The country faces growing inflows of irregular migrants from Africa, Brazil, and South Asia, creating administrative strain in processing visas, asylum claims, and residency permits, leading to backlogs and delays.

Migration has become more contentious recently, with pressure to tighten rules after years of relatively open policies. At the same time, labour shortages mean Portugal still depends heavily on migrant workers.

Portugal is not unique in its border management challenges and must strengthen surveillance, streamline bureaucracy, and enhance EU cooperation while maintaining its rights-based migration approach.

The World Border Security Congress is a high level 3 day event that will discuss and debate current and future policies, implementation issues and challenges as well as new and developing technologies that contribute towards safe and secure border and migration management.

Join us in Lisbon, Portugal on 13th-15th April 2027 for the next gathering of international border security, protection and migration management professionals.

www.world-border-congress.com

for the international border management and security industry

Co-hosted by:

Sistema de Segurança Interna

Polícia Segurança Pública

GNR Guarda Nacional Republicana

To discuss exhibiting and sponsorship opportunities and your involvement contact:

Paul Gloc
Rest of World
E: paulg@torchmarketing.co.uk
T: +44 (0) 7786 270 820

Bruce Bassin
Americas
E: bruceb@torchmarketing.co.uk
T: +1 702.600.4651

Jerome Merite
France
E: j.callumerite@gmail.com
T: +33 (0) 6 11 27 10 53

Supported by:

OSCE Organization for Security and Co-operation in Europe

European Association of Airport and Seaport Police

African Young People Support Center

ISIO

International Association of CIP Professionals

NSARE

Media Partners:

World Border Security Network

Border Security Report

World Security-Index.com

CONTENTS

BORDER SECURITY REPORT


» p.33


» p.66


» p.56


» p.56

6 CONNECTING THE FRAGMENTS: WHY PASSENGER DATA AND FRONTLINE OPERATIONS MUST WORK AS ONE

12 AI AT THE BORDER

24 AGENCY REPORTS

30 SMART BORDERS ALBANIA 2030: FROM TRAVEL INTELLIGENCE TO INTELLIGENT BORDER MANAGEMENT

34 PREVENTING CRIME AT BORDERS WITH UNITED NATIONS SUPPORT: HOW MONGOLIA USES PASSENGER DATA TO STOP THREATS IN REAL TIME

38 AGENCY NEWS

42 EUROPE'S EASTERN FRONTIER FACES A NEW ERA OF BORDER SECURITY CHALLENGE

48 STRENGTHENING EUROPE'S EASTERN BORDERS WITH ELECTROMAGNETIC AWARENESS

56 AUTOMATED BORDERS, E-GATES AND KIOSKS - HOW EES IS ACCELERATING THE GLOBAL TRANSFORMATION OF BORDER CONTROL

62 ILLEGAL MINING AND ARMED BANDITRY IN NIGERIA: IMPLICATIONS FOR BORDER SECURITY, ECONOMIC STABILITY AND NATIONAL DEVELOPMENT

68 2027 WORLD BORDER SECURITY CONGRESS

72 INDUSTRY NEWS

CONTACTS

Editorial:
Tony Kingham
E: tonyk@border-security-report.com

Assistant Editor:
Neil Walker
E: neilw@torchmarketing.co.uk

Design, Marketing & Production:
Neil Walker
E: neilw@torchmarketing.co.uk

Subscriptions:
Tony Kingham
E: tonyk@border-security-report.com

Border Security Report is a bi-monthly electronic magazine and is the border management industry magazine delivering agency and industry news and developments, as well as more in-depth features and analysis to over 30,000 border agencies, agencies at the borders and industry professionals, policymakers and practitioners, worldwide.

Copyright of KNM Media and Torch Marketing.

Synthetic Drugs are Changing the World



The illicit drug landscape is undergoing a profound transformation. While cocaine, heroin and cannabis trafficking remain major concerns, border agencies are increasingly confronting a more adaptable threat: synthetic drugs and the criminal networks behind them.

Unlike plant-based narcotics, synthetic drugs are not tied to growing regions or harvest cycles. Production can occur almost anywhere, often concealed within industrial facilities, private properties or legitimate businesses. Many precursor chemicals also have lawful industrial uses, making detection and regulation more difficult. As authorities ban one substance, criminal groups rapidly introduce new variants, creating a constant cycle of adaptation.

Organised crime is evolving as well. Rather than operating through rigid hierarchies, many networks now function as flexible ecosystems of specialists. Separate groups may handle production, document fraud, logistics, online distribution or financial transactions. This structure makes criminal organisations highly resilient and difficult to disrupt.

Technology has further strengthened these networks. Encrypted communications, digital payment systems and online marketplaces allow criminals to coordinate across multiple jurisdictions with unprecedented speed. The border is no longer simply a physical crossing point. It is part of a wider operational environment spanning cyberspace, financial systems and global supply chains.

For border agencies, success increasingly depends on intelligence-led operations. Advanced analytics, risk assessment, artificial intelligence and international information sharing are becoming as important as traditional enforcement measures.

The rise of synthetic drugs is more than a narcotics challenge. It reflects the broader evolution of organised crime and underscores the need for border security agencies to embrace technology, cooperation and intelligence if they are to stay ahead of increasingly agile and innovative adversaries.

Tony Kingham
Editor

Ketamine seizures reach 15 year high



The World Customs Organization (WCO), through the WCO–JICA (Japan International Cooperation Agency) Border Force has seized a record amount of ketamine at the UK border, preventing almost 1.3 tonnes of the dangerous drug from reaching communities across the country.

Officers seized 1,298kg of ketamine during the first quarter of 2026, a 42% increase on the final three months of 2025, when almost 915kg was intercepted before entering the UK illegally. The figure is the highest quarterly total for 15 years and exceeds the previous record of 1,238kg seized in the second quarter of 2025.

The milestone comes amid increasing concern over the harm caused by ketamine misuse, particularly among young people. Regular use can lead to severe and permanent health problems, including irreversible damage to the bladder and urinary tract. In the most serious cases, ketamine misuse can be fatal.

Border Force officers at Harwich International Port alone have seized 300kg of ketamine over the past year. Two major interceptions involving drivers arriving from the Hook of Holland in February and May resulted in seizures of 100kg and 200kg respectively.

The latest figures also highlight the scale of wider enforcement activity at the border. Officers seized more than 59,000 doses of nitrous oxide in the first quarter of 2026, compared with just over 35,000 doses in the previous quarter. More than 9,000kg of cocaine was intercepted during the same period, while herbal cannabis accounted for around 85% of all drug seizures by weight.

The figures come as the Home Secretary secured a new agreement with Five Eyes partners – the US, Canada, Australia and New Zealand – at the Five Country Ministerial in Sydney to strengthen the international response to synthetic opioids.

Synthetic opioids are among the most dangerous drugs in circulation. Nitazenes can be between 50 and 500 times more potent than heroin, creating a significant risk of accidental overdose.

Their extreme potency means even tiny quantities can be difficult to detect and intercept. More than 1,000 confirmed deaths in the UK were linked to synthetic opioids between 1 June 2023 and 5 June 2025.

Under the new agreement, Five Eyes partners will deepen co-operation with industry and international organisations to target criminal networks involved in synthetic drugs and precursor chemicals.

Ministers also agreed closer collaboration on regulation and intelligence sharing to strengthen controls on precursor chemicals, prevent diversion into illicit supply chains and disrupt organised crime groups involved in production and trafficking.

Progress has also been made on last year's commitment to develop a synthetic opioid pills profiler. Early versions of the database are now being used across Border Force and policing, enhancing frontline capability to identify and respond to emerging synthetic drug threats.

Home Office Minister Jo White said, "The record amount of ketamine seized at our border reflects the dedication, professionalism and vigilance of Border Force officers, who work around the clock to keep dangerous drugs off our streets. As criminal networks adapt and new threats emerge, our response will remain relentless. We will continue strengthening our borders, targeting organised crime and preventing harmful drugs from reaching our communities."

CONNECTING THE FRAGMENTS: WHY PASSENGER DATA AND FRONTLINE OPERATIONS MUST WORK AS ONE

By Cristian Fanelli, Law Enforcement Expert, United Nations Office on Drugs and Crime (UNODC), Border Management Branch – Passenger and Cargo Control Programme

A recent seizure at Delhi airport shows how targeting, observation and examination produce results together that none of them would achieve alone, and why the same logic must extend across every agency at the air border.

On 9 September, Customs officers at Indira Gandhi International Airport in Delhi intercepted a consignment that shows how modern border control works when its components are connected. According to published reports, two passengers arriving from Bangkok were flagged through Advance Passenger Information (API) profiling and placed under surveillance, while their checked baggage was monitored. As the operation unfolded, officers saw two other travellers, who had arrived on a separate flight from Kathmandu, moving to collect the Bangkok passengers' bags. The Kathmandu travellers were stopped at the Green

Channel and admitted they had been instructed to pick up the luggage.

The Bangkok passengers were then intercepted, and X-ray and physical examination of the baggage revealed 27.45 kg of suspected hydroponic cannabis.

The quantity is significant, but the method is more instructive. Examined separately, each element of the case would have told only part of the story. The Bangkok passengers, the Kathmandu collectors and the baggage connecting them were each incomplete pieces of evidence, and the result came from linking them. The operation was conducted by Customs, which shows how much profiling, surveillance and examination can achieve when integrated within a single service. The same approach is far more powerful when it is applied across the several agencies that share responsibility for an airport. That requires Passenger Information Units (PIUs), Customs, Immigration, Police and Airport Authorities to cooperate in a structured way.

From data to operational opportunity

A PIU sees what frontline officers cannot: the shape of a journey before the traveller arrives. This capability now rests on an international normative basis. United Nations Security Council Resolution 2396 (2017) obliges States to develop the capacity to collect, process and analyse Passenger



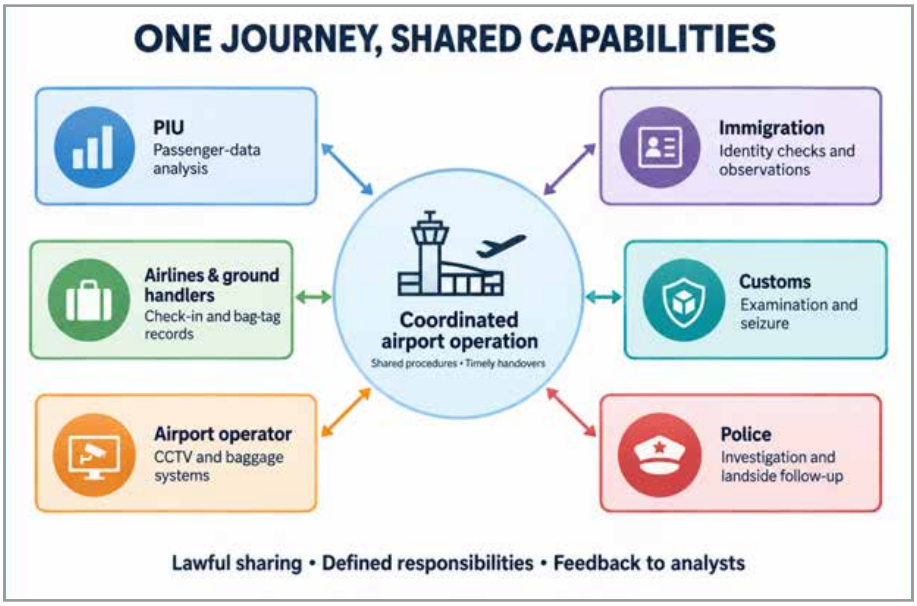
Name Record (PNR) data. In 2020, the International Civil Aviation Organisation (ICAO) adopted Amendment 28 to Annex 9 to the Chicago Convention, establishing Standards and Recommended Practices (SARPs) on the collection, use, processing and protection of PNR data, alongside the obligation for States to operate API systems.

The two data sets answer different questions. API establishes the identity of who is actually on board a given flight and generally becomes available around the time of departure. PNR shows how the trip was put together: who booked alongside whom, when and how the ticket was paid for, which contact details were provided, whether the itinerary changed and, where the carrier records it, baggage details. Read together, they expose routings, booking behaviour, travel histories and associations between passengers that are invisible in the arrivals hall.

Flagging a journey of interest is only where the work begins. An analytical product has value only if it reaches the operational level in time, and in a form that frontline officers can act on. Surveillance, baggage tracking, Immigration checks, Customs examination and behavioural observation then test the initial assessment, confirming it, contradicting it or widening it. In Delhi, the analysis pointed to two travellers from Bangkok. The case changed once officers saw passengers from a different origin approach the same baggage, and from that point the task was mapping relationships rather than profiling individuals.

Targeting relationships, not only individuals

Conventional targeting asks questions about the individual:



identity, origin, itinerary and the presence of known risk indicators. These remain indispensable, but criminal networks seldom operate through lone actors. The courier, the facilitator, the collector and the organiser may travel on different flights and routes, and they usually take care to appear unconnected. Often the link between travellers reveals more than anything about a single passenger.

The Delhi seizure appears to fit a wider pattern. In May, Customs at the same airport reported a case in which a traveller arriving from Bangkok was placed under observation, and a passenger arriving from Sharjah later admitted he had been told to collect a suitcase booked under the Bangkok passenger's name. When the same division of roles appears twice in a few months, it can no longer be treated as a one-off, and it can be converted into indicators. Examples include:

- travellers from different origins converging on the same terminal within a narrow time window;
- passengers waiting at a reclaim belt allocated to a flight they were not on;
- baggage checked in by one person and handled by another;
- the combination of arrivals with heavy checked baggage and others with none.

No single indicator is conclusive. Combined with passenger data, they help concentrate surveillance resources on the relationships most likely to matter.

Advanced targeting therefore needs to move from assessing individuals to analysing links and networks. A traveller who attracts no attention alone may become central once associated with another passenger, a particular bag, a recurring booking pattern or an observation made on the ground. These elements are rarely held in one place. The PIU may detect the link in the booking data, Customs the baggage anomaly and Immigration the inconsistency in a traveller's account. The Police may already hold intelligence on associates, and the Airport Authority may have the CCTV footage (closed-circuit television) or baggage-system records that tie them together.

Surveillance as a shared capability

The operational phase of a case like Delhi depends on keeping people and baggage under uninterrupted observation from the aircraft stand to the terminal exit. At most airports, the capabilities needed for this are distributed among several actors.

Airlines and ground handlers hold the check-in and bag-tag records that tie each item of baggage to the passenger who checked it in, and they control its loading and unloading. The airport operator usually manages the CCTV network, the baggage handling system, the reclaim belts and access control between airside and landside. Immigration officers encounter every arriving passenger at the primary line, where they can verify identity against the passenger data

and observe behaviour. Where procedures permit, they can also manage the timing of a passenger's progress without alerting them. Customs controls the exit channels and holds the examination tools, including X-ray screening, detector dogs and the power to search and seize. The police or specialised drug enforcement units generally hold mobile surveillance capacity, arrest powers beyond the border zone and the investigative lead once a case moves landside. Throughout, the PIU remains the analytical reference point. It can run fresh queries as events develop, for example to check whether newly identified collectors share bookings, contact details or travel history with the original subjects.

Any of these links can fail. A bag that cannot be followed through the baggage system, camera coverage that cannot be accessed in real time, or a surveillance team whose authority ends at the terminal doors can limit an operation that began with excellent analysis. Continuous observation is a collective capability, and it has to be planned and rehearsed as one. It cannot be assembled at short notice while the subjects are already walking through the arrivals hall.

Observe or intercept: the decision that must be prepared

Relational targeting raises a question that individual targeting



seldom does: when to intervene. Stopping a flagged passenger at the first opportunity secures the evidence and removes the immediate risk, but may catch only the courier. Letting the operation run, as in Delhi, where the collectors were allowed to take the bags and were followed before being stopped, can expose additional members of the network, at the cost of a higher risk of losing the subjects or the goods. Extending observation beyond the airport can reach recipients and organisers further up the chain. Controlled delivery requires legal authorisation, prosecutorial involvement and landside surveillance capacity to be in place beforehand.

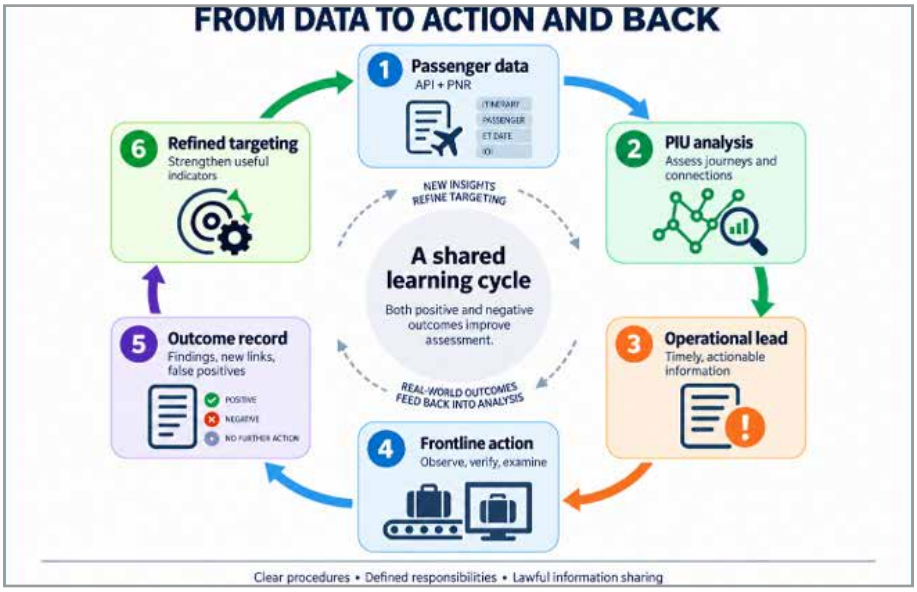
Choices of this kind cannot be made reliably in the few minutes available on the arrivals floor. Standard Operating Procedures (SOPs) should settle in advance the criteria for each option, who has authority to decide, which agencies must be informed and what happens if contact with the subjects is lost.

Structure rather than improvisation

This is where cooperation and genuine interoperability differ. In many airports, agencies work together when a case calls for it. Officers know each other, information flows informally, and joint action is arranged as needed. This can succeed, but it depends on personal relationships rather than on procedure, and it tends to weaken when people move on.

A more robust model rests on defined arrangements. These should establish:

- how a PIU disseminates an operational lead and to whom;



- how urgency is graded, from immediate action on an inbound flight to longer-term analytical work;
- which agency coordinates an intervention and holds command while it is underway;
- how operations are deconflicted when another service is already investigating the same individuals;
- what information may be shared, and on what legal basis;
- how results are reported back to the analysts.

Joint airport units, in which officers from different agencies work in a common operational space under shared procedures, are one practical way of turning such rules into routine. Data protection must be part of the design from the start. The ICAO PNR SARPs set safeguards on purpose limitation, retention, onward transfer and independent oversight, and sharing arrangements built around them are both more sustainable and more defensible before a court than informal exchanges.

The goal is not simply to exchange more information. It is to establish an operational cycle in which information reaches the right place at the right moment: analysis prompts action, action produces fresh intelligence, and that intelligence sharpens the next round of analysis. Without such a cycle, passenger-data systems risk becoming analytical archives, while frontline services continue to react case by case.

