BTR: Growing Threat Complexity Drives Demand for Cross-Disciplinary Intelligence Collaboration

WASHINGTON, DC, UNITED STATES, June 18, 2026 /EINPresswire.com/ -- Intelligence organizations are expanding collaboration across agencies, sectors, and professional disciplines as increasingly sophisticated threats expose the limits of traditional approaches to intelligence analysis, training, and information sharing.

> We have an over-availability of information. It can lead to overconfidence through information bias, or conversely can trigger analysis paralysis."
>
> *Nadia Tuominen, i2 Group*

Criminal enterprises, cyber adversaries, fraud networks, and other bad actors routinely operate across borders, jurisdictions, and technologies. They share expertise, leverage common infrastructure, and exploit digital tools that allow them to move faster than many of the institutions attempting to stop them.

Indeed, the World Economic Forum's Global Cybersecurity Outlook 2025 found that cybercrime ecosystems have become increasingly specialized and interconnected. Threat actors are leveraging cybercrime-as-a-service offerings, shared infrastructure, and collaborative networks to lower barriers to entry and accelerate attack execution. Similarly, Europol has reported that organized crime groups are increasingly operating as flexible networks that combine expertise across multiple criminal specialties and jurisdictions.

At the same time, intelligence professionals are being asked to evaluate larger volumes of information, adopt new technologies, and respond to increasingly complex operational environments, often without corresponding increases in staffing or resources.

Research from Gartner and IDC has consistently highlighted the challenges organizations face in managing rapidly expanding data volumes while addressing persistent skills shortages. Gartner has also warned that information overload and increasing technology complexity can undermine decision-making effectiveness, while workforce constraints continue to place additional pressure on analysts and investigators across both public- and private-sector organizations.

During a recent BizTechReports executive vidcast interview, Nadia Tuominen, Community

Champion at i2 Group, said these converging pressures are creating new incentives for intelligence professionals to learn from one another and share knowledge across traditional organizational boundaries.


Nadia Tuominen, i2 Group

"If adversarial criminal actors can collaborate with each other for their greater success, then absolutely we should be doing the same for the greater good," Tuominen said.

Her observation reflects a growing recognition that modern intelligence work increasingly depends on the ability to connect expertise across disciplines, organizations, and sectors.

Threats Are Becoming More Networked and Collaborative

The intelligence community has long operated in an environment defined by information sharing restrictions, organizational boundaries, and clearly defined areas of responsibility. While those principles remain important, the threats confronting organizations today are becoming increasingly interconnected.

Cybercriminal groups purchase services from specialized providers. Fraud networks coordinate across regions and jurisdictions. Criminal organizations exploit digital payment systems, encrypted communications platforms, and emerging technologies that allow them to operate with greater speed and flexibility. Many adversaries have become highly effective at combining capabilities from multiple sources to achieve their objectives.

To this point, the OECD's 2026 Anti-Corruption and Integrity Outlook found that criminal networks are increasingly exploiting cross-border money laundering schemes and digital tools, with dark markets, cryptocurrencies, and encrypted communications platforms enabling more effective sharing of knowledge and resources among criminal actors across jurisdictions.

The result is a threat landscape that rarely conforms to the structures used by government agencies, law enforcement organizations, or corporate security teams.

"Threat actors do not distinguish between public and private sectors. They do not operate

according to organizational charts. They do not recognize the boundaries that separate intelligence, investigations, technology operations, and executive leadership," said Tuominen.

As a result, intelligence organizations increasingly require input from multiple disciplines to understand and respond to emerging threats.

Analysts, investigators, technology specialists, systems architects, operational leaders, and executive decision-makers each possess different perspectives that can contribute to a more complete understanding of risk.

The challenge is ensuring that those perspectives are connected.

Intelligence Professionals Face Challenges Amid Information Abundance

For intelligence practitioners, the challenge today is less about finding information than managing it. The consequences of that shift are showing up in how analysts make decisions, assess confidence, and sustain performance over time.

Organizations have access to unprecedented quantities of information. Open-source intelligence, digital records, social media activity, sensor data, financial transactions, and AI-enabled tools have dramatically expanded the amount of information available for analysis.

The trend is creating a paradox in which access to more information should theoretically lead to better decisions, but, in practice, the volume itself has become a challenge.

Tuominen cautions that intelligence professionals face the risk of becoming overwhelmed by information abundance. Large data sets can create analysis paralysis. Easy access to information can create overconfidence. The growing availability of artificial intelligence tools introduces the possibility of cognitive offloading, where critical thinking is increasingly delegated to technology.

"We have an over-availability of information," Tuominen said, adding that it creates the potential for negative outcomes. “It can lead to overconfidence through information bias, or conversely can trigger analysis paralysis.”

The challenge is compounded by workforce realities.

Many intelligence-led organizations are expected to manage growing workloads with limited personnel resources. At the same time, hybrid and remote work environments have reduced many of the informal opportunities for professional interaction that once occurred naturally.

"The workload is increasing. The number of people available to do it is decreasing. And opportunities to talk about how to address these issues in impromptu scenarios have diminished," Tuominen observed.

That combination creates risks not only for analytical quality but also for professional development and workforce resilience.

Click here to read the rest of the article.

Airrion Andrews
BizTechReports
email us here