# BTR: Intelligence Agencies Harness AI in Response to Dynamic Threat Landscape


Jamie Caffrey, i2 Group

WASHINGTON, DC, UNITED STATES, December 10, 2025 / EINPresswire.com/ -- As artificial intelligence systems reshape the global security landscape, intelligence agencies and law enforcement organizations are confronting more data, more complexity, and more scrutiny, without corresponding increases in budget or personnel. For many in the field, the question is no longer whether artificial intelligence (AI) will be incorporated into intelligence workflows, but how to do so in a way that improves accuracy, increases speed, and maintains public trust.

These tensions were the focus of a recent BizTechReports executive vidcast with Jamie Caffrey, Group Leader at i2 Group, a long-standing provider of intelligence analysis software used across national security, law enforcement, and commercial risk management. Caffrey, who works closely with investigative and intelligence teams around the world, says AI's rapid advance is forcing agencies to balance operational urgency with ethical constraints.

The shift is coming during a period of geopolitical volatility, accelerating digital exposure, and persistent resource constraints. "You're not talking about a needle in a haystack," Caffrey said. "You're talking about hunting for a haystack in a sea of haystacks."

A Technology Roots Deep in Intelligence Workflows

The i2 platform (Analyst's Notebook) predates the current AI wave by decades. Founded in Cambridge in the early 1990s, the company helped digitize investigative techniques that had traditionally been managed with paper, whiteboards, and manual cross-referencing. Investigators used early i2 systems to visualize connections between people, communications,

> AI can accelerate how analysts prepare data and find patterns. But the core reasoning — the investigative intuition — still sits with humans."
>
> *Jamie Caffrey, i2 Group*

locations, financial transactions, and other indicators of criminal networks.

Caffrey notes that the company emerged "at the dawn of graph and digital networks," as law enforcement agencies sought to replace manual link analysis with tools capable of tracking increasingly complex criminal and activity. Over time, those capabilities expanded into national intelligence, military operations, and commercial sectors such as financial services, insurance, and retail fraud.

The main problem — that data keeps growing faster than agencies can effectively handle — hasn't changed over the years.

"We produce more evidence today in our day-to-day lives than ever before," Caffrey said. "Smartphones, mobility data, payments, vehicles, digital interactions — everything creates breadcrumbs. The question is whether investigators can capture and assemble them quickly, reliably, and defensibly."

Ethics, Transparency, and the Risks of the "Black Box"

The rise of generative AI has introduced compelling new tools for addressing this challenge. But new capability brings new scrutiny, particularly around how these tools shape decisions that affect people's rights and public trust.

Caffrey argues that the intelligence community cannot afford to treat AI as a mysterious oracle. "Anything that goes into intelligence analysis has to be honest, transparent, unbiased," he said. "Policing is by consent. If investigators rely on a black box they can't explain, public trust collapses — and cases collapse with it."

Several jurisdictions have already begun codifying those expectations. Caffrey pointed to emerging U.S. regulations requiring that AI-assisted intelligence reports include disclosures about the use of automated tools. At least one state also mandates that agencies explain how AI contributed to a conclusion in any criminal proceeding.

"These models must be explainable," he said. "If you get an answer from a system and you cannot reconstruct the reasoning by hand, it won't stand up in court."

That emphasis reflects growing concerns that AI-generated inferences — even when useful — could contain hidden biases or errors that undermine the integrity of an investigation.

The Expanding Universe of Digital Evidence

At the same time, Caffrey argues that AI can materially increase the speed at which agencies process digital evidence. He cited a recent U.S. investigation that moved from homicide to arrest in just five days — a timeline that would have been nearly impossible a decade ago.

Investigators analyzed mobile phone records, traffic camera footage, rental-car GPS data, credit-card transactions, and even location trails from a dockless scooter. Tools like i2 Analyst's Notebook helped investigators stitch those disparate clues into a coherent timeline.

"What used to take months now takes days," Caffrey said. "The challenge today does not stem from a lack of data — it's the overwhelming volume."

As the demands on investigators grow, the gaps created by specialized skill requirements and technical competencies are also shrinking. New analytical tools can absorb tasks that once required advanced training or large teams, lowering the barriers to rapid, high-quality assessments and helping analysts convert raw evidence into meaningful outcomes. Natural language processing, machine learning, and image and audio analysis have become essential in narrowing that volume into actionable insights. But Caffrey cautioned that agencies must still understand each step of the chain of inference.

