BORDER SECURITY REPORT

VOLUME 40
JANUARY / FEBRUARY 2025

THE JOURNAL OF BORDER SECURITY AND TRANSNATIONAL CRIME FOR THE WORLD'S BORDER PROTECTION, MANAGEMENT AND SECURITY INDUSTRY POLICY-MAKERS AND PRACTITIONERS

COVER STORY

REIMAGINING IMAGING AT THE AIRPORT

HARNESSING OSINT TO COUNTER TERRORISM AND RADICALIZATION

bY By Mohamad El-Hamalawy, Babel Street

Jacques Rene Chirac, the late former President and Prime Minister of France once said, “Terrorism has become the systematic weapon of a war that knows no borders and seldom has a face.”

Cross-border terrorism remains a significant threat, with ongoing conflicts in regions such as Eastern Europe and the Middle East potentially intensifying recruitment and radicalization. Terrorist organizations are increasingly using open-source platforms for communication, recruitment, and logistical coordination. This makes use of Open Source Intelligence (OSINT), which pulls data from these platforms, an indispensable tool for counterterrorism efforts and enhanced border control security.

For border security personnel, OSINT tools provide enhanced situational awareness and actionable intelligence to flag potential terrorist activities, enabling proactive responses to emerging threats. This capability is particularly useful in identifying false identities, monitoring extremist narratives and tracking the movement of known terror suspects across borders.

When combined with traditional intelligence methods, OSINT significantly bolsters the ability of border security forces to mitigate terrorism-related risks, by identifying possible threats, tracking suspicious activity, and anticipating potential risks associated with suspected terrorist movements.

Two Types of Border Security Threats

Border security professionals face two prominent and evolving threats: organized terrorist groups and the rising phenomenon of "lone wolf" attacks. While terrorist groups often leverage coordinated strategies and networks to plan large-scale assaults, lone-wolf attackers operate independently, driven by personal ideologies or grievances. Both types of threats require distinct yet complementary approaches to ensure effective prevention and response, highlighting the need for robust intelligence, community engagement, and adaptive security measures. Understanding these threats in tandem is crucial for developing comprehensive strategies that safeguard national borders and protect public safety.

Organized Networks

Organized terrorist networks, cells, and groups use social media platforms and dark web forums for the dissemination of propaganda, for planning, and for general communications.

For example, Hezbollah, considered by many to be a terrorist organization, is one of many global organizations acting as proxies for the Iranian regime in the Middle East and as far out as central and Latin America. Hezbollah operates a vast network of online outlets to promote their ideology and narratives. This includes the popular Telegram platform where Hezbollah's "information" unit consistently publishes material to promote their propaganda and more importantly, conduct recruitment efforts and issue calls to arms.

Leveraging OSINT, border security professionals can start their analyses with a keyword search. Hundreds of thousands of documents posted over the last 30 days may be returned. From this point, analysts study a group's past activities to predict its future actions. For example, mainstream news sources could report on a group's activities, which would inform the analysts' understanding of a given situation. They may also learn more about the group's relationship with others, for example, its relationship with rival groups. Analysts trying to predict likely future events can benefit from this information.

Analysts also can view and filter information by data source, or for a deeper dive, they may opt to filter by reputable news source. They also can search social media posts for keywords aligning with the organization. If they want to access chatter or possible future plans, they can enter search terms that align with known code words used by the group.

AI-enabled OSINT's time-saving persistent search capabilities are an important part of this effort.

Persistent search continuously attaches new documents to search terms whenever new information is found, regardless of whether users are actively searching at the time.

Analysts concerned about a group's relationships with other individuals and groups, and about possible future strikes against a target, may want to see which group members are in some way connected to other members. Using names and aliases found in previous searches, analysts can use OSINT to chart relationships.

Individual Extremists: The Lone Wolves

Another term often used for individual extremists in border security contexts is "lone wolves." This term emphasizes the solitary nature of their actions while recognizing their motivations, which may stem from personal ideologies or grievances rather than organized group affiliations.

