COMBATING TERRORISM CENTER AT WEST POINT

CTC SENTINEL

OBJECTIVE · RELEVANT · RIGOROUS | NOVEMBER 2024 · VOLUME 17, ISSUE 10

THE COUNTERTERRORISM ISSUE

FEATURE ARTICLE

Conceptualizing Counterterrorism for a New Era

Don Rassler

A VIEW FROM THE CT FOXHOLE

General Bryan Fenton

Commander, U.S. Special Operations Command

Contents

FEATURE ARTICLE

INTERVIEW

ANALYSIS

FEATURE COMMENTARY

FROM THE DIRECTOR

I'm thankful to borrow this space from our Editor-in Chief, Paul Cruikshank. Our *CTC Sentinel*, its editorial board, and our incredible contributors have long provided our readers with details, data, and insight on terrorist groups, tools of violence, trends, and counterterrorism. In short, *Sentinel* has helped drive the conversations on *what* to think about for our global audience. As the United States changes administrations in the face of extraordinary complexity, we opted to frame this issue slightly differently. This issue is focused on *how* we think about terrorism and counterterrorism.

The feature article this month comes from Don Rassler and focuses on the pressure states place on violent extremist organizations (VEOs) and how those campaigns of pressure can defend against threats and degrade the capabilities of VEOs.

We are privileged to feature General Bryan Fenton, Commander of U.S. Special Operations Command, in this month's Foxhole interview. He shares his insight on the global threat, the critical role of SOF in strategic competition, and the importance of allies and partners in the global CT fight.

Brian Fishman, co-founder of Cinder and formerly Director of Counterterrorism, Dangerous Organizations, and Content Policy at Facebook, helps us understand the realm of online and digital counter terrorism through five key lessons from his time in industry.

Dr. Daniel Milton, Director of Terrorism Studies at the George C. Marshall Center, gives us critical insight into how groups choose to expand to external operations (EXOPS) based on a group's opportunity and willingness to "go big." In a complementary article, our Executive Director, Brian Dodwell, teams up with Don Rassler and Paul Cruickshank to use survey data to provide perspectives on indicators and warning (I&W) for terrorism, key challenges in the I&W space, and how I&W approaches could evolve.

Finally, I collaborate with Don Rassler to offer a few thoughts on CT return on investment, specifically at the intersection of CT and strategic competition, through a new framework designed by Don and informed by interviews with regional experts and partners from the CT community. The article demonstrates the returns to key efforts with regard to mitigation and influence where CT and strategic competition converge.

Colonel Sean Morrow, *Director, Combating Terrorism Center*

CTC SENTINEL

Editor in Chief
Paul Cruickshank

Managing Editor
Kristina Hummel

CONTACT

Combating Terrorism Center
U.S. Military Academy
752 Thayer Road, Mahan Hall
West Point, NY 10996
Phone: (845) 938-8495
Email: ctc@westpoint.edu
Web: www.ctc.westpoint.edu/ctc-sentinel/

SUBMISSIONS

The *CTC Sentinel* welcomes submissions. Contact us at ctc@westpoint.edu.

The views expressed in this report are those of the authors and not of the U.S. Military Academy, the Department of the Army, or any other agency of the U.S. Government.

Cover: A member of the Syrian Democratic Forces (foreground) and U.S. soldiers are pictured near an armored military vehicle on the outskirts of Rumaylan in Syria's northeastern Hasakeh province, bordering Turkey, on March 27, 2023. (Delil souleiman/AFP via Getty Images)

Smart Pressure: Conceptualizing Counterterrorism for a New Era

By Don Rassler

When it comes to counterterrorism, the United States has been living through an inflection point. It wants to focus less on terrorism so it can place more emphasis on strategic competition, but key terrorist adversaries remain committed. The terrorism landscape and the approaches used by key terror adversaries have also been evolving. The United States and its partners have been placing various forms of pressure against priority networks such as the Islamic State and al-Qa`ida in key locations to keep the threats these groups pose degraded, and to restrict their ability to conduct external operations and other impactful acts of terror. But over the past two years, there have been growing signs that the Islamic State is evolving around the pressure that has been placed against it, developments that highlight the limits of existing CT pressure approaches and the need for those approaches to evolve. This article introduces two frameworks: 1) a framework to help conceptualize non-state VEO power and CT pressure efforts to degrade those elements of power and 2) a defense and degradation in depth framework that can be used to help strategically guide future CT pressure campaigns. It is hoped that these frameworks provoke debate within the counterterrorism community and that they help the United States and its allies adjust their CT approaches so they can evolve to stay ahead of the threat.

The uptick in attacks and plots linked to the Islamic State and its Central Asian affiliate—Islamic State Khorasan (ISK)— in Europe and other places over the past two years is a cautionary tale. It is a reminder of the steadfast commitment of key salafi-jihadi groups, the persistent threats that these types of networks pose, and the need for ongoing forms of pressure to keep entities such as ISK off-balance and their capabilities, reach, and potential for surprise degraded.

Another lesson from the last two decades is that terror threats rarely stay the same: They change and adapt.[1] "The history of global jihadism," as noted by *The Economist*, "is one of reinvention under pressure from the West."[2] That pressure has helped to keep the threat posed by the Islamic State and its key affiliates at bay. But over the past two years, there have been growing signs that the Islamic State is evolving around the pressure that has been placed against it. Some key examples include ISK's March 2024 attack in Moscow, Russia's deadliest terror attack in 20 years;[3] the doubling of Islamic State attacks in Syria in 2024;[4] the intensification of local and regional activity by Islamic State affiliates in Africa;[5] and the arrest of eight Tajik nationals who entered the United States from the southern border over terrorism concerns and links to Islamic State members.[6] As reported by *The New York Times*, "heightened concerns about a potential attack in at least one location triggered the arrest of all eight men … on immigration charges."[7]