"AI can accelerate how analysts prepare data and find patterns," he said. "But the core reasoning — the investigative intuition — still sits with humans."

Breaking Down Silos: A Long-Standing Problem, a New Opportunity

Reliance on human judgment becomes even more critical when information is scattered across disconnected systems — a longstanding structural problem for intelligence agencies.

For decades, intelligence and law enforcement organizations have struggled with siloed data. After the 9/11 attacks in 2001, fusion centers and interagency task forces in the U.S. were rapidly stood up to bridge those gaps. Similar structures exist across the Five Eyes alliance – the long-standing intelligence-sharing partnership among the United States, the United Kingdom, Canada, Australia, and New Zealand — to facilitate cooperation across national borders and coordinate responses to shared threats.

That said, many agencies still rely on isolated systems, manual processes, or informal sharing practices.

Much of that fragmentation stems from long-standing classification rules, which give departments strong incentives to protect their own data, limit access, and maintain tight control over who can see what. Those safeguards are essential for national security, but they also complicate efforts to share information quickly or build a unified picture across organizations.

Caffrey says AI technology is providing new paths to securely share information across departments without undermining classification protocols.

“There is a growing consensus that the technology is there,” he said. “You can enforce permissions, redactions, and hashes to share information safely.”

However, political will remains uneven. Intelligence agencies often have incentives to withhold certain data, while law enforcement organizations operate under evidentiary requirements that prioritize transparency.
That divide makes it essential for senior leaders to understand both the potential and the constraints of emerging AI tools — and to steer adoption in ways that improve outcomes without exposing agencies to new legal, ethical, or operational risks. Effective use of these technologies requires informed oversight, not just technical enthusiasm.

“The leadership question is important,” Caffrey said. “Technology can help, but collaboration has to be driven at the top.”

He cited U.K. efforts targeting “county lines” drug trafficking networks — criminal groups that move operations across regional borders — as an example of cross-jurisdictional collaboration that has yielded results. “Success drives more collaboration,” he said. “People stop hoarding information when they see what sharing can achieve.”

Resources Are Static. Threats Are Not.

Many agencies face widening gaps between the scale of emerging threats and the resources available to address them. Digital crime has expanded. Geopolitical tensions have intensified. And cyberattacks — particularly ransomware — have grown in frequency and sophistication.

At the same time, budgets remain flat and the number of trained analysts is finite.

Caffrey believes AI can help narrow that gap, not by replacing analysts but by expanding their reach. “Technology is moving at such a pace that what wasn’t possible two years ago is now routine,” he said. “You can analyze unstructured text, video, images, audio, and signals intelligence at scale.”

He describes today’s analysts as hybrid professionals — part investigator, part technologist, often with data-science skills. Younger analysts entering the field, he adds, are digital natives who expect advanced tools in their workflow.

“Agencies should see AI as an investment in their people and not just as a purchase of technology,” he said. “The best analysts evolve as dynamic AI tools also learn and self-optimize to amplify their ability to capture, process and disseminate intelligence.”

A Cautious, Incremental Approach to Generative AI

While i2 has incorporated AI techniques — particularly natural language processing and pattern recognition — into its products for years, the company is taking a measured approach to generative AI.

Caffrey says the goal is to enhance, not automate, the analytical process. That includes helping investigators ask complex questions in plain language, reducing the need for specialized query skills, and democratizing advanced analysis across teams.

But the company is prioritizing transparency. “We are building generative capabilities that are explainable from end to end,” Caffrey said. “Our customers need to be able to take an intelligence product to court and show every step, and that is what we are providing.”

The Road Ahead

As 2025 draws to a close, the intelligence community is still calibrating its relationship with AI. For some agencies, the technology represents a long-awaited force multiplier that could offset decades of resource constraints. For others, it introduces new risks, new transparency obligations, and new governance challenges.

Caffrey believes the benefits will ultimately outweigh the risks if agencies commit to ethical and operational discipline.

“Generative AI is only three years old,” he said. “We are still in the early days. But combined with decades of experience in network-based intelligence analysis, it opens tremendous opportunities.”

The organizations that lead, he argues, will be those that invest equally in tools, people, oversight, and cross-agency cooperation.

“Technology is an enabler,” he said. “But leadership — political, operational, and ethical — will determine how effectively we use it.”

Click here to read the Q&A based on this interview.

Airrion Andrews
BizTechReports
email us here

try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.