Closing the loop through feedback

Feedback is the part of the cycle most often neglected. When a passenger identified by a PIU is controlled, the outcome frequently disappears into another agency's reporting system, and the analysts never learn what the intervention produced. They need to know:

- whether the assessment was accurate and whether anything was found;
- whether the passenger was linked to others;
- whether a new concealment method came to light;
- whether routes, telephone numbers, addresses, financial connections or travel patterns emerged;
- whether the result was a false positive.

Anecdotal feedback is not enough. Each disseminated lead should generate a minimum standard record covering the action taken, the outcome, the indicators that proved relevant and any new associations identified. That record allows simple measures to be tracked over time, such as the hit rate, the false-positive rate and the interval between alert and action.

Positive outcomes refine targeting rules and open further lines into a network. Negative outcomes are just as useful, because they allow weak indicators to be discarded and spare legitimate travellers unnecessary controls. Intelligence then works as a learning system rather than a one-way flow.

One journey, one operational space

The Delhi case also shows why no agency should examine only the segment of a journey that falls within its own remit. For a criminal organisation, passenger data, border checks, baggage, airport surveillance, Customs examination, police intelligence and follow-up investigation are not separate domains. These boundaries exist in administrative charts, while networks move freely across them. The same is true of the divisions between passenger and cargo flows, between airports and land borders, and between pre-arrival targeting and post-seizure investigation. The more these areas are joined up, the better the chance of detecting patterns that no single system can reveal.

What the case teaches

The value of the Delhi seizure lies less in the quantity recovered than in what it shows about connected capabilities. Passenger data opened the opportunity, observation on the ground developed it, the movement of baggage exposed further relationships, and coordinated action turned information into an interception. This is the practical advantage of an integrated border-control model.

PIUs should not operate as detached analytical cells, and frontline services should not be passive recipients of occasional



alerts. Both belong to a single intelligence and operational system. Building that system depends on capacity as well as procedure: officers from different agencies need to train together, review cases jointly and practise the handovers on which a live operation relies. When clear procedures, defined responsibilities, trusted channels and systematic feedback support that relationship, the combined system achieves far more than its individual parts.

Intelligence that never leads to action achieves little, and action without intelligence remains reactive. The best results come when the two are joined through cooperation that is structured, continuous and genuinely interagency.

AI AT THE BORDER

How a Decade of European Research is Reshaping Border Management, Customs Controls and Traveller Processing

Standfirst

Artificial intelligence is rapidly becoming the intelligence layer connecting sensors, surveillance systems, customs controls, biometrics and operational decision-making. A major Joint Research Centre review of 75 EU-funded projects reveals how Europe is building the foundations for a new generation of border management capabilities. This article examines the technologies, projects and operational lessons shaping the future border ecosystem.

The Rise of the Intelligent Border

Over the past decade artificial intelligence has evolved from a promising research topic into one of the most strategically important technologies in border management. The European Commission Joint Research Centre analysed 75 EU-funded projects launched between 2015 and 2024 and identified around €376 million of investment directed towards AI applications in border management and customs control. The significance of this investment lies not only in the amount spent but in the breadth of operational challenges addressed. Researchers are applying AI to

maritime awareness, customs inspections, risk analysis, traveller identification, document security and autonomous systems. The projects collectively demonstrate a major shift in thinking. Border agencies are no longer seeking isolated technology upgrades. They are building digital ecosystems capable of transforming information into operational advantage. Border authorities face increasing traveller numbers, expanding maritime zones, evolving organised crime networks and growing expectations from political leaders and the public. Artificial intelligence is increasingly viewed as a force multiplier capable of helping existing personnel analyse more information and make decisions more quickly. The result is the emergence of the intelligent border, where data, analytics and operational systems are linked together in ways that were impossible only a few years ago. Over the past decade artificial intelligence has evolved from a promising research topic into one of the most strategically important technologies in border management. The European Commission Joint Research Centre analysed 75 EU-funded projects launched between 2015 and 2024 and identified around €376 million of investment directed towards AI applications in border management and customs control. The significance of this investment lies not only in the amount spent but in the breadth of operational challenges addressed. Researchers are applying AI to



maritime awareness, customs inspections, risk analysis, traveller identification, document security and autonomous systems. The projects collectively demonstrate a major shift in thinking. Border agencies are no longer seeking isolated technology upgrades. They are building digital ecosystems capable of transforming information into operational advantage. Border authorities face increasing traveller numbers, expanding maritime zones, evolving organised crime networks and growing expectations from political leaders and the public. Artificial intelligence is increasingly viewed as a force multiplier capable of helping existing personnel analyse more information and make decisions more quickly. The result is the emergence of the intelligent border, where data, analytics and operational systems are linked together in ways that were impossible only a few years ago. Over the past decade artificial intelligence has evolved from a promising research topic into one of the most strategically important technologies in border management. The European Commission Joint Research Centre analysed 75 EU-funded projects launched between 2015 and 2024 and identified around €376 million of investment directed towards AI applications in border management and customs control. The significance of this investment lies not only in the amount spent but in the breadth of operational challenges addressed. Researchers are applying AI to maritime awareness, customs inspections, risk analysis, traveller identification, document security and autonomous systems. The projects collectively demonstrate a major shift in thinking. Border agencies are no longer seeking isolated technology upgrades. They are building digital ecosystems



capable of transforming information into operational advantage. Border authorities face increasing traveller numbers, expanding maritime zones, evolving organised crime networks and growing expectations from political leaders and the public. Artificial intelligence is increasingly viewed as a force multiplier capable of helping existing personnel analyse more information and make decisions more quickly. The result is the emergence of the intelligent border, where data, analytics and operational systems are linked together in ways that were impossible only a few years ago.

Maritime Surveillance Comes of Age

Maritime surveillance represents the largest concentration of projects identified in the study. Programmes such as MARISA, CAMELOT, COMPASS2020, EFFECTOR, EURMARS and I-SEAMORE illustrate how European researchers are attempting to build persistent situational awareness across vast maritime areas. The common challenge is managing enormous quantities of information generated by vessels, satellites, coastal radars, drones and other surveillance assets. MARISA focused on data fusion, combining conventional surveillance sources with open-source intelligence and social media information to support decision making. CAMELOT explored advanced command-and-control environments capable of coordinating manned and unmanned platforms. COMPASS2020 demonstrated how offshore patrol vessels can operate as launch and control centres for autonomous aerial and underwater systems. EFFECTOR concentrated on interoperability and the integration of maritime information sources through advanced data-lake architectures. More recent projects including EURMARS and I-SEAMORE seek to integrate high-altitude platforms, UxVs, satellite imagery and AI-powered analytics into unified operational environments. Together these programmes highlight the growing importance of collaboration, interoperability and common operational pictures. Future maritime surveillance will likely depend on collecting information from multiple sources and sharing it rapidly across organisations. Maritime surveillance represents the largest concentration of projects identified in the study. Programmes such as MARISA, CAMELOT, COMPASS2020, EFFECTOR, EURMARS and I-SEAMORE illustrate how European researchers are attempting to build persistent situational awareness across vast maritime areas. The common challenge is managing enormous quantities of information generated by vessels, satellites, coastal radars, drones and other surveillance assets. MARISA focused on data fusion, combining conventional surveillance sources with open-source intelligence and social media information to support decision making. CAMELOT explored advanced command-and-control environments capable of coordinating manned and unmanned platforms. COMPASS2020 demonstrated how offshore patrol vessels can

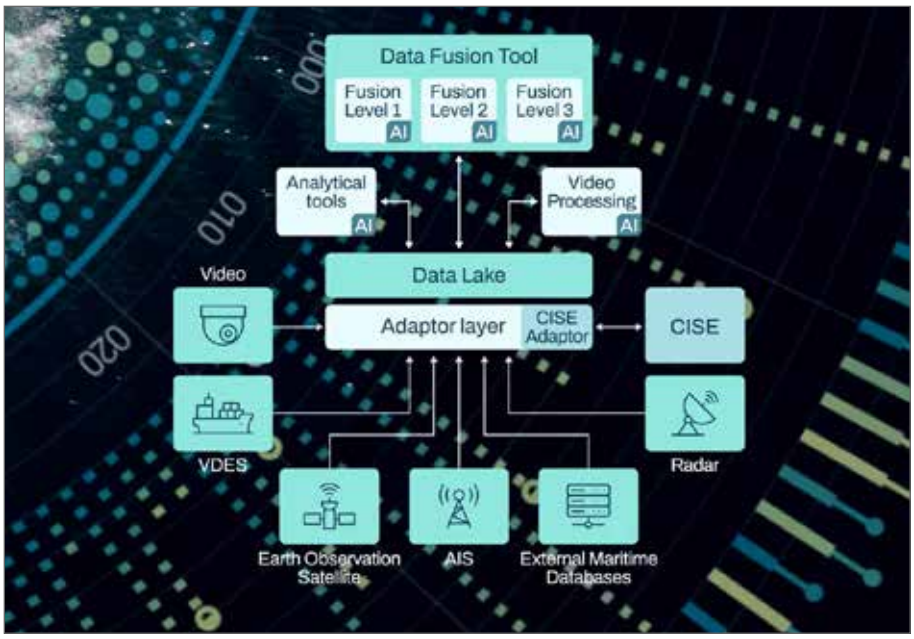
operate as launch and control centres for autonomous aerial and underwater systems. EFFECTOR concentrated on interoperability and the integration of maritime information sources through advanced data-lake architectures. More recent projects including EURMARS and I-SEAMORE seek to integrate high-altitude platforms, UxVs, satellite imagery and AI-powered analytics into unified operational environments. Together these programmes highlight the growing importance of collaboration, interoperability and common operational pictures. Future maritime surveillance will likely depend on collecting information from multiple sources and sharing it rapidly across organisations. Maritime surveillance represents the largest concentration of projects identified in the study. Programmes such as MARISA, CAMELOT, COMPASS2020, EFFECTOR, EURMARS and I-SEAMORE illustrate how European researchers are attempting to build persistent situational awareness across vast maritime areas. The common challenge is managing enormous quantities of information generated by vessels, satellites, coastal radars, drones and other surveillance assets. MARISA focused on data fusion, combining conventional surveillance sources with open-source intelligence and social media information to support decision making. CAMELOT explored advanced command-and-control environments



capable of coordinating manned and unmanned platforms. COMPASS2020 demonstrated how offshore patrol vessels can operate as launch and control centres for autonomous aerial and underwater systems. EFFECTOR concentrated on interoperability and the integration of maritime information sources through advanced data-lake architectures. More recent projects including EURMARS and I-SEAMORE seek to integrate high-altitude platforms, UxVs, satellite imagery and AI-powered analytics into unified operational environments. Together these programmes highlight the growing importance of collaboration, interoperability and common operational pictures. Future maritime surveillance will likely depend on collecting information from multiple sources and sharing it rapidly across organisations.

The New Era of Data Fusion and Anomaly Detection

If a single theme runs through the report it is data fusion. Border organisations already possess a wealth of information. The challenge is connecting disparate systems and extracting meaningful intelligence. Projects such as EFFECTOR, PROMENADE and AI-ARC aim to address precisely this problem. PROMENADE developed a suite of AI-based services capable of vessel detection, behaviour analysis, route classification and anomaly identification using radar data, AIS transmissions, imagery and open-source intelligence. AI-ARC created a Virtual Control Room designed to reduce information overload by presenting operators with customised operational pictures. Research associated with the project demonstrated how artificial intelligence can identify dark vessels, unusual movement patterns and suspicious maritime activities. EFFECTOR showed how interoperability between systems can support faster operational responses by bringing together information



from multiple authorities. Anomaly detection is becoming one of the most valuable use cases for artificial intelligence because it allows human operators to focus on genuinely suspicious behaviour rather than routine activity. Future systems are expected not just to report what is happening but also assess risk levels and identify activities that differ from established patterns. This transition from observation towards predictive awareness could fundamentally alter maritime security operations. If a single theme runs through the report it is data fusion. Border organisations already possess a wealth of information. The challenge is connecting disparate systems and extracting meaningful intelligence. Projects such as EFFECTOR, PROMENADE and AI-ARC aim to address precisely this problem. PROMENADE developed a suite of AI-based services capable of vessel detection, behaviour analysis, route classification and anomaly identification using radar data, AIS transmissions, imagery and open-source intelligence. AI-ARC created a Virtual Control Room designed to reduce information overload by presenting operators with customised operational pictures. Research associated with the project demonstrated how artificial intelligence can identify dark vessels, unusual movement patterns and suspicious maritime activities. EFFECTOR showed how interoperability between systems can support faster operational responses by bringing together information from multiple authorities. Anomaly detection is becoming one of the most valuable use cases for artificial intelligence because it allows human operators to focus on genuinely suspicious behaviour rather than routine activity. Future systems are expected not just to report what

is happening but also assess risk levels and identify activities that differ from established patterns. This transition from observation towards predictive awareness could fundamentally alter maritime security operations. If a single theme runs through the report it is data fusion. Border organisations already possess a wealth of information. The challenge is connecting disparate systems and extracting meaningful intelligence. Projects such as EFFECTOR, PROMENADE and AI-ARC aim to address precisely this problem. PROMENADE developed a suite of AI-based services capable of vessel detection, behaviour analysis, route classification and anomaly identification using radar data, AIS transmissions, imagery and open-source intelligence. AI-ARC created a Virtual Control Room designed to reduce information overload by presenting operators with customised operational pictures. Research associated with the project demonstrated how artificial intelligence can identify dark vessels, unusual movement patterns and suspicious maritime activities. EFFECTOR showed how interoperability between systems can support faster operational responses by bringing together information from multiple authorities. Anomaly detection is becoming one of the most valuable use cases for artificial intelligence because it allows human operators to focus on genuinely suspicious behaviour rather than routine activity. Future systems are expected not just to report what

is happening but also assess risk levels and identify activities that differ from established patterns. This transition from observation towards predictive awareness could fundamentally alter maritime security operations.

Smart Customs and Cargo Security

The report provides equally compelling insights into the transformation of customs inspections. Growing international trade volumes make comprehensive physical inspection impossible. Customs agencies therefore increasingly rely upon risk-based approaches supported by advanced technology. Projects including C-BORD, ENTRANCE, SilentBorder and MULTISCAN 3D examined how machine learning and advanced sensing technologies could improve cargo screening operations. Rather than opening containers unnecessarily, future customs systems may automatically identify anomalies within scan images and prioritise shipments presenting elevated risk. Similar research is underway for baggage and parcel inspection through initiatives such as PARSEC and BAG-INTEL. The objective is to improve detection rates for narcotics, weapons, contraband and other illicit goods without disrupting legitimate commerce. Artificial intelligence is particularly valuable when analysing large image datasets that would otherwise require extensive manual review.



The customs sector therefore offers one of the clearest examples of AI delivering measurable operational benefits. Faster inspections, improved detection accuracy and more efficient allocation of resources are recurring themes across the projects reviewed. As trade flows continue to expand, intelligent inspection systems are likely to become increasingly important. The report provides equally compelling insights into the transformation of customs inspections. Growing international trade volumes make comprehensive physical inspection impossible. Customs agencies therefore increasingly rely upon risk-based approaches supported by advanced technology. Projects including C-BORD, ENTRANCE, SilentBorder and MULTISCAN 3D examined how machine learning and advanced sensing technologies could improve cargo screening operations. Rather than opening containers unnecessarily, future customs systems may automatically identify anomalies within scan images and prioritise shipments presenting elevated risk. Similar research is underway for baggage and parcel inspection through initiatives such as PARSEC and BAG-INTEL. The objective is to improve detection rates for narcotics, weapons, contraband and other illicit goods without disrupting legitimate commerce. Artificial intelligence is particularly valuable when analysing large image datasets that would otherwise require extensive manual review. The customs sector therefore offers one of the clearest examples of AI delivering measurable operational benefits. Faster inspections, improved detection accuracy and more efficient allocation of resources are recurring themes across the



projects reviewed. As trade flows continue to expand, intelligent inspection systems are likely to become increasingly important. The report provides equally compelling insights into the transformation of customs inspections. Growing international trade volumes make comprehensive physical inspection impossible. Customs agencies therefore increasingly rely upon risk-based approaches supported by advanced technology. Projects including C-BORD, ENTRANCE, SilentBorder and MULTISCAN 3D examined how machine learning and advanced sensing technologies could improve cargo screening operations. Rather than opening containers unnecessarily, future customs systems may automatically identify anomalies within scan images and prioritise shipments presenting elevated risk. Similar research is underway for baggage and parcel inspection through initiatives such as PARSEC and BAG-INTEL. The objective is to improve detection rates for narcotics, weapons, contraband and other illicit goods without disrupting legitimate commerce. Artificial intelligence is particularly valuable when analysing large image datasets that would otherwise require extensive manual review. The customs sector therefore offers one of the clearest examples of AI delivering measurable operational benefits. Faster inspections, improved detection accuracy and more efficient allocation of resources are recurring themes across the projects reviewed. As trade flows continue to expand, intelligent inspection systems are likely to become increasingly important.

Biometrics, Digital Identity and Trusted Travel

Identity verification remains one of the most visible applications of artificial intelligence in border environments. Multiple projects examined biometric technologies, document security and digital identity management. Programmes such as iBorderCtrl, PROTECT, SMILE, eBORDER and ODYSSEUS explored how contactless biometrics and multimodal identity verification might support faster traveller processing. Researchers investigated facial recognition, iris recognition, liveness detection and behavioural indicators while simultaneously examining privacy implications. Document security projects such as Smart-Trust and SafeTravellers focused on detecting fraudulent travel documents and identity manipulation techniques. The long-term objective is a frictionless travel experience in which legitimate travellers move rapidly through border controls while security risks are identified more effectively. Digital identity ecosystems are expected to play a significant role in future border management strategies. Trusted traveller concepts, mobile identities and advanced authentication methods all feature prominently within the research portfolio. Despite technological progress, deployment remains closely linked to regulatory compliance and

public acceptance. The challenge facing agencies is therefore not simply technical implementation but creating systems capable of maintaining trust while delivering operational benefits. Identity verification remains one of the most visible applications of artificial intelligence in border environments. Multiple projects examined biometric technologies, document security and digital identity management. Programmes such as iBorderCtrl, PROTECT, SMILE, eBORDER and ODYSSEUS explored how contactless biometrics and multimodal identity verification might support faster traveller processing. Researchers investigated facial recognition, iris recognition, liveness detection and behavioural indicators while simultaneously examining privacy implications. Document security projects such as Smart-Trust and SafeTravellers focused on detecting fraudulent travel documents and identity manipulation techniques. The long-term objective is a frictionless travel experience in which legitimate travellers move rapidly through border controls while security risks are identified more effectively. Digital identity ecosystems are expected to play a significant role in future border management strategies. Trusted traveller concepts, mobile identities and advanced authentication methods all feature prominently within the research portfolio. Despite technological progress,



deployment remains closely linked to regulatory compliance and public acceptance. The challenge facing agencies is therefore not simply technical implementation but creating systems capable of maintaining trust while delivering operational benefits. Identity verification remains one of the most visible applications of artificial intelligence in border environments. Multiple projects examined biometric technologies, document security and digital identity management. Programmes such as iBorderCtrl, PROTECT, SMILE, eBORDER and ODYSSEUS explored how contactless biometrics and multimodal identity verification might support faster traveller processing. Researchers investigated facial recognition, iris recognition, liveness detection and behavioural indicators while simultaneously examining privacy implications. Document security projects such as Smart-Trust and SafeTravellers focused on detecting fraudulent travel documents and identity manipulation techniques. The long-term objective is a frictionless travel experience in which legitimate travellers move rapidly through border controls while security risks are identified more effectively. Digital identity ecosystems are expected to play a significant role in future border management strategies. Trusted traveller concepts, mobile identities and advanced authentication methods all feature prominently within the research portfolio. Despite technological progress, deployment remains closely linked to regulatory compliance and public acceptance. The challenge facing agencies is therefore not simply technical implementation but creating systems



capable of maintaining trust while delivering operational benefits.

