Show and Tell: Expert Perspectives on Indicators and Warning Approaches for External Terror Ops

By Brian Dodwell, Don Rassler, and Paul Cruickshank

It is critical for the counterterrorism community to have a sophisticated understanding of the components of external operations and the indicators that help to signal that a network's interest, capabilities, or attack planning are advancing. It is even more critical to be able to effectively provide warning when an external operations terror attack is imminent. To help enhance and validate existing indicators and warning approaches, the authors conducted a survey of 30 practitioners, academics, and private sector specialists to acquire unique and varied insights on this important issue. This article provides a summary of key indicators that could indicate a change in a group's intent and capability to conduct an external operations attack. It then examines existing shortfalls and offers potential solutions in the areas of artificial intelligence, data prioritization, and information sharing, before concluding with some unique models to consider from other fields that can help existing I&W approaches to evolve.

When it comes to terrorism, the indicators and warning (I&W) space is a tough business. In many ways, it is a space full of dichotomies. I&W practitioners can disrupt scores of attacks and not receive much public credit, but when the enterprise misses something, the public can be quick to look beyond prior successes and focus instead on a single case of failure. At its core, I&W activity is also a competition, a contest between 'hunters'—governmental actors who seek to identify and detect—and 'evaders'—terrorists who want to hide and circumvent. There are dichotomies in the data dimension and the art and science of I&W work, too. In today's environment, I&W practitioners need to contend with and devise strategies to assess increasingly voluminous amounts of data; they need to engage with data at scale because no stone can be left unturned. But the data that ends up being useful may only be a singular piece of data or a small collection of data, the proverbial 'needle in a haystack,' which the practitioners need to find or stitch together. Approaches to I&W for terrorism vary: Some are highly technical; others are more analog, 'old school,' and centered around experience; and some are a mix of the two.

A key factor that undergirds the United States' shift to strategic competition is that it needs to be more risk accepting when it comes to terrorism. In 2023, the Department of Homeland Security's Counterterrorism Coordinator Nicholas Rasmussen made that point clear: "As a result of diminished forward-deployed resources and government attention, the counterterrorism strategy focuses more on risk management and risk mitigation."[1] Due to this, I&W, and specifically I&W designed to detect and prevent external operations by terror networks, has taken on even greater importance. While the I&W space has always been a terrorism safety catch, in the United States today it is an even more important guardrail. The increased importance placed on I&W is reflected in the place it holds in National Security Memorandum 13, where "Strengthen Capacity to Warn" was featured as the third line of effort behind "Strengthen Defenses" and "Build and Leverage Partner Capacity."[2]

It is an area that the United States needs to get right. The United States needs to ensure that its I&W approaches are built to handle today's terror threats, especially those that come from more predictable directions such as the Islamic State. But that same I&W system also needs to be postured for tomorrow's terror threats, which may come from less clear avenues. For example, it is well known and appreciated that Islamic State Khorasan (ISK) is a big external operations risk. While that does not make the I&W challenge easy, the perpetrator is known, and the network's typical *modus operandi* and patterns of behavior are better understood. Identifying the specific details are what makes the ISK case, and others like it, hard. There are also threats whose direction and capacity are not as clear. A lot has happened since Hamas' deadly terror attack on October 7, 2023, for example, and the ongoing conflict between Israel and Hamas, Hezbollah, Iran, and other entities could create other external operations outputs that lead to new dangers. It is plausible, and some would argue likely, that Hamas, or individuals or small cells inspired by Hamas or Palestinian grievances, will try to conduct some type of high-profile attack in a Western country, as a form of retribution. The

Brian Dodwell is the Executive Director of the Combating Terrorism Center at West Point, and an Assistant Professor in the Department of Social Sciences at the United States Military Academy. He has conducted research on various topics, to include Islamic State affiliates, foreign fighters, jihadi terrorism in the United States, and U.S. homeland security challenges.

Don Rassler is an Assistant Professor in the Department of Social Sciences and Director of Strategic Initiatives at the Combating Terrorism Center at the U.S. Military Academy. His research interests are focused on how terrorist groups innovate and use technology; counterterrorism performance; and understanding the changing dynamics of militancy in Asia. X: @DonRassler

Paul Cruickshank has been the editor in chief of CTC Sentinel *since 2015. X: @CruickshankPaul*

Houthi movement, which has demonstrated considerable force projection and reach over the past year, is another entity that deserves attention. The Houthis are not a current or predictable external operations threat, but depending on how conflicts in the Middle East evolve, they could evolve into one in the years ahead. A good I&W system would be postured to engage with a diverse mix of threats, including ones that are nascent or that might not be receiving a lot of attention.

The article by Daniel Milton in this issue of *CTC Sentinel* provides a strategic framework for thinking about terror group expansion.[3] It focuses on the factors that may drive or influence a group to expand its attacks beyond the theater of its normal operations. This article intends to supplement Milton's strategic approach with a more operational assessment of how this process plays out in practice and, more importantly, how counterterrorism practitioners can detect this activity while underway. It includes a summary of responses from interviews that the authors conducted with a diverse mix of 30 experts. Those interviews focused on and explored indicators and warning for external terror group operations, key related lessons, and challenges relevant to that practice area. After a brief discussion of methodology, the next section of this article discusses intent and capability indicators that the interviewees believed provide insight into a terror network's calculus to conduct an external operations attack, and it provides examples of past cases where those specific indicators were notable. The next section identifies key challenges encountered by governments when trying to identify these indicators, including examples of where these efforts fell short. The article then turns to a discussion of potential solutions to these challenges based on feedback from interviewees regarding how to improve I&W for external operations, and will close with a summary of potential alternative models used in other fields and industries that might help government practitioners to evolve I&W approaches.

Methodology and Focus

For this article, the authors conducted interviews with 30 experts. Participants generally fell into three categories: counterterrorism practitioners from military, intelligence, and law enforcement agencies (mostly U.S., but with some international participation); researchers and academics; and participants from private sector fields to include finance, technology, risk management, and countering violent extremism.

The interviewees were asked a series of standardized questions, and they were told that their responses should focus on the activity of organizations and networks, not individuals. The questions focused on four themes. These included:

- Indicators and metrics most important to identify a change in a terrorist group's intent and capability to conduct external operations against the United States and its interests and allies.
- Learning from prior events, as viewed through key plots and attacks or mistakes and failures by governments.
- Accounting for scale, dynamism, and change, with emphasis placed on finding the right data and methods to address these challenges.
- Identifying unique approaches and models from other fields that could inform and help improve existing indicator and warning efforts focused on terrorism.

This article provides an analytical summary of the content and findings that emerged from the 30 interviews. The content from the interviews has been anonymized, and no content is cited to specific participants. Those interviewees who agreed to be identified as participants for this article are listed in the footnote below.[a] The rest chose to remain anonymous. Other than just a handful of exceptions, all the content in this article is sourced to the interviews, regardless of whether that content has been summarized, paraphrased, or directly quoted.

Identifying Key Indicators

Participants were asked to provide input on indicators across two categories—intent and capability—and they were asked to identify the top five indicators or metrics for each category. Before highlighting those responses, it is important to outline points of caution and challenges that were raised by some interviewees. To be clear, there was no consensus among experts on this front, but the points they raised about this approach itself were thought provoking. For example, several interviewees highlighted how the variation of potential indicators can be so wide and dependent on so many variables that there is a danger that a prioritized list of key intent and capability metrics might not hold much practical utility.