These and other data points of concern were underscored by a June *Foreign Affairs* article by Graham Allison and Michael Morell entitled "The Terrorism Warning Lights are Blinking Red Again,"[8] a reference to a phrase that George Tenet used during the summer of 2001 in the lead up to 9/11.[9] The title could not have been more ominous, but it was also a reminder about how the United States needs to be careful and that it might not be doing enough on the counterterrorism front to contain the threat. The blinking red lights may have also been a sign that U.S. CT efforts may not be keeping up with the evolution, direction, or pace of the threat. The United States and its partners have been working hard to adjust and to optimize approaches to counterterrorism, but environmental changes have made that an increasing hard thing to do. For example, the United States and its partners today face a more diverse, complex, and ever-evolving threat landscape (which includes a rise in state sponsored terrorism) and need to confront the threats with fewer resources and less attention than they did a decade ago. The United States and its allies must also contend with ongoing technological change that has been "transforming the worlds of extremism, terrorism, and counterterrorism,"[10] challenges that are difficult for bureaucracies to respond to in practice.

This article explores the topic of counterterrorism pressure, and it introduces several concepts as well as two frameworks to help guide strategic thinking about CT pressure and how it can be applied and evaluated. It is organized in three parts. Part I describes the risk-optimization conundrum that has been challenging the evolution of U.S. counterterrorism over the past several years. To level set the conversation, Part I also provides a short overview of key counterterrorism instruments and how different CT strategies have sought to integrate them. Part II introduces several concepts, including: 1) a framework to conceptualize violent extremist organization (VEO) power and CT pressure efforts to degrade those elements of power and 2) a defense and degradation in depth framework that can be used to help strategically guide and

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

assess future CT pressure campaigns. Part III applies some of the introduced concepts to the case of the Islamic State to highlight their practical utility and application.

PART I: The Problem and CT Pressure Tools

The Risk-Optimization Conundrum: Key Considerations and Caveats

The United States' shift in 2018 to strategic competition—with more emphasis and priority placed on near-peer threats—was a move that was overdue. Since then, the U.S. counterterrorism community has been navigating what that shift means for the CT enterprise in practice, what tradeoffs it entails, and how the enterprise can evolve, all so that it can create space for the United States to focus on strategic competition while also protecting the American people against a diverse and committed range of terror threats. This challenge has been underpinned by a principal conundrum. Networks such as the Islamic State and al-Qa`ida, for example, cannot be left alone. They are committed and persistent. As a result, consistent and sustained forms of counterterrorism pressure are required to keep these networks off-balance and to degrade, and limit, their capabilities, reach, and ultimately the type of threats they pose. But what level of pressure is 'enough' or 'sufficient' to keep the threats these (and other) terror networks pose to the U.S. homeland and U.S. interests contained is much less clear.

This conundrum is highlighted by Figure 1, which attempts to visualize how the United States is trying to optimize its CT efforts in relation to risk—to apply enough pressure, and devote enough resources, to keep key terror movements off-balance so that the maximum amount of time, attention, and resources can be transitioned to strategic competition priorities.

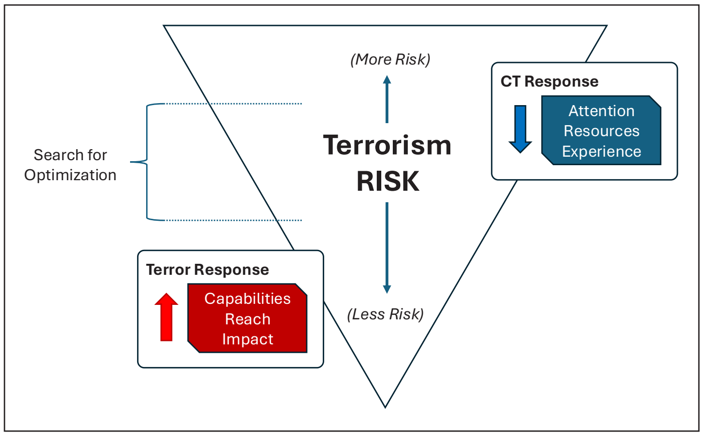


Figure 1: CT Risk-Optimization Conundrum

In theory, as more CT pressure is placed against a network, the level of terrorism risk goes down. Likewise, as less CT attention and resources, and as a result pressure, is applied against committed terror networks the terrorism risk goes up. As part of its efforts to make efficient use of government resources, the U.S. CT enterprise has been exploring, and trying to identify, how CT pressure can be optimized. This pursuit is conceptually reflected by the 'Search for Optimization' bracket on the left of Figure 1, which tries to situate CT pressure along a sliding scale of risk.

While theoretical in many respects, the conversation is also an important and practical one, as having a better sense of the issue can help the CT enterprise to be more intentional about how it seeks to manage risk. The approach, though, is not without its own share of hazards, and important cautions and caveats should be considered. For example, given the diverse nature of today's terrorism threat and various unknowns—or less well knowns—it is important to be cautious in the quest to find a minimal level of CT pressure, as it suggests that counterterrorism, and counterterrorism impacts, can be scientifically approached or quantified. Further, while the United States and its partners have learned a lot about the Islamic State and other terror networks over the past decade, there is still a lot that the community does not know, and likely will not have the ability to know with good certainty about the posture, inner-workings, and standing of key VEOs for the foreseeable future. This 'we only know what we know' issue is also compounded by the fact that in various locales, the United States has less visibility into the inner workings of key VEO networks, not more, than it had several years ago. Another important cautionary factor to consider is that threat networks evolve and adjust their approaches in response to pressure—which highlights the dynamic way in which terror and counterterror entities interact and adapt in relation to each other. Those changes, or the direction of those changes, are not always apparent or immediately visible.

"The CT community would be wise to not be dogmatic about, or rigidly beholden to, what it believes should be the minimum amount of pressure that should be applied to entities such as the Islamic State."

