Osprey's approach to the Russia-Ukraine conflict

PREDICTIVE RISK INTELLIGENCE

Matthew Borie discusses the part that data can play in predicting aviation security risks

The development of machine learning (ML) and artificial intelligence (AI) tools in recent years is now enabling aviation security practitioners to harness the power of data in new and innovative ways. AI tools can be used to aggregate incredible amounts of data – with a specific focus on aviation security incidents and events – in a continuous and scalable fashion. Machine learning models can then be applied to categorise the data in a structured format. AI anomaly detection tools can then be applied to the structured data to identify trends and patterns that a human analyst or even a team of analysts would be unable to foresee within the global aviation operating environment.

AI-enabled data collection tools can gather data from a very broad spectrum of sources. Such sources include social media platforms, major international media outlets, local news publications, national-level authorities, law enforcement, government departments, industry organisations, special interest groups with a focus on aviation, think tanks and third-party intelligence providers. Using advanced computing techniques, these AI tools can gather data every few minutes from hundreds of thousands of open sources in dozens of different languages.

Automated categorisation, multi-source corroboration, geolocation and date/time stamping are the fundamental components of ML models that can be applied to aggregated data. These all require AI capabilities to be effective and accurate. The continuous and automated improvement that ML enables ensures that systems, processes and analytical methodologies can, extremely quickly, become significantly more capable and more accurate, with little or no drain on resources.

Within the risk intelligence landscape, when applied to a verified security incident database that is continuously updated, AI anomaly detection tools can leverage the speed of modern technology to facilitate predictive forecasting and enable proactive decision-making. AI anomaly detection can identify trends and patterns within the global aviation operating environment at the airspace, country and airport levels when applied to a verified security incident database. AI anomaly detection within the global aviation operating environment can be used to identify: increases/decreases in overall activity; activity occurring in new areas; new types of security incident; and unusual combinations of security incident types

While AI-enabled data collection tools and ML models of security incident categorisation can save significant amounts of time and improve operational efficiency, such applications alone do not provide a step change in using incident data to predict aviation security risk. However, AI anomaly detection tools applied to a verified incident database can generate predictive risk intelligence, which can be leveraged by aviation security practitioners to make highly accurate and proactive forecasts.

Listed below are several examples of cases in which AI anomaly detection tools applied to a verified security incident database have generated predictive risk intelligence.

The Russian invasion of Ukraine on 24 February 2022 led to airspace closures and flight bans, which severely impacted civilian flight operations, particularly regarding the use of Russian and Ukrainian airspace. This meant aviation operators had to avoid notable swathes of airspace, partially due to a lack of dynamic, timely and accurate data-led risk intelligence. New routings created further issues in terms of added time, increased fuel costs, limited divert options and additional conflict zone risks.

The fallout of the Russia-Ukraine conflict continues to reverberate across the global aviation operating environment. However, this conflict between Russia and Ukraine was not an unforeseen event and, by using AI tools for anomaly detection within verified security incident data, the invasion itself and the likely impacts could have been and, in specific cases, were accurately forecast.

Osprey's AI tool detected 24 anomalies within verified security incident database in the five months prior to the Russian invasion of Ukraine. AI techniques such as anomaly detection within a verified security incident database can allow aviation security practitioners to create a more resilient, objective, consistent, dynamic and comprehensive picture of any conflict zone environment, as evidenced by the Russia-Ukraine example. Relying on verified incident data and applying AI anomaly detection techniques to identify emerging trends and patterns can cut through subjective noise and remove elements of bias from threat identification and risk analysis as part of the risk management process.

In late March 2022, Sri Lanka began seeing protests over socio-economic grievances coupled with power and telecommunications outages. The protests escalated on 1 April, which led to the declaration of a state of emergency and curfew. No direct aviation impacts occurred up to 1 April 2022, and the Bandaranaike International Airport (VCBI/CMB) operated normally with no ground transport disruption due to its location well north of Colombo city centre, where protests took place. By 8 April, the security situation in Colombo deteriorated further, and ground transport to/from Bandaranaike Airport was disrupted. The next three weeks saw significant unrest in Colombo and disruption to operations at Bandaranaike International Airport as foreign air carriers cancelled flights.