Other interviewees argued that there is, in fact, a path to finding utility in this exercise, but, to summarize one participant's perspective on this, "We want this indicator and warnings enterprise to be easier than it actually is. We want the checklist of the five things we need to look for, and we want the score that tells us if there is a threat or not." But, as they pointed out, the reality is that it is much more complex than that and there is no one set of indicators that will predict the output. The challenge is that there are multiple sets of indicators displayed by different entities and multiple pathways to the same result. So, one has to embrace the entire universe of indicators and not fixate on one set path of factors arranged in a linear, causal pattern. The only way to do this is by using tools and models that incorporate many more indicators, not a top five or 10.

Another challenge this same participant highlighted is the fact that there is "an inverse relationship between the diagnosticity of indicators and the likelihood of us observing them," meaning the indicators that are the most diagnostic in predicting the adversary's future behavior are typically the ones we are least likely to pick up on. And, inversely, the indicators we are likely to see are typically the least helpful in predicting future behavior. Therefore, it is only when we see "constellations of indicators pointing in the same direction" that we should heighten our attention.

Another practitioner suggested that such an effort to identify indicators at the terrorist group level is especially challenging in today's environment given the prevalence and rapid spread of both lone attackers and inspired attackers. Identifying indicators for lone actors is a fundamentally different and a more challenging exercise. This practitioner's warning is that we should not assume that we have an easier job when examining a group's decision to

[a] The authors wish to provide their sincere gratitude to all those who participated as interviewees for this project. This includes eight anonymous contributors, in addition to Gary Ackerman, Marc-André Argentino, Mustafa Ayad, Nicholas Clark, Colin Clarke, Bennett Clifford, Alex Gallo, Gary Greco, Jim Griffin, Daniel H. Heinke, Scott Helfstein, Amira Jadoon, Matthew Levitt, Tony Manganiello, Erin Miller, Petter Nesser, Vidhya Ramalingam, Alexandre Rodde, Yannick Veilleux-Lepage, Charles Winter, Juan Zarate, and Aaron Zelin.

MIR AIMAL KANSI murdered two persons and injured three others, then fled the United States. U.S. law enforcement is offering a reward of up to $100,000 for information leading to his arrest. Private citizens and organizations in the U.S. are offering substantial additional reward money. The identity of anyone providing information will be held in the strictest confidence.

قام الأرهابيون الذين فجروا مركز التجارة الدولي
في نيويورك بقتل ستة من الأبرياء، وجرح أكثر من
١٠٠٠ آخرين، وتركوا أطفال المدارس المروعين
محتجزين لساعات داخل المصعد. وقد هرب المشتبه
في قيامه بالتفجير عبد الرحمن ياسين من الولايات
المتحدة وما زال حراً طليقاً. وستبقى حياة الأبرياء
الآخرين مهددة طالما بقي ياسين حراً. وتقدم وزارة
الخارجية الأمريكية مكافأة تصل إلى ٢ مليون دولار
مقابل تقديم معلومات تؤدي الى القبض عليه. فإذا
كان لديك معلومات عن ياسين اتصل بالسفارة أو

Matchbooks depicting several terrorists, including Ramzi Yousef who perpetrated the 1993 World Trade Center bombing (Jeffrey Markowitz/Sygma via Getty Images)

conduct an external operations attack, because in this current environment, that group is more likely to incorporate the use of inspired individuals into its attack strategy.

Despite these cautions and caveats, a number of overarching themes and commonalities were present across the interviews. The overarching theme seen in answers across both the intent and capability categories was change: Any kind of change in activity or behavior by a terrorist group should be noted, monitored, and examined more closely to determine what is driving that change.

Intent

On the question of how one can identify a change in a group's *intent* to conduct an external operations attack, two categories dominated the responses: They will show you and they will tell you. For the former, they will show you in their operations and in their organization's activities. This point highlights an inherent overlap between intent and capability, as different participants drew different boundaries between those two categories. For example, identical indicators appeared in the intent category for one respondent and the capability category for another. Several respondents identified this overlap explicitly, pointing out that the development of specialized capability is a major indicator of intent. For the sake of streamlining this article, all discussion of capabilities has been consolidated in the next section, even though many participants highlighted these during their discussion of intent.

The most cited indictor of a change in a group's intent is that they will message their intent in their media and other communications. While this seems to be an obvious and simple statement, interviewees believed it to be an underappreciated fact, perhaps because it seems *too* obvious. Various interviewees held the view that when groups tell us plainly what their intentions are, in far too many cases they are not taken seriously. In other cases, the statements may be believed, but insufficient action is taken in response, for any number of reasons. Out of the 30 participants, 21 highlighted this as an indicator of primary concern. As one interviewee stated, "We always bend over backwards looking for these magic tricks to figure out who these groups want to target and why and when. But 70 percent of the solution is just reading what they're saying they're going to do. And I think we often fail to do that."

The most notable example of a group clearly stating its intent is al-Qa`ida in the 1990s. Usama bin Ladin was prolific in publicly announcing his intentions. He gave interviews to Western media outlets, he issued public statements, and he held press conferences, all articulating not only his goals for the group to target the United States and its interests, but also his detailed rationale for doing so. The most famous examples of this are two *fatwas* that al-Qa`ida released in the late 1990s: the August 1996 "Declaration of War against the Americans Occupying the Land of the Two Holy Places" and the February 1998 "Jihad Against Jews and Crusaders." The latter was followed shortly by the August 1998 East Africa embassy bombings, al-Qa`ida's first major direct strike against the United States. It is important to note that while bin Ladin's statements were not taken seriously enough at the time, it would be unfair to suggest no one was listening or that no one appreciated the threat. Some in the U.S. government did. These statements, in conjunction with the group's early attacks, famously resulted in numerous intelligence reports in the run-up to 9/11 highlighting the group's intention to attack the U.S. homeland. But, as the 9/11 Commission Report makes clear, these were not sufficient to drive a real appreciation for the threat al-Qa`ida posed and a significant policy focus on the group.

So why, despite learning this lesson and despite the tragedy of 9/11 and the proliferation of jihadi activity since, does it remain so difficult to make sound decisions and accurate assessments based on the words of our adversaries? A partial answer to this question is that in the ensuing years, the jihadi propaganda landscape has become so saturated with content that the challenge is no longer simply convincing leaders to pay attention. The challenge instead has become distinguishing the legitimate threats from all the noise. As a more recent example of publicly stated intent, several interviewees pointed to Islamic State Khorasan's (ISK) media releases prior to its attack on the Crocus City Hall in Moscow in March 2024. Many in the media expressed surprise at this attack, despite the fact that ISK's media had been overwhelmingly focused on Russia for at least two years prior. Since the start of the war in Ukraine, ISK had been releasing numerous products celebrating Russian misfortunes and calling for attacks on Russians.[4]

Adding to the complexity of what, on its face, seems an obvious indicator, is the fact that statements of intent are not always as blunt as the examples just provided. Sometimes, the verbal indicators of an impending attack are less explicit and analysts have to read into the language of our adversaries to see the threat building. One participant highlighted the example of the 2006 al-Askari mosque bombing by al-Qa`ida in Iraq (AQI) in Samarra, Iraq, pointing out that analysts failed to appreciate that AQI's consistent anti-Shi`a rhetoric actually meant something, and therefore missed both this specific attack and its importance as a precursor to future events.

Several participants advocated for more nuanced assessments of terrorists' public statements and identified specific media indicators to look for that could point to terrorist expansion. From a U.S. perspective, as one interviewee described, most significant would be a noticeable uptick in a group's anti-Western rhetoric or more commentary on Western issues or themes. This could include specific references to U.S. government officials, linking local adversaries to the United States or other Western governments, or attributing various regional crises to Western actions. An increase in magnitude of media content of this type, especially in Western languages, would be cause for concern.