This places the idea, or pursuit, of identifying a minimum amount of pressure more into the realm of art than science, and the CT community would be wise to not be dogmatic about, or rigidly beholden to, what it believes should be the minimum amount of pressure that should be applied to entities such as the Islamic State (or other terror networks). This is because it assumes that such a formula exists and that terrorism risk, and the dynamics of surprise, can be controlled. Those risks can certainly be managed, but the past two decades of CT experience provide plenty of evidence that highlights how even when key networks are placed under a considerable amount of pressure, they can still find gaps and seams to exploit, and ways to attack. Thus, efforts that aim to quantify minimum amounts of CT pressure should be viewed as a general guide that needs to remain flexible and responsive to evolving conditions and change, rather than as a doctrinal number or level. The same 'need to remain flexible' idea should also be applied to the different types of pressure placed against VEOs, as predictable CT approaches arguably make it easier for terror groups to adapt and regenerate around those forms of pressure over time.

CT Instruments and the Orchestration of Pressure

While CT pressure efforts are operationally driven by the various instruments of counterterrorism, they are, or should be, guided by strategy. In addition to outlining key goals and areas of focus, strategy sets the vision for how different instruments of counterterrorism, including kinetic and non-kinetic forms, should be brought together and orchestrated. To level set what is meant by pressure, this short section outlines key CT instruments. It also discusses how different counterterrorism strategies have conceptually sought to strategically orient these instruments.

There are different ways to bucket the instruments of counterterrorism. One well-known framework is the diplomatic, informational, military, and economic (DIME), and the DIME-FIL (which also includes finance, intelligence, and law enforcement), model. There are also the similar categories – diplomacy, criminal law, financial controls, military force, intelligence—that U.S. intelligence community veteran Paul Pillar outlined in his classic article "The Instruments of Counterterrorism."[11] A brief overview of key instruments relevant to CT today follows.

Diplomacy: At a high level, diplomatic activity helps to shape, enable, and set the conditions for counterterrorism actions and campaigns to take place, or to enhance their positive, or limit their negative, effects. For example, diplomatic activity is critical for coalition building, facilitating access and placement for operational CT forces, influencing host nation CT actions, enabling local partnering and security cooperation, and overseeing hostage and other negotiations. Signaling—whether viewed through the lens of deterrence, or through specific tools such as the U.S. State Department's Foreign Terrorist Organization (FTO) designations list—is another important element that diplomacy brings to counterterrorism.

Military Force and Foreign Kinetic Activity: Like diplomacy, military contributions to CT are multi-faceted. The most discussed area is direct action, which can include contributions from military forces and other government elements. These types of unilateral or partnered operations can take the form of precision strikes or raids to remove or capture key VEO leaders, to degrade VEO infrastructure or specific VEO capabilities (e.g., strikes against locations where money or weapons are stored), or achieve other effects.

Security Cooperation: Security cooperation is another key mechanism that is used to develop, augment, and reinforce other forms of CT pressure. Through global train and equip programs, defense trade and arms transfers, international education and training initiatives, and institutional capacity building projects, the U.S. government helps partner nations to develop their CT capacity and capabilities. If executed well, these types of efforts can help specific countries to combat VEOs on their own and to apply pressure against key networks over the longer term.

Law Enforcement and Criminal Law: As noted by Pillar, "the prosecution of individual terrorists in criminal courts has been one of the most heavily relied upon counterterrorist tools." While the contributions of local, tribal, state, and federal law enforcement entities are rooted in the forensic and investigative actions they take to charge, arrest, and prosecute terrorism suspects (and their enablers), the law enforcement community makes other important CT contributions. Examples include community outreach, measures taken to harden and protect key infrastructure, and engagement with international law enforcement partners.

Intelligence: Intelligence cuts across all dimensions and instruments of counterterrorism, from enabling operations to preventing acts of terrorism in the first place. It includes collection and analysis of different types of intelligence, such as human intelligence (HUMINT), signals intelligence (SIGINT), geospatial intelligence (GEOINT), and open-source data (OSINT).

Resource Controls and Counter Threat Finance: Like any organization, terror networks need resources to survive, and they also need to be able to store and move financial and other resources. The United States and its partners have developed various sanctions regimes to freeze or seize assets used by individual terrorists, entities, and their supporters, and to prohibit access to sensitive technologies and dual use items. Key tools in the U.S. context that enable this activity include Executive Order 13224, the U.S. Treasury Department's Specially Designated Nationals List, and Export Control actions taken by the U.S. Commerce Department.

Terrorist Travel: Another pillar of counterterrorism activity involves preventing the movement of terrorists and individuals with concerning ties to terrorism. The U.S. government's approach to this issue is layered, and it involves inputs from multiple U.S. departments and agencies. For example, it includes watchlisting data generated by the Departments of Defense and Treasury and FBI, and information shared by foreign partners. These data inputs are designed to complicate and prohibit terrorist travel abroad, and to ensure that individuals with terrorism ties are prevented entry into the U.S. homeland by frontline law enforcement entities such as U.S. Customs and Border Protection agents.

Digital Actions: The rise in social media and digital platforms over the past two decades has broadened and diversified the counterterrorism landscape in profound ways. One important change is that it has led to an increase in the number of private companies "who either have been meaningfully shaping, or have a role in, the world of counterterrorism and how specific counterterrorism actions or responses take place."[12] This includes companies such as Meta, YouTube, and Discord, that—to varying degrees—promote policies or engage in activity on their platforms that are designed to limit extremism or how their platforms might be used to promote an act of terrorism (e.g., Livestreaming, access to an attacker's manifesto, etc.). In addition to corporate actions that can be pursued unilaterally, through consortiums (e.g., Global Internet Forum to Counter Terrorism-GIFCT), or at the behest of a government or in partnership with it (e.g., some of the activity of Europol's Internet Referral Unit), digital CT actions can also encompass offensive cyber operations to deny or destroy terrorist cyber resources and online influence and counterinfluence activities.