Autonomous Systems and Infrastructure Protection

Another significant trend identified by the report is the rapid growth of autonomous systems. Drones, unmanned surface vessels and underwater vehicles appear across multiple projects. Researchers increasingly view autonomous assets as force multipliers capable of extending surveillance coverage while reducing operational costs. Projects such as COMPASS2020, SEAGUARD and I-SEAMORE explored how multiple autonomous systems can operate together within integrated surveillance frameworks. At the same time projects including UnderSec, SMAUG and VIGIMARE investigated protection of underwater infrastructure such as pipelines, cables and port facilities. Recent geopolitical developments have increased concern regarding maritime infrastructure resilience. Artificial intelligence is being used to analyse sonar data, detect underwater anomalies and support threat identification. Machine learning models can recognise subtle indicators that may signal interference, sabotage or suspicious activity. Combined with autonomous platforms, these capabilities offer authorities new methods for monitoring high-value assets. The result is a growing convergence between border security, maritime resilience and critical infrastructure protection.

Another significant trend identified by the report is the rapid growth of autonomous systems. Drones, unmanned surface vessels and underwater vehicles appear across multiple projects. Researchers increasingly view autonomous assets as force multipliers capable of extending surveillance coverage while reducing operational costs. Projects such as COMPASS2020, SEAGUARD and I-SEAMORE explored how multiple autonomous systems can operate together within integrated surveillance frameworks. At the same time projects including UnderSec, SMAUG and VIGIMARE investigated protection of underwater infrastructure such as pipelines, cables and port facilities. Recent geopolitical developments have increased concern regarding maritime infrastructure resilience. Artificial intelligence is being used to analyse sonar data, detect underwater anomalies and support threat identification. Machine learning models can recognise subtle indicators that may signal interference, sabotage or suspicious activity. Combined with autonomous platforms, these capabilities offer authorities new methods for monitoring high-value assets. The result is a growing convergence between border security, maritime resilience and critical infrastructure protection.

Ethics, Trust and the AI Act

One of the defining characteristics of the European approach to artificial intelligence is the attention devoted to ethics and governance. Unlike many technology programmes that focus exclusively on performance, several projects examined transparency, explainability, privacy and societal acceptance. Researchers recognise that public trust will influence adoption every bit as much as technical capability.

The report repeatedly references concerns relating to surveillance, bias, accountability and database interoperability. These issues become particularly important in applications involving biometrics and law enforcement. The introduction of the EU AI Act further reinforces the importance of governance. High-risk AI applications face requirements relating to transparency, human oversight and data governance. Border agencies therefore operate within one of the most demanding regulatory environments for artificial intelligence anywhere in the world. Yet many researchers view this not as a barrier but as an opportunity to create systems that are robust, explainable and trusted. Ensuring that AI augments rather than replaces human judgement remains a central principle throughout the projects examined. One of the defining characteristics of the European approach to artificial intelligence is the attention devoted to ethics and governance. Unlike many technology programmes that focus exclusively on performance, several projects examined transparency, explainability, privacy and societal acceptance. Researchers recognise that public trust will influence adoption every bit as much as technical capability.



the EU AI Act further reinforces the importance of governance. High-risk AI applications face requirements relating to transparency, human oversight and data governance. Border agencies therefore operate within one of the most demanding regulatory environments for artificial intelligence anywhere in the world. Yet many researchers view this not as a barrier but as an opportunity to create systems that are robust, explainable and trusted. Ensuring that AI augments rather than replaces human judgement remains a central principle throughout the projects examined.

What Border Security Leaders Should Watch Next

The overall lesson from a decade of research is that artificial intelligence is becoming the connective tissue linking modern border ecosystems. Future operational environments are likely to be characterised by human-machine teaming, data sharing, autonomous systems and integrated command centres. Agencies that successfully connect sensors, databases and operators will gain the greatest operational advantage. Maritime awareness, customs targeting, traveller processing and critical infrastructure protection increasingly rely on the same underlying capabilities: data fusion, analytics and decision support. The projects reviewed by the Joint Research Centre do not suggest a future in which machines replace border officers. Instead they point towards environments in which personnel are supported by intelligent systems capable of processing much larger quantities of information. The border of the future may therefore be less about physical infrastructure and more about the intelligence layer sitting

behind it. Europe's research portfolio demonstrates that this future is already beginning to take shape. The overall lesson from a decade of research is that artificial intelligence is becoming the connective tissue linking modern border ecosystems. Future operational environments are likely to be characterised by human-machine teaming, data sharing, autonomous systems and integrated command centres. Agencies that successfully connect sensors, databases and operators will gain the greatest operational advantage. Maritime awareness, customs targeting, traveller processing and critical infrastructure protection increasingly rely on the same underlying capabilities: data fusion, analytics and decision support. The projects reviewed by the Joint Research Centre do not suggest a future in which machines replace border officers. Instead they point towards environments in which personnel are supported by intelligent systems capable of processing much larger quantities of information. The border of the future may therefore be less about physical infrastructure and more about the intelligence layer sitting behind it. Europe's research portfolio demonstrates that this future is already beginning to take shape.

The overall lesson from a decade of research is that artificial intelligence is becoming the connective tissue linking modern border ecosystems. Future operational environments are likely to be characterised by human-machine teaming, data sharing, autonomous systems and integrated command centres. Agencies that successfully connect sensors, databases and operators will gain the greatest operational advantage. Maritime awareness, customs targeting, traveller processing and critical infrastructure protection increasingly rely on the same underlying capabilities: data fusion, analytics and decision support. The projects reviewed by the Joint Research Centre do not suggest a future in which machines replace border officers. Instead they point towards environments in which personnel are supported by intelligent systems capable of processing much larger quantities of information. The border of the future may therefore be less about physical infrastructure and more about the intelligence layer sitting behind it. Europe's research portfolio demonstrates that this future is already beginning to take shape.

This article is a summary of a report by ANDERSON, D., BELCINEANU, A.-I. and TZVETKOVA, M., - AI for Border Management and Customs Controls - Anthology of EU-funded projects, 2015-2024

https://data.europa.eu/doi/10.2760/1286492, JRC143223

More than 200 reptiles and arrested three people involved in the trafficking of protected species



The Guardia Civil has arrested three people for the trafficking of reptiles in Valencia. They operated as a company engaged in the shipment of animals, but illicitly marketed with species protected by the Convention on International Trade in Endangered Species of Wild Fauna and Flora (CITES). They had started to raise specimens clandestinely.

Within the framework of the operation, the agents have carried out two searches in the towns of Jérica and Sot de Ferrer (Castellón). In total, 209 reptiles have been intervened, of which 110 were under different degree of protection CITES. Among them, there is an endemic iguana of the Fijian islands in serious danger of extinction.

In addition, incubators, transport containers and various terrariums have been found, indicators of the activity being developed. Outside of animal-related activity, the Guardia Civil has also seized four unlicensed pistols, nearly 200 short-weapon ammunition cartridges, a compressed air rifle, a taser, an extensible defense, a multitude of electronic devices and abundant documentation.

They used one of these addresses as the headquarters of a company dedicated to the sending of animals, apparently legal. However, the people at the forefront of this activity illegally marketed with reptiles protected by the Cites Convention.

They used contacts from various countries in the Americas, Africa and Asia to obtain specimens extracted directly from their environment. They also raised copies clandestinely without giving an account to the administrative authority of the Ministry for Ecological Transition and Demographic Challenge.

Subsequently, the specimens were transferred to several European fairs where illicit sale is reconciled within the legal market taking advantage of the legal limbo that exists in terms of documentation that certifies the origin of these animals.

No snakes on the plane: ABF thwart reptile smuggling plot



The visas of two Danish nationals were cancelled at Perth Airport this week after Australian Border Force (ABF) found evidence they intended to capture and smuggle native reptiles out of the country for profit.

The men arrived as a traveling party of three on a Doha flight on tourist visas and were selected for a baggage examination and formal interviews with ABF officers.

A number of tools used to capture snakes were located, along with a guide about Australian snakes with tabs on various pages on specific python species. Officers also found evidence on their mobile phones discussing the capture and transport of Australian reptiles back to Denmark.

Seven arrests in Brazil during crackdown on South America-Europe cocaine pipeline



Europol has supported law enforcement agencies from Italy and Brazil in dismantling a major drug trafficking and money laundering network linked to the Italian 'Ndrangheta. The operation, code-named operation 'EREDITÀ', led to seven arrests and is the culmination of a multi-year investigation into large-scale cocaine trafficking and money laundering between South America and Europe. This success builds on previous Italian and Brazilian operations 'SAMBA' and 'MAFIUSI', which led to 28 arrests across both countries.

As a result of the investigation, Brazilian authorities with the operational support of Italian law enforcement and a Europol expert, launched synchronised operations culminating in an action day on 16 September 2026 in São Paulo, Brazil. As a result, seven persons of Italian and Brazilian nationality allegedly involved in drug trafficking and money laundering were arrested.

Thousands of horses caught up in Europe-wide trafficking scheme

Europol has supported a major operation against a criminal network suspected of trafficking horses across Europe using falsified documents and manipulated microchips to conceal the animals' true identities.

At the centre of this investigation led by Belgium is a suspected large-scale trade in horses whose identities and histories were allegedly manipulated to allow them to be moved and resold across Europe. Some of the animals may ultimately have been diverted into the food chain without their true origin and history being known.

This undermines the traceability systems designed to protect animal welfare and food safety and could result in horses not intended for human consumption being illegally sent for slaughter.

Investigators suspect that forged horse passports and manipulated microchips were used to effectively give animals new identities. This allowed the suspects to obscure where the horses had come from, their previous history and whether they were eligible to enter the food chain. Investigators are now working to establish the final destination of the animals.

Crackdown on Italian organised criminal network involved in large-scale euro counterfeiting

Europol has supported an international operation targeting a criminal network linked to the Italian mafia-type organisation Camorra. The operation, coordinated by the Baden-Württemberg State Criminal Police Office and the Stuttgart Public Prosecutor's Office, resulted in the execution of six arrest warrants and simultaneous searches of 16 residential and commercial properties across Germany, Italy, and Spain. In Germany, two illegally held pistols with ammunition were seized, as well as counterfeit euro banknotes of Italian origin linked to the so-called "Napoli Group".

Counter-terrorism operation leverages artificial intelligence to identify 126 terrorism suspects



A first-of-its-kind operation to disrupt terrorist networks in the digital domain has harnessed artificial intelligence to identify suspected terrorists.

Operation Shams II, coordinated by INTERPOL, brought together 28 specialized officers and experts from 11 countries. During the five days of coordinated action, held in Tunis, Tunisia, law enforcement officers extracted 108,076 facial images from visual content published by jihadist groups.

Programmed AI agents and advanced AI-generated scripts were used to automate parts of the data collection and investigative processes, enabling the system to deduplicate and quality-check the images. This narrowed the dataset to 6,362 unique, high-quality facial images ready for processing through INTERPOL's Facial Recognition System. AI-generated output was subject to review and verification by trained officers and analysts in accordance with INTERPOL's Rules on the Processing of Data.

Counter-terrorism operation nets eight Red Notice suspects

A transnational border security operation coordinated by INTERPOL spanning five countries in the Middle East and North Africa has led to a total of 48 arrests, including eight involving individuals wanted internationally under INTERPOL Red Notices and one under an INTERPOL Wanted Persons Diffusion.

It was the first cross-Middle East and North Africa operation where female police officers had full operational responsibility.

Significant Red Notice successes included the arrest at Houari Bou Madian International Airport in the Algerian capital, Algiers, of the suspected mastermind behind a 2022 shooting in Toulouse, France. The suspect had previously escaped from prison after being sentenced to eight years for drug trafficking, participation in a criminal conspiracy, and possession of weapons.

Police Chiefs from Middle East and North Africa convene to tackle evolving regional crime threats

Police leaders from across the Middle East and North Africa (MENA) region gathered in Cairo for high-level discussions focused on strengthening international police cooperation and coordinating responses to the region's most pressing security challenges.

The meeting served as a strategic platform for Police Chiefs to share leadership perspectives on transnational organized crime, national security priorities and the jurisdictional challenges posed by emerging threats.

Central to the discussions was the enhancement of regional coordination and the adoption of the new INTERPOL Operational Task Force Model to ensure a more agile and integrated response to criminal networks.

OSCE strengthens capacities in Bosnia and Herzegovina, Montenegro, and Serbia through regional forged document training-of-trainers



The OSCE Transnational Threats Department, in close co-operation with the OSCE Missions to Bosnia and Herzegovina (BiH), Montenegro and, Serbia, held a regional training-of-trainers (ToT) course on detecting forged documents and impostors at border crossing points. Hosted at the Police Cooperation Centre in Trebinje, BiH, the course brought together 18 experienced border police officers and forensic document experts from BiH, Montenegro and Serbia to strengthen their technical expertise and build their capacity as trainers, ensuring the long-term transfer of skills within their national border police services.

Delivered by experts from BiH and Serbia, the programme combined theory, hands-on exercises with genuine and forged specimens, peer learning, and participants' presentations to build their confidence in training their colleagues. Sessions covered practical detection skills, including substrate analysis, security printing techniques, recognition of printing methods and document evaluation under realistic conditions.

OSCE Chairman-in-Office concludes official visit to Turkmenistan, highlighting strong partnership and continued co-operation

The OSCE Chairman-in-Office, Swiss Federal Councillor Ignazio Cassis, has concluded his official visit to Turkmenistan, where he met with the country's leadership to reaffirm the OSCE's strong partnership with Turkmenistan and discuss ways to further deepen co-operation in support of comprehensive security.

The discussions focused on the long-standing co-operation between the OSCE and Turkmenistan and explored opportunities to strengthen joint efforts across all three dimensions of security. The Chairman-in-Office also highlighted the important contribution of the OSCE Centre in Ashgabat towards a constructive and trust-based co-operation and dialogue with the host country.

OSCE Economic and Environmental Forum focuses on anticipating technologies and science diplomacy for emerging security risks

The OSCE opened its 32nd Economic and Environmental Forum (EEF) in Prague, focusing on how anticipating technological developments and strengthening science-based diplomacy can contribute to security and stability across the OSCE area by helping participating States better prepare for both existing and emerging challenges.

In his address to the EEF participants, OSCE Chairman-in-Office, Swiss Federal Councillor Ignazio Cassis, recalled that "Anticipation is a political necessity. This is why Switzerland has chosen Anticipating technologies as a priority of its Chairpersonship. We must anchor this approach in the OSCE, because technology already affects all three dimensions of the OSCE."

Participants are discussing how the OSCE can make better use of technological and scientific expertise in decision-making, strengthen anticipatory capacities and preparedness, and develop effective approaches to new technologies, including in relation to economic and environmental issues, in particular water, energy and economic good governance.

OSCE
Organization for Security and Co-operation in Europe

3.9 Million People Displaced in Ukraine as Families Struggle to Cope, IOM Report Finds



The latest data from the International Organization for Migration (IOM) show that 129,438 people, or 21,573 households, have been displaced across seven governorates in Yemen as families flee escalating insecurity.

"Nearly 130,000 people have been forced from their homes in just a few weeks. Many have already moved more than once to find safety," said Othman Belbeisi, IOM Regional Director for the Middle East and North Africa. "The numbers keep climbing. On 18 September we recorded 118,086 displaced people. Three days later, the figure has risen by 11,352".

This update from IOM's Displacement Tracking Matrix (DTM) shows that Ta'iz Governorate hosts the most displaced people, with 73,494. Lahj follows with 33,828, then Aden with 8,946 and Al Hodeidah with 8,244. Abyan (3,324), Hadramawt (1,008) and Ma'rib (594) have also received new arrivals.

Migration Routes Grow Dangerous Even as Irregular Arrivals Fall in 2026, New IOM Data Show

Migrant deaths more than doubled along the Central Mediterranean Route and tripled along the Eastern Mediterranean Route in the first four months of 2026 compared with the same period in 2025, even as the number of people arriving in Europe fell sharply, according to new data released today by the International Organization for Migration (IOM).

New IOM route-based data show that severe weather, conflict, economic pressure and changing migration policies reshaped migration journeys across multiple regions during the first four months of 2026. Along the Central Mediterranean, 821 people died or went missing, an increase of 111 per cent, while arrivals fell by 46 per cent to 8,577. More than half of those deaths, 430, were recorded in January alone, when Cyclone Harry struck the region. Along the Eastern Mediterranean, 244 people died, a rise of 259 per cent, with many fatalities linked to sea crossings that ended in disasters near Crete.

IOM data also show that along the Western African Atlantic Route, arrivals to Spain fell by 78 per cent to 2,276, the steepest decline of any route to Europe. Departure points have continued to shift further south along the West African coast, lengthening the sea crossing and raising the risks people face.

Tanzania at Heart of East Africa Migration Response

The United Republic of Tanzania and the IOM are strengthening cooperation on safe and regular migration, labour mobility, migrant protection and climate-related mobility, as countries across East and Southern Africa work together to respond to growing migration pressures and opportunities.

Migration remains a defining feature of the region, which hosts more than 12.7 million international migrants, over 16 million internally displaced people and approximately 5.4 million refugees.

As a country of origin, transit, destination and refuge, Tanzania serves as a key hub for migration dialogue and coordination across East and Southern Africa. The country currently chairs the Regional Ministerial Forum on Migration and hosts IOM's African Capacity Building Centre (ACBC), which supports migration governance and professional training across the continent.

IOM UN MIGRATION

Frontex Executive Director visits Pakistan to enhance border management cooperation



Frontex Executive Director Hans Leijtens concluded his first visit to Pakistan. He held talks with the country's Minister of Interior to explore opportunities for providing support to Pakistan through targeted activities on the country's road of reforming its border management system.

Hans Leijtens met Mohsin Naqvi, the Federal Minister for Interior of Pakistan, and was received by the Additional Secretary Europe from the Ministry of Foreign Affairs followed by a roundtable with high level officials from the Ministry of Interior and its entities chaired by Ministry of Interior's Special Secretary. The Executive Director also met his counterpart, Director General of the Federal Investigation Agency responsible for border and immigration control Dr Usman Anwar.

The sides reiterated their commitment to further deepen their relationship in line with Pakistan's efforts to curb irregular migration and smuggling networks. The discussions covered areas of cooperation including information exchange, risk analysis, document security as well as expert dialogue, and capacity building.

More than 156 tonnes of drugs seized and dozens of criminal networks dismantled in a global operation co-led by Frontex

More than 156 tonnes of drugs were seized and over 490 people arrested in an international operation that dismantled dozens of criminal networks moving cocaine and other illicit goods across the Atlantic. Operation ATLAS NEXUS was co-led by Frontex. It is the largest joint operation against organised crime carried out to date between Europe, Latin America and the Caribbean.

The operation targeted five priority criminal markets: drug trafficking, trafficking in human beings, document fraud, firearms trafficking, and environmental crime. Authorities from 34 countries took part, together with more than 8,680 police and judicial officers.