Another change to take note of would be a shift in rhetoric from more aspirational or ideological content toward more action-oriented goals and directives. As one participant stated, "With Hezbollah, Hamas, and ISIS, and even groups such as Atomwaffen, prior to them doing attacks we've seen the rhetoric change from mobilizing individuals to 'this is how you carry it out, these are the tactics that you need to use.'" In general, analysts should also be looking for changes not just in the content of these messages, but also changes in language, changes in tone, and changes in sentiment. Of note, numerous tools exist for measuring those types of nuance.

While public statements and the development of capability were the two most cited categories of indicators of intent, the remaining indicators can be sorted into three categories. First, participants highlighted the role of broader environmental factors that analysts should pay attention to if they appear to be occurring in a terrorist group's home region. Within this category, the most mentioned indicator was having a U.S. policy or perceived provocation impact their primary area of operation. Certainly, for jihadi groups, any U.S. military action in a group's region is an indicator because it could likely lead to intent to attack U.S. interests or speed up that process. Any perceived provocation is something that an organization can use as an opportunistic tool to motivate an intention to attack beyond their typical area of operations. As an example, one respondent pointed out that when it came to the November 2015 Paris attacks and the March 2016 Brussels airport attack, the intent to launch those attacks was a direct response to U.S. and allied counterterrorism pressure in Syria. Any setback like this in their primary area of operations can provide an impetus for a group to compensate by attacking abroad. As highlighted by an interviewee, a key way to regain power, to regain influence, and overcome loss or humiliation is to attack in a way you have not before. Other environmental factors that could prompt an external operations attacks include shifts in the geopolitical environment, disruptive economic factors, and local governance issues.

The next category of indicators of intent is organizational dynamics, chief among them being leadership changes. This could be an actual change in leaders or a change in existing leaders' behavior. If a change in style or level of aggression is apparent in the leadership of a terrorist group, this could be an indicator to examine more closely to see if it has or could translate into a change in targeting. And of course, if it is an actual change in leadership, that would be something to monitor. A new leader might have a different ideological perspective that drives them to focus more globally. Or they might be looking to solidify their new status with a demonstrative act showing their strength. Another organizational factor that interviewees cited as indicative of a change in intent to conduct an external operations attack was any shift in external allies or rivalries. New allies might be more inclined to target new geographic regions, which could influence the group in question. And new rivalries might result in outbidding strategies to win support in their constituency, with the group expanding its target set to demonstrate power and authority. A particularly dramatic organizational dynamic is when a portion of a group splinters off to form a new group. One participant highlighted these splinter groups as being especially dangerous due to their tendency to conduct a large attack shortly after splintering off, possibly to "put their stake in the ground," and legitimize themselves to their constituency.

The final category of responses centered on past actions as indicators of future intent. Do the group's attack and plotting history indicate a potential shift in their focus to a target set beyond their traditional area of operations? If we go back to Milton's expansion framework, while the focus of this study is predicting attacks conducted outside a group's existing area of operation, attacks on a foreign embassy *inside* that area could be a clear indicator of intent and potential to expand geographically.[5] Any shift toward targeting a foreign presence locally and regionally could indicate a broader change in strategy to one that involves international external operations. For example, the February 2022 attack by ISK on the Russian Embassy in Kabul should have served as a stark warning to the Russians of what was to come two years later in Moscow. Finally, several participants emphasized that tracking and assessing plots is equally important as tracking actual attacks.[6] Attempts are just as important as successes in illustrating interest and potentially capability, especially if they use failures as learning experiences for the future. Staying with the ISK example, while everyone paid a lot more attention to the group after the Moscow attack, there were several well publicized arrests in Europe, going back for over a year,[7] that should have been given more credence to the organization's intent.

Capability

Participants in this study described a wide range of potential indicators of a change in a terrorist group's capability to conduct an external operations attack. Given the breadth of perspectives offered, it is not possible to examine each in sufficient detail here. This section instead will highlight and provide a brief description of those indicators mentioned by respondents most frequently. The categories below are presented in order from the most cited to the least cited.

Personnel and Recruiting. Almost every respondent mentioned acquisition of the right people as a critical indicator of capability, making it by far the most commonly cited indicator. If a group is looking to expand its operations beyond its local area, it will need to acquire the right people with the right attributes. Terrorist groups often conduct deliberate recruiting campaigns as part of an outcome-driven personnel strategy. As one interviewee pointed out, the Islamic State was well known for recruiting in this manner, especially for its media operations. It would seek out special skill sets and offer incentives to people who had a background in media operations. But it did not limit this activity to its media work. As part of its personnel intake process, it would highlight individuals who had a wide range of needed skill sets, from medical training to military experience to computer hacking.[8]

Experience in the region where the group aspires to operate is a critical attribute, and efforts to recruit that experience are therefore an important indicator. For jihadi groups in particular, an observable increase in recruitment efforts aimed at individuals with Western ties or even at U.S.-based sympathizers may indicate the group's interest in external operations in the U.S. homeland. Similarly, U.S. or Western persons elevated or incorporated in an organization illustrates the group leadership's interest in them and likely also that person's home country.

We see these dynamics occurring in other regions, too. For example, as ISK turned its focus on Russia, it targeted Central Asians for recruitment. As one respondent pointed out, from 2018 onward, radical preachers in Afghanistan made a shift in how they marketed themselves, switching from Pashto and Dari to Cyrillic languages targeting Central Asian populations. This group included a half a dozen Afghan preachers who rebranded themselves to this different market. They played an important radicalizing role, and their audience shift was an important missed indicator.

Acquiring access to personnel who have familiarity with a target country and who can therefore serve as key enablers provides significant benefit to a group planning external operations. Local operators have local knowledge and local access, and bring a savviness to the table that cannot be matched by foreigners who tend to struggle to plan in an unfamiliar environment. It is for this reason that terrorist groups often try to connect with local criminal networks for access to weapons and other resources. As noted by an interviewee, the Islamic State regularly worked to recruit European jihadis that had a criminal background that was useful to it.

Movement of People. Closely related to the recruitment of personnel is the movement of personnel. A critical indicator of external operations is when members or affiliates of an adversary group are found to be traveling to a region outside of their usual base of operations. As several interviewees pointed out, when operatives begin moving across borders, particularly into countries with U.S. interests or allies, this can indicate the final stages of planning for an external operation. The movement of senior operatives with a history of orchestrating attacks is especially telling. So, the indicators could include, for example, patterns of travel, meetings of key members, changes in residence, new travel and/or smuggling routes being used, intercepted communications indicating travel instructions issues by the organization, or a new ability to forge or obtain travel documents.

Given the points made above about personnel movement and the appeal of recruits with local knowledge, foreign fighter flows should be of significant interest to those looking to prevent external operations in their country. This would include monitoring individuals leaving the country in question to travel to a location where a jihadi group is active, and carefully tracking efforts by those same personnel to return. Numerous interviewees discussed the significance of uncovering a growing number of travelers returning from conflict zones. This seems like it would be an obvious red flag, but the previous decade saw several cases where returning foreign fighters were able to successfully infiltrate back into their home countries or regions and conduct attacks.[9] Perhaps the most glaring examples would be the 2015 Paris attacks, when European security personnel missed or underestimated the growing number of French returnees who had no reason to return other than to attack. This return of foreign fighters proved to be more coordinated than expected.