Safe Communities and Societal Resilience: Approaches to counterterrorism also involve efforts focused on both the left (prior to an incident) and right (after an incident) sides of terrorism. This includes programs that promote healthy and safe communities and that aim to identify and prevent individuals and organizations from engaging in terrorism and political violence in the first place, or that provide off-ramps to radicalized individuals (e.g., intervention and deradicalization initiatives). It also includes initiatives that promote societal resilience to terrorism that help societies to recover from acts of terror after they occur.

Strategy provides a framework for how these different CT instruments—the mechanisms of CT pressure—should be brought together so their collective utility and power can be actualized. As Pillar noted: "Every tool used in the fight against terrorism has something to contribute, but also significant limits to what it can accomplish. Thus, counterterrorism requires using all the tools available, because no one of them can do the job. Just as terrorism itself is multifaceted, so too must be the campaign against it."[13] Identifying the right mix of instruments is critical, but being flexible

> **"Is it more efficient and effective to continue to surge, apply, and reapply pressure on VEOs when they reach, are close to reaching, or regain global capability status? Or would it be more efficient over the longer term to apply consistent forms of pressure against key networks that have global ambitions but who still operate at the local and regional levels so their capabilities can be degraded earlier, before they reach the global level?"**

and adjusting where and how that mix is applied, given changing conditions, is arguably just as important for CT strategies to be effective, and to remain effective.

Since 9/11, different countries and administrations have framed their approaches in different ways. For example, the United Kingdom's counterterrorism strategy (CONTEST), which serves as a model for many countries in Europe, organizes CT activity around four 'P' pillars: prevent, pursue, protect, and prepare.[14] In its first term, the Trump administration's CT strategy framed its approach around six key lines of effort: 1) pursuing terrorists at their source; 2) isolating terrorists from financial, material, and logistical sources of support; 3) modernizing and integrating a broader set of tools and authorities; 4) protecting U.S. infrastructure and enhancing preparedness; 5) countering terrorist radicalization and recruitment; and 6) strengthening the CT abilities of international partners.[15] The Biden administration's approach, as reflected in the declassified version of National Security Memorandum 13 (NSM 13), embraces seven lines of effort.[a] Those seven lines share a lot of common ground with the Trump administration's CT strategy in its first term, but they are framed differently.

As the United States looks forward on the CT front, it is important that any future CT pressure effort or campaign be nested within, or designed to support, a broader CT strategy—and that it considers policy implications, including constraints, and practical feasibility, too.

PART II: CT Pressure Concepts and Frameworks

VEO Power and CT Pressure Targets: Core Areas of Focus

This section introduces a new framework to conceptualize non-state VEO power and CT pressure efforts to degrade those elements of power.[b] The framework is centered around a network's or movement's ability to operate within and across local, regional, and global levels. While many VEO groups begin their campaigns of violence locally and will remain locally focused, the targeting interests and priorities of other VEOs evolve, and some—such as the Islamic State and al-Qa`ida—have global ambitions from the start. The arrow at the top end of the graphic is designed to illustrate how the danger a VEO poses to U.S. interests and global security becomes more concerning as its operational impact and reach, as reflected by its targeting preferences, moves from left to right—from local to regional and global. This is not to suggest that VEO groups that have not yet 'gone global' and that remain focused regionally or locally are not a CT concern or priority (some are), but rather that VEO entities that operate across all levels are the most concerning and deserving of U.S. CT pressure and attention. That aspect is captured by the 'Level of Prioritization' arrow at the bottom of the graphic in Figure 2. This arrow, which moves from right to left, captures how the level of U.S. prioritization, and as a result CT pressure, is deeply influenced by a VEO's impact and reach.

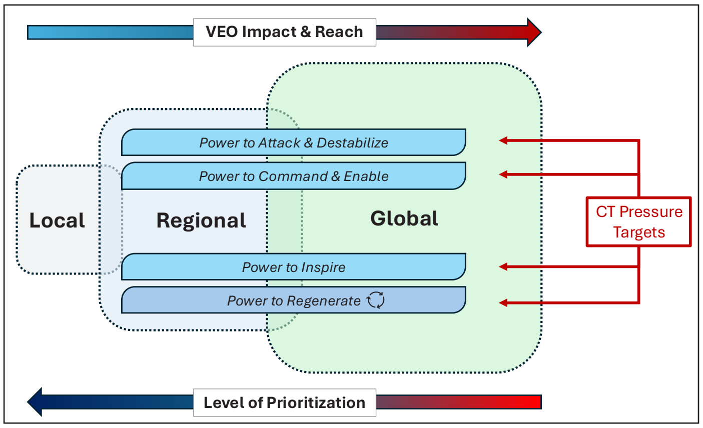


Figure 2: VEO Power and CT Pressure Framework

One important issue to consider is when, at what point, across a VEO's lifecycle does it make sense to apply or reapply CT pressure.[16] While the answer may seem simple on the surface—'it should be when VEOs have demonstrated global reach and impact'—how the United States and its partners approach the question can also have a bearing on the efficiency and potential long-term sustainability of CT efforts. For example, is it more efficient and effective to continue to surge, apply, and reapply pressure on VEOs when they reach, are close to reaching, or regain global capability status? Or would it be more efficient over the longer term to apply consistent forms of pressure against key networks that have global ambitions but who still operate at the local and regional levels so their capabilities can be degraded earlier, before they reach the global level? While the latter approach might require more upfront investment, it could also prove more efficient over the longer term. Both approaches involve tradeoffs and different types of risk, however. Applying pressure against local and regional groups, for example, may embolden them or provide incentives for them to develop global capabilities faster. But if governments wait too long to apply CT

[a] These include: LOE 1 Strengthen Defenses, LOE 2 Build and Leverage Partner Capacity, LOE 3 Strengthen Our Capacity to Warn, LOE 4 Narrowly Focus Direct Action CT Operations, LOE 5 Deter and Disrupt State Sponsored Terrorism, LOE 6 Degrade Transnational Enablers of Terrorism, and LOE 7 Integrating CT with other U.S. foreign policy and national security efforts. For background, see Gia Kokotakis, "Biden Administration Declassifies Two Counterterrorism Memorandums," Lawfare, July 5, 2023.

