TURNING THE TIDE

David Janson *examines how AI-powered open-source intelligence can be a key tool in border security*

Open-source intelligence is an essential weapon against cross-border smuggling and human trafficking networks

Every minute, thousands of posts promoting illegal immigration flood social media, fuelling dangerous journeys and organised crime. With 80 percent of Channel crossings linked to online activity, the challenge is clear: manual monitoring can't keep pace. The fight against illegal immigration now hinges on advanced technology. Tackling the UK's ongoing problem with illegal immigration demands a "cross spectrum" approach, Martin Hewitt, the UK's border security commander, told MPs in October (2025).

Hewitt, a former senior police officer with 30 years' experience, expressed frustration that numbers of Channel crossings have remained significant, with French authorities struggling to disable boats as they leave the coast of Northern France. So far this year, more than 36,000 people have entered the UK illegally across the Channel.

Given the UK's ongoing challenges in combating human traffickers and managing a backlog of thousands of asylum cases, AI-powered open-source intelligence (OSINT) should be a key tool in border security. Advanced AI-driven OSINT can detect suspicious activities across mainstream and niche social media platforms, as well as obscure forums and websites where people-smuggling gangs operate and coordinate. With this real-time information, border authorities can quickly respond to prevent illegal crossings and other forms of people smuggling involving vehicles.

The Home Office recognises that social media is crucial in illegal immigration. In August, analysis revealed that 80 of illegal migrants crossing by boat used social media to find or contact an agent linked to organised crime groups. These platforms are not only used for advertising illegal crossings, but also for misleading migrants about opportunities to live and work in the UK. The problem is not unique to the UK. Before the Trump administration's crackdown on illegal immigration to the US, social media played an influential role in connecting would-be migrants with smugglers. In the UK, however, the problem is sufficiently acute that the government has proposed criminalising the creation or posting of material that promotes breaches of UK immigration law. Offending content could include the offer of fake travel documents or the promise of illegal work opportunities.

The Border Security, Asylum and Immigration Bill, which aims to criminalise these promotional activities, was described by a government minister as crucial for expanding "extra-territorial reach." This means that if a social media advertisement is created overseas, the UK can take action if the perpetrator enters the country.

To combat the explosion of social media content promoting illegal immigration, the National Crime Agency (NCA) has worked with social media companies to remove approximately 22,000 posts since 2021. More than 8,000 were removed in 2024, which was a 40 percent increase on 2023. Following online monitoring, the NCA took action against Albanians promoting £12,000 package deals that included accommodation and employment upon arrival. There were also more localised offenders, like a gang from South Wales that smuggled thousands across Europe and Preston-based smuggler Amanj Hasan Zada, who posted videos of criminals expressing gratitude for his assistance.

While these measures may help reduce organised crime networks' involvement in illegal immigration, they probably won't fully tackle the extent of social media misuse or cover all the online channels, forums and dark websites used by criminals. Addressing these issues requires continuous monitoring and specialised skills, combined with automated OSINT technology, to identify and access the ever-evolving range of sites in use. Open-source intelligence is clearly an essential weapon in the battle against cross-border smuggling and human trafficking networks anywhere in the world. The groups behind people smuggling need to be online to advertise and collaborate. Criminals based in mainland Europe are, for example, able to orchestrate the illicit movement of people right across the continent.

While border security agencies collaborate with social media companies to remove promotional content, they require more sophisticated tools to effectively combat it. Once posts are removed, the responsible groups quickly set up new ones, forcing human analysts to continually chase them across various platforms. The gangs frequently switch accounts, create new profiles and shift their focus to different platforms without warning.

AI-driven social media intelligence (SOCMINT) has become crucial as intelligence teams lack the time to sift through millions of social media accounts and forum posts. How can a human realistically access and review such vast amounts of data and gather timely intelligence to effectively disrupt a gang's operations? SOCMINT is designed to collect intelligence and insights from mainstream platforms, niche sites and country-specific websites. The near-real-time capabilities of more advanced tools are vital because many people-smugglers deliberately operate on short notice to avoid detection and often change accounts frequently. The UK government has acknowledged the importance of improved intelligence and plans to invest in AI-powered data analysis tools with its £100-million funding increase for border security announced in August (2025).