Finally, several participants highlighted the recent changes in global migration trends, which have provided increased opportunity for terrorist organizations to move people into presumed target locations. The challenges along the southwest U.S. border highlight these dynamics. As the migrant population has significantly diversified and includes increased numbers of people from regions beyond South and Central America, the numbers of Special Interest Alien encounters at the border have gone up, as have encounters with Known or Suspected Terrorists.[10] This challenge was publicly highlighted with the recent arrest on immigration charges in June 2024 of eight Tajikistan nationals with suspected ties to the Islamic State who had crossed into the United States through the southern border.[11]

Training and Access to Territory. Training is a key indicator of attack planning. This article already discussed recruiting for specific skill sets, but the other way to acquire a desired capability is through upskilling existing personnel. The classic example is the 9/11 plot, when considerable effort and risk went into getting flight training for certain hijackers. This activity was risky because it exposed the hijackers to possible discovery by raising their signature.

Testing and conducting dry runs are another training activity that can serve as a key indicator. As one respondent highlighted, for example, prior to the October 7 Hamas attacks, Israel observed Hamas operatives practicing breaching the security fence. This interviewee also cited the Japanese Red Army who, when they first hijacked a plane, rented out a conference hall and organized all the chairs like the layout of an aircraft and practiced moving around in that space.

Access to space to train and plan was also highlighted by numerous interviewees as a key indicator. When a group has territorial control in a relatively permissive environment, it can establish infrastructure and training camps. Having this safe haven can help to build capability, culture, cohesion, and group bonds. A related indicator of a group looking to expand its operations is if it is using these training spaces to transfer innovative technical knowledge. Are new recruits being paired with experts to learn not just basic fighting skills, but also knowledge that would be useful in external operations? For example, learning how to turn an artillery shell into an improvised explosive device is not useful for an attack in New York, but developing explosives using commercially available products is. Analysts should also be looking out for any changes in how training camps are being structured and organized, or any changes to the content in captured training manuals, as these could indicate changes in strategy and targeting.

Acquisition of Material and Technology. The next most commonly cited indicator of development of capability for external operations is the acquisition or development of weapons and resources well suited for attacks in the target country of concern, such as the United States. This is typically assumed to mean increasingly sophisticated capabilities, such as specialized explosives or drones, but it does not have to be. It could be something as simple as truck rentals given the prevalence of vehicle ramming attacks in the West.

Attempts to connect with criminal organizations are also indicators of note, as several participants pointed out. For example, in the 2015 Paris attack plotting, the ability to accumulate a significant amount of weapons in a European country with significant restrictions on weapons acquisition was a surprise. A historical assumption by some that terrorist groups would not use criminal groups for logistical support was unfounded.

There are also key indicators regarding weapons acquisition to be found on the internet. According to one interviewee, there are locations that are easier to access than is often assumed where individuals talk about weapons capabilities, innovations, and blueprints for making things. The key is to then monitor those locations and look at how those innovations are or are not being implemented. You might witness significant conversation "… about 3D-printed drones or 3D-printed guns, for example, but if you don't see any actual manifestations of that kind of theoretical capability in the physical domain, then obviously that should temper one's assessment of the threat from bad actors using that kind of technology." So, according to this participant, the indicator would be an increase in or an emergence of a new trend or dynamic or focus on a particular technology and pairing that up with what is happening in the physical space. They added that there is a very significant community of jihadis swapping views and tips in one of these channels on how to build explosives and what kind of precursors are easiest to work with. The availability of this information is something to have on the radar from a counterterrorism perspective, not just because it is available to the adversary, and that means that there is a threat derived from it, but also because it is available to monitor from an interdiction perspective.

Movement of Funding. Another important category of indicators of capability is funding and the movement of financial resources. As groups expand their geographic footprint and explore external operations, they will inevitably have to move money. Steps participants highlighted that groups might be taking as they expand include, but are not limited to:

- Diversifying funding in order to have access to multiple sources of funds (e.g., extortion, donations, legitimate businesses);
- Moving funds to target areas;
- Exhibiting growing sophistication in moving funds (e.g., using modern technologies such as cryptocurrency, mobile banking, etcetera, in addition to more traditional mechanisms (e.g., *hawala* system, donations));
- Establishing structure to provide financial support to families of members, and;
- Ensuring sufficient cash flow in the run-up to an attack

Other Capability Indicators. Interview participants discussed a host of other interesting and useful indicators of changes in an organization's ability to conduct an external operation. There is not sufficient space here to describe them in detail, but they include research and surveillance of targets, group infrastructure development, operational leadership changes, cyber and CBRN capability development, smuggling networks for key materials, and communications going 'dark.'

Examining Challenges and Shortfalls

The prior section focused on 'what to look for'—the range of indicators that can signal that a group may be expanding its focus and/or planning an external operations attack. This section summarizes several key challenges and shortfalls that interviewees believed hampered, and in many cases still hamper, I&W efforts.

Information Overload

Most of the interview participants seemed to agree that while there are certainly new sources of data that should be exploited, the primary failures in the past were not due to lack of information. In most cases, the data was available, but the challenge was being able to sort that data and correctly assess it. So while the counterterrorism community is effective at collecting large amounts of data, it needs help sifting through it to separate the signal from the noise. As one participant stated: "You're almost a victim of your own success. Like, yeah, we're great at collecting data, but are we good at analyzing it and picking out trends and patterns? And I think that's where we're still a little bit behind the eight ball."

While artificial intelligence and machine learning tools have been explored to help with this challenge, the consensus in this study was that much more needs to be done. One interviewee pointed out that even the most capable and resourced agencies have a backlog and struggle to triage due to the magnitude of the data. As one interviewee stated, "the volume of data [is the] hardest challenge set for me as an analyst. Information overload is probably the biggest issue. There's so much potential information out there. The vast majority of which isn't useful, but still needs to be looked at, and that's a critical issue."

A related challenge is the lack of time spent prioritizing. Too often, all this data is treated as equal instead of being appropriately weighted. There is a perceived lack of an analytical framework through which indicators can be 'racked and stacked' according to priority, risk, and relevance.

There was also the view that the community struggles with looking across categories of indicators and sources of data, and there is a tendency to look at them in isolation instead of looking at how they interact with each other. According to one participant, "Our intelligence community takes in a lot of information and we vertically read it, meaning we value each information as if it's the same. We read it literally from top to bottom about the [specific] group [in question], instead of looking laterally and trying to make connections across information. And because we vertically read, we miss the dot [and therefore can't] connect the dots to the picture. We get lost in the data instead of laterally reading and being able to paint a picture. That picture becomes a hypothesis that you can test over time, and you can find out if it's valid or invalid."

An additional challenge to the data sorting problem is classification. One participant highlighted this issue, pointing out that "when you have data that exists at multiple levels of classification, and there has to be an air gap between them, you are slowing down the collection of the data, which slows down the analytics, which slows down the answers to the questions, and that could allow the enemy to get into your decision cycle." This individual pointed out that there is actually commercially available data that is just as good as the comparable government source, but does not sit at the classified level and is therefore easier to work with in various tools.

There was one exception to the information overload problem that was highlighted by several participants, and that is the reality that the U.S. military is no longer in as many forward deployed locations, and therefore has reduced access to information from critical sources that were relied upon in the past. As one participant noted, "We're being asked to do more with less. The community is being asked to identify all kinds of threats, for example, from ISK, but to do so at a time when we're no longer on the ground in Afghanistan and we're no longer flying drones over Afghanistan, like we used to. So we're being asked to have better indicators and warning with fewer inputs and so, at a minimum, then you have got to be able to do a better job of mining what you have."