[b] The framework may not be as useful for state-sponsored/supported entities that engage in terrorism.

pressure against a local or regional group that is poised to expand, they could also be locking themselves into providing off-and-on surge support, which can also be resource intensive.

In addition to the 'when' to apply pressure question, consideration should also be given to what types of pressure would be most effective against different VEOs, where those forms of pressure can be applied, and what level of pressure intensity and periodicity will lead to ideal outcomes.

A second component of the framework is the four high-level elements of VEO power. These include a VEO's: 1) power to attack and destabilize, 2) power to command and enable, 3) power to inspire, and 4) power to regenerate.[c] The local, regional, and global construct can be used to evaluate a VEO's power in relation to each of the four areas. For example, a VEO might be assessed as having the ability to inspire at the global level, but not have the power to conduct attacks at that level. These four elements of VEO power can also be used to orient CT pressure (and CT strategy more broadly) as part of a campaign to degrade a VEO's ability across the four power areas. While these four VEO powers can be understood as distinct power areas, there can be interplay and dependencies between them, too. A network's power to inspire, for instance, can also enhance that network's ability to regenerate. A brief explanation of each of the four VEO power areas follows.

Power to Attack and Destabilize: This power area includes a VEO's ability to conduct attacks within and across geographic areas and its ability to destabilize or complicate environments. While a VEO's ability to conduct attacks, especially global terror operations, is a more straightforward way to assess the danger a VEO poses to U.S. interests and international security, a VEO's ability to destabilize is also an important factor to consider. This is because a VEO's ability to destabilize, especially its ability to consolidate control over a specific location or progressively destabilize wider geographic areas, can evolve into a strategic problem for the United States and its partners. This can take various forms, such as a VEO overthrowing, or assisting in the overthrow of, a country's government or a VEO being able to threaten several regional governments and gain control over territory. These developments can help a VEO to develop safe haven, that provide networks with more time and space to plot and plan, to train, and to consolidate their control and influence. While not the norm, the October 7th attack highlights how regional destabilization can be triggered by a terror attack, which highlights how these two areas—attack and destabilize—can converge.

Power to Command and Enable: This power area is designed to evaluate a VEO's ability to command and enable core elements of the network, its affiliated networks, its members, and more loosely connected individuals across local, regional, and global levels. It includes a VEO's ability to lead, to maintain unity and cohesion within and across its movement (e.g., ensuring that its component parts are engaging in activity that is aligned with the movement's vision, ideology, and goals), and to provide direction, resources, and technical know-how that enables cells and individuals to act.

Power to Inspire: This power area focuses on a VEO's ability to inspire and motivate across local, regional, and global levels through in-person and digital means. It includes a VEO's ability to brand itself; to provide a compelling vision and to effectively market that message; to recruit people and bring resources into its movement; to retain recruits and key supporters (and keep them motivated); and to inspire disconnected or loosely connected individuals to conduct acts of violence, or engage in operational activity, on behalf of the network. Another way to view a VEO's ability to inspire is the capability it has to 'push' out and 'sell' its ideology and vision so it results in a 'pull' of individuals and resources that the network can use to consolidate its position or evolve into new areas.

"A VEO's ability to destabilize, especially its ability to consolidate control over a specific location or progressively destabilize wider geographic areas, can evolve into a strategic problem for the United States and its partners."

Power to Regenerate: The resilience of key terror networks, such as the Islamic State and al-Qa`ida, and their ability to rebuild and regenerate their capabilities after loses and setbacks has proven to be an enduring feature during the post-9/11 period. This is because these types of VEO networks and their ideologies are focused on long-term success, even if it entails considerable suffering and setbacks spread across decades. This is a core reason why the threats these networks pose are persistent. Thus, a terror network's ability to regenerate is a key factor that needs to be addressed as part of any CT pressure approach or CT strategy. This is so the ability and power of key VEO networks, and their supporters, is degraded not just over the short-term (e.g., through the removal of key leaders and other actions, such as sanctions), but also so their appeal, capabilities, and ability to sustain themselves is also degraded over a longer period of time.

This will likely require learning more about the strengths and vulnerabilities of key VEO networks, and in experimenting with new approaches. For example, for the past two decades a core element of al-Qa`ida's senior leadership has received shelter and support from the Iranian government.[17] A pressure campaign focused on al-Qa`ida's regenerative capacity would devise ways—beyond what has already been done—to expose, further degrade, weaponize, or further problematize the support that Iran provides to the group. While those pressure approaches could share common ground with other efforts, such as leadership decapitation approaches focused on the Islamic State in Syria, they will also arguably need to be different given differences across operating environments. Another strand focused on regenerative pressure could target financial resources and aim to identify key funders and sources of financial support that have received less attention. Emphasis could also be placed on disrupting or subverting VEO supply chains, particularly those that involve dual-use technologies or other key inputs.

