ONTIC SUMMIT 2026

Geopolitical Intelligence as an Untapped Business Asset

This session examined how corporate security teams can transform geopolitical intelligence from passive monitoring into a driver of business decisions. Panelists emphasized translating complex global events into actionable insights, aligning intelligence with business priorities, and preparing for second- and third-order impacts. The discussion highlighted the importance of relationships, credibility, and communication, while addressing emerging challenges such as AI, misinformation, and asymmetric threats. Ultimately, success depends on integrating human judgment with structured processes and cross-functional collaboration

Speakers

Aaron Gertje
Sr Manager Resilience, Intelligence, & Crisis
Amazon

Adrienne Galbrecht
Senior Team Lead, Strategic Services
Ontic

Beth Sanner
Former Deputy Director
Office of the Director of National Intelligence

Justin Lamb
Sr Manager - Global Intelligence
Stryker

Key Themes and Topics

Intelligence Must Drive Business Decisions

Geopolitical intelligence only creates value when it directly informs business actions. Security teams must move beyond reporting events and instead explain relevance, impact, and required decisions. Executives expect clarity on why information matters and how it affects operations, risk, and strategy.

Second- and Third-Order Effects Are Critical

Immediate threats are often visible, but indirect impacts such as supply chain disruption, reputational risk, and employee safety emerge later. Organizations that proactively model cascading effects are better positioned to respond strategically rather than react tactically during prolonged crises.

Credibility and Relationships Enable Influence

Intelligence teams must build trust with stakeholders before crises occur. Strong internal and external relationships increase access to non-public information and ensure recommendations are acted upon. Without credibility, even high-quality intelligence risks being ignored or deprioritized.

Continued on next page

Key Themes and Topics

Communication Must Be Tailored and Practical

Technical analysis alone is insufficient. Security professionals must translate intelligence into language that aligns with executive priorities and decision frameworks. Tailoring messaging to individual stakeholders improves comprehension, urgency, and the likelihood of action.

AI Changes Speed, Not Accountability

AI accelerates access to information but does not replace human judgment. Overreliance risks shallow analysis and false confidence. The competitive advantage now lies in contextualization, critical thinking, and access to non-public intelligence rather than raw data processing.

Actionable Takeaways

Build Executive-Aligned Intelligence Frameworks

Define intelligence priorities based on what senior leaders need to make decisions, not what analysts find interesting. Map intelligence outputs directly to business risks, operational impacts, and decision triggers to ensure relevance and consistent executive engagement.

Develop Scenario Planning with Clear Tripwires

Create structured scenarios that include escalation pathways and predefined triggers for action. Establish tripwires tied to business decisions such as travel restrictions or supply chain shifts, enabling faster and more confident responses during rapidly evolving crises.

Institutionalize Relationship Building

Invest time in building networks across internal teams, industry peers, and government partners before crises occur. These relationships provide access to critical insights and improve coordination when events unfold, reducing reliance on incomplete or delayed public information.

Integrate Intelligence with Business Functions

Embed intelligence teams within operational workflows rather than isolating them within security. Collaborate closely with product, HR, legal, and supply chain teams to ensure intelligence informs real-time decisions and reflects cross-functional priorities.

Continued on next page

Actionable Takeaways

Establish Responsible AI Use Guidelines

Define clear rules for how analysts should and should not use AI. Position AI as a tool for challenging assumptions and accelerating research, while reinforcing that human analysis and validation remain essential for accuracy and accountability.

Prepare for Misinformation and Asymmetric Threats

Develop processes to verify information before escalation and train teams to recognize disinformation risks. Incorporate emerging threats such as deepfakes, cyber-physical convergence, and AI-enabled attacks into risk models and executive briefings.

Notable Quote

> **“it's easy for us to get lost in jargon, especially in the intel community or the security world. And so not only just leveraging those relationships, being able to communicate in a way that is relatable to your audience and particularly your decision makers is incredibly important.”**

- Aaron Gertje
Sr Manager Resilience, Intelligence & Crisis Innovation, Amazon

Final Message

Corporate security leaders must evolve from information providers to strategic advisors. The advantage lies not in access to data, but in judgment, relationships, and the ability to translate uncertainty into action. Organizations that operationalize intelligence will outperform those that simply monitor risk.