Conference Report: AFCEA/INSA 2025 Intelligence & National Security Summit

By Dr. Joshua Sinai

On September 18-19, 2025, more than 2,000 intelligence, defense, and national security professionals attended the annual AFCEA/INSA Summit., which was held at the Gaylord National Resort in National Harbor, MD. AFCEA is the acronym for the Armed Forces Communications and Electronics Association, while INSA is the acronym for the Intelligence & National Security Association. AFCEA publishes "Signal," a monthly journal covering latest developments and events in the field. At the Summit, leading government officials and private sector experts discussed topics

such as redefining national security, prioritizing intelligence agencies' information technology (IT) needs, including leveraging latest advances in artificial intelligence (AI) open-source intelligence (OSINT) for operational advantage, and upgrading homeland defense coordination and readiness to address emerging adversarial threats.

On September 18-19, 2025, more than 2,000 intelligence, defense, and national security professionals attended the annual AFCEA/INSA Summit., which was held at the Gaylord National Resort in National Harbor, MD. AFCEA is the acronym for the Armed Forces Communications and Electronics Association, while INSA is the acronym for the Intelligence & National Security Association. AFCEA publishes "Signal," a monthly journal covering latest developments and events in the field. At the Summit, leading government officials and private sector experts discussed topics such as redefining national security, prioritizing intelligence agencies' information technology (IT) needs, including leveraging latest advances in artificial intelligence (AI) open-source intelligence (OSINT) for operational advantage, and upgrading homeland defense coordination and readiness to address emerging adversarial threats.

The Conference's Exhibitors

The meeting was highlighted by significant private sector intelligence companies and organizations that displayed their latest technological innovations and services in the large exhibit floor. Of special interest were the latest technologies that covered fields such as artificial intelligence, counterintelligence, cybersecurity, data management & analytics, intelligence software, investigative solutions, security threat monitoring technologies, and surveillance technologies.

Of special interest were the latest technologies that covered fields such as artificial intelligence, counterintelligence, cybersecurity, data management & analytics, intelligence software, investigative solutions, security threat monitoring technologies, and surveillance technologies.

Intelligence Research Institutes

- **Applied Research Laboratory for Intelligence and Security (ARLIS),** University of Maryland (www.arlis.umd.edu) – established in 2018, it conducts research and development for the Department of Defense and the U.S. Government in the intelligence and security domains.
- **OSINT Academy** (www.osintacademy.com) – It provides training courses on the skills and strategic approach required to conduct OSINT-based investigations, including social media intelligence, cryptocurrency analysis, and digital situational awareness.

Threat-Related OSINT Intelligence Datamining

- **Accrete** (www.accrete.ai) – Its dual-use artificial intelligence-driven knowledge engine technology supports rapidly capturing and analyzing massive amount of disparate data, including social media, information warfare, threat detection and tracing, and document exploitation.
- **Airis Labs** (www.airis-labs.com) – Its AI-driven User-Generated Field Intelligence software transforms large volumes of unstructured, user-generated videos and photos from social media and captured devices, as well as surveillance cameras, to reveal hidden criminal and terrorism threat-related connections and insights.
- **Babel Street** (www.babelstreet.com) – Babel Street Analytics integrates artificial intelligence and natural language processing (NLP) from multilingual and unstructured open source information data systems to provide rapid access to insights about security threat-related individuals, their associations, organizations, and events.
- **BAE Systems** (www.baesystems.com) – BAE Systems' software GXP Ecosystem delivers advanced mission-critical geospatial multi-INT data for military, security, and incident response operations.
- **Censys** (www.censys.com) – Its AI-powered Censys Internet Map continuously scans the global internet infrastructure to provide investigators real-time coverage of exposed assets, adversary infrastructure and evolving attack vectors.
- **Danti AI, Inc.** (www.danti.ai/government) – An AI-powered knowledge engine that mines multiple structured and unstructured data, such as from imagery, news, social media, etc., by fusing large language models (LLMs) with machine learning to deliver contextual answers in seconds.