Ketamine among more than 12 kg of drugs seized at Madrid airport in operation co-led by Frontex

Ketamine, cannabis and a substance resembling toxic mushrooms, some of it hidden inside shoe boxes, were seized at Madrid airport during a week-long operation against synthetic drug trafficking through the air, co-led by Frontex.

The operation, called Aerial Routes, delivered the following results: 1,536 grams of ketamine, a new psychoactive substance; 11 kg of cannabis, in five bags; 15 plastic boxes hidden inside shoe boxes, containing a plant-based substance resembling toxic mushrooms.

The operation ran for a week at Adolfo Suarez Madrid-Barajas Airport. Led by the Spanish Guardia Civil and Frontex as an operational action under the Synthetic Drugs and New Psychoactive Substances (SYD/NPS) priority of EMPACT, the European Multidisciplinary Platform Against Criminal Threats, Operation Aerial Routes brought together seven Member States and European agencies.

Migration dialogues at the UN General Assembly, in high-level event co-hosted with Denmark, Jordan, Malta, Syria on regional security and cooperation



ICMPD Deputy Director General Sedef Dearing joined high-level discussion on the role of migration dialogues as catalyst for cooperation in the face of mounting pressures and security and geopolitical tensions globally. At the sidelines of the 81st session of the United Nations General Assembly, Ms Dearing, along with co-hosts Malta, Jordan, the Syrian Arab Republic and Denmark discussed the need to strengthen the resilience of migration governance through sustained, demand-driven partnerships.

The panel explored how migration capacity partnerships help institutions and countries strengthen their resilience through sustained cooperation, shared priorities, continued exchange, and complementary capacities. They also emphasised on demand-driven approaches that are grounded in national institutional realities and designed to build capacities and relationships that endure beyond individual projects. Two concrete experiences from ICMPD's work provided framing: the Migration Capacity Partnerships for the Mediterranean (MCP Med), and the BRIDGE programme in the Jordan-Syria context.

Budapest Process Thematic Working Group on legal pathways for migration highlights the role of the private sector on skills mobility partnerships

The Working Group examined how labour-market demand can be better matched with skills development, qualification recognition and fair recruitment across the Silk Routes region.

Co-chaired by Pakistan and Italy, the Thematic Working Group on Legal Pathways for Migration meeting built on the conclusions of the 2025 Thematic Meeting in Islamabad, particularly its recommendation to strengthen private sector engagement in skills-based labour migration partnership. Bringing employers into a dialogue previously conducted largely among governments, has marked a practical step in implementing Priority Goal 2 of the 2024 Budapest Process Ministerial Declaration and its Call for Action 2025–2030. This particularly refers to commitments to enhance cooperation on legal migration pathways and promote skills development and matching through partnerships with [private sector] employers.

Côte d'Ivoire begins turning its national border policy into practice

Adopting a national border policy provides a framework for action. Putting that framework into practice requires engagement with the institutions and communities working along the country's frontiers. In Côte d'Ivoire, this process is now taking place region by region, with ICMPD support through the Demand-Driven Facility (DDF) of the EU-funded FMM West Africa Phase II project.

In June 2024, Côte d'Ivoire adopted its National Integrated Border Management Policy (PNGIF-CI), setting out a framework for how the country will manage its borders. Turning that policy into practice along the country's frontiers is now a key focus for the government, with regional discussions helping identify how national priorities can be applied across different border areas.

ICMPD
International Centre for Migration Policy Development

SMART BORDERS ALBANIA 2030: FROM TRAVEL INTELLIGENCE TO INTELLIGENT BORDER MANAGEMENT

By PhD Chief Commissioner Artur Beu, Travel Intelligence Sector (SIU), Albanian State Police

Albania's journey towards a Smart Borders ecosystem is not simply a technology project. It represents a fundamental shift in the way travel data, intelligence, automation and privacy protection are brought together to manage modern mobility. With the adoption of Law No. 38/2025 on the Processing of Travel Information and Law No. 124/2024 on Personal Data Protection, Albania has established the legal and operational foundations for a new generation of intelligence-led border management systems aligned with European and international standards.

Across Europe and beyond, border authorities face a common challenge. International travel continues to expand while criminal



Figure 1. Conceptual Smart Borders architecture linking passenger data, travel intelligence and operational border systems.

networks, traffickers and terrorist organisations increasingly exploit the same transportation systems used by legitimate travellers. Traditional border controls alone are no longer sufficient. Modern agencies require advance visibility of passenger movements, rapid risk assessment capabilities and the ability to identify high-risk subjects before arrival, while ensuring the smooth movement of legitimate travellers.

This reality has driven the emergence of Smart Borders programmes around the world. Supported by ICAO, IATA, the United Nations and the OSCE, these initiatives seek to combine passenger data, biometrics, automation and intelligence into a single risk-based border management framework.

For Albania, the transition begins with the evolution of the former Passenger Information Unit into a broader Travel Intelligence Sector. Rather than focusing solely on collecting passenger data, the SIU is intended to become a centre for strategic analysis, targeting, intelligence production and operational cooperation. The scope of travel intelligence now extends beyond aviation to include information from maritime and land transport operators, creating a much richer understanding of travel patterns and mobility trends.

The transformation reflects a move from passive information collection to proactive intelligence generation. Advance Passenger Information, interactive API and Passenger Name Record data provide the raw material from which analysts can identify trafficking indicators, uncover organised crime networks, detect suspicious travel behaviour and support counter-terrorism operations.

A future Albanian Smart Borders platform is likely to rest on several interconnected capabilities. Central to the concept is a Passenger Data Single Window, recommended by ICAO Annex 9, allowing carriers to submit traveller information through a single technical gateway. Such an approach simplifies connectivity, improves data quality and creates a common operational picture across government agencies.

Advanced analytics will play an equally important role. Artificial intelligence and predictive modelling systems can assist analysts by identifying hidden relationships within large travel datasets, highlighting anomalies and providing early warning indicators. Human oversight, however, remains essential to ensure accountability, transparency and compliance with privacy obligations.

At the border itself, automation will increasingly shape the traveller experience. e-Gates, self-service kiosks, biometric verification and contactless processing technologies have the potential to reduce waiting times while enabling officers to concentrate resources on higher-risk individuals. Figure 1 illustrates the conceptual relationship between passenger data, travel intelligence and Smart Borders operations.

The success of any Smart Borders programme depends not only on technology but on interoperability. Effective information sharing between border authorities, law enforcement

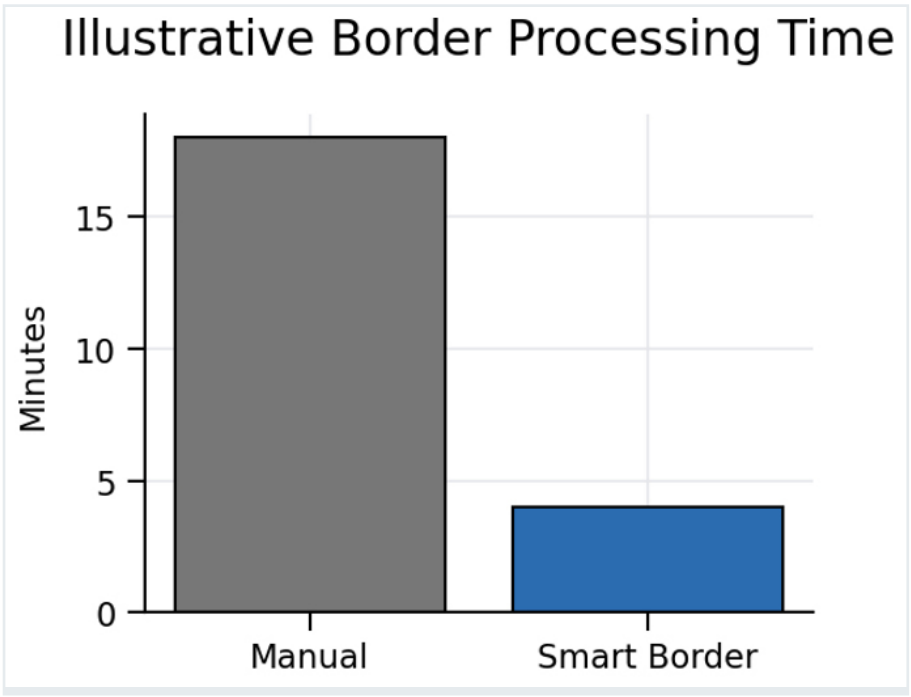


Figure 2. Illustrative comparison of manual and automated border processing times.

agencies, customs organisations, intelligence services and international partners is essential if travel intelligence is to generate operational value. The SIU is positioned to become the central hub for lawful travel information exchange and coordinated risk assessment.

Albania's ambitious vision also places privacy at the centre of system design. Security and privacy should not be viewed as competing objectives. Instead, successful Smart Borders architectures embed data protection principles from the outset through transparency, lawful processing, purpose limitation, auditability and robust governance mechanisms. Encryption, access controls, retention policies and independent oversight are all critical components of public trust.

The alignment of Albanian legislation with GDPR and the EU Law Enforcement Directive demonstrates a commitment to ensuring that travel intelligence capabilities develop within a clear legal framework. This approach reflects a broader European trend towards privacy-by-design governance where technological innovation is accompanied by strong safeguards for individual rights.

International standards provide an equally important foundation. ICAO guidance on API, PNR and Passenger Data Single Windows, IATA's One ID vision, United Nations counter-terrorism initiatives and OSCE border management principles all contribute to a common framework that supports secure mobility. By aligning with these standards, Albania strengthens both national security and its ability to cooperate with regional and international partners.

Figure 2 demonstrates the potential operational impact of Smart Border technologies. While actual performance depends on infrastructure, procedures and traffic volumes, the comparison illustrates how automation can significantly reduce processing times while maintaining security oversight.

Conclusion

Albania is positioning itself to become one of Southeast Europe's most progressive Smart Borders environments. By integrating API, PNR, travel intelligence, analytics and privacy-by-design governance into a coherent operational architecture, the country is laying the groundwork for intelligence-led border management that strengthens security while facilitating legitimate travel. The establishment of the Travel Intelligence Sector provides a platform for future interoperability, advanced analytics and automated border control capabilities. If successfully implemented, the model could serve as a regional example of how technology, intelligence and democratic safeguards can be brought together to support secure and efficient mobility.

Criminal Networks Work Across Borders. So Must States, IOM Chief Tells UN



Smugglers and criminal networks operate across borders, exploiting gaps. Governments must respond the same way with solutions across the routes people travel. That is the message IOM Director General Amy Pope is bringing to the UN General Assembly.

The International Organization for Migration (IOM) is calling on states to address shared challenges and opportunities across entire migration routes, from where they leave to where they arrive. The aim is solutions that work for everyone.

“Smugglers don’t see borders. They see a route, and they run it like a business. They plan ahead, and they move to exploit gaps between countries.” said DG Pope. “When countries work together, they can save lives, disrupt criminal networks, and manage their borders more effectively. That is one of the main topics we are putting on the table this week.”

This is in line with the Route-Based Approach, which involves identifying the challenges along key migration routes and making sure partners work together to address them effectively - from tackling root causes of irregular migration to disrupting smuggling networks to ensuring migrants’ rights are protected along the whole route. Countries plan together and act at the same time. Each government retains full control of its own borders and laws, while sharing information, coordinating actions, and closing the gaps criminal networks seek to exploit.

War, climate shocks and economic hardship are forcing millions of people from their homes. More than 83 million were living in internal displacement at the end of 2024, according to IOM’s World Migration Report 2026. Many others cross several countries on one journey, and smugglers and traffickers exploit them along the way. Smuggling and trafficking are both billion-dollar businesses, and people pay with their lives.

Nearly 8,000 people died or went missing on migration routes worldwide in 2025, according to IOM data. As of 15 September, arrivals in Europe by sea this year are down 39 per cent, yet at least 2,292 people have died or gone missing on the way, up from 1,999 at the same point last year. In July, IOM warned that hundreds of thousands of people have been trafficked and forced to run online scams.

IOM is calling on governments at the Assembly to focus on three practical areas: share information along their routes; expand more legal ways to work and travel, so fewer people turn to smugglers; and invest in people at home, with jobs and help after climate shocks, so leaving is a choice, not the only option. Well-managed migration also builds public trust, because people can see order, fairness and results.

Business has a role to play too. Companies create jobs, and legal jobs offer a safer alternative to abusive journeys. IOM is working through the UN Network on Migration and with private-sector partners, local communities and faith groups along the key migration routes.

As Member States call for a UN that delivers more effectively, IOM continues to contribute to UN80, the UN’s reform effort to reduce duplication and focus on results. IOM is sharing services, data and innovation with other UN agencies to deliver just that. More than 93 per cent of its operational budget goes directly to field projects.

“Every dollar has to work. Governments are right to ask that, and we hold ourselves to the same standard,” said DG Pope. “But efficiency is not the only goal. People are at heart of this, making sure the resources entrusted to us reach the people who need them most.”

PREVENTING CRIME AT BORDERS WITH UNITED NATIONS SUPPORT: HOW MONGOLIA USES PASSENGER DATA TO STOP THREATS IN REAL TIME

Mongolia is strengthening its ability to stop criminal activity at its borders before it happens.

Mongolia is strengthening its ability to stop criminal activity at its borders before it happens.

In 2026, Mongolia's Passenger Information Unit (PIU) helped identify a range of serious crimes, including suspected smuggling, drug trafficking, money laundering, and terrorist financing.

Authorities reported detecting attempted illegal cross-border smuggling cases valued at approximately MNT 700 billion (around USD 200 million) across Mongolia's border points. The PIU also helped identify around USD 10 million in undeclared cash and eight individuals wanted under INTERPOL notices, whose cases were referred to the relevant authorities.

In two separate cases, authorities intercepted 446.81 grams of methamphetamine that was being smuggled into the country. The PIU also helped uncover attempts to bring unregistered and prohibited medicines into Mongolia concealed in passengers' carry-on luggage. In another case, authorities identified a fugitive who had been wanted for 30 years.

These results were made possible through cooperation between Mongolia and the United Nations Countering Terrorist Travel (CT Travel) Programme, which supported the establishment of Mongolia's Passenger Information Unit in December 2023.

Using Passenger Data to Identify High-Risk Travelers

The Passenger Information Unit uses the United Nations goTravel software system to receive and analyse passenger information provided by airlines before international flights arrive in Mongolia.

By analysing travel routes, patterns, and other risk indicators, the system helps authorities identify potentially high-risk travellers in advance. It can also compare passenger information against national and international watchlists and facilitate information-sharing among relevant agencies.

Today, the PIU receives passenger data from seven airlines, covering around 90 per cent of Mongolia's international commercial air traffic.



Before the system was introduced, passenger data was used in a more limited and largely manual way. The new platform automates the collection and analysis of information, allowing analysts to focus on assessing risks rather than processing data.

According to Colonel Adiyajav Enkhtur, Head of Mongolia's Passenger Information Unit, the goal is not to subject every traveler to additional scrutiny. "The primary objective of the Mongolian PIU is not to subject all passengers to additional scrutiny, but rather to identify high-risk passengers in advance through intelligence-led risk assessment and to effectively support the operations of competent and law enforcement authorities," he said.

"API and PNR data enables low-risk passengers to move through border controls quickly and seamlessly, enhancing overall efficiency."

Protecting Privacy and Human Rights

Mongolia's Passenger Information Unit operates under legal safeguards designed to protect privacy, data security, and human rights. Access to passenger information is restricted to authorized personnel, and the system maintains records of how data is accessed and used. Passenger information may only be processed for specific legal purposes and is protected through security measures designed to prevent misuse.

According to Colonel Enkhtur, Mongolia is continuing to strengthen its legal framework governing the use and exchange of passenger information, with particular attention to human rights, confidentiality, and data protection standards.

How the UN CT Travel Programme Supported Mongolia

Mongolia joined the United



Nations Countering Terrorist Travel Programme in 2020. With support from United Nations partners, the country developed legislation governing the use of airline passenger data, established its Passenger Information Unit, and deployed the UN goTravel software system.

The legal framework was adopted by the Parliament of Mongolia in January 2023. The Passenger Information Unit was officially inaugurated in December 2023, and the goTravel system became fully operational in January 2025.

The programme also provided training on passenger data analysis, risk assessment, privacy protections, and use of the goTravel platform.

Today, Mongolia is one of seven programme beneficiary countries operating the UN-developed goTravel system.

About the UN Countering Terrorist Travel Programme

The United Nations Countering Terrorist Travel (CT Travel) Programme, led by the United Nations Office of Counter-Terrorism (UNOCT), helps Member States use Advance Passenger Information (API) and Passenger Name Record (PNR) data to detect and prevent terrorism and other serious crime while upholding human rights and data protection standards.

Through legal, operational, and technical assistance, including the deployment of the UN-developed goTravel system, the Programme supports countries in strengthening border security and information-sharing. CT Travel is implemented through a “One-UN” partnership with the United Nations Counter-Terrorism Committee Executive Directorate (CTED), the United Nations Office on Drugs and Crime (UNODC), the International Civil Aviation Organization (ICAO), the United Nations Office of Information and Communication Technology (UNOICT), the International Criminal Police Organization (INTERPOL), and the International Organization for Migration (IOM).

Web story: https://www.un.org/counterterrorism/en/events/preventing-crime-borders-united-nations-support-mongolia

ICAO alignment will accelerate global roll out of contact-free and seamless travel technologies



Air travelers around the world will soon encounter faster, more seamless airport journeys following renewed commitments by governments and industry at the International Civil Aviation Organization (ICAO) to accelerate the shift to digital identity and contact-free border processing.

ICAO's 21st TRIP Symposium brought together over 600 government officials and industry leaders representing 70 countries and seven international organizations. Delegates reported new progress in traveler identification systems, border security and privacy safeguards. Many of these advances are already in use at airports worldwide, leading to measurable gains in efficiency, economic growth and the overall passenger experience.

Countries are moving forward with national programs using multimodal biometrics, automated gates, and even contactless and digitally enabled travel for their residents. Automation is now shifting officers away from manual checks toward more oversight and risk-based decision-making.

Crucially, States recognized that alignment with ICAO specifications and standards will enable States and industry to respond to the challenges of accelerating the global roll out. Participants emphasized that interoperability remains the key enabler of seamless travel. While technologies and operational models may differ across States, alignment with ICAO Standards and Recommended Practices (SARPs), technical specifications and guidance material is essential to ensuring global trust, recognition and cross-border compatibility.

The three-day gathering revealed precisely how while some countries have deployed cutting-edge biometrics and digital credentials, others are working to overcome technical and operational hurdles. Officials warned that uneven adoption leaves gaps in the global travel system, reducing resilience and efficiency.

There is now consensus that automation and data-driven risk management enable most travelers to be processed with less friction while frontline officers can focus on higher-risk cases. Redesigned operational models can allow one officer to oversee several automated lanes, reducing staffing burdens and overtime. However, not all countries have the same legal frameworks or institutional readiness, and many challenges remain.

Industry and government representatives shared success stories involving biometrics, digital identity tools and modernized border procedures, highlighting the importance of aligning with the international frameworks specified in Annex 9 – Facilitation of the 1944 Convention on International Civil Aviation and related ICAO guidance materials.

They also pointed to ICAO's crucial ongoing role in developing the ICAO Digital Travel Credential and maintaining the ICAO Public Key Directory, which support compatibility and security across national systems. This role is further supported by international and regional cooperation, which has proven especially effective at rapidly scaling new best practices.