ANALYSTS CAN FINE-TUNE AI RISK DETECTORS TO SWIFTLY IDENTIFY SUSPICIOUS PATTERNS

A key element of this extra funding is to: "allow more intelligence to be gathered on organised immigration crime gang members, support upstream capacity building, purchase sophisticated technology and equipment to strengthen UK border security and disrupt the people-smuggling gangs". Achieving this requires technology that can analyse billions of data points with high precision across major social media platforms as well as in the less explored regions of the surface, deep and dark web.

Analysts must detect digital discussions on illegal entry and migration early to support European agencies in implementing proactive strategies. Moreover, they need the ability to analyse long-term patterns of criminal activity on social media and the dark web, allowing for better resource allocation to areas of greatest impact.

AI capabilities are essential because of the need to analyse vast amounts of social media content at high speed and with high accuracy. This provides scalable, near-real-time data from digital conversations and online chatter. AI-powered OSINT can also identify and correlate SOCMINT with other classified and publicly available information, including watch lists, police intelligence, people and company databases – a feat which humans would find very time-consuming.

Multi-lingual risk analysis capabilities are essential for helping analysts automatically identify risk indicators across various regions. Covering billions of data points and featuring user-friendly tools that do not require data science skills, AI-driven OSINT will save thousands of analyst hours, especially when public sector budgets are tight. Data visualisations allow quick insights into connections between people and groups across regions and nations. They can reveal complex networks and suspicious links within hours or even minutes, whereas manual analysis can take days or weeks to

sift through the massive data volumes involved. AI-enabled OSINT's capacity to identify criminal activities on social media and link them to dark web operations offers significant benefits in managing another aspect of illegal migration. It can track agents, proxies and affiliates of hostile nations or terror organisations as they attempt to enter a country or coordinate attacks. Agencies are forewarned about the likelihood of dangerous individuals attempting to bypass standard immigration controls and can concentrate their efforts on disrupting criminal enterprises or arresting suspects upon arrival.

THE UK GOVERNMENT HAS UNVEILED PLANS TO INVEST IN AI-POWERED DATA ANALYSIS TOOLS

When agencies doubt the identities of asylum seekers arriving in the UK or question the validity of their documents, AI-powered OSINT proves highly effective for screening. Analysts can fine-tune AI risk detectors to swiftly identify suspicious patterns within extensive datasets. Open-source intelligence offers valuable insights into criminal activities or false identities, complementing traditional human intelligence and signals intelligence sources, like data from the UK's National Cyber Security Centre. This has significant potential to assist large-scale asylum application screening as it is considerably quicker and more accurate than manual methods. AI-based automated

vetting that follows ethical standards can verify social media accounts more than 20 times faster than humans.

These improvements in speed and efficiency are crucial as the UK faces a significant backlog of asylum applications, which strains public resources and leads to delays. These delays often leave thousands in expensive temporary accommodations, such as hotels. AI-driven vetting can also help identify criminals and individuals with violent records among asylum seekers, helping to isolate these individuals and enhance safety for other applicants and the public.

AI-driven OSINT will not replace the judgment of experienced analysts and investigators. All data generated by the technology can be manually verified before a skilled analyst passes the information up the chain of command. The implementation of the technology reduces the likelihood that under-resourced officials with limited access to intelligence will make poorly informed asylum decisions. It allows analysts to handle more cases efficiently and focus on the most urgent, high-risk situations. This enhances both national security and fairness. The faster process also significantly improves accuracy, while obfuscation protects the anonymity and safety of intelligence teams.

Although no single technology can solve all risks associated with immigration, AI-powered OSINT and SOCMINT should play a key role in enhancing the detection and interruption of people-smuggling, as well as in efficiently vetting asylum-seekers. Final judgments on the severity of threats should always be made by Border Control officers and the NCA, relying on their experience and understanding of the broader context. However, with real-time AI-powered insights, senior officers can make more informed, faster decisions about the most appropriate actions ●

David Janson is VP EMEA at Fivecast.

80 percent of illegal migrants crossing by boat used social media to find or contact an agent linked to organised crime groups