- **Datenna** (*www.datenna.com*) – An open-source-based intelligence platform, including geo-location data, to investigate China's defense, technological, and economic landscape.
- **Delinea** (*www.delinea.com*) – Its technology provides a centralized, risk-based security platform to detect anomalies in employees' privileged information technology (IT) account behavior that might indicate potential insider risks.
- **DomainTools** (*www.domaintools.com*) – Provide mission-critical Internet intelligence to support defense and intelligence organizations in gaining near real-time context and machine-learning driven risk analytics in identifying external risks. These include threat actor monitoring, counter-intelligence operations, attack surface management, and conducting red teaming exercises.
- **GraphAware** (*www.graphaware.com*) – Leverages graph technologies throughout its software stack, making data analysis fast, scalable, contextual, and AI-ready to produce a streamlined view of complex intelligence collected threat data.
- **Janes** (*www.janes.com*) – Janes utilizes its comprehensive collection of data sets, with more than 150 million validated OSINT connections and tradecraft processes between defense and security data points, to provide a foundation for its government and private sector clients' intelligence workflows. Their products include ORBAT (military orders of battle), military equipment, military capabilities, defense industry intelligence, and national security events the impact security risks.
- **Kharon** (*www.kharon.com*) – Kharon utilizes open-source data and analytic solutions to investigate and analyze matters at the intersection of global security and commerce. The global security threats include illicit finance, terrorism, WMD proliferation, jurisdictions of concern (such as Russia, North Korea, China, and Iran, and supply chain security.
- **Maltego** (*www.maltego.com*) – A comprehensive 'all-in-one' investigation platform to monitor, search, graph, and generate evidence on hard-to-reach social media data across multiple networks to quickly detect hidden patterns and connections of threat targets.
- **Moody's** (*www.moodys.com*) – An American business and financial services company best known for its financial credit rating agency that rates companies and countries. It also provides actionable intelligence services through its database that covers more than 570 million entities and companies around the world, with customers using its data and analytics to uncover national security-related threats. These include terror funding management, foreign interference and influence, geopolitical shifts and foreign national state threats, organized crime activity, and emerging disruptive technologies.
- **Nightwing** (*www.nightwing.com*) – While protecting critical information technology systems, its AI/Machine Learning technology also supports offensive cyber operations.
- **Penlink** (*www.penlink.com*) – Its AI-driven platform collects, normalizes and analyzes threat-related data from hundreds of diverse open sources to support criminal investigations, intelligence analysis, surveillance operations, and courtroom presentations.
- **Primer** (*www.primer.ai*) – Primer builds AI platforms for national security enterprise environments to uncover hidden patterns and relationships with OSINT and proprietary datasets generate early warning about adversaries motivations, affiliations, and influence networks.
- **Rakia** (*www.rakia.ai*) – Rakia's real-time open-source data fusion, AI, and cognitive analysis tool supports investigations of terrorism, money laundering, fraud, illegal immigration, and human trafficking across the world.
- **Recorded Future** (*www.recorded-future.com*) – A threat intelligence company that utilizes advanced technology and extensive open source data collections and searchers to collect, analyze, and provide real-time analytical insights on open and dark web-based physical- and cyber-related security threats through conflict monitoring, terrorism activities, and military, diplomatic and economic developments. It also provides tailored training workshops and educational briefing programs to support their clients.
- **Sayari** (*www.sayari.com*) – Sayari applies intelligence methods and technologies for its intelligence and defense clients to data mine open source information about adversaries threats, such as counterintelligence, strategic competition by China and Russia, investigations of foreign ownership of American companies, foreign information operations, supply chain risk management, and illicit finance transactions.
- **Seerist** (*www.seerist.com*) – Combining artificial intelligence and human analysis, it delivers real-time, actionable insights from millions of data sources to support decision-making and strategic planning on indications and warning (I&W) on emerging global threats, such as foreign influence operations, travel safety, logistics risks, homeland security, and disaster response.
- **ShadowDragon** (*www.shadowdragon.io*) – ShadowDragon's Horizon Monitor and Social Net technology platforms investigate the digital tracks of threat-related individuals, their social networks and activities.
- **Skopenow** (*www.skopenow.com*) – an integrated OSINT platform, enhanced by AI, that utilizes algorithms to mine publicly available raw information to incorporate threat-related data about

terrorist and criminal suspects and networks into investigative processes to disrupt operations and dismantle groups' leaderships.