AGENCY NEWS AND UPDATES

CBP hits trade transgression trifecta with seizures of counterfeit, unsafe, and fraudulently imported goods



U.S. Customs and Border Protection officers recently seized five shipments that illustrate the wide scope of trade violations.

These violations covered counterfeit goods, goods determined to be potentially unsafe by consumer protection authorities, and goods imported using identity theft. Collectively, these goods were valued at nearly $856,000.

CBP officers seized 1,500 rolls of rugs from Turkey for violating the Flammable Fabrics Act.

In the most recent seizure, CBP officers seized 697 cartons of short-sleeved and long-sleeved dry fit t-shirts on Tuesday that were being fraudulently imported from Morocco to Albany, N.Y., using a victim's stolen identity. The dry-fit t-shirts were valued at $61,240.

CBP officers seized a shipment of 1,500 rugs that the Consumer Product and Safety Commission determined violated the Flammable Fabrics Act. That shipment, which arrived from Turkey and was destined to Tustin, Calif., was valued at $3,720.

Geelong man charged following 9kg methadone detection at Melbourne Airport



The AFP has charged a Geelong man for importing a commercial quantity of methadone into Melbourne.

The man, 48, was arrested by the AFP at Melbourne Airport.

Australian Border Force (ABF) officers identified anomalies during an X-ray examination of the man's luggage after he arrived on a flight from Thailand.

A subsequent examination located five plastic bags, allegedly containing about 2500 pills collectively weighing nine kilograms, hidden inside.

Dismantled a criminal organization that laundered more than four million euros from scams by sending the money to Nigeria



The Guardia Civil has dismantled a criminal organization specialized in money laundering from scams committed both in Spain and in other

countries. The operation has resulted in the arrest of 20 people and the investigation of 11 others as alleged perpetrators of the crimes of fraud, money laundering, documentary falsification, usurpation of civil status and membership of a criminal organization.

During the records, forged identity documents and passports, mobile phones, SIM cards, cash, jewelry, bank documentation and abundant documentation related to money laundering activity were intervened. The researchers also located more than 400 documents used to make the money transfers.

So far, the investigation has identified more than 200 victims spread across different Spanish provinces.

14 nabbed in crackdown on illegal cross-border transport services

A total of 14 people have been caught in recent enforcement operations against illegal cross-border transport services, said Senior Minister of State for Transport Sun Xueling.

The Land Transport Authority (LTA) has been conducting the operations islandwide - including at Changi Airport and Gardens by the Bay - over the past few weeks, said Ms Sun.

LTA and the Immigration & Checkpoints Authority (ICA) also conducted a joint enforcement operation at Singapore's land checkpoints at Woodlands and Tuas.

This is "part of our continued efforts to safeguard commuter safety and protect the livelihoods of our local point-to-point drivers from illegal cross-border transport services", added Ms Sun.

Coast Guard transfers 10 aliens to the Bahamas following interdiction near Fort Lauderdale

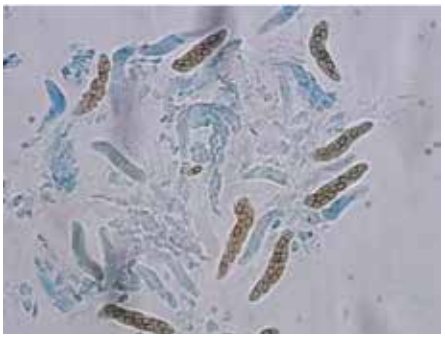


Coast Guard Cutter Margaret Novell's crew transferred 10 aliens to the Bahamas, Sunday, following an interdiction of a 30-foot vessel approximately forty miles east of Fort Lauderdale.

Coast Guard Cutter Robert Yered's crew boarded a 30-foot sailing vessel, Friday, and discovered 10 people aboard. The aliens were transferred to the ship for processing. The aliens were further transferred to USCGC Margaret Norvell.

"In the face of daunting, 8-foot seas, the crew of the Robert Yered demonstrated extraordinary professionalism and dedication for hours on end," said Lt. Richard Rodriguez, the cutter's commanding officer. "It is precisely this level of steadfast commitment that allows us to succeed in our missions. Their performance was a testament to our readiness to save lives and protect our nation's maritime borders, even under the most grueling conditions."

CBP protects U.S. agriculture with first-in-nation pathogen interception at George Bush Intercontinental Airport



U.S. Customs and Border Protection agriculture specialists at George Bush Intercontinental Airport (IAH) recently intercepted a plant pathogen never before detected at a U.S. port of entry.

During an inspection of baggage belonging to a traveler from New Zealand, CBP agriculture specialists discovered eucalyptus leaves that exhibited signs of a suspected plant disease. Recognizing the potential risk to U.S. agriculture, CBP agriculture specialists intercepted the items and forwarded samples to the U.S. Department of Agriculture plant pathologists for further analysis.

The USDA laboratory confirmed the pathogen as Davisoniella eucalypti (Mycosphaerellaceae). This detection marks the first time this specific pathogen has been intercepted in the United States.

ABF sanctions NSW aged care provider for migrant worker exploitation

A New South Wales, South Coast, aged care provider has been sanctioned by the Australian Border Force

(ABF) requiring them to repay nearly $120,000 to sponsored employees, following an investigation that found it had unlawfully recovered sponsorship-related costs from migrant workers.

Acting on a Border Watch report, ABF officers from the Department of Home Affairs Sponsor Monitoring Unit launched an investigation into the company.

The investigation revealed the business had sponsored 19 workers under the Skills in Demand (Subclass 482) visa, with 13 workers affected by breaches totalling $118,197.

Officers conducted an unannounced site visit, interviewing sponsored workers and company representatives. The investigation revealed that sponsorship-related costs had been recovered from migrant workers, which is prohibited under Australia's migration laws.

Two workers told officers they had paid $17,449 and $19,847 respectively toward nomination and visa application costs and provided supporting evidence.

Philadelphia CBP officers intercept two Europe-bound marijuana loads, Troopers arrest two

Two women are facing felony drug possession charges after U.S. Customs and Border Protection officers intercepted 97 pounds of marijuana in smuggling attempts on consecutive days this week at Philadelphia International Airport.

CBP officers seized 41 pounds of marijuana on March 16 and another 56 pounds that were discovered in baggage being loaded onto flights bound for Europe. CBP narcotics detector dog Fredo, a 3-year-old male German shepherd, alerted officers to the marijuana.

Officers stopped Taveras at the departure gate to a London-bound flight and stopped Cromwell as she attempted to board a flight to Frankfurt, Germany. Officers identified both women based on the baggage tags on their checked baggage.

Four arrested in Germany as part of major international operation targeting Channel small boat people smuggling network



National Crime Agency officers have joined international partners in a major operation which has seen four people arrested in Germany, as part of an investigation targeting a network suspected of supplying equipment to cross-Channel small boat people smugglers.

The raids, which took place in the North Rhine-Westphalia region, also saw boats and engines seized, as well as petrol cans, pumps and life jackets, as officers raided a number of suspected storage warehouses linked to the gang. Residential properties were also searched.

Twelve locations in the western cities of Essen, Gelsenkirchen, Marl, Bottrop, Herdecke, and Lüdenscheid were targeted, with more than 450 police officers involved. A team of NCA officers deployed to Germany to assist.

Record seizures highlight intensified crackdown on illicit tobacco



New data shows the Australian Border Force (ABF) continues to deliver significant results in disrupting illicit tobacco supply chains, seizing over 2,300 tonnes of illicit tobacco and 13.2 million vapes last financial year, preventing them from entering the community and cutting off funds to criminal syndicates.

Along with record seizures, the ABF's ability to leverage a full end-to-end compliance model has targeted every stage of the criminal supply chain, offshore, at the border and domestically - making it progressively difficult for organised crime to conduct their business.

The ABF's exceptional pre-border results demonstrate the critical role

international partnerships, intelligence sharing and targeted disruption play in preventing illicit tobacco from entering the Australian community.

These illicit tobacco products represent estimated tobacco duty evasion in excess of $236.6 million (excl. GST)

More Than 10kg of Cannabis Detected at Tuas Checkpoint



A 36-year-old Malaysian man and a 35-year-old Malaysian woman have been arrested for attempting to smuggle drugs, including more than 10kg of cannabis, in a Malaysia-registered motorcycle arriving at Tuas Checkpoint.

Based on information received from the Immigration & Checkpoints Authority (ICA)'s Integrated Targeting Centre, ICA officers referred the motorcycle for enhanced checks. In the course of the checks, ICA officers uncovered four bundles of vegetable matter believed to be controlled drugs underneath the motorcycle seat. Central Narcotics Bureau (CNB) officers were immediately alerted to the detection and conducted further checks, uncovering six more bundles of vegetable matter believed to be controlled drugs in a black haversack on the motorcycle's handlebar. The seized bundles were found to contain a total of about 10,164g of cannabis.

The drugs seized have an estimated worth of more than $203,000 and could potentially feed the addiction of about 1,450 abusers for a week.

Five Tonnes of Cocaine Seized by the Portuguese Authorities in MAOC-N Supported Operation



The Portuguese Judicial Police, in close cooperation with the Portuguese Navy and the Portuguese Air Force, intercepted a container vessel during a maritime operation that resulted in the seizure of approximately five tonnes of cocaine destined for the European market.

The operation led to the arrest of two individuals found clandestinely on board the vessel, as well as one crew member suspected of involvement in the trafficking venture. Several items allegedly used to facilitate the navigation, overboard deployment and subsequent recovery of the narcotics were also seized.

The investigation began shortly after intelligence was first shared through the Centre and is being developed in close cooperation with the United Kingdom's National Crime Agency (NCA) and the Spanish National Police.

The container vessel was subsequently escorted by the Portuguese Navy to the Port of Sines, where the narcotics were offloaded.

Visa cancellations follow $250,000 illicit tobacco airport bust



Four Chinese nationals have been refused entry to Australia after attempting to smuggle approximately $250,000 worth of illicit cigarettes in their luggage.

The travellers arrived at Melbourne Airport from Shanghai and were selected by Australian Border Force (ABF) officers for a full baggage examination.

A total of 145,529 cigarettes were seized across the four travellers' luggage with a total duty evasion of approximately $250,000. One traveller was also in possession of around 2,320 prohibited heat sticks and vape accessories.

Following examination, three men and one woman aged 65, 67, 67, 64 respectively, were referred for visa cancellation under s116(1)(d) and Subdivision C s102 and refused immigration clearance.

EUROPE'S EASTERN FRONTIER FACES A NEW ERA OF BORDER SECURITY CHALLENGES

By: Tony Kingham, Editor, Border Security Report

The European Union's eastern border has become one of the most strategically important frontiers in the world. Running from Finland in the north through the Baltic States and Poland before stretching southwards towards Romania and the Black Sea, it is no longer simply a line separating neighbouring states. Instead, it has become a complex security environment where geopolitical tensions, migration pressures, organised crime and emerging technologies increasingly converge. Issues that were once considered separate are now closely interconnected, placing growing demands on border agencies and governments alike.

The transformation of the eastern frontier has been driven largely by Russia's invasion of Ukraine in 2022, which fundamentally altered the security environment across Eastern Europe. Countries such as Poland,

Slovakia, Hungary and Romania suddenly found themselves on the frontline of Europe's response to the conflict, managing the movement of millions of Ukrainian refugees while maintaining the integrity of the European Union's external borders. The scale of these movements tested border infrastructure, personnel and processing systems in ways few could have anticipated.

While the refugee response demonstrated the resilience and professionalism of European border agencies, it also highlighted the broader security implications of instability on the EU's eastern doorstep. Frontex has repeatedly warned that continued geopolitical volatility east of the European Union could generate further migration pressures and create new operational challenges for border services. As the agency noted in its Risk Analysis, European Integrated Border Management is being forced to operate in an increasingly turbulent and hostile geopolitical environment.

The war has also reinforced concerns about wider regional instability. European law enforcement agencies remain alert to the opportunities that conflict can create for organised criminal groups, particularly those involved in smuggling, trafficking and other forms of cross-border criminality. Europol's latest Serious and Organised Crime Threat Assessment identifies organised crime as one of the most significant threats facing the European Union, warning that criminal networks are becoming increasingly adaptable, technologically enabled and international in their operations.

Alongside the consequences of the war in Ukraine, Europe's eastern borders have become a focal point for a different type of threat: hybrid activity.

Over the past several years, Poland, Lithuania and Latvia have experienced sustained migration pressure on their borders with Belarus. The European Commission has described these activities as the weaponisation of migration, arguing that Russia and Belarus are exploiting vulnerable people as part of a broader campaign designed to place pressure on the European Union. According to the Commission, the tactic forms part of a wider hybrid threat environment targeting the EU's external borders and broader security interests.

European Commission President Ursula von der Leyen has described the situation as an example of "Russia's and Belarus's unacceptable weaponisation of migration", warning that frontline states are facing increasing pressure to guarantee both national security and the integrity of the Schengen Area. The Commission has subsequently announced additional funding for surveillance systems, communications infrastructure, mobile detection equipment and counter-drone



capabilities along affected sections of the eastern frontier.

For border agencies, these incidents create particularly difficult operational challenges. Officers are required to prevent illegal crossings, maintain border integrity and protect national security while simultaneously operating within legal and humanitarian obligations. Unlike conventional migration flows, these situations often have wider political and strategic implications, requiring close coordination between border authorities, law enforcement agencies and national governments.

Migration itself continues to remain a major operational challenge along the eastern frontier. While the Mediterranean routes often dominate headlines, migration



pressure can rapidly shift in response to geopolitical events, economic conditions and enforcement measures. Frontex assessments have repeatedly highlighted how global instability, food insecurity and economic hardship can contribute to migration movements towards Europe, often creating opportunities for criminal smuggling organisations to exploit vulnerable populations.

These movements are frequently facilitated by sophisticated smuggling networks. According to Frontex, the number of detected people smugglers increased significantly as irregular migration pressures rose across the EU's external borders. The agency has warned that migrant smuggling continues to evolve into an increasingly sophisticated criminal business model, closely linked to wider organised criminal activity. Many networks now operate across multiple jurisdictions, adapting routes and methods in response to evolving enforcement measures.

Organised crime remains one of the most persistent concerns facing border authorities across Eastern Europe. The region's geographic position between Europe, Asia and the Middle East makes it a natural transit corridor for a wide range of illicit activities. Criminal groups are involved in narcotics trafficking, human trafficking, illicit tobacco movements, counterfeit goods and financial crimes, often using the same logistics networks that facilitate legitimate trade.

Europol's latest assessments highlight the increasingly international nature of organised crime. Networks operate across borders, adapt rapidly to enforcement activity and use modern communications technologies to coordinate operations. The agency has also warned that organised crime is becoming increasingly intertwined with broader security threats, further complicating the task facing law enforcement and border authorities. For border agencies, this means that traditional interception and inspection activities must be complemented by intelligence-led operations, international cooperation and information sharing.

While much of the discussion surrounding the EU's eastern frontier focuses on the land borders with Russia and Belarus, the Black Sea has emerged as an increasingly important border security environment in its own right. Romania's coastline represents the European Union's principal Black Sea maritime border, while neighbouring Bulgaria occupies a key position along one of the region's busiest maritime corridors. Since the outbreak of the war in Ukraine, the strategic importance of the Black Sea has increased significantly as commercial shipping routes, energy infrastructure and regional security concerns have become ever more closely linked.

For maritime border authorities, the challenge is far broader than managing vessel movements. The region lies at the crossroads of Europe, the Caucasus and the wider Black Sea basin, creating opportunities for smuggling and organised criminal activity alongside legitimate commercial trade. As shipping patterns have adapted to the realities of the conflict, authorities have faced growing demands for vessel monitoring, maritime

surveillance and cross-border intelligence sharing. Ports on the western Black Sea have meanwhile become increasingly important for Ukrainian exports, adding a further layer of complexity to maritime security operations and requiring enhanced cooperation between border guards, coast guards, customs authorities and naval forces.

The protection of critical maritime infrastructure has become another growing concern. Ports, energy facilities, offshore installations and logistics hubs all form part of a broader security picture that extends well beyond traditional border management. In response, coastal states have expanded investments in maritime domain awareness capabilities, combining radar systems, electro-optical sensors, aerial surveillance assets and unmanned systems to improve coverage across large maritime areas. For border agencies operating in the region, the Black Sea is no longer simply a maritime border. It has become an extension of the wider eastern frontier security environment where border management, organised crime, regional instability and strategic security considerations increasingly converge.

Technology is increasingly central to how these challenges are addressed.

The sheer geography of the eastern border presents difficulties that cannot be solved through manpower alone. Large stretches of forest,



wetlands, lakes and remote rural areas make continuous physical monitoring difficult. In response, governments have invested heavily in surveillance technologies designed to improve situational awareness and provide earlier warning of potential incidents. The European Commission's support package for borders with Russia and Belarus includes substantial investment in upgraded electronic surveillance systems, enhanced telecommunications networks and mobile detection technologies.

Modern border surveillance systems increasingly combine radar, thermal imaging cameras, electro-optical sensors and automated monitoring tools. These capabilities allow border authorities to observe larger areas, identify suspicious activity more quickly and direct resources more efficiently. Across Europe, agencies are increasingly investing in integrated surveillance architectures designed to provide real-time operational awareness across both land and maritime environments.

There is also growing interest in mobile surveillance systems capable of being deployed rapidly in response to changing operational demands. Industry experts argue that mobile and autonomous surveillance platforms can provide flexibility that traditional fixed infrastructure cannot, particularly across remote and difficult terrain where conventional patrol coverage may be limited.

Unmanned systems are playing an increasingly important role. Drones equipped with thermal imaging cameras and advanced sensors are now routinely used to monitor remote terrain, assist patrol units and provide rapid situational awareness. These



systems can cover large areas more efficiently than traditional patrols and are becoming an increasingly important part of the modern border security toolkit.

At the same time, unmanned aerial systems present their own challenges. Recognising the growing threat posed by drone incursions, the European Commission has specifically allocated funding to help frontline states improve their ability to detect and counter unauthorised drone activity along the eastern border.

Physical security infrastructure also continues to play an important role. Frontex has noted the substantial expansion of border fencing and physical barriers across Europe's external borders over the past decade. While such measures remain politically debated, many border agencies regard them as one component of a broader border management strategy. Physical barriers can slow unauthorised movements, channel crossings towards designated control points and provide valuable response time for security forces.

Yet technology and infrastructure alone cannot solve the challenges facing Europe's eastern border. Personnel remain the most important element of effective border management. Across Europe, agencies are investing in training, specialist capabilities and technological skills to meet increasingly complex operational requirements. Modern border guards are expected to understand advanced surveillance systems, identify sophisticated fraudulent documents, support intelligence-led operations and respond to a wide range of security incidents.

The eastern frontier is likely to remain one of Europe's most demanding border security environments for the foreseeable future. The war in Ukraine shows no sign of bringing immediate stability to the region, while tensions between Russia, Belarus and the European Union continue to shape the threat landscape. Organised crime networks remain highly adaptable, migration pressures continue to fluctuate, and emerging technologies are creating both new opportunities and new operational challenges.

For Europe's border security community, the challenge is clear. The eastern border is no longer simply a line on a map. It is a dynamic operational environment where geopolitical competition, criminal activity and migration pressures converge. Securing it will require continued investment in technology, intelligence, infrastructure and personnel, as well as close cooperation between national authorities, Frontex and international partners.

What is certain is that the importance of the European Union's eastern frontier will continue to grow, making it one of the defining border security challenges of the decade.