By their very nature, lone wolf terrorists fly under the radar. Analysts have no organization or personal name to search for, no reputable news sources to examine for insight, so how can analysts use OSINT to track them? In these cases, analysts use OSINT to find search terms related to lone wolf terrorism. From there, they can delve deeper into the people using those terms in online communications.

Searches can be performed on a variety of sites — in dark web chat groups and marketplaces, and in

mainstream and niche social media sites, among others. The key is to know what terms are associated with potential individual extremists in a specific area or situation. Terms such as "annihilate," "bloodbath," or "xplode" might be typical and used in phrases or with hashtags, for example. Some OSINT software also can search for emojis meant to evoke violence, including depictions of guns, skulls, bombs, and swords.

The Evolution of Counter Terrorism Threat Detection

OSINT is becoming more vital every day for counter terrorism. As the volume of data continues to grow, the ability to filter and analyze relevant information effectively is essential.

OSINT is also vital to work upstream for the monitoring of online radicalization, which can occur on both mainstream and niche social media platforms, including unexpected ones such as Pinterest. Extremists increasingly leverage these online communities of interest that are borderless, that are not restricted to language or platform — or even a particular political ideology.

Moreover, as technology advances, so too does terrorists' use to expand its reach and influence online. In a study by Tech Against Terrorism, the group found more than 5,000 pieces of AI-generated content produced by terrorist and violent extremist actors (TVE) to augment current efforts to create and disseminate propaganda.

Counter terrorism requires technology that can canvas online sources in a language agnostic way, in a data structure agnostic way, and in a platform agnostic way — at scale. And this is where analytical capabilities like those that can understand, "Muhammad" is two ms, or Muhamad is one m or phonetically spelled in a completely different language altogether, but it's the very same individual "Muhammad". So entity resolution, language capability, and ultimately, automation, must be a key part of a technology solution that looks at detecting threats and to counter radicalization, online.

This is vital to enhance contextual understanding and integrating OSINT with other intelligence sources for improved effectiveness. These efficiencies can help counter global workforce shortages. They can also streamline processing to help facilitate legitimate trade and travel.

By efficiently analyzing massive volumes of data and distilling it into actionable information in a timely manner, OSINT is a force-multiplier, allowing humans to focus on more difficult tasks, such as problem-solving, crisis management, and decision-making. It augments human capabilities, enabling analysis at speed and scale beyond human capacity, without replacing human involvement. The goal of OSINT is to bring insights closer to decision-makers while maintaining the human element in critical decision-making.

It also enhances border security capabilities, especially in instances of "broken travel," where individuals avoid traditional travel routes to enter conflict regions, making it difficult to detect threats. OSINT and analytics can help reveal these threats through analysis of both structured and unstructured data.

Refactoring to Be Fit for the Fight

Worldwide, we must refactor to be fit for the counter terrorism fight,

using new digital tools to aggregate structured and unstructured data and analysis for terrorist threat detection as well to combat the growing radicalization proving ground, also known as the Internet.

OSINT enables border security personnel and law enforcement to identify potential lone wolf and organized-network threats, track suspicious activities, and monitor extremist content. By combining OSINT with traditional intelligence methods, authorities can proactively respond to emerging risks, detect false identities, and track the movement of known terror suspects, significantly enhancing capabilities to mitigate terrorism-related risks. At the same time, using technology to distill massive amounts of information into actionable intelligence helps address the need to do more with less given budget and resource constraints.

And finally, given the need for counter terrorism intelligence sharing among nations, OSINT is an invaluable resource to support information sharing among nations, further paving the way for more effective counter terrorism measures and increased agility in a constantly evolving threat landscape.

As Senior Vice President and General Manager of Identity, Risk, and Border Programs, Mohamad El-Hamalawy oversees Babel Street's Large and Enterprise accounts within its Federal Civilian client base. He has over 25 years of experience spearheading numerous large-scale initiatives for the development and delivery of cutting-edge technology solutions for border, vetting, customs, risk and transnational challenges for the US and international clients.