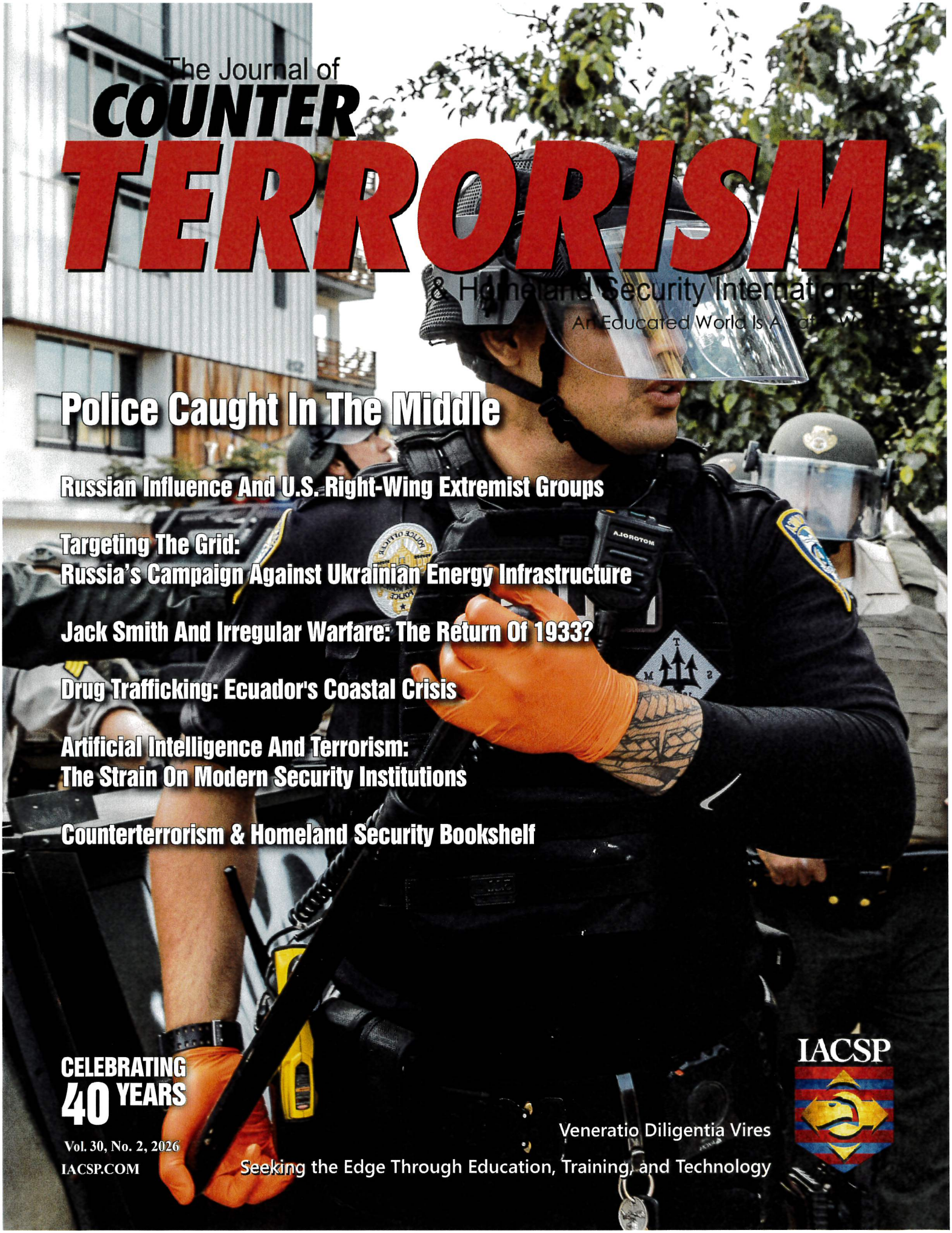
- **SpyCloud** (www.spycloud.com) – Its Identity Intelligence tool accesses data in the deep and dark web, which, together with its rich analytics, offers a streamlined tool for compiling insights to identify and target threat-related individuals, their organizational relationships, and connections to shell companies.
- **Terrogence** (info@terrogence.com) – One of its products, IRIS, is an AI engine that penetrates open source concealed instant messaging applications groups to continuously extract real-time actionable threat intelligence, including identities, group affiliations, and behavioral patterns regarding individuals with a possible nexus to terrorism. Another product, CODEX, is a weapons technical intelligence repository platform containing thousands of expert reports and raw data about terrorism threat-related content for use by government agencies and customers to populate their databases for training, forensics, and R&D purposes.
- **TextOre, Inc.** (www.textore.net) – Its OSINT-based datamining search technology focuses on China, Russia, and Middle East and North Africa (MENA) to monitor and analyze foreign malign influence and narratives, political threats , foreign military leadership and capabilities, as well as cyber threats.
- **UiPath** (www.uipath.com) – Its product, the UiPath Maestro command center, is a process intelligence-based agentic automation tool that records and analyzes workflows on user's desktops to detect and counter potential insider threats by understanding deviations from the standard operating procedures.
- **Venntel** (www.ventel.com) – Specialize applying algorithm-based technological intelligence tools to transform complex human mobility data into actionable insights to locate adversary threat locations, cross-border movements, and vulnerabilities to develop proactive mitigation strategies for military and intelligence agencies.