Sources: Frontex Risk Analysis 2023/24; European Commission Communication on Countering Hybrid Threats and the Weaponisation of Migration (2024); Europol EU Serious and Organised Crime Threat Assessment (EU-SOCTA) 2025; European Parliament Research Service briefing on eastern EU border regions (2025).

Arab and Turkish Experts Meet in Istanbul to Advance Border Governance

Senior officials and experts from across the Arab region and Türkiye are meeting in Istanbul this week to discuss how countries can strengthen border security while ensuring safe and regular movement and better protection for people on the move.

With countries across the Arab region increasingly serving as places of origin, transit, destination and return, migration and border management are becoming more closely interconnected. Conflict, economic disparities, environmental pressures and demographic change are also contributing to increasingly complex patterns of human mobility.

“At a time when mobility, security and development are increasingly interconnected, our task is to strengthen border governance systems that are secure, effective and responsive, while remaining firmly anchored in the dignity and rights of every person. Effective border governance does not require a choice between security and protection. It requires both,” said Othman Belbeisi, IOM Regional Director for the Middle East and North Africa.

Held under the framework of the Arab Centre for Technical Cooperation on Migration and Border Management (ACTC-MBM), established by IOM and NAUSS in 2022, the symposium provides a forum for practitioners and policymakers to exchange experience and identify practical approaches to border governance that can be applied across different national contexts.



Feature sponsored by: CRFS

STRENGTHENING EUROPE'S EASTERN BORDERS WITH ELECTROMAGNETIC AWARENESS

Drone incursions present a significant security challenge along Europe's eastern borders, with implications for national borders, airspace, nearby communities, and critical infrastructure.

A distributed electromagnetic sensing network could strengthen early warning and threat assessment, allowing local sites to serve their own operational needs while joining together to contribute to a shared national picture.

One Baltic morning

At 07.00, border guards in a Baltic nation spot an unidentified drone crossing into national airspace. Ten minutes later, coastal surveillance detects several vessels approaching territorial waters with no Automatic Identification System (AIS) transmitting. At 07.20, residents report drones flying near an international airport.

Three incidents within twenty minutes. Are they connected?

In this hypothetical scenario, each report sets a different response in

motion. Border guards alert military authorities. Maritime agencies investigate the suspect vessels. Airport authorities immediately close airspace to assess whether flight operations can continue safely. Each organisation holds information that could be vital for national security, yet there is no complete local or national intelligence picture.

Disruption will begin long before hostile intent is established. Inevitably, flights will be delayed, maritime traffic diverted, and security resources committed while authorities determine the scale of the threat.

When addressing this situation, there are two main challenges: The first is to manage the incident locally. The second is for the national authorities to understand the wider picture and rapidly establish whether these separate observations are unrelated or indicate a wider pattern. Electromagnetic awareness could provide some of the intelligence required to address both challenges.

While this scenario is hypothetical, the threat drones pose to European security is very real.

Multiple incidents, one security problem

Recent incidents across Europe have shown how quickly a drone detection can become a national security emergency.

In the early morning of 15 September 2026, Italian Eurofighters operating under NATO intercepted a drone that



had entered Lithuanian airspace. On recovering the wreckage, authorities neutralised its explosive payload. The incident highlights the importance of persistently monitoring national airspace so authorities can assess threats while there is still time for intervention.

Further south, drone incursions have provoked military responses and endangered lives. Violations of Polish airspace on 10 September 2025 prompted measures to strengthen surveillance and defence along the eastern flank. In Romania, a drone struck a residential building in Galați on 29 May 2026. The drone was detected before it entered Romanian air space; however, continuous tracking, assessment, and having increased decision time also contribute to successful defences.

Vulnerability also extends west. In August 2026, flight operations at Leipzig/Halle Airport were suspended after an employee discovered a drone carrying an explosive device. Threats to national security can emerge well beyond Europe's eastern borders.

Disruption is cheap, while security is expensive

Relatively inexpensive drones can impose costs far beyond their unit price. An incursion will likely delay flights, disrupt freight, divert police resources, and drive a military response. Even without physical



damage, disruption can undermine public confidence in government and the authorities.

Disrupting one specific site can have consequences beyond the immediate incident. Concentrating personnel and assets in one area may reduce security elsewhere, creating further vulnerabilities. Repeated incidents compound the problem. Authorities must remain perpetually alert, businesses must absorb shocks, and governments must divert resources to combat threats with unclear intentions.

The strategic challenge is maintaining effective protection as incidents become more frequent while the next target remains unclear. This requires local authorities to monitor their own sites while national authorities can connect the national picture.

Given recent incidents, the case could be made for additional sensing capabilities that improve electromagnetic situational awareness. Drones that transmit control, telemetry, or video signals can reveal their presence through these emissions. Detecting and locating signals can give border units, infrastructure operators, and security agencies critical data for early warning and analysis.

What is electromagnetic awareness?

Electromagnetic awareness is understanding how the radio frequency (RF) spectrum is being used by all wireless technologies. It provides intelligence on what is transmitting, where the signal is coming from, and how the signal changes over time. To gain electromagnetic awareness, a network of passive RF sensors must be deployed around a target location, and a normal pattern of activity established, potentially including emitters from cellular networks, broadcast networks, and emergency services communications.

Passive RF sensors ‘listen’ for all RF transmissions, including drone control links and video feeds, without emitting signals themselves. This allows them to ‘see without being seen’. Software allows operators to characterise emissions and geolocate them over time.



Data from RF sensing contributes to the Recognised Electromagnetic Picture: an assessed view of signal activities across a specific geographic area that provides information about a signal's location, behaviour, and changes over time. An unfamiliar signal may warrant closer investigation, but a low probability of detection signal transmitted on a frequency consistent with known drone telemetry links may require immediate further assessment.

Electromagnetic information can complement any existing air surveillance, which often struggles to detect drones because of their size, shape, construction materials, and low flight paths. Any available video imagery, acoustic sensing, or drone tracking software can be used to provide additional intelligence.

Passive RF sensing can provide intelligence in areas where there is no radar coverage, due to gaps or the high installation cost of installing radar. It can also be used to cue radar in situations when radar cannot operate persistently. The relatively low cost of establishing a network makes it easier to detect threats in the spectrum before they are visually confirmed.

From local surveillance to a shared national picture

Although the ultimate goal is to obtain a shared national electromagnetic picture, the project begins with the operational needs of individual sites:



airports, ports, energy facilities, and border units. Each unit operates its own sensing network, understanding normal RF activity so any deviations can be investigated quickly.

Organisations operating individual networks retain total control of their systems, while also being able to connect to other networks through federation. They can share selected information through common standards and access rules. This means that one site can contribute relevant observations without making all its data available to every other user.

Regionally, organisations could correlate observations and exchange alerts. Think back to the airport and border unit described in the hypothetical scenario. Joint examination of timing, locations, and signal characteristics could reveal key information about the threats or an adversary's behaviour.

National agencies could correlate RF data with air-surveillance intelligence to assess wider patterns. International networks involving neighbouring countries could extended early warning and intelligence gathering across borders.



The value of joining separate networks is that the whole is greater than the sum of its parts. While an individual site would benefit locally, it would also benefit from joining a network spanning the whole eastern border of Europe.

While spectrum sensing cannot prevent drones being launched, its value lies in earlier warning and shared intelligence, meaning less disruption and more effective use of resources. As part of a layered security system using other sensors, electromagnetic monitoring can give authorities more time to assess activity and select a proportionate, cost-effective response.

Conclusion: contributing to Europe's wider security effort

This proposed approach is consistent with the European Commission's 2026 Action Plan on Drone and Counter Drone Security, which addresses shared situational awareness, critical infrastructure, and external borders. The plan proposes integrating relevant information into a shared air display and supporting counter-drone capabilities for infrastructure and border protection. These priorities provide a policy context for considering how locally operated electromagnetic sensing networks could contribute to wider surveillance systems.

The debate over a European "drone wall" raises a related challenge. In his October 2025 Chatham House analysis, Tim Chattell argues for cooperation across borders, and clear frameworks for safe and rapid intervention. Protecting Europe's eastern borders also depends on whether institutions can share information, exercise clear responsibilities, and maintain public confidence when incidents occur. Electromagnetic sensing can play a role in achieving these goals.



New Travel Industry Coalition Calls for EU Digital Omnibus to Enable Secure, Seamless Biometric Journeys

ACI EUROPE, Amadeus, IATA, IDEMIA Public Security and SITA have announced the formation of the Responsible Biometrics Travel Industry Coalition, calling on EU policymakers to ensure the Digital Omnibus actively supports the voluntary and secure use of biometrics in travel while protecting passenger choice and privacy.

The coalition is seeking a balanced regulatory approach that enables a more efficient and convenient experience for air travelers and maintains strong safeguards around the responsible use of biometric technologies.

The Digital Omnibus is intended to simplify Europe's digital rulebook, support innovation and strengthen competitiveness. It also preserves high standards of data protection and cybersecurity. Yet the legislative proposal could place unintended restrictions on the voluntary use of biometrics by passengers across Europe.

The coalition is urging policymakers to ensure the Digital Omnibus preserves passenger choice and allows citizens to benefit from the opportunities that biometrics can offer.

Why Biometrics Matter

Biometrics make travel more seamless for passengers and deliver significant operational benefits for airports and airlines. By reducing repeated manual document checks, biometric verification increases throughput, improves passenger flows and helps airports use existing terminal infrastructure more efficiently. It also helps airports better manage peak periods and traffic growth, allowing staff to focus on passengers who need assistance or additional attention.

Combined, these benefits boost Europe's competitiveness by promoting efficient, well-connected airports and innovation across the travel and technology sectors. A clear regulatory framework can encourage continued investment and enable European technology companies to innovate and scale trusted solutions in their home market.

To unlock the full potential of biometrics in European air travel, the coalition calls for the Digital Omnibus to adopt technology-neutral rules that allow the voluntary use of biometric data (where appropriate safeguards are in place) and offer passengers non-biometric alternatives.

Protecting Privacy and Passenger Choice

The coalition firmly believes the benefits of biometrics should go hand in hand with strong protections for passenger privacy and passengers' ability to choose whether to share or request to delete their data at any time. The use of biometric solutions should be voluntary, secure and limited to a defined journey.

Research cited by the coalition found that 74% of travelers surveyed were willing to share biometric data in place of showing a passport or boarding pass, according to IATA's Global Passenger Survey.

Manifesto

EU policymakers have the opportunity to put Europe in the global lead on biometric regulation. The benefits of the latest technologies are clear: they can protect passenger data privacy and open a more seamless and efficient travel process. This will enhance the region's overall competitiveness. At the same time, biometric journeys should always be based on passenger choice and voluntary participation.

The 'Advancing Responsible Biometrics in Europe' Manifesto outlines a balanced, evidence-based approach to biometric technologies with the aim of:

- Supporting public-private dialog on biometrics to help Europe respond to growing passenger volumes and limited airport capacity, while strengthening the competitiveness of its transport and tourism sectors.[1]
- Promoting greater legal clarity around the use of biometric data to facilitate the responsible deployment of technologies that can bring tangible benefits to travelers.

The coalition brings together expertise from across the travel ecosystem to provide practical insights and engage with policymakers and regulators. Coalition members believe that continued collaboration between industry and public authorities will be essential to maintaining Europe's high standards of privacy and fundamental rights while enabling future innovation in travel.

critical infrastructure PROTECTION AND RESILIENCE EUROPE

20th-22nd October 2026
Brussels, Belgium

www.cipre-expo.com

The International Association for CIP Professionals (IACIPP) is proud to announce that CIP Week Europe 2026 will take place in Brussels, Belgium, in the heart that shapes policy for CIPR.

Invitation to Participate

As Europe's leading forum for the critical infrastructure protection and resilience community, Critical Infrastructure Protection and Resilience Europe (CIPRE) brings together senior leaders from industry, operators, agencies, and government to strengthen collaboration and drive innovation in protecting Europe's essential systems and services.

Register today — Early Bird rates end 20th September 2026.

Now in its 11th year, the conference addresses the most pressing challenges facing operators and agencies, including NIS2 and CER Directive implementation, business continuity, and the resilience of critical infrastructure and entities.

CIPRE features an outstanding international speaker faculty, delivering expert insight, practical experience, and valuable knowledge to support ongoing professional development.

For further information and registration, **visit www.cipre-expo.com**

Join us in Brussels and network with leading decision makers from corporate and government establishments, agencies and operators tasked with Critical Infrastructure Protection and Resilience.

Co-Hosted by:

International Association of CIP Professionals

Global Cybersecurity Partner:

ESET Cybersecurity Progress. Protected.

Gold Sponsor:

IndraMind

Silver Sponsor:

FORTINET

Executive Sponsors:

AUTO-ISAC, CRISR, AVIATION ISAC, CCNE Crisis Communications Network Europe, Health-ISAC, CoESS, ASD, African Young People Support Center











Critical Infrastructure Protection Week *in Europe*

International Association of CIP Professionals

20th-22nd October 2026 - Brussels, Belgium

WCO Global Canine Forum strengthens international cooperation against illicit drug trafficking



Customs canine programme leaders from around the world gathered in Tashkent, Uzbekistan for the 7th WCO Global Canine Forum, hosted by the State Customs Committee of Uzbekistan.

The Forum provided an opportunity for the WCO Canine Expert to brief Members on the Synthetic Drugs Detection Project (SDDP) and its canine-related initiatives, as well as to provide updates on ongoing and planned activities.

The SDDP aims to contribute to reducing drug trafficking by strengthening detection capabilities, enhancing internal coordination and fostering international cooperation to more effectively counter the activities of Organized Crime Groups (OCGs).

During the session, the WCO Canine Expert highlighted the growing challenges posed by synthetic drugs, which are increasingly gaining ground in illicit drug markets. Against this evolving threat landscape, the SDDP supports Members in strengthening the capacity of canine teams to detect synthetic drugs and in promoting the development and sharing of effective practices.

The Project's activities are structured around two complementary pillars:

- Strengthening synthetic drug detection capabilities through scoping missions to assess national needs and capabilities, national training to strengthen operational capacity, and regional workshops to facilitate practical cooperation and the exchange of expertise.

- Promoting best practices and guidelines through knowledge-sharing among Members and experts and strengthened multilateral connections.

Operation COLIBRI ZAFIRO: Customs and partner agencies join forces to crack down on General Aviation Crime

The World Customs Organization (WCO) COLIBRI Project has concluded Operation ZAFIRO, the third and largest international operation under this project, which is funded by the European Union. Customs administrations, police, anti-narcotics units, civil aviation authorities and military forces in 19 partner countries across Latin America and the Caribbean (LAC) and West and Central Africa (WCA) placed General Aviation – privately operated aircraft outside scheduled commercial services – under coordinated scrutiny.

General Aviation accounts for most civil aviation movements worldwide and, in remote or sparsely populated regions, it is often the only practical way to travel or move goods. This makes it attractive to organized crime: discretion, the ability to use small and remote airstrips, and lighter oversight than scheduled commercial flights. Across Latin America, the Caribbean and West and Central Africa, criminal networks have made General Aviation a key link in drug routes and use it to move gold, weapons and cash. Aircraft that evade Customs and tax obligations also generate significant revenue losses for governments.

In total, 1,938 operational events were recorded on the WCO Geoportal, the innovative geospatial intelligence platform the WCO developed that supports the Project: 1,431 controls, 367 observations, 125 runways and 15 seizures. Behind these numbers is a shift the Project has been working towards for three years: controls driven by prior risk analysis rather than non-targeted interventions.

BORDER SECURITY REPORT

AUTOMATED BORDERS, E-GATES AND KIOSKS - HOW EES IS ACCELERATING THE GLOBAL TRANSFORMATION OF BORDER CONTROL

By: Tony Kingham, Editor, Border Security Report

The implementation of the European Union's Entry/Exit System (EES) has become the single most important driver of investment in border automation technology anywhere in the world. Since becoming fully operational across the Schengen Area in April 2026, EES has fundamentally altered how European states manage their external borders. The system replaces manual passport stamping with the electronic registration of traveller movements, recording biographic information, facial images and biometric data while enabling the automatic identification of overstayers and individuals attempting identity fraud. European authorities have openly acknowledged that EES is intended to support wider use of

automated border controls and self-service systems across air, land and maritime border crossings.

For border agencies, airports and governments, EES is far more than a regulatory requirement. It represents a catalyst for the rapid deployment of automated border control (ABC) technologies, including self-service enrolment kiosks, biometric e-Gates, mobile enrolment systems and cloud-based identity management platforms. For suppliers, it has created one of the largest procurement opportunities seen in border security for decades.



While Europe currently dominates the discussion, the technologies underpinning EES are not entirely new. Many of the concepts now being deployed at European borders were pioneered in the United States, Canada, Australia and Singapore. What makes EES unique is not the technology itself but the scale. Never before has a regional bloc attempted to standardise biometric border processing across almost thirty countries using a single legal and technical framework.

The New Border Architecture

Historically, most travellers arriving in Europe presented a passport to a border officer who conducted document inspection and manually stamped the travel document. EES changes that process dramatically.

First-time travellers entering the Schengen Area must provide biometric data, including facial images and, where applicable, fingerprints. This creates significant operational challenges, particularly at large airports already processing tens of millions of passengers annually. Without automation, border authorities would struggle to meet throughput requirements while maintaining acceptable service levels.

The solution has been the widespread adoption of automated border infrastructures. Increasingly, travellers begin the process at self-service kiosks where passports are scanned, biometric data collected and identity checks performed before they arrive at primary inspection points. They then proceed through biometric e-Gates or are directed to officers for additional inspection when required.

The border officer remains part of the process but increasingly acts as an exception handler rather than the primary processor of every traveller.

Understanding the Supplier Market

The automated border industry is often misunderstood because suppliers perform very different roles. Some manufacturers produce physical kiosks and gates. Others specialise in biometrics or digital identity technologies. A third category focuses primarily on systems integration.

Manufacturers of Kiosks and e-Gates

Among the genuine manufacturers of border kiosks and automated gates, several companies dominate the global market.

IDEMIA remains one of the most influential suppliers in the ABC sector. The company designs and manufactures both self-service kiosks and automated e-Gates while also supplying biometric and identity



verification technologies. IDEMIA systems can be found throughout Europe, North America, the Middle East and Asia, with deployments at major hubs including Paris Charles de Gaulle and Amsterdam Schiphol.

Vision-Box, now part of Amadeus, is another major manufacturer. The company's portfolio includes biometric enrolment kiosks, automated border gates and end-to-end passenger journey platforms. Vision-Box has been heavily involved in automated border deployments at airports in Europe, Latin America, the Gulf and North America.

secunet, best known for Germany's EasyPASS programme, manufactures border kiosks, enrolment stations and gate systems specifically designed for government border agencies. The company has become particularly important in EES-related projects across Germany and neighbouring states.

Gunnebo Entrance Control and Dormakaba also offer automated access-control platforms and



gate systems that can be incorporated into border processing environments.

The Biometric Specialists

Behind every automated border system sits a biometric engine.

Dermalog specialises in fingerprint and facial recognition technologies and has developed a substantial presence within government identity and border-management projects.

Thales has become one of the world's most important border technology suppliers through its combination of biometrics, digital identity management, document verification and integrated border-management solutions.

Veridos, the German identity specialist, has similarly built a strong presence through electronic passports, identity credentials and secure border technologies.

Japanese company NEC has secured numerous contracts supporting airport automation and border modernisation programmes globally.