High-level benchmarks could be created for each of the four VEO power areas, and these could be used to evaluate the evolution of a VEO network's capabilities and the effectiveness of

[c] These four VEO power elements are a modified and updated version of a prior framework the Combating Terrorism Center developed in 2009. The five power aspects that article highlighted included: the power to destroy, power to inspire, power to humiliate, power to command, and power to unify. For background, see "Five Aspects of Al-Qa`ida's Power," *CTC Sentinel* 2:1 (2009).

a CT pressure campaign over time. For example, one high-level metric that could be used for the 'Power to Attack and Destabilize' area is the number of attacks a VEO network was able to execute, and the failed plots it was not able to bring to fruition, measured across local, regional, and global levels on a monthly, quarterly, or annual basis. Other metrics for that power area could include the size and significance of the territory a VEO network controls or over which it wields meaningful influence, or a VEO's ability to regionally expand the reach of its operations. Similarly, global data on the number of successful or disrupted plots involving inspired individuals, organized by specific VEO networks, could be compiled to inform and measure time-bound change in a VEO's 'Power to Inspire.' The number of individuals arrested for providing material support to a VEO could also be used to evaluate that aspect of VEO power. To help scale the effort, data collection for some or all benchmarks could be automated or leverage data inputs from existing approaches. The indicators for each power area could be measured as a scorecard and could be used to inform and modulate where and how CT pressure is applied. For example, if 'Power to Inspire' metrics point to a VEO having achieved more power in that area over an annual period, that finding could inform kinetic targeting strategies, digital forms of pressure, and/or outreach efforts to technology partners.

Defense and Degradation in Depth: A Framework to Guide CT Pressure

This section builds on the previous one, and it introduces two additional concepts that can be used to operationalize and evaluate CT pressure efforts. The first concept (Figure 3) identifies common points of orientation that can help guide an interagency CT pressure approach focused on the four VEO power areas just discussed. Since an overarching goal of U.S. and partner CT efforts is to limit the reach and impact of key VEOs across geographic areas, it is recommended that emphasis be placed on key factors that enable VEOs to operationalize their reach, and that these serve as common orientation points to focus interagency CT pressure efforts. Figure 3 identifies four key factors: people, resources, direction, and knowledge. In many ways, these four factors are already points of emphasis for the U.S. CT community, but they are being presented to showcase how CT pressure efforts could be more intentionally oriented around them.

For the U.S. CT enterprise, the operatives of terrorist groups and their resources have been a consistent point of focus for more than two decades; this is something the community is exceptionally good at focusing on. Those two factors, and the need for pressure emphasis on them, are far from new. The importance of, and need to limit, VEO operational direction and technical knowledge transfer are also appreciated by the U.S. CT community. But despite their importance, those two factors can be more difficult to 'see' and disrupt, and as a result have arguably received less attention.

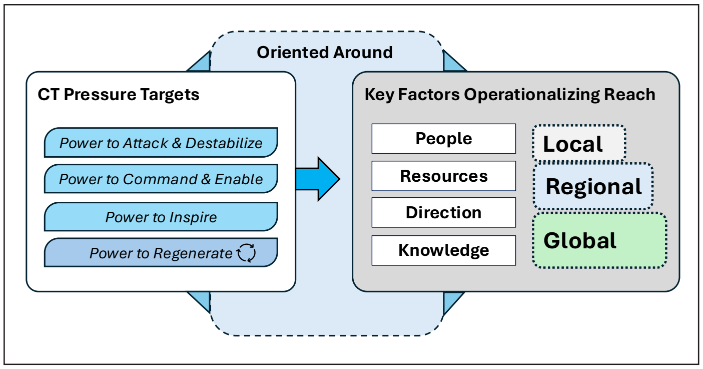


Figure 3: Common Points of Orientation for CT Pressure

An Islamic State plot disrupted in 2017 highlights how these four enabling factors come together. That year, Australian authorities arrested two brothers, Khaled Khayat and Mahmoud Khayat, living in Sydney who tried to place a bomb on an Etihad flight and later also sought to conduct a terror attack in Australia using an improvised chemical weapon.[18] In addition to the Australia-based Khayat brothers, two other people—both Islamic State operatives based in the Levant—played critical roles in the plot. This included Tarek Khayat, another brother of Mahmoud and Khaled, and Basil Hassan. One of the unique and innovative features of the plot was that the "Islamic State had provided direct logistical support" to the plot "by mailing the [Australia-based] Khayat brothers a partially constructed bomb," a key resource.[19] The package that Islamic State figures sent to Australia from Turkey via DHL "contained a welding machine with an explosive substance hidden inside a copper coil."[20] External direction was also a key feature, as "during the course of the plot" an Islamic State operative "provided guidance and instructions via the Telegram messaging app to the Khayat brother in Sydney."[21] The instructions provided included details "for how to wire the bomb," a form of knowledge transfer. This involved a technical back and forth as Khaled "repeatedly sent photos to both Tarek and Hassan to demonstrate his progress and seek feedback." When the plan to smuggle a bomb onto the Etihad flight ran into problems, "Khaled was sent [additional] instructions on how to create a chemical compound that could be dispersed as a lethal gas."[22] The 2017 foiled plot—described as "the most serious Islamic State plot" Australia "has ever faced"[23]—highlights the importance of the four key enabling factors and how the Islamic State creatively used them in combination to almost pull off a devasting terror attack.

The second concept, Figure 4, introduces a layered, defense and degradation in depth CT pressure framework. While layered defense, or defense in depth, is not a new idea or concept, over the past decade it has not been as well used to conceptually guide U.S. counterterrorism strategy or efforts.[d] This is unfortunate because the general defense in depth construct can help to strategically orient CT strategy and CT pressure campaigns—and gauge the strategic effectiveness of those efforts.

Some modifications to the general defense in depth concept help bring the idea, and its value, to life. The first is expanding the posture of the concept itself so it includes offensive components as a core element, in addition to those that are defensively focused. One of the key lessons the United States learned from 9/11 and the past two decades of counterterrorism activity is that offensive and persistent forms of CT activity are needed to degrade and disrupt key VEO actors. A defensive posture, even one oriented around defense in depth, is not enough. Figure 4 incorporates the offensive element by positioning the framework around defense *and* degradation in depth.

The second modification is the overlaying of key CT actions

[d] In the early years after 9/11, the concepts of layered defense and defense in depth were used to help orient the United States' approach to counterterrorism.