AI TOOLS CAN GATHER DATA EVERY FEW MINUTES FROM HUNDREDS OF THOUSANDS OF SOURCES

The AI anomaly detection tool developed by Osprey Flight Solutions was monitoring this situation. Security situation anomalies were detected in 2022 on 23 March, 26 March, 29 March, 2 April and 6 April – all prior to the ground transportation disruption from protests on the highway leading North of Colombo to Bandaranaike International Airport on 8 April. More importantly, these anomalies were detected weeks prior to airlines cancelling flight operations at Bandaranaike International Airport due to the deterioration in the security environment in Colombo in the final weeks of April. The anomalies detected by the Osprey AI tool are not common for Sri Lanka. For context, the only previous Squawks for Sri Lanka occurred on 17 and 20 September 2021 in relation to increased security at Bandaranaike International Airport following a threat made against the facility, which was later declared "false" by authorities.

This example highlights the unique ability of an AI anomaly detection tool to keep aviation security practitioners informed of changes to the operating environment – in this case, a week before the declaration of a state of emergency, two weeks prior to airport ground transport disruption and several weeks prior to significant flight schedule disruption.

Prior to May 2023, there have been several bouts of significant armed clashes between Israel and Palestinian militant groups, including Hamas and the Palestinian Islamic Jihad (PIJ), the two most recent of which occurred in May 2021 and August 2022. Escalations in tensions between Israel and Palestinian militant groups frequently result in armed clashes, which can pose a risk to aviation operators using Israeli airspace and the country's airports, including Tel Aviv's Ben Gurion International Airport (LLBG/TLV).

The most recent bout of significant armed clashes between Israel and the PIJ in Gaza occurred from 10-13 May and was monitored by the AI anomaly

The conflict in Ukraine was not an unforeseen event and the invasion and its impact were accurately forecast

detection tool developed by Osprey Flight Solutions. Security situation anomalies were detected over 8-10 May and, while such individual anomalies in Israel are not unusual in isolation, the occurrence of these on three consecutive days was a deviation from the norm. In fact, the Osprey AI tool had previously detected three straight days of security anomalies from 7-9 May 2021 prior to significant armed clashes between Israel and Palestinian armed groups in Gaza. Similarly, three straight days of security anomalies were detected by the Osprey AI tool from 5-7 August 2022 immediately preceding the significant armed clashes between Israel and the PIJ in Gaza.

AI ANOMALY DETECTION TOOLS CAN BE APPLIED TO DATA TO IDENTIFY TRENDS AND PATTERNS

This highlights the ability of an AI anomaly detection tool to keep aviation security practitioners informed of changes to the operating environment – in this case, days in advance of airspace restrictions issued by Israel starting 10 May 2023 and a conflict zone-related NOTAM issued for FIR Tel Aviv (LLLL) airspace on 11 May 2023.

What does the future hold for the intersection of technology, aviation security and risk intelligence? It will almost certainly involve the use of AI/ML tools for data collection, security incident categorisation and anomaly detection. Such

techniques are no longer a pipe dream on a white board – they are facilitating predictive forecasting and enabling proactive decision-making via the production of data-led risk intelligence outputs. Using the above AI/ML tools – combined with a specialist team of security practitioners – organisations can ensure that at any one time there is an objective and consistent picture of the global aviation operating environment that continuously improves and notifies when change occurs.

A large quantity of high-quality verified security incident data is essential for accurate and objective risk intelligence to be produced via AI anomaly detection. Irrelevant data creates 'noise', makes analysis and assessments less accurate and reduces the value of identifying patterns and anomalies. Data must be categorised into clearly defined risk and threat categories. Using highly trained and therefore accurate ML models is also necessary to ensure a high level of consistency. Such consistency is unachievable through human classification alone – it requires technology and innovation.

The above AI/ML capabilities offer huge opportunities to the aviation security industry. Embracing AI/ML techniques and combining it with human security practitioner expertise is a unique way to overcome the dynamic challenges within the global aviation operating environment. Security practitioners need to embrace the use of AI/ML techniques to better understand — and continuously improve that understanding — of the global aviation operating environment, the risks present and the measures that need to be taken to ensure that everyone is as safe and secure as possible when travelling by air ●

Matthew Borie is Chief Intelligence Officer at Osprey.

AI techniques can allow aviation security practitioners to create a more comprehensive picture of any conflict zone environment

Picture credit: US Dept of Defense