INTERPOL

Innovation SNAPSHOTS

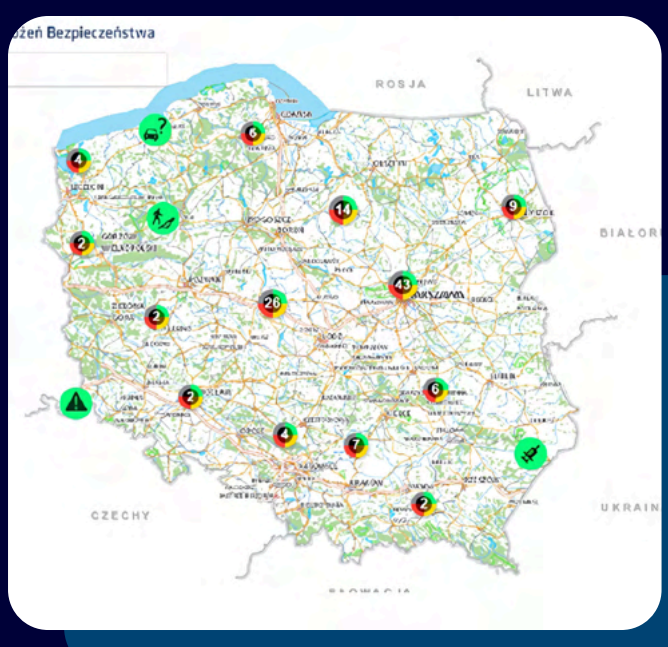
Volume 5 Issue 3 JUN 2025 ▶ Innovation Centre ▶ IC-Snapshots@interpol.int

IN THIS ISSUE

POLAND'S NATIONAL SECURITY THREAT MAP

In 2016, the Polish National Police have developed a National Security Threat Map (NSTM) which enables citizens to anonymously report locations where they feel unsafe or impacting their sense of security. The threat map, free of charge for the public, is considered an essential element of the public security process, aiming to ensure that the public feels safe.

Police in Poland utilize a variety of technologies to reach a broad audience. Information is gathered from police information systems, direct contacts with citizens, representatives of local government and non-governmental organizations, and through an information exchange platform.



However, for the purposes of developing the NSTM, extensive public consultations were conducted, on the basis of which 24 categories of threats relevant to the community, especially the local community, were identified. It is important to note that not every threat constitutes a crime, but all are verified by the police and reported to the appropriate authorities for resolution.

The application is designed to be user-friendly, requiring only access to Internet via computer or smartphone. Access to NSTM is available through the Policja.pl portal and the websites of police units. Reporting a threat takes just a few seconds: users select one of the 24 threats, indicate the location, and click the 'REPORT' button. They can also provide additional details (e.g., description and photograph). The user can then track the status of the report.

The verification process for reported threats is conducted by police officers in the affected area as part of their statutory duties. NSTM serves as an additional information source for analysing the security situation and deploying resources. The verification process follows a seven-day timeline, ensuring thorough checks and that police officers are not diverted from urgent tasks. Confirming or excluding a threat does not conclude police activities in the area. The NSTM aims to provide a reliable and clear identification of the scale and types of threats to local communities, and in particular to build public trust in the police.

It is important to note that NSTM is not intended for reporting typical crimes – in such cases, it is recommended to contact the police directly. NSTM has been functioning for nine years and has recorded about four million threats.

Source: Lieutenant Magdalena Kołodziejczak, Polish National Police; National Map of Security Threats - Policja.pl - Polish Police Portal

URUGUAY NATIONAL POLICE INCORPORATE ENCRYPTION TECHNOLOGY

The National Police of Uruguay have launched equipment with advanced technology that allows for the encryption and encapsulation of communication, preventing unauthorized devices from accessing the information. This new equipment provides greater protection against interference and ensures consistent connectivity. An exclusive radio base for the National Police covers up to 12 square kilometres, specifically to avoid the use of shared networks and reduce the possibility of external interference.

In the event of losing coverage, the equipment automatically migrates to LTE technology, and as a last resort, it can operate as a conventional radio. This ensures the equipment remains stable and secure, maintaining consistent communication in any situation.