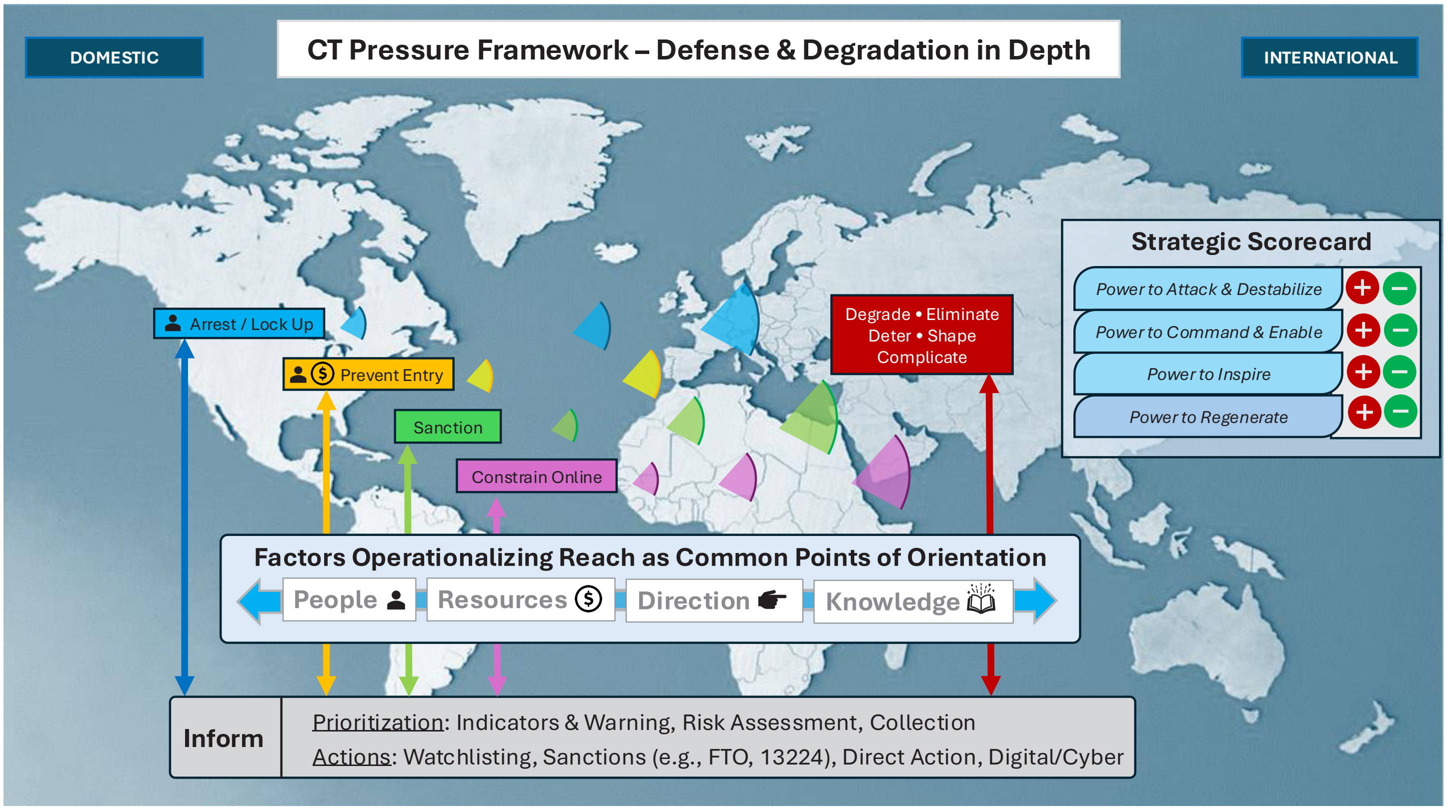

DOMESTIC
CT Pressure Framework – Defense & Degradation in Depth
INTERNATIONAL
Strategic Scorecard
Power to Attack & Destabilize
Power to Command & Enable
Power to Inspire
Power to Regenerate
Arrest / Lock Up
Prevent Entry
Sanction
Constrain Online
Degrade • Eliminate
Deter • Shape
Complicate
Factors Operationalizing Reach as Common Points of Orientation
People
Resources
Direction
Knowledge
Inform
Prioritization: Indicators & Warning, Risk Assessment, Collection
Actions: Watchlisting, Sanctions (e.g., FTO, 13224), Direct Action, Digital/Cyber

Figure 4: CT Pressure Framework – Defense and Degradation in Depth

onto the framework. While the examples highlighted in Figure 4—arrest/lock up, prevent entry, sanction, constrain online, and degrade, deter, etc.—are not exhaustive, they highlight how each of these action areas, and how they are approached, can be layered. In many ways, the United States and its partners have already been approaching some of these CT action areas in that type of manner.

The arrest and lock up action area, highlighted in blue, is a useful example. U.S. efforts to identify, arrest, and convict extremists and prevent acts of terrorism are strongly rooted in the U.S. homeland, and include actions taken by the FBI, various DHS components, state, local, tribal, and territorial law enforcement partners, and engagement with civil society organizations, communities at risk, and private sector companies. Through various mechanisms—multi-nationally through entities like Interpol, Europol, and Operation Gallant Phoenix; bilaterally through country-to-country partnerships; and jointly or unilaterally through direct action—the United States can extend both the defensive/protective and offensive/disruptive elements of the arrest/lock up area. This extension is represented by the shaded blue arcs that extend geographically that have a dual purpose. Offensively, they enable and bolster layered mechanisms for the United States to apply CT pressure in different geographic locations, and defensively, they create layered obstacles that complicate VEO efforts. Efforts that aim to prevent entry, sanction, constrain online, and pursue terrorists and their enablers abroad can be guided or bolstered by similar layered approaches.