Insufficient Information Sharing

Another issue that impacts the identification of indicators of external operations is a continued struggle to effectively and sufficiently share information. Numerous study participants identified this as a remaining concern, over two decades after 9/11 and the lessons the community learned about the consequences of a failure to share key information. Some suggested that significant improvements had been made in the aftermath of 9/11, but that in the years since, the community has suffered backsliding, especially as counterterrorism became less of a priority in the United States. As one participant describes: "Frankly, I am really surprised how siloed up we've become again, and how often [we] have to fight for information. I was disheartened to see how we've fallen back on pre-9/11 ways. A lot of what's going on today is in different reporting channels [and information may be held separately]. You know, it's not like anybody's doing it on purpose. It's just organizations—that's what we do. We close up. We try to hold what's near and dear to us. And I find that very sad." Another participant pointed out that in reality, most agencies are not incentivized to cooperate and share.[12]

Information sharing requires improvement across the full range of relationships. An area cited by multiple interviewees was international information sharing, with several people pointing out that there is a gap internationally in what partners are willing and/or able to share. Here are a few examples shared by participants:

Sharing of information between nations and agencies was not necessarily flagged regarding people traveling to Syria during the height of the Islamic State's so-called caliphate. And the same was the case for cross-border movements in general and communication between leadership.

There was a lack of intelligence cooperation between Belgium and France in the lead up to the 2015 Paris attacks. This was due to poor communications, lack of capacity, and lack of political will.

In the lead up to the 2019 Easter bombings in Sri Lanka, India did in fact share useful intelligence regarding the planned attacks, but the information was not trusted or acted upon in Sri Lanka.[13]

Another avenue for increased information sharing would be between intelligence and law enforcement agencies, especially local law enforcement. Participants stated that while there are laws and regulations that necessarily govern, and at times limit, this sharing, more can be done to change mindsets and break down barriers. The focus on local law enforcement was due to that community's role in being the initial touch point with terrorist actors conducting activities out in communities. A European interviewee highlighted how local police in certain locations do not get the full picture due to overclassification, and are often told to take certain actions without being given context. For example, "[Federal] police do not share that the cellphone of an individual is what would be most helpful, and this has created some gaps and seams, where local police do not understand that this is key, which has created opportunities for suspects to wipe their cellphones." There is a need for more sharing and more context and detailed instructions to be provided to local law enforcement.

Analytical Failures

Information overload and insufficient information sharing both hamper analysts' ability to effectively assess threats and identify indicators of terrorist expansion and interest in external operations. As we look back on the past few decades, there are unfortunately numerous examples of analytical failure, driven by various causes. Study participants highlighted several of these as indicative of the challenge.

One participant identified the attempted Christmas Day 2009 AQAP airline attack as an analytic failure: "We had assumptions about how a terror group operates. It was a major analytic failure. The FBI indictment outlines what we knew soon after the attack. The FBI and others had access to useful data prior to the attack. What we missed was the intent piece. AQAP looked at the time like a regional threat. We were seeing signs that a person of a certain background wanted to meet Anwar al-Awlaki. The [bomber's] dad was also raising concerns about his son being missing. Signs were there before … There were examples of AQAP attacking regionally: the attack in Saudi Arabia that tried to kill Saudi prince Mohamed bin Nayef, which ended up only killing the attacker, but it was not clear that AQAP had an intent to attack the [U.S.] homeland. Individual level intent indicators for [the bomber] were missed. Group intent indicators were less clear."

Another respondent also highlighted this case, but stated that there were signs of AQAP intent, but that they were not accurately assessed: "One that definitely comes to mind most probably is AQAP's emergence in 2009. I mean the group certainly had been violent …, associated with lots of attacks on the Arabian Peninsula. But in their public messaging … the group was very explicitly talking about … the United States as the adversary, as the key, as a prime enemy. It just was not recognized that if we're the prime enemy, you're not going to get that many good targets in Yemen. So, it's the public statements for that group that were not missed. We knew them, but we just didn't really weight them accordingly."

In addition to struggling to discern intent, analysts have also, at times, been hesitant to break away from orthodox thinking about key threat actors. An interviewee broke down this challenge: "You have the Madrid bombing where … the actors were known to the Spanish authorities. Part of the problem was different parts of that network and cell were known to different parts of the [government], and part of that had to do with what they were being looked at for, so there was part of the group being looked at for terrorism, the other part being looked at for petty crime and drug trafficking. And the problem with that was not just that they weren't talking or there weren't mechanisms … it was more about the assumptions and the silos of how we classify these groups. And so if this is a drug trafficking gang, you wouldn't imagine that they would be part of a broader international terrorism plot. So it's clearly failures of, as they say in the 9/11 Commission report, imagination. We tend to have orthodoxies as to how we think about how these networks operate. It's the folly of thinking of these worlds in binary ways that really then leads to challenges, and I think if we're not careful, we don't see merging relationships that matter. So, Russia with the Taliban when we were still in Afghanistan. Iran facilitating al Qa`ida leadership despite the longstanding rivalry and suspicion. Hezbollah and drug trafficking organizations, despite whatever is pronounced morally about this. These assumptions that we build in that reinforce silos and orthodoxies as to how these groups are supposed to operate creates huge challenges for when they're operating in ways that we're not assuming, and [they] are breaking those silos. And [when they] break those silos, we're not seeing … the threat."

Several participants identified a lack of appreciation for jihadis' commitment to the cause as a prior and, in some areas, ongoing issue for the counterterrorism community. This would be another example of an analytical failure. One interviewee provided a particularly comprehensive description of this issue: "[Regarding] the element of strategic surprise, you look at Hamas on October 7th. You look at the Paris attacks. You look at some of the attacks in Moscow. You look at the rise of ISIS in different parts of the world, including in Afghanistan and in East and West Africa. What strikes me as pretty consistent is an underestimation of the continued intent of these groups to bring to life global ambitions, and the ferocity of their ideology. It's not just local, and then maybe global; it's both. And I think there is a lack of appreciation for that embedded global jihadi DNA in many of these groups. [We failed to see] how committed some of these groups are, how committed they are to take advantage of lack of governance, how willing they are to bring to light their ambitions. I think that was the folly in the rise of ISIS in Iraq. It's the lack of appreciation of all of that. And I think [we] failed then to appreciate the extent to which they would go to achieve those means, both in terms of creativity, in terms of persistency, and in terms of overall commitment."

Another participant highlighted how the same lack of appreciation challenge also existed two decades ago: "We didn't understand the whole Egyptian connection through the blind Sheikh and what we … totally got wrong, and I would contend we still get wrong today, is we failed to see their ambition of what they wanted to do. We looked at this as a joke that they went to parking lot and blew down a parking lot … [W]here we didn't really understand, or we didn't give it enough thought and credit, is looking at strategy and ideology." The same individual recounted *Time* magazine's interview with bin Ladin in May 1996 in which "he talked about defeating the West. And I can tell you people were laughing at that … Then we have East Africa. We have the Cole … by that time maybe we have to take these guys serious. But it's already too late."

As we look ahead and think about how to prevent analytical failure, the challenge could increase the further we move away from the post-9/11 period and the operational tempo of that period. As one participant stated, "We have a whole new cadre who have not experienced transnational plots and attacks. So, the problem is compounded by the diminishment of expertise. We need more robust training that incorporates case studies of prior attacks, particularly cases studies that are not as clear." Another interviewee highlighted the need for additional training and education to address the lack of ideological understanding, which he stated was a factor in at least one significant U.S. jihadi attack.