One of the devices presented has multiple functionalities, including operating as a tablet, recording news, capturing ambient sound, and live transmission to other equipment. This allows agents to communicate hands-free, providing them with greater freedom in the field.

These devices also enable real-time transmission to colleagues away from the scene, offering a shared vision of the intervention area for those offsite. This technology has been tested in helicopters to demonstrate its ability to transmit images and sounds over long distances. This tool is crucial for surveillance and control operations over wider areas.

Sources: Presidencia Uruguay ; Imágenes de presentación de equipos de comunicaciones para la Policía Nacional.

KAZAKHSTAN'S DIGITAL POLICEMAN: A NEW ERA OF SMART POLICING

In response to the growing digital age of AI and smart policing, Kazakhstan's "Digital Policeman" initiative has emerged as a model of technological innovation in policing.

This initiative integrates advanced technologies such as smart badges to empower officers, increase efficiency and ensure accountability. Unlike traditional body cameras, these smart badges offer continuous, tamper-proof video recording, GPS tracking, encrypted data handling, and emergency alert systems for patrolling officers.

The Digital Policeman initiative in total has demonstrated significant results. Since its launch, it has recorded over 6,000 bribery attempts, documented 443,765 administrative violations, and contributed to solving 2,613 crimes.

Source: CIO

By eliminating vulnerabilities associated with tamper-prone video recorders, it has reduced corruption, improved efficiency, and enhanced officer safety. Kazakhstan's Digital Policeman initiative is a reflection of the growing presence of these smart technologies within law enforcement.

DID YOU KNOW?

Intelligent Holographic Surveying is transforming frontline policing by combining 3D holographic imaging, AI analytics, and augmented reality (AR) overlays to revolutionize crime scene investigations, tactical planning, and search and rescue operations. Through real-time virtual reconstructions, officers can revisit crime scenes, plan high-risk interventions using holographic building models, and deploy resources more efficiently in emergencies.

This advanced capability not only enhances evidence preservation and operational readiness but also supports intelligence-led policing strategies, adding a new dimension to crime prevention and public safety.

Source: Policing Insight (Chief Philip Lukens, AI & Policing expert, The International Association of Chiefs of Police)

POLICE SCOTLAND: REIMAGINING HOW SERVICES ARE DELIVERED

Driven by the high costs of maintaining ageing police buildings, decline in walk-ins to traditional stations, and more people engaging with police services online or by phone, Police Scotland is leading a major shift in how policing services are delivered. The aim is to create more efficient and flexible policing services while still ensuring that officers remain visible and accessible to the public by replacing traditional police stations with modern, shared community hubs.

These hubs are set to be located in places such as libraries, council offices, and shopping centres, making it easier for officers to be visible and accessible to the public. As part of a wider plan, officers will spend more time in public spaces rather than behind closed doors in stations. They will continue to serve local communities at these new "community touch points", where the public can report crimes and interact with police.

Sources: Police Oracle; Police Scotland - Scottish Digital Academy

CALL FOR SPEAKERS

INTERPOL event: Conference on AI in Digital Forensics, October 2025, Japan
Sectors: Law enforcement, AI private sector/industry, academia
Required expertise: AI (including generative AI), synthetic media, digital forensics, mobile forensics, misinformation/disinformation

Register your interest via the link below or by scanning a QR code.

https://www.research.net/r/S9WW2R8

You will be contacted if you have been shortlisted for an interview. Thank you!

ADVANCING COUNTER-DRONE STRATEGIES: INSIGHTS FROM THE INTERPOL DRONE COUNTERMEASURE EXERCISE IN SPAIN

The increase in the availability and accessibility of drones has led to new security challenges, prompting law enforcement and security agencies worldwide to refine their counter-unmanned aerial system (C-UAS) strategies. In May 2025, the INTERPOL Innovation Centre organized a four-day INTERPOL Drone Countermeasure Exercise in Seville, Spain, in collaboration with Policía Nacional (National Police). It served as a critical testing ground for evaluating the effectiveness of current technologies and operational tactics against real-world drone threats.