The Systems Integrators

Not every company associated with border kiosks manufactures the hardware itself.

SITA remains one of the most influential players in global border automation, but its primary role is that of a systems integrator. The company reports deployments of more than 5,500 border kiosks worldwide and provides an



integrated ecosystem covering biometric enrolment, passenger flow management, traveller identity orchestration and automated clearance systems. Rather than focusing solely on hardware manufacturing, SITA's strength lies in connecting government systems, airport infrastructure and airline operations into a single operational environment.

Materna Intelligent Passenger Solutions (IPS) is similarly better understood as a passenger-processing specialist and integrator. While it delivers kiosk-based solutions, its expertise centres on workflow design, deployment, software integration and passenger experience rather than the manufacture of proprietary border-control hardware.

Indra and Travizory increasingly occupy comparable positions, providing the software and identity-management frameworks that allow governments to integrate multiple technologies into a functioning border ecosystem.

Unlike traditional e-Gate and kiosk suppliers, Travizory focuses on digital border management, using AI, biometrics and traveller intelligence to enable risk assessment and decision-making before a traveller reaches the border.

The United States: The World's Largest Biometric Border Programme

If Europe represents the future of automated borders, the United States represents the most mature large-scale deployment.

For more than a decade, U.S. Customs and Border Protection (CBP) has pursued one of the most ambitious biometric border programmes ever undertaken. Unlike Europe's heavy reliance on



e-Gates, the American model is primarily based on facial biometric verification integrated directly into border processing workflows.

Today, travellers arriving at major international airports frequently undergo facial verification rather than traditional document inspection. Images are matched against government-held records within seconds, enabling rapid identity confirmation while reducing officer workload.

The programme extends well beyond arrival halls. Biometric verification is now increasingly embedded within departure environments, seaports and land crossings.

This strategy has created substantial opportunities for companies including IDEMIA, NEC, Thales, Collins Aerospace and Vision-Box, all of which have participated in various elements of U.S. border modernisation programmes.

The American experience has also demonstrated that biometric processing can be scaled nationally. Europe's EES architects have watched these developments closely, particularly regarding passenger throughput, privacy protection and operational resilience.

Global Entry: A Blueprint for Trusted Traveller Automation

Long before EES entered development, the United States was refining trusted traveller programmes through Global Entry.

Initially based around self-service immigration kiosks, Global Entry allowed pre-vetted travellers to complete border formalities quickly and efficiently. The programme proved that low-risk passengers could be processed largely through automated systems without compromising security.

Many subsequent programmes worldwide borrowed heavily from this model, including Canada's NEXUS initiative, Australia's SmartGate programme and various European trusted traveller schemes.

Canada's Home-Grown Kiosk Industry

Canada occupies a unique position in border automation because it has produced two of North America's most significant indigenous kiosk manufacturers.

The first is Embross, based in Toronto. The company's VelocityOnePIK platform was developed specifically to support the Canada Border Services Agency's Primary Inspection Kiosk programme and has been deployed at airports including Calgary, Ottawa, Edmonton and Billy Bishop Toronto City Airport. Its systems incorporate passport-reading technology, biometric facial imaging and fingerprint capture capabilities.

The second is Innovative Travel Solutions (ITS), a business unit of Vancouver International Airport. ITS developed the highly successful BorderXpress platform, one of the most widely deployed border kiosk systems globally. The company expanded BorderXpress to support CBSA's Primary Inspection Kiosk

programme and has reported deployments exceeding 1,000 kiosks worldwide.

Unlike many border technology suppliers, both organisations emerged directly from the Canadian aviation sector, proving that border innovation does not necessarily originate from the traditional defence industry.

South America: A Rapidly Expanding Market

While less frequently discussed than Europe or North America, South America has quietly become one of the fastest-growing regions for automated border control technologies.

Brazil has emerged as the continent's largest market, driven by growing passenger numbers and major airport modernisation programmes. Airports in São Paulo, Rio de Janeiro and Brasília have increasingly adopted biometric processing technologies supplied by international providers including IDEMIA and NEC.

Argentina has also invested steadily in immigration automation, while Chile's strength in digital government services has supported broader adoption of biometric identity technologies.

Colombia, Peru and several Central American states are pursuing similar initiatives as aviation traffic continues to increase throughout the region.



Perhaps most significantly, many tourism-dependent economies across the Caribbean have recognised that rapid border processing is not merely a security issue but a commercial necessity. Faster border clearance improves passenger experience and enhances competitiveness in attracting international visitors.

Beyond EES

The real significance of EES is not that it introduces biometrics to Europe's borders. Those technologies already exist and are widely deployed. The importance of EES lies in creating the world's largest interoperable automated border environment.

The technologies developed by IDEMIA, Vision-Box, Embross, BorderXpress, secunet, NEC, Thales, Veridos, SITA and numerous others are converging toward a future in which biometric identity becomes the primary credential used for border crossing.

Within the next decade, kiosks may evolve into mobile enrolment platforms, digital travel credentials may reduce dependence on physical passports and biometric verification could begin before a traveller even arrives at a border crossing.

For border agencies, the objective remains unchanged: stronger security combined with faster processing. EES is not the destination. It is the platform upon which the next generation of automated borders will be built.

ILLEGAL MINING AND ARMED BANDITRY IN NIGERIA: IMPLICATIONS FOR BORDER SECURITY, ECONOMIC STABILITY AND NATIONAL DEVELOPMENT

By George-Okoli Francisco Chidi is the National 1st Vice President, West African Action Network on Small Arms (WAANSA) Nigeria

Illegal mining and armed banditry are no longer best understood as isolated criminal activities in Nigeria. In several parts of the North-West and North-Central regions, the extraction and movement of minerals have become intertwined with extortion, territorial control, kidnapping, arms trafficking and other illicit markets. The result is an informal conflict economy in which mineral resources can generate income for armed actors, while insecurity enables those actors to control access to mining areas and transportation routes. Recent research by WAANSA Nigeria similarly identifies the relationship between weak governance, unregulated artisanal mining and the expansion of banditry in rural communities.

The connection between mining and banditry operates through several channels. Several armed groups impose levies on miners, charge access fees, take a share of mineral output, provide or enforce protection, or take direct control of productive sites. The former Chief of Defence Staff Gen. Christopher Musa highlighted this in 2025 when he warned that armed groups increasingly rely on gold revenues to finance their operations, making it more difficult to dismantle their networks. It also reports allegations that proceeds from illicit mining have been converted into weapons and other equipment. One reported statement attributed to Kachalla Mati was: “We exchange the gold for weapons. We give them the gold, and they bring us the guns. Sometimes we sell it here; sometimes we send it to Dubai.” These accounts illustrate how an apparently local mining activity can become connected to transnational criminal supply chains.

The security problem goes beyond the financing of violence. Where government institutions have limited reach, armed groups can acquire influence over communities and economic activity. They may determine access to mining locations, impose payments on farmers and traders, restrict movement and regulate informal markets. WAANSA Nigeria describes this transformation as a shift from opportunistic extortion towards organised systems of control. Such conditions weaken



Pictures of illegal miners in Zamfara State, Nigeria

public authority and make the recovery of territory more difficult because the armed group becomes embedded in the local economy.

The economic consequences for Nigeria are severe. According to the Nigeria Extractive Industries Transparency Initiative (NEITI), more than 70 per cent of mining activity nationwide is undertaken by artisanal operators working outside formal regulatory arrangements, while 80% of illegal mining activities are prevalent in some northern states. NEITI also estimates that Nigeriaan annual loses approximately US$9 billion through illegal extraction and mineral smuggling. Beyond fiscal losses, insecurity can destroy farms, interrupt trade, displace households, discourage investment and expose communities to environmental degradation. The economic burden is therefore shared by government, legitimate businesses and rural households.

Illegal mineral extraction becomes a border-security issue when gold and other commodities move through informal routes into neighbouring states and international trading centres. The source material identifies connections through Niger and Mali to wider Sahelian criminal networks and notes the role of external markets in the movement of Nigerian gold. This creates a chain involving extraction sites, local brokers, transporters, border crossings, traders and financial intermediaries. Effective intervention consequently requires more than operations at mining sites. Border agencies need better intelligence exchange, risk profiling, customs cooperation, financial investigation and coordinated action against smuggling networks.

Nigeria has responded with enforcement operations, mining restrictions and the deployment of Mining Marshals to disrupt unauthorised operations. Enforcement remains necessary, but



Pictures of some group of bandits in Northern Nigeria Forest

a security-only approach is unlikely to eliminate the economic incentives behind illegal mining. The Ministry of Solid Minerals Development already identifies formalisation of artisanal and small-scale mining, mining-site mapping, extension services, access to finance and development of mining clusters among its activities. A stronger formalisation programme can move legitimate miners into traceable cooperatives and licensed markets while making it harder for armed groups to control production and trade.

The central policy challenge is to separate legitimate mineral production from criminal control. Nigeria needs a system in which minerals can be legally extracted, documented, transported, processed and sold, while illicit proceeds and weapons movements are actively disrupted. This requires coordination among mining regulators, security agencies, customs authorities, financial-intelligence institutions, state governments, local communities and regional partners. The objective should be to protect communities and national assets while ensuring that mineral wealth contributes to lawful economic activity rather than financing violence.

From WAANSA Nigeria security and border-governance perspective, the relationship between illegal mining, armed banditry, illicit arms flows and porous borders should be treated as a connected national-security problem. In summary, WAANSA Nigeria advocates an integrated approach combining security enforcement, border control, mining formalisation, financial intelligence and community development to prevent Nigeria's mineral resources from financing banditry and transnational crime.

In conclusion, WAANSA Nigeria's assessment is that illegal mining and armed banditry should be addressed as mutually reinforcing components of a wider illicit economy rather than as separate problems. The evidence available in the source article and recent Nigerian policy discussions indicates that weak regulation, insecurity, mineral smuggling and illicit financial flows can reinforce one another. The appropriate response therefore combines security enforcement with mineral-sector reform, border management, financial investigation, community participation and legitimate economic opportunities. Nigeria can reduce the space available to armed groups by making mineral production more transparent, disrupting criminal supply chains and ensuring that communities derive lawful benefits from the resources around them. The long-term objective should be a secure mining environment in which mineral wealth supports public revenue, employment and national development instead of sustaining violence and cross-border criminality.

NAPTIP Recovers Over 180 Trafficked Children Across Five States in Nigeria in a Latest Counter Trafficking Operation



Operatives from the National Agency for the Prohibition of Trafficking in Persons (NAPTIP) have rescued over 180 children who were allegedly trafficked from five states across the federation by certain organized criminal groups that are posing as members of civil society organizations, misleading parents in various communities and taking their children away under false pretences.

The most recent rescue involved the recovery of three children allegedly trafficked from a distressed parent in Kajuru, Kaduna State, from a high-rise private building in a desirable area of Onitsha, Anambra State. Additionally, another child was found in the care of a Clinical staff member at the Federal Medical Centre in Onitsha.

The development came just as the Director General of the Agency, Binta Adamu Bello, OON, raised concerns about the alarming activities of some suspected trafficking syndicates that now move from one crisis-ridden community to the other, trafficking children under the guise of educational support and back-to-school programmes.

It should be recalled that, following a series of reported cases of missing children across the country, the Director General of NAPTIP established a Special Squad within the Investigation and Monitoring Department a few months ago. This squad was tasked with recovering children who were allegedly trafficked and bringing the traffickers to justice.

The first batch of recovered children consisted of those reportedly taken from various communities in Benue and Nasarawa States. These children were distributed to orphanages in Abuja and other states, where they were sold to unidentified individuals under the guise of adoption, after substantial amounts of money were paid.

In his statement shortly before he was reunited with his son, the father of one of the Children (name withheld) commended the management of NAPTIP for helping him to recover his Son.

Goods worth nearly half a million hryvnias were discovered at the Shehyni crossing point

At the Ukrainian Shehyni border crossing point, servicemen from the 7th Carpathian Border Detachment, acting on advance intelligence from operational officers and working alongside customs officials, discovered an undeclared shipment of perfumes.

During an inspection of a Mercedes vehicle driven by a 32-year-old resident of the Ternopil region, 29 bottles of perfume from various brands were found in the luggage compartment among personal belongings.

The driver stated that he was transporting the goods from Italy to Ternopil for personal use.

The estimated value of the discovered perfume products is 435,000 hryvnias.

Customs officials drew up a formal report regarding the violation. The goods were seized and transferred to a customs warehouse.

WCO builds freight forwarders capacity to manage rules of origin, ensuring enhanced compliance and increased preferential tariff treatment use



Some of the world's biggest underground bankers have been targeted in an international law enforcement operation against a sophisticated financial network suspected of financing drug trafficking and laundering criminal proceeds around the world.

The investigation, led by the Spanish National Police (Policía Nacional) and supported by Europol, has resulted in the arrest of 21 suspects for offences including participation in a criminal organisation, drug trafficking and money laundering.

An action day resulted in the arrest of 15 suspects. Spanish authorities also issued 19 international arrest warrants against suspects located outside the country. Six of these warrants have since been executed, resulting in four arrests in the United Arab Emirates, one in Egypt and one in the Netherlands.

Among those arrested is a leading figure in a major underground banking network known as the "Dubai Bank". Identified by Europol as a High Value Target, the suspect is believed to have played a key role in providing financial services for major drug trafficking operations worldwide.

Authorities have identified, seized or frozen assets worth approximately EUR 20 million. These include 48 properties valued at more than EUR 14 million, high-end vehicles worth over EUR 1.6 million and 121 bank accounts containing EUR 2.3 million.

Cocaine investigation leads to the money

Operation DRAKKAR grew out of an investigation into a major cocaine shipment intercepted by the Spanish National Police in February 2021. Officers boarded a vessel in waters off the Spanish coast and discovered 1 835 kilograms of cocaine. All nine crew members were arrested. After the crew and drugs had been removed, the vessel was towed to the port of Gijón, Spain. The ship subsequently sank after taking on water through a leak allegedly caused by its captain.

Investigators later discovered why: another 1 650 kilograms of cocaine had been concealed on board. Members of the criminal network are suspected of subsequently entering the sunken vessel and recovering the hidden shipment. It was established that both cocaine shipments had been loaded in South America in January 2021. The plan was to transfer the drugs at sea to high-speed boats, which would then bring the cocaine ashore in Spain.

The investigation into those behind the shipment gradually led investigators further up the criminal chain. Links were established to other suspected drug trafficking operations around the world, while following the financial trail exposed the individuals suspected of financing the shipments and laundering the proceeds.

This ultimately led investigators to a sophisticated international financial infrastructure used to provide underground banking services to organised crime.

The "Dubai Bank"

At the heart of the investigation was a clandestine money-transfer network referred to as the "Dubai Bank". The network is suspected of making large amounts of money available to criminal organisations in different countries within very short periods of time, providing the financial infrastructure needed to fund major drug shipments and move the resulting criminal proceeds.

Rather than physically transferring money across borders for every transaction, underground banking

networks can move value between jurisdictions through networks of brokers. Payments can be settled through internal accounting and compensation mechanisms, including trade transactions, companies and their bank accounts, cash pooling or transfers of other assets.

The network operated on a commission basis, with fees varying depending on the transaction and other factors.

Investigators also identified the use of tokens to authenticate cash transactions. A unique identifier, frequently the serial number of a banknote, could be passed through the transfer chain. Presenting the matching identifier when collecting the cash allowed those involved to verify that the money was being handed to the intended recipient.

The financial investigation also identified assets suspected of having been acquired using illicit funds, including a luxury property in Ibiza.

Europol has supported the investigation by facilitating international information exchange and providing operational and financial analysis that helped identify key money brokers within the network. Since October 2024, the investigation has also been supported through an



Operational Taskforce set up at Europol.

Europol provided specialised expertise on underground banking, and asset tracing and recovery. Specialists were deployed to Spain for the action day, where a money laundering specialist supported investigators on the ground with a mobile office.

Given the global reach of the network, international cooperation was central to the investigation. Authorities from the Netherlands, Sweden and the United States, including the US Drug Enforcement Administration (DEA), contributed to the investigation.

North and Eastern African Governments Take Steps to Strengthen a Data-Driven, Route-Based Approach to Climate, Health and Human Mobility

Against the backdrop of accelerating climate change impacts across the migration corridors connecting to North Africa, the dialogue addressed how climate change continues to act as a risk multiplier for public health and influence human mobility dynamics. Rising temperatures, drought, water scarcity, desertification, coastal hazards, and extreme weather events are increasingly undermining livelihoods, straining health systems, and shaping migration dynamics across North Africa.

The event focused on strengthening climate-resilient and migration-sensitive health systems; addressing climate-related health risks along migration routes; and enhancing cross-border disease surveillance, early warning systems, and coordinated response across origin, transit, and destination contexts. Discussions also strongly emphasized closing data and evidence gaps, highlighting the need for harmonized, disaggregated, route-based climate–health–mobility data systems to support anticipatory action and informed policymaking.

The event provided a platform to translate evidence and operational experience into practical collaboration, while promoting cross-sectoral exchange among institutions responsible for health, climate and environment, migration, and data and statistics.

Following three working group discussions, participating countries proposed strengthening cross-border health coordination by harmonizing data along migration routes, engaging relevant sectors beyond health, leveraging digital health information systems, and building health personnel's capacity to detect and report communicable diseases.

2027 WORLD BORDER SECURITY CONGRESS

World Border Security Congress

13th-15th April 2027

Lisbon, Portugal

www.world-border-congress.com

Lisbon and Portugal's Atlantic Frontier: Confronting the Convergence of Migration, Human Trafficking and Transatlantic Drug Flows

Portugal occupies a unique position on Europe's security map. Situated on the western edge of the continent and facing directly onto the Atlantic Ocean, the country serves not only as one of the European Union's external maritime frontiers but also as a critical gateway between Europe, Africa and the Americas. Lisbon, located at the mouth of the River Tagus and home to one of Europe's most important Atlantic ports and airports, sits at the intersection of several strategic routes used by legitimate trade, migration, and increasingly, transnational criminal networks.

While Portugal is often perceived as being removed from the migration pressures facing the central Mediterranean, the realities of modern border security suggest otherwise. The country's extensive

Atlantic coastline, overseas maritime approaches, and historical connections with lusophone Africa and Latin America place Lisbon at the centre of some of the most significant border security challenges currently confronting Europe.

One of the most pressing concerns is the growing use of Atlantic migration routes connecting West Africa to the Iberian Peninsula. As enforcement activities have intensified in parts of the Mediterranean, migrant smuggling networks have demonstrated a remarkable ability to adapt, shifting routes and identifying new entry points into Europe. Portuguese authorities have increasingly recognised the potential vulnerability of the country's coastline to irregular migration flows originating from Morocco, Mauritania, Senegal, Guinea-Bissau and other West African states. Earlier World Border Security Congress assessments noted that the Algarve coast was increasingly viewed by migrants transiting through Morocco as an alternative gateway to Europe, a trend driven in part by pressure on Mediterranean routes.

The migration challenge extends far beyond border crossings themselves. Human trafficking networks continue to exploit instability, poverty and a lack of economic opportunity across parts of Africa. Organised criminal groups facilitate the movement of migrants through complex routes linking West Africa, North Africa and Europe, generating enormous profits while exposing vulnerable people to abuse, exploitation and forced labour. The World Border Security



Congress has consistently identified human trafficking, irregular migration and organised smuggling networks as among the most significant challenges facing border authorities worldwide.