- **WireScreen** (www.wirescreen.ai) – An open-source intelligence (OSINT) platform tailored for intelligence gathering and lead generation on China-focused military, geo-political, economic and national security-related security risk topics.
- **Zignal Labs** (www.zignallabs.com) – Ziganl employs AI/ML technologies to obtain narrative signals and geolocated visual detection information to identify critical intelligence hidden in massive volumes of open-source information for military and counternarcotics operations.

The annually-held AFCEA/INSA Summits are valuable in featuring insights on how the U.S. Intelligence Community in government and the private sector are continuously innovating methodologically and technologically, especially in the evolving artificial intelligence/machine learning sector, to address the new requirements to be competitive and gain superiority over rival countries and sub-state actors who threaten the security of the global system.

About the Author

Dr. Joshua Sinai is Professor of Practice, Intelligence and Global Security Studies, at Capitol Technology University. He writes the "Counterterrorism & Homeland Security Bookshelf" review column for the magazine. He can be reached at: Joshua.sinai@comcast.net.



The Journal of
COUNTER TERRORISM
& Homeland Security International
An Educated World Is A Safer World

Police Caught In The Middle

Russian Influence And U.S. Right-Wing Extremist Groups

**Targeting The Grid:
Russia's Campaign Against Ukrainian Energy Infrastructure**

Jack Smith And Irregular Warfare: The Return Of 1933?

Drug Trafficking: Ecuador's Coastal Crisis

**Artificial Intelligence And Terrorism:
The Strain On Modern Security Institutions**

Counterterrorism & Homeland Security Bookshelf

CELEBRATING
40 YEARS

Vol. 30, No. 2, 2026
IACSP.COM

IACSP

Veneratio Diligentia Vires

Seeking the Edge Through Education, Training, and Technology

Vol. 30, No. 2, 2026

IN THIS ISSUE

THE JOURNAL OF COUNTERTERRORISM & HOMELAND SECURITY INT'L is published by SecureWorld- net, Ltd., PO Box 100688, Arlington, VA 22210, USA, (ISSN#1552-5155) in cooperation with the International Association for Counterterrorism & Security Professionals and Counterterrorism & Security Education and Research Foundation. Editorial correspondence should be addressed to: The Journal of Counterterrorism & Homeland Security International, PO Box 100688, Arlington, VA 22210, USA, (571) 216-8205, FAX: (202) 315-3459 . Membership $65/year, add $10 for overseas memberships. Postmaster: send address changes to: The Journal of Counterterrorism & Homeland Security International, PO Box 100688, Arlington, VA 22210, USA. Web site: www.iacsp.com

PHOTO CREDITS:
Reuters, Army.mil, Navy.mil, shutterstock.com, Pixabay and other sources and authors where applicable.

ON THE COVER:
Toronto, Canada - January 1 2024 Luigi Mangione is charged in the deadly shooting of UnitedHealthcare CEO Brian Thompson.