This section provided a summary of the most prevalent examples of areas where the counterterrorism community experienced shortfalls in efforts to execute the indicators and warning mission regarding terrorist external operations. While not comprehensive of all the interesting input received from the study participants, it offers a useful starting point for the subsequent section on how the community can improve its capabilities.

Proposed Solutions

The interviewees offered up a diverse and fascinating list of ideas for how to enhance I&W efforts for terrorism. While there were too many to include here, this section has identified several categories into which the most common ideas have been sorted, offering a consolidated assessment of the most significant steps that can be taken to enhance I&W for terrorist external operations.

Artificial Intelligence and Machine Learning

Given that the most commonly mentioned challenge was an inability to sufficiently sort and assess all the available data, it comes as no surprise that the most discussed solution to that problem was artificial intelligence (AI) and machine learning (ML). Almost every participant made some mention of AI as part of their answer for how to effectively find and exploit data to identify and disrupt terrorist external operations. Most believed that the combination of the information overload challenge discussed above with the realities of diminishing counterterrorism resources is tailor made for an AI solution. To summarize the challenge, there is a large amount of available data, but insufficient means to triage and sort it, and then analyze it to identify trends and patterns.

Using AI/ML approaches and tools to process unstructured data can massively scale the abilities of analysts to do the high-value analytical tasks of reviewing patterns, new abnormalities, and in assessing 'so what' implications rather than those analysts spending time on collecting, processing, and cleaning data. As one participant stated, "It really is a factor of being able to, at a much faster pace, review much larger volumes of information to be able to give you more timely results. But the other [factor] is the ability to then act on that and when you see patterns to be able to maneuver your platforms. We can't be everywhere all the time."

Another interviewee summarized the goal: "You create systems where these analytic tools that are deployable that allow analysts … the ability to constantly query, and to dynamically access datasets in ways that will give them earlier and earlier indicators of potential risk. It's moving further and further left of the moment of the act terrorism."

Despite universal identification of AI/ML approaches as a key solution to CT-related data problems, most interviewees agreed that we should "approach the space with caution" and only use AI "in a reasoned and limited and very tightly constrained way." The consistent message was that AI and ML should not be seen as a panacea. AI can sort the data for you, but there was the view it cannot reliably answer the questions you are trying to answer. Or in other words, it is only going to get the community so far at this moment in time.

As numerous respondents pointed out, it is critical to keep a human in the loop. "I think there is a really good case for exactly why humans need to be involved in this process. We live in an age where technology can speed up so much stuff and that's great. Whether it's collection of data, cleaning of data, processing of data, visualizing of data, so on and so forth. So it's kind of identifying and having dynamic alerts to indicators that emerge within a given ecosystem. But it's not enough to just rely on a machine to do all of that stuff; I think you need to hardwire [human] expertise in a dynamic way into what machines are working with, what they're doing, what they're trying to do. So I think especially as you're dealing with a dynamic kind of environment, the humans need to come in there to push the machines in the right direction with their intuition of how the environment is changing." As another participant summarizes, "[This technology gives you the] ability to move algorithms to look for signals of risk that then allows humans to go hunt for what the problem is."

Participants suggested that these humans in the loop should be both the traditional intelligence analysts and data scientists. Agencies should recruit and maintain qualified people to integrate quantitative methodologies into how we analyze and understand the threat landscape. Qualified data scientists can work with AI tools to ensure models are appropriately developed and managed. "I think that as we have more data sources and have more tools to leverage, we need to not lose sight of the fundamentals and the fact that these models can't run on themselves. They need something concrete at the ground truth to feed into them, to come up with any kind of pattern matching or anything like that. And so I think we certainly do need to continue to invest in the data collection, the original inputs to these things, and also make sure that we're leveraging AI tools in a way that has a healthy skepticism for what they are and are not capable of."

While highlighting the critical role AI can play in enhancing counterterrorism efforts, interviewees also cautioned that governments do not have a good track record of efficiency or innovation in this field. They argued that government moves slowly in this space, while the private sector drives forward, and so the government is at a disadvantage. As one interviewee pointed out, governments cannot afford to be five years behind on technology development, but are hindered by numerous regulations and restrictions governing how they acquire and use technology. One participant expressed frustration with this process: "You know you have to go out to a vendor and that takes how many months? Also, the vendors that the intel community or the government is willing to take risk on are usually a big, typical Beltway provider … that's not the kind of company that has the skilled, technology savvy workforce to be able to do the kind of technology development that you're talking about. We still haven't figured that out. I see it all the time. You have these big vendors, and I'm like, 'That's not what they do. Why did we hire them to do some type of software development? That's not what they do. They give you butts in seats who rack and stack data that they don't develop.'"

Data Prioritization

If the general consensus of this study's group of experts is that the counterterrorism community needs to leverage automation to sort and help make sense of data, but maintain the human role to direct this effort, that raises the question of what principles should be used to determine how they direct it. There are two key variables that impact the answer: first, the massive amount of available data, as discussed above, and second, an environment of diminished counterterrorism resources.

The way to balance these conflicting variables is through prioritization. One interviewee walked through how he thinks about this challenge: "I think the challenge in the size and scale of the data now is if you look everywhere, you look nowhere. If I was asking, 'How are we going to get after this?' it's to make that big data problem a little bit smaller and to pick a couple of key metrics and you record that over time and you figure out what normal looks like first. We [then] monitor the same thing over time. Once we jump out of that tolerance, we then have to dig into it a little bit more. I think right now the CT community is no different than a lot of other communities in that we have so many tools and data at our fingertips that we become overwhelmed with it, and we try to try to eat that entire elephant without realizing that most of the data is irrelevant. We end up neglecting the big things to try to chase all the small little what-ifs. We need to focus and do fewer, better. Right now the problem I think is too big if we try to take on everything."

Another participant made the same point about the need for greater prioritization and focusing of the large amount of data in analysts' possession, but tied it to the resourcing challenge: "I think it would be far better to direct resources to high priority targets with greater threats attached to them. Be a bit more selective with what we attach resourcing to, and I think that perhaps also applies in terms of divisions of labor between organizations as well. It's no good [to have] organizations duplicating everyone's effort. I think there needs to be clear responsibilities attached to individual organizations, so that there isn't wasted effort. [Previously], we didn't have to prioritize as much because we were present pretty much in all the key locations. Now as it gets smaller, both on the collect side and the operation side, the ability to move something quickly is going to be even more important, and I think that's a challenge coming to grips with, particularly in the U.S. Department of Defense, which has got an awful lot of capacity, but it takes time to turn."

Collaboration and Information Sharing

Given the discussion above about backsliding when it comes to information sharing, numerous study participants focused on addressing this challenge in their answers to the questions about how to improve indicators and warning for external operations. One interviewee proposed the establishment of a common framework of indicators and warning for external operations across the community, because without a framework to guide the effort it is hard to be more dynamic, or embrace more dynamic approaches, as you do not have a place to hang or to situate data across the community. This individual added that: "Everybody has their own set of indicators. There is a need for something like the MITRE framework for cyber attacks. Everyone [in that community from public to private] has the same starting point. The ideas are there but operationalizing that type of framework is a key issue, as unless ODNI [Office for the Director of National Intelligence] or the NIC [National Intelligence Council] direct it [or lead it] it likely is not going to happen."

Another participant commented that the answer to the information problem "would be more collaboration between silos, whether that's between nationalities, government and business, government and education, CT experts and regional experts, [oriented around] trying to leverage collective resources of those who are still working the problem set. [An important] caveat to that, of course, is that that collaboration is all easier said than done. It takes time and effort from an individual analyst perspective. To get something up and running and sustain it. And it also, quite crucially, requires organizational leadership, buy in, and support. Which aren't necessarily a given. So, it's really difficult, and it is a big challenge ahead of us to sustain momentum, if not increase it."