For Portugal, the challenge is compounded by geography. The country's Atlantic position means threats often emerge far from its territorial waters. Criminal networks increasingly utilise motherships, fishing vessels and concealed maritime routes that stretch from the Gulf of Guinea and the West African coast towards the Iberian Peninsula. Surveillance of these vast maritime approaches requires extensive cooperation between the Portuguese Navy, Guarda Nacional Republicana, Polícia de Segurança Pública, Frontex and neighbouring European partners. Portugal's border security responsibilities are further shaped by its role within the Schengen Area, meaning that an individual or shipment successfully entering Portugal may subsequently move across much of Europe without additional border checks.

Drug trafficking presents an equally significant threat. Portugal lies directly on the principal Atlantic cocaine highways connecting South American production regions with European consumer markets. Recent analysis published in BSRJulAug2026.pdf highlights how cocaine trafficking networks increasingly rely on transatlantic routes extending from Brazil through West African transit hubs before entering Europe. These routes frequently involve criminal partnerships linking Brazilian organisations, West African logistical facilitators and European distribution networks. The report notes that the lusophone axis connecting Brazil with Guinea-Bissau, Cape Verde and Portugal remains particularly attractive because common language, historic



ties and established commercial relationships reduce operational risks for traffickers.

The Port of Santos in Brazil remains one of the primary cocaine export gateways, while criminal organisations continue to exploit West African transit states as staging points before onward movement into Europe. Authorities have observed increasing use of container shipping, commercial transport networks, semi-submersible vessels and sophisticated concealment techniques designed to evade detection. Rather than relying on a single route, criminal groups now operate highly adaptable logistical systems capable of rapidly shifting trafficking corridors in response to law enforcement pressure.

Portugal's own border security community has long recognised this vulnerability. Previous World Border Security Congress materials highlighted warnings from the Portuguese Judicial Police that Portugal's maritime and air borders continue to serve as gateways into Europe for significant quantities of cocaine originating in Latin America. The seizure of transatlantic narco-submersibles operating in Atlantic waters further illustrated the attractiveness of the Portuguese and Spanish coastlines for major trafficking operations.

These threats rarely exist in isolation. Modern organised crime increasingly combines drug trafficking, migrant smuggling, financial crime and document fraud within the same criminal ecosystems. Networks facilitating the movement of cocaine can also provide logistics, corruption mechanisms, forged documents and maritime transportation for human trafficking operations. The result is a highly interconnected threat environment in which border agencies must simultaneously manage migration pressures, organised crime, terrorism concerns, customs enforcement and maritime security challenges. The 2027 World Border Security Congress prospectus specifically identifies irregular migration, organised crime, narcotics trafficking, money laundering, exploitation of migration systems and cross-border financial crime among the key challenges facing border authorities.

Technology and intelligence-sharing are becoming increasingly important in addressing these threats. Advanced maritime surveillance systems, unmanned aerial systems, biometric identity management, passenger data analytics and risk-assessment platforms now form





essential components of modern border management strategies. However, technology alone cannot solve the challenge. Effective border security in Lisbon and across Portugal requires close cooperation between European agencies, African partners, customs organisations, law enforcement services and international institutions.

For this reason, Lisbon represents an ideal venue for discussing the future of border security. The city stands at the crossroads of the Atlantic routes that connect South America, Africa and Europe. It faces many of the same challenges confronting border agencies across the world: organised crime, irregular migration, human trafficking, drug smuggling, identity fraud and increasing pressure on migration management systems. As criminal networks become more sophisticated and transnational routes become more interconnected, Portugal's experience demonstrates that border security is no longer simply about protecting a line on a map. It is about safeguarding a vast



network of maritime approaches, transport corridors and international partnerships that extend far beyond the physical frontier itself.

We look forward to welcoming the border security, protection and management community to the beautiful city of Lisbon from 13th–15th April 2027.

Co-hosted & Supported by:

SISTEMA DE SEGURANÇA INTERNA

POLÍCIA SEGURANÇA PÚBLICA

GNR GUARDA NACIONAL REPUBLICANA



ClanTect HPDS Secures First Major Contract Under 3DX-Ray Ownership

ClanTect, as part of the 3DX-RAY Ltd portfolio, has secured a significant contract to supply six ClanTect Human Presence Detection systems to support state border security operations in Eurasia.



The award represents the first major contract secured by ClanTect since becoming part of 3DX-Ray and marks another important milestone in the continued international deployment of advanced clandestine detection technology.

ClanTect HPDS is designed to provide a fast, highly accurate, non-intrusive system for detecting the presence of human beings concealed within vehicles, trucks and trailers. The system uses a proprietary vibration detection methodology that distinguishes between external environmental vibrations and movement generated from within a vehicle, enabling highly effective screening without intrusive inspection procedures.

The latest version of the ClanTect HPDS incorporates wireless sensor technology that enables multiple vehicles to be screened simultaneously, significantly increasing throughput at border checkpoints, ports and other security-critical locations.

ClanTect systems are already deployed at high-security prisons and border crossings around the world, including operations supporting the UK Border Force and Frontex, the European Border and Coast Guard Agency. The technology helps authorities detect clandestine entrants, fugitives, and other concealed persons hidden within commercial and private vehicles.

Rohde & Schwarz Introduces QPS Walk500 Security Scanner for High-Throughput Event Screening

Rohde & Schwarz has unveiled the QPS Walk500, a new walk-through security scanner designed to deliver fast, reliable screening in high-throughput environments.



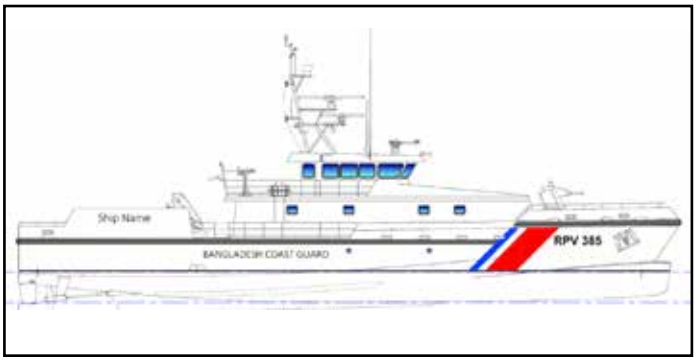
The system combines advanced millimeter-wave sensing with AI-driven threat detection to help operators enhance security while maintaining the smooth flow of passengers, visitors and staff.

The QPS Walk500 has been developed for locations where large numbers of people must be screened quickly and efficiently without compromising security. While particularly suited to major public venues, the solution is also well positioned for deployment at airports, border crossings, critical infrastructure facilities and transportation hubs, where maintaining passenger and traveller throughput is a constant operational challenge. Rohde & Schwarz notes that its security screening technologies are already used across sectors including aviation, border control and critical infrastructure protection.

Unlike conventional screening systems that often require travellers to stop, divest personal items or remove outer clothing, the QPS Walk500 allows individuals to pass through the checkpoint without interruption. With a processing capability of up to 750 people per hour, the system is designed to reduce congestion while supporting efficient security operations in demanding environments.

Bangladesh Coast Guard Selects MAURIC Design for Five New Riverine Patrol Vessels

The Bangladesh Coast Guard has selected French naval architecture specialist MAURIC to undertake the design studies for five new 38-metre Riverine Patrol Vessels, strengthening the service's capability to conduct maritime security, surveillance and counter-trafficking operations in the country's extensive riverine and coastal environments.



The contract represents another success for MAURIC in the Asian market and will see the company working alongside Norwegian partner NORDIC NAVAL AS to provide the complete design package and major equipment selection for the programme. Construction of the five vessels is scheduled to begin during the fourth quarter of 2026 at Dockyard & Engineering Works Limited in Bangladesh.

Designed specifically for riverine and coastal security operations, the new patrol vessels will measure 38 metres in length, feature a steel hull with aluminium superstructures and be capable of speeds of up to 22 knots. Each vessel will be fitted with a remotely operated 30 mm weapon station and will accommodate up to 29 personnel during missions of up to 10 days' duration.

The vessels are expected to support a broad range of operational tasks, including maritime surveillance, counter-trafficking missions, law enforcement operations and the protection of Bangladesh's territorial waters and critical maritime infrastructure.

SITA launches SITA Border Flow Lane

SITA has launched SITA Border Flow Lane, a new border processing solution that turns border control from a stop-and-check process into a data-driven, pre-clearance and move-through experience. Instead of stopping at a gate, kiosk, or officer checkpoint to present a passport, travelers are verified before they depart and upon arrival, as they move through the immigration hall.



For decades, border agencies have invested in technologies that answer three fundamental questions earlier and with greater certainty: Can this person travel? Who are they? What does their journey tell us?

Today, more is known about a traveler before they board a flight than at any point in history. The question is no longer whether border authorities have the information they need to take the right decisions. The question is: if those decisions can already be made before a traveler arrives, why should every traveler still have to stop and present documents at the border?

The result is border clearance up to eight times faster than traditional border control eGates, helping trusted travelers keep moving while allowing border officers to focus on the cases that need closer attention.

Border Flow Lane is the latest innovation, resulting from our decades of experience helping governments use quality passenger data and intelligence earlier in the journey.

Brazilian Federal Police Modernizes Nationwide Forensic Examination with Regula Technologies

The Brazilian Federal Police has upgraded part of its forensic examination infrastructure with the latest generation of Regula technologies, a global developer of forensic devices and identity verification solutions.



The implementation covers the national laboratory network in Brazil and supports investigations involving forged identity documents and counterfeit banknotes. The technologies help forensic experts conduct more consistent and high-quality document examinations.

The modernization builds on a long-standing partnership between the Brazilian Federal Police and Regula. For more than a decade, some forensic laboratories across the country have relied on Regula's forensic examination technologies in their daily work. The new phase of the project renews part of the existing Regula forensic infrastructure, supporting the Federal Police's ongoing efforts to modernize its forensic capabilities while maintaining standardized examination workflows across its nationwide laboratory network.

The project covers the deployment of Regula 4308 dual-video spectral comparators in the Federal Police laboratories. The devices enable experts to perform forensic analysis with greater speed, consistency, and precision.

The modernization initiative comes as forensic laboratories worldwide face growing pressure to keep pace with increasingly sophisticated document fraud techniques while maintaining operational efficiency across distributed laboratory networks.

As document fraud methods become increasingly sophisticated, the Brazilian Federal Police continues to modernize its forensic laboratory capabilities, ensuring its laboratories remain equipped to meet evolving operational requirements.

ADVERTISING SALES

Becky Starling
(UK and RoW)
E: beckys@torchmarketing.co.uk
T: +44 (0) 7516 791952

Bruce Bassin
(Americas)
E: bruceb@torchmarketing.co.uk
T: +1-702.600.4651

Jerome Merite
(France)
E: j.callumerite@gmail.com
T: +33 (0) 6 11 27 10 53



Are you sure your national infrastructure is secure?

Co-Hosted by:

International Association of CIP Professionals

INFRAGARD MEMBERS ALLIANCE LOUISIANA

The rapidly evolving threat environment—driven by climate change, geopolitical conflict, supply chain disruption, and increasingly sophisticated cyber and physical attacks—demands continuous modernization of policy, regulatory frameworks, operational practices, and protective technologies to address escalating and interconnected risks.

Invitation to Participate

The current Administration recently rolled out a new critical infrastructure memorandum, titled National Security Memorandum on Critical Infrastructure Security and Resilience (NSM-22) which is intended to set forth the role of the federal government, including responsibilities for specific federal agencies, in protecting U.S. critical infrastructure.

NSM-22 serves to supplant PPD-21, formally known as the Presidential Policy Directive – Critical Infrastructure Security and Resilience (pdf). PPD-21, a memorandum issued during the previous Administration, designated 16 critical infrastructure sectors that will be subject to additional oversight through the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA).

Are you prepared?

The Nation's critical infrastructure provides the essential services that underpin American society. Proactive and coordinated efforts are necessary to strengthen and maintain secure, functioning, and resilient critical infrastructure – including assets, networks, and systems – that are vital to public confidence and the Nation's safety, prosperity, and well-being.

Critical infrastructure must be secure and able to withstand and rapidly recover from all hazards. Achieving this will require integration with the national preparedness system across prevention, protection, mitigation, response, and recovery.

Join us in Lake Charles, LA for the leading forum dedicated to operators and government bodies responsible for advancing Critical Infrastructure Protection and Resilience across the region.

For further details visit **www.ciprna-expo.com**

The premier discussion for securing America's critical infrastructure

- Chemical Sector
- Commercial Facilities Sector
- Communications Sector
- Critical Manufacturing Sector
- Dams Sector
- Defense Industrial Base Sector
- Emergency Services Sector
- Energy Sector
- Financial Services Sector
- Food and Agriculture Sector
- Government Facilities Sector
- Healthcare and Public Health Sector
- Information Technology Sector
- Nuclear Reactors, Materials, and Waste Sector
- Transportation Systems Sector
- Water and Wastewater Systems Sector

To discuss exhibiting and sponsorship opportunities contact:

Bruce Bassin
(Americas)
E: bruceb@torchmarketing.co.uk
T: +1 702.600.4651

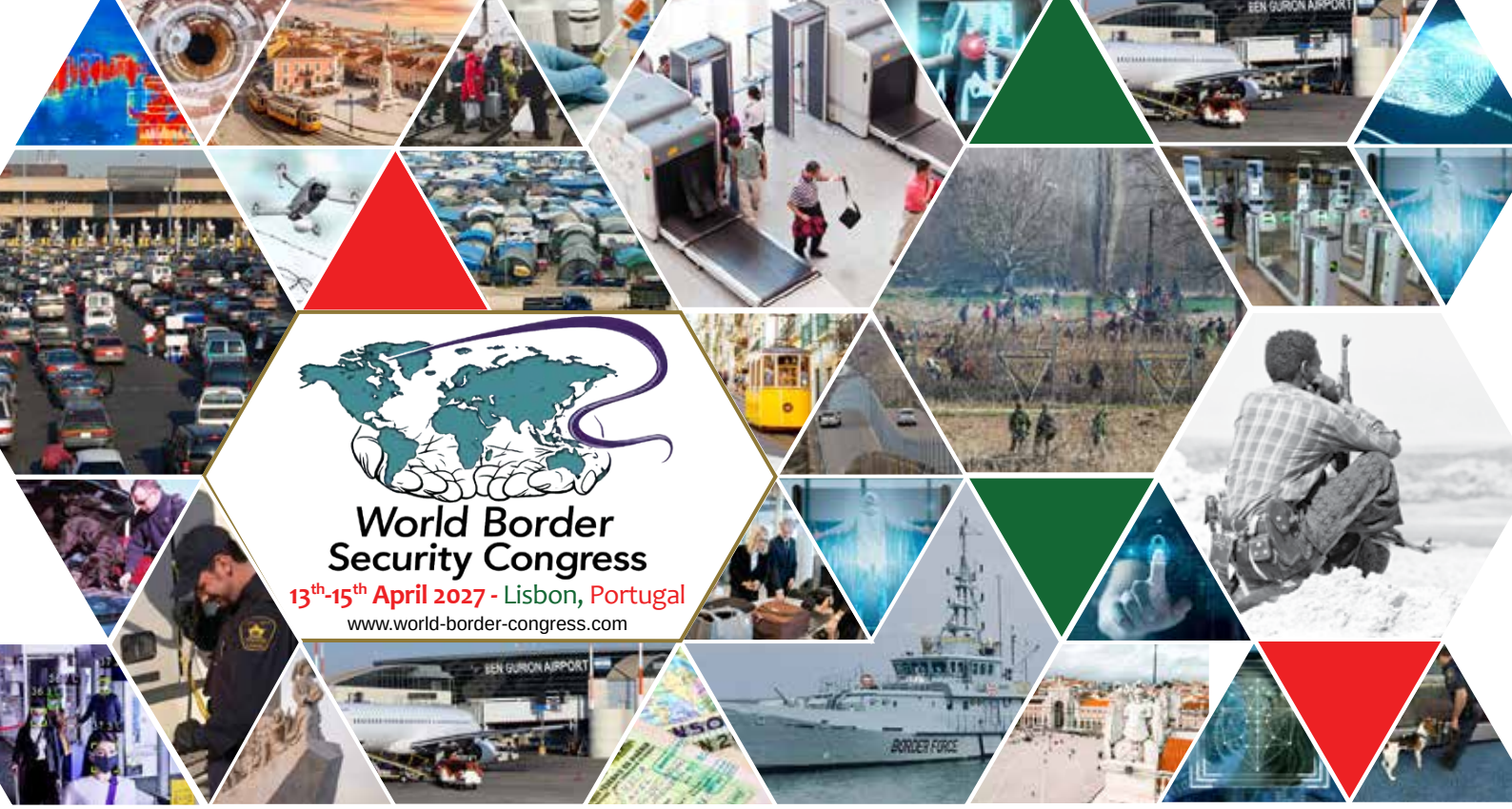
Paul Gloc
(Rest of World)
E: paulg@torchmarketing.co.uk
T: +44 (0) 7786 270 820

Supporting Organisations:

International Association of CIP Professionals · Help2Protect · ISIO – International Security Industry Organisation · CAMO · Marine Safe 811

Flagship Media Partner:

critical infrastructure PROTECTION AND RESILIENCE NEWS



Transforming Border Management Strategies Through Co-operation and Technology

SAVE THE DATES

Portugal's border security is shaped by its geography and role within the Schengen Area, placing responsibility on protecting the EU's external frontier. Since the dissolution of the SEF, the border security function is coordinated by the Sistema de Seguranca Interna (Internal Security System) and implemented by the Polícia de Segurança Pública (PSP) and Guarda Nacional Republicana (GNR).

Administrative overload and legal migration pressure remains Portugal's main challenges, but the country relies on maritime and airport surveillance rather than land borders. Its Atlantic coastline presents monitoring challenges, particularly for irregular migration routes and drug trafficking. The country faces growing inflows of irregular migrants from Africa, Brazil, and South Asia, creating administrative strain in processing visas, asylum claims, and residency permits, leading to backlogs and delays.

Migration has become more contentious recently, with pressure to tighten rules after years of relatively open policies. At the same time, labour shortages mean Portugal still depends heavily on migrant workers.

Portugal is not unique in its border management challenges and must strengthen surveillance, streamline bureaucracy, and enhance EU cooperation while maintaining its rights-based migration approach.

The World Border Security Congress is a high level 3 day event that will discuss and debate current and future policies, implementation issues and challenges as well as new and developing technologies that contribute towards safe and secure border and migration management.

Join us in Lisbon, Portugal on 13th-15th April 2027 for the next gathering of international border security, protection and migration management professionals.

www.world-border-congress.com

for the international border management and security industry

Co-hosted by:

Sistema de Segurança Interna

Polícia Segurança Pública

GNR Guarda Nacional Republicana

To discuss exhibiting and sponsorship opportunities and your involvement contact:

Paul Gloc
Rest of World
E: paulg@torchmarketing.co.uk
T: +44 (0) 7786 270 820

Bruce Bassin
Americas
E: bruceb@torchmarketing.co.uk
T: +1 702.600.4651

Jerome Merite
France
E: j.callumerite@gmail.com
T: +33 (0) 6 11 27 10 53

Supported by:

OSCE Organization for Security and Co-operation in Europe

European Association of Airport and Seaport Police

African Young People Support Center

ISIO

International Association of CIP Professionals

NSaRG

Media Partners:

World Border Security Network

Border Security Report

World Security-index.com