The exercise's collaborative approach ensured that findings from the exercise would contribute to global C-UAS frameworks, enhancing international counter-drone protocols. Unlike controlled laboratory tests, this exercise was conducted in real-world environments, ensuring that counter-drone measures were evaluated in dynamic, unpredictable situations.

Key scenarios included:

- Protection of Critical Infrastructure: Airports, power plants, and government buildings were subjected to simulated drone incursions, testing multi-layered detection and mitigation strategies.
- VIP Security in a Moving Cavalcade: Mobile counter-drone systems were deployed to protect high-profile individuals while in transit, examining response efficiency against drone surveillance and attack attempts.
- Rapid Response to Drone Incursions: Law enforcement units reacted to rogue drone activities in real time, assessing detection speed and neutralization methods.
- Drone Neutralization: Jamming and takeover of a drone entering a protected airspace.

To mirror authentic threat landscapes, the exercise was structured around Red and Blue teaming:

- Red Team: Operated drones to simulate adversarial tactics, including smuggling, surveillance, electronic warfare, and swarm attacks.
- Blue Team: Utilized C-UAS technology to track, detect, and neutralize incoming drone threats.

The INTERPOL Drone Countermeasure Exercise in Seville was one of a series of exercises exploring the use and effectiveness of drone countermeasures. With drones continuing to evolve in capability and accessibility, exercises like this remain essential for staying ahead of adversaries.

The next exercise will be held in September in San Diego, United States. INTERPOL is also part of an EU-funded project that is standardizing the selection, testing, and assessment for CUAS for law enforcement and will develop an EU-wide drone threat reporting system. For more information, please contact dfl@interpol.int.

PROJECT SYNTHWAVE: ADDRESSING SYNTHETIC MEDIA THREATS

The INTERPOL Innovation Centre recently organized the Project SynthWave Strategic Meeting at the INTERPOL Global Complex for Innovation in Singapore. Kicking off Project SynthWave, this Strategic Meeting brought together law enforcement representatives from Southeast Asian countries to share insights and experiences on the impact of synthetic media.

Synthetic media refers to media content, such as images, videos, audios, or text, that has been totally or partially generated or manipulated using Artificial Intelligence (AI) algorithms. Although synthetic media holds potential as a valuable tool, it also poses significant threats for law enforcement and raises complex questions about its impact on law enforcement operations.

Supported by the Government of Japan, the INTERPOL Innovation Centre has launched Project SynthWave, which aims to aid the participating countries in addressing synthetic media threats through community building, knowledge sharing, and regional collaboration. Through its role as a hub for global dialogue on emerging technologies, the INTERPOL Innovation Centre will be able to assess common challenges and specific needs in tackling this issue. The Strategic Meeting brought together law enforcement officers from the participating countries, academia, and technology experts to discuss the impact of AI-generated synthetic media.

Project SynthWave aims to develop law enforcement capabilities by maximizing knowledge opportunities and tackling the threats from synthetic media. Based on the findings and outcomes of the Strategic Meeting, the Innovation Centre will develop tailored INTERPOL guidelines to support the detection and response to synthetic media across the region. A comprehensive Global Research Study will also be conducted, incorporating a wide range of perspectives and insights from around the world. Lastly, an expert forum will be convened in Tokyo, Japan in October as a platform for further discussions.

INTERPOL

CALL FOR CONTRIBUTIONS

Spotlight your innovations

- Law enforcement is evolving at an unprecedented pace, fueled by technological innovations and collaborative efforts that redefine policing.
- The Innovation Snapshots newsletter captures and showcases these transformative advancements and invites you to join the conversation.
- We welcome stories from law enforcement, industry innovators, and academic researchers that showcase technologies and novel approaches to drive advancement together.

Submission Guidelines

- Keep contributions to ~400 words.
- Include relevant, high-quality photos with usage rights and credits.
- Maintain a neutral and factual tone.
- Email your contribution to IC-Snapshots@interpol.int and a brief bio of yourself or your organization.

INTERPOL Innovation Centre | **@INTERPOL_IC** | **IC.INTERPOL.INT** | **innovation@interpol.int**

INTERPOL

INTERPOL Innovation Centre
INTERPOL Global Complex for Innovation
18 Napier Road
Singapore 258510