Increased international collaboration was advocated for by numerous study participants. This would include intelligence, law enforcement, and outside experts. Liaising with counterparts in partner nations is critical in the current environment as partners may have greater access to on the ground networks in places overseas where U.S. footprints have been reduced. There was even discussion about the creation of some kind of centralized hub that could include non-traditional entities like researchers and NGOs that have data and collect on, monitor, and track various movements. Finding a way for law enforcement to connect with these sources would add significant value. A similar idea advocated for the creation of and investment in a system that pulls from and compiles court records from different countries and makes those centrally available.

Many interviewees held the view that the private sector is a resource with significant value that must be connected to the indicators and warning network. As government collection has gone down with the reduced footprint, private sector collection has gone up. So, how can government best take advantage of and use data from private sector? As one participant pointed out, academia does this better, in part because they are not shackled by the same regulations and restrictions, but also because they do not have the same institutional bias the government has that government data sources are better and more reliable.

But government must do better because, regarding indicators and warning of external operations, as one participant stated, "there are signs and signals in the international system often seen by the private sector or sensed by the private sector much earlier than government. [For example], I've often said that we need to think about networks of human sensors or even technical sensors at ports to be advanced warning signs as to what they're seeing, changes that they're seeing, risks and suspicions that are being raised. [In addition], insurance companies are often seeing signals in the marketplace of changes because they have to. They've got to monitor these things. Certainly, we do that with banks to a certain extent with the compliance teams and the chief risk officers or the chief security officers in major multinational corporations, which, by the way, are often former Secret Service, former DIA, former FBI anyway. Those are all human sensors and networks that we don't fully leverage, and we need to think about that networked capability. You're not talking about coopting the private sector, but it's more than just a conference once a year to talk about trends. We're talking about some degree of operational connectivity, where the private sector is feeding into the government while government analysts are looking at their data and trying to analyze it dynamically."

Alternative Models

In addition to specific ways to improve indicators and warning, participants were also asked to think creatively about any approaches or models used by other industries or fields that could inform and help improve existing government I&W approaches. A wide range of ideas were offered by the group. While there is not sufficient room to explore them all here, this section describes some of the key ideas that were shared.

Before discussing those ideas, it is important to highlight two framing issues that were raised by some interviewees. The first is the uniqueness of the I&W problem set as it relates to terrorism. For example, when one interviewee was asked what other models the CT community should look at to draw lessons and approaches from, the individual responded: "I don't have a really good answer … What I found is, looking at just about all the other conventional I&W problem sets, you have the ability to prove a negative. You know you can. You can look at SS-27 missile batteries [and determine that] those are all … still in garrison. Hey, are the North Koreans, is their artillery in garrison? Is it out of garrison? … I've confirmed all of Iran's submarines are in port. OK, great. I'm not worried about a sudden effort to close the Straits of Hormuz. But we … can't ever say, 'Hey, we've looked everywhere and nobody's trying to be a terrorist right now.' That, to me, has always been the biggest challenge on the I&W, as it relates to CT. In a lot of the other problems you have the ability to … say, 'How much do I need to be worried today?' … U.S. Forces Korea can get up in the morning and go, 'Do I need to worry about a lot today' and barring some huge deception plan, which you have to take into account, [a commander's] … staff can tell him … 'You don't have to worry.'"

Two other interviewees made similar comments and expressed reservations about the potential usefulness of other models. When asked the same other model question, another interviewee said: "The tolerances for error in other in other fields are much different than they are in this field, and that's my concern with that." A third interviewee added more color: The "core challenge in [the] terrorism [and] CT space is that terrorism is a low probability, high impact event. And the community spends a whole lot of time on events that are not normally distributed." This individual added, "We are good at identifying linear change, but terrible when it comes to non-linear change."

The second framing issue focused on mathematical models and the need for them to be refined. As noted by one interviewee: "When we talk about analytics, we talk about building a mathematical model that would go ahead and do the analysis. But what the government doesn't understand and what a lot of financial companies still don't understand is that models change. When a trader came in in the morning, he built a model, a trading strategy that would go ahead and get him some profit. But as we all know, the trading day or the world situation or the national situation changes, and that model is no good probably by two o'clock in the afternoon. So, they have to go ahead and change it. They didn't have any time to go back to a vendor and say, 'Hey, this model isn't working. Can you fix it?' And [they will] … say, 'We'll get back to you in a couple months.'"

Military

One of the models discussed was existing AI-driven model Maven Smart System, a data analysis and decision-making tool that is part of the U.S. Department of Defense's broader Project Maven, which was originally created for counterterrorism purposes. When a participant was asked whether the Maven Smart System would be a good model to look at, the individual responded: "The problem is with Maven—and I commend those guys for what they did because … I now know the environment they had to go ahead and work through—is how long it took. Let me back up a little. So, in the utilization of data, there's basically four basic types of analysis. There's descriptive, what you just described [with] the data; there's a diagnostic where you're diagnosing a problem—something failed and you wanna know why. It's prescriptive where you wanna go ahead and recommend the solution, and then it's predictive, which is extremely hard. So other basic data companies are usually pretty good if they get the data, and the most basic level of analytics is descriptive, visualizing it. You know, how many people are in the square, how many are in this a truck, an SUV, or is this a motorcycle? And Maven does all that stuff. They've been doing, they've been doing it for a while, and they did that by pulling in data from all over the place to go ahead and help. That's a commendable thing that they did. But they haven't advanced the ball in a long time. I mean, that's like saying, 'OK, I can go ahead and pull in all the trades from all over the place, but I can't really do anything other than show it to you.' In order to be useful, we need to get our systems up to that level of analysis that could be useful to the commander. Like 'why did this thing go wrong?' OK. Diagnostic analytics. 'All of this is screwed up. How am I gonna fix it? Give me some courses of action, some prescriptive analytics.' Or 'Hey, what do I think is gonna happen, given this and that and some predictive courses of action?' Maven's not there yet; we're not there yet."

Finance

The finance community was seen by a number of study participants as a useful resource for ideas on how to think about the indicators and warning challenge more creatively. Some interesting contributions from participants are listed below:

"Using models from the financial markets around when a trend is a significant trend is something that I think has a lot of utility. And so specifically looking for death crosses[b] and golden crosses[c] in the rolling average dynamic that you're interested in. So it could be if there is a golden cross, which is just when two rolling averages across different time frames cross each other. The question would be, might you notice a golden cross in relation to how frequently Shi`a militia groups in Iraq are talking about U.S. people, positions, interests or assets, etcetera? But if there is a cross between the 50-day rolling average amount of references and the 200-day amount of references, essentially that tells you that what you're looking at is not just an anomaly, but is an emergent trend. And if you can address the emergent trend when it is still emergent, that gives you better ability to respond to it."

"Consistently forecasting out. Everything [the] finance industry does is based on forecasts and expectations. Only thing that drives change in value is when outcome deviates from forecast. So it might be worth consistently taking time to forecast groups/networks. Treat them like individual companies and forecast, and then continually revisit those forecasts."

"There's a conceptual idea emerging in the private sector around a kind of dynamic risk modeling, risk grading. And so just to give you an example: Most institutions, especially financial institutions, have to do risk assessments of various sorts. These are traditionally once a year, once every three years in the anti-money laundering context. You've got different degrees of risk reviews for different kinds of clients. You've got very high-risk clients—former politically exposed persons, former government officials, that kind of thing that requires more diligence. So those happen more often, but that's usually once a year. Low-risk persons or clients are like once every three years. It is kind of a file refresh. That's a very 1970s analog, [so] where some of the data providers and compliance tech are going is to try to provide continuous risk ratings on clients, customers, or behavior. And part of that is just constant analysis around their behavior, their transactions, their activity. It's also then the ability to [essentially] risk rate and to provide output to people who have got thousands or millions customers. What's the output that lets you really focus on where a higher risk sits versus the medium risk versus the low, and then that changes overtime. So I think this idea of real-time consistent risk rating around behaviors is an interesting dynamic happening, one that I would imagine we would want to think about for counterterrorism purposes."

Medical

The medical community was also a particularly popular source of ideas across the interviewees:

"The first thing that comes to mind is public health and methods used in terms of assessing people's data in public health … and the strong data sharing in public health. Also, the methods used in assessing mental health conditions."

"Borrow from public health models (where possible), predictive models that can forecast patient outcomes. Such predictive models operate at the individual level rather than organizational level, but can still be useful to identify high-risk individuals or regions for attacks."

"Epidemiology could be useful since there's a contagion element to jihadi plots and attacks that get a momentum of their own, and whether we see endemic plots/attacks versus truly pandemic-level plots/attacks, and the different waves we then see over time between the peaks and valleys."

"The other thing [of interest] was diagnostics. I looked at medical literature on this and how they think about diagnosing diseases. It is an interesting area to compare … diagnostics in particular. We don't train our intelligence analysts well enough to be able to diagnose the situation. And again, that goes to information and assessment. You know, creating hypotheses and then being able to recommend approaches that addresses the cancer but doesn't kill the body."

[b] "The death cross is a chart pattern that indicates the transition from a bull market to a bear market. This technical indicator occurs when a security's short-term moving average (e.g., 50-day) crosses from above to below a long-term moving average (e.g., 200-day)." "Death Cross," Corporate Finance Institute, n.d.

[c] "A Golden Cross is a basic technical indicator that occurs in the market when a short-term moving average (50-day) of an asset rises above a long-term moving average (200-day). When traders see a Golden Cross occur, they view this chart pattern as indicative of a strong bull market." "Golden Cross," Corporate Finance Institute, n.d.

Insurance

The insurance industry was also referenced several times, as participants highlighted that industry's ability to look at risks and to estimate risks.

"Insurance companies have been doing risk analysis for cities at a local level for years. Earlier this year, there were threats against stadiums in Europe from ISIS sympathizers. Insurance companies may be able to pinpoint the risks at a venue based on all their data on accidents and choke points, etcetera."

"I would draw from how the insurance industry is using online data to better predict risk. And again, use AI and automated tools—LLMs—to process large amounts of information and be able to forecast where risk of offline violence might happen. That is something that the insurance industry has been doing for years now, which we can benefit from."

Cyber

Participants also cited the cyber community as a source for models to emulate. For example, looking at how the National Security Agency and the Cybersecurity and Infrastructure Security Agency conduct information sharing on indicators and warning with the private sector in relation to cyber activity and threats.

One participant suggested "adopting cybersecurity incident response models, and what that means is develop a response meant more for identifying and using threat reduction measures and not waiting for something to be imminent. But when you perceive a potential threat, you act on it and have a multilayer defense system, in terms of counterterrorism. When you're looking at these digital approaches, you could act earlier on to mitigate and reduce the threat."

As noted earlier, another interviewee suggested that the community develop "something like the MITRE framework for cyber attacks" so that CT community members had a common reference.

Child Exploitation

One interesting idea was to look to the child sexual exploitation and child trafficking field, with one participant saying:

"Project Lantern is a great example of how they've been able to do multi-agency coordination in order to mitigate CSAM [child sexual abuse material] and child trafficking. There are probably ways that we could adopt this stuff. I'm thinking of centers such as the National Center for Exploited and Missing Children, acting as a global hub in a way for reporting of CSAM and then being connected to Interpol, the FBI, the RCMP [Royal Canadian Mounted Police] and being able to share that information out as a non-government agency and having actions carried out [through] their capacity to coordinate, but also more importantly, it's also the support of victims after the fact as well to mitigate recidivism or potential reactionary violence from a victim of an attack."

Statistics

An interviewee also suggested tapping into statisticians:

"How do we analyze violence more effectively? How do we build out models for this? There's a lot of work that's been done recently in what are called self-exciting statistical models that capture these bursts of activity that you tend to see. So looking to the statistical community to see what's out there right now in terms of modeling [could have value]. Maybe [taking something] from seismology and then [using it] in crime and violence. So, I think some of the statistical models might be interesting to help us kind of conceptualize why we see clusters of violence."

Conclusion

Identifying indicators and providing warning of possible attacks by clandestine and dynamic terrorist groups is a remarkably difficult challenge. The goal of this article is to provide the counterterrorism community with a wide range of input on this topic from experienced professionals in the field. As their input suggests, this mission presents both data challenges and analytical challenges. Practitioners must ensure they are collecting the right data in order to have visibility on the wide range of potential indicators discussed in the first part of this article. Doing this has resulted in the collection of vast amounts of data, to the point that participants highlighted information overload as one of the most significant problems they face. That information needs to be efficiently processed, effectively analyzed, and then disseminated in order to provide warning to the community. Participants focused on technology, specifically artificial intelligence and machine learning, as the critical component to meeting these challenges. But they cautioned not to ignore the critical role humans must continue to play in this process to maximize the potential of technology and ensure the analytical output is useful to policymakers. Other models were also discussed and provide potential pathways for the I&W community to consider as it works to refine and evolve its approaches. CTC

Citations

[1] Nicolas Rasmussen, "Navigating the Dynamic Homeland Threat Landscape," Washington Institute, PolicyWatch 3741, May 18, 2023.

[2] Gia Kokotakis, "Biden Administration Declassifies Two Counterterrorism Memorandums," Lawfare, July 5, 2023.

[3] Daniel Milton, "Go Big or Stay Home? A Framework for Understanding Terrorist Group Expansion," *CTC Sentinel* 10:7 (2024).

[4] Lucas Webber, Riccardo Valle, and Colin P. Clarke, "The Islamic State Has a New Target: Russia," *Foreign Policy*, May 9, 2023.

[5] Milton.

[6] For background, see Petter Nesser, "Introducing the Jihadi Plots in Europe Dataset (JPED)," *Journal of Peace Research* 61:2 (2023).

[7] For background, see Aaron Y. Zelin, "ISKP Goes Global: External Operations from Afghanistan," Washington Institute, *PolicyWatch* 3778, September 11, 2023.

[8] Brian Dodwell, Daniel Milton, and Don Rassler, *The Caliphate's Global Workforce: An Inside Look at the Islamic State's Foreign Fighter Paper Trail* (West Point, NY: Combating Terrorism Center, 2016).

[9] David Malet and Rachel Hayes, "Foreign Fighter Returnees: An Indefinite Threat?" *Terrorism and Political Violence* 32:8 (2020).

[10] "CBP Enforcement Statistics," U.S. Customs and Border Protection.

[11] Nicole Sganga, "Tajikistan nationals with alleged ISIS ties removed in immigration proceedings, U.S. officials say," CBS News, October 6, 2024.

[12] See also scholarship on organizational dynamics. For example, Donald Kettl, *System under Stress: The Challenge to 21st Century Governance* (Washington, D.C.: CQ Press, 2013).

[13] "Sri Lanka attacks: Government admits 'major intelligence lapse,'" BBC, April 25, 2019.