The framework also includes two types of cross-cutting factors. These include: 1) the four factors—people, resources, direction, and knowledge—that help VEOs to operationalize their reach, which, as discussed earlier, can serve as common points of orientation for CT pressure and 2) data injects from key CT actions that can inform key tasks (e.g., threat prioritization, risk assessments, indicators and warning effort, collection) and tee-up future kinetic and non-kinetic CT pressure approaches.

The framework's final contribution is a strategic VEO power scorecard,[e] with the goal being for U.S. CT pressure efforts to be evaluated in relation to the four VEO power areas. Data and metrics from various sources, including CT actions, other U.S. interagency activity (e.g., relevant U.S. Customs and Border Protection enforcement data, etc.), from partners, and open sources could be used to populate and score VEO power across time. Those results could also inform how, where, and in what manner CT pressure efforts should be modulated.

PART III: Applying the Concepts and Frameworks

The Islamic State Case

This final section evaluates the Islamic State in relation to the VEO power score card. It also examines some of the action elements of the defense and degradation in depth framework so that the evaluative capacity and features of the frameworks presented in this article are brought to life.

As a global movement, the Islamic State draws strength from its ideology and vision of the world *and* its globally distributed array of formal regional affiliates, which provide reach and network resilience. Since losing control of its territorial 'caliphate' in 2019,

[e] There have been other approaches to scorecard the threats posed by al-Qa`ida and the Islamic State. One key example is the Critical Threat Project's "State of al Qaeda and ISIS" annual series. For an example, see Katherine Zimmerman and Nathan Vincent, "The State of al Qaeda and ISIS in 2023," Critical Threats Project, September 11, 2023.

the Islamic State's core network based in Syria and Iraq has sought to rebuild. Some regional Islamic State affiliates, such as the Islamic State node still active in the Philippines, have followed suit.[24] Other regional affiliates—especially those based in West Africa and the Sahel—have intensified their local and regional activity and have made territorial and regional reach gains, while still others including ISK have played a much more active and leading role in external operations over the past several years.

Given its diverse makeup, there are important differences in the strength, orientation, and capabilities of the different Islamic State affiliates. But when the Islamic State is viewed wholistically as a broad-based movement, or system, it has demonstrated an ability over the past two years to make gains across at least three of the four VEO power areas despite considerable forms of CT pressure in some geographic areas. The danger is that the Islamic State continues to make advancements across VEO power areas and/or that its gains intensify.

Power to Attack and Destabilize

Over the past five years, the United States and its partners have placed a considerable amount of pressure on the Islamic State's core element based in Syria and Iraq. This has included the removal of at least three Islamic State 'caliphs' through direct action CT raids in fairly quick succession. That form of pressure has been complemented by pressure being applied against the Islamic State's mid- to senior-level leadership ranks. For example, since late August 2024 "U.S. forces in the Middle East have killed 163 Islamic State group militants and captured another 33 [militants] in dozens of operations in Iraq and Syria."[25] This included the removal of "over 30 senior and mid-level ISIS leaders."[26]

While those operations are important and have made it harder for the Islamic State to function and plan attacks, other data points suggest that the type and form of pressure has not been enough. This is because while the Islamic State "mostly remains on the back foot in Iraq, the U.S. is struggling to contain the group's growing foothold in Syria's Badiya."[27] In 2024, "the number of [Islamic State] attacks in Syria has more than doubled … despite an increase in U.S. air strikes."[28] Some analysts believe that the "reality is far worse" though, as the Islamic State "claims only a fraction of its attacks in Syria and Iraq in an apparent effort to conceal its methodical recovery," which may mask the true picture.[29]

Just as worrying are signs the Islamic State in its previous core base of Iraq and Syria is reconstituting its external operations capabilities. The commander of U.S. Central Command, General Michael Kurilla, has also warned that "Isis in Syria and Iraq has grown so rapidly that it is again capable of carrying out attacks abroad."[30 f] In October, Ken McCallum, the head of MI5, expressed similar concerns about the reconstitution of the Islamic States' external operations capabilities, with particular concern focused on ISK: "Today's Islamic State is not the force it was a decade ago … but after a few years of being pinned well back, they've resumed their efforts to export terrorism."[31]

ISK's power to attack and destabilize has evolved in a different way over the past five years. As reflected in Table 1 below, the network's ability or interest in conducting attacks in Afghanistan has declined considerably since 2021 and 2022.[32] Across the border in Pakistan, the number of attacks attributed to ISK over the same five-year period has remained more consistent, but low.[33]

Table 1: Attacks in Afghanistan Claimed by ISK, 2018-2023[34]

Year	ISK Attacks
2018-2019	400
2019-2020	157
2020-2021	275
2021-2022	314
2022-2023	69

Since 2017, the Islamic State has claimed responsibility for at least four terror attacks in Iran. This has included attacks in 2017, 2018, 2022, and 2024.[35 g] While the 2024 attack was claimed by the Islamic State, and not directly by ISK, it is believed that ISK played a key role in its execution,[36 h] illustrating how external operations involve different inputs from across the movement.[37]

The drop in local ISK attacks in Afghanistan and the steadier, low-level pace of regional ISK operations is contrasted by the "tick up" in the number of transnational terror plots and attacks that involved inputs or have been tied to ISK over the past two years.[38] This has resulted in an "increased external threat from ISIS-Khorasan."[39] As noted by *The Economist*, the network's highly lethal attack in Moscow in March of this year "was *the* clearest warning that Islamic State …, seemingly smashed five years ago, is returning to spectacular acts of international terrorism."[40]

The orientation and activity of Islamic State-affiliated networks in Africa have been more locally and regionally focused, but the ability of the Islamic State's nodes on the continent to destabilize is not dropping; for many, it has increased. As noted by Aaron Zelin in March of this year, "the Islamic State is once again racking up territorial gains around Africa." For example, "In Mali, [Islamic State] forces seized portions of the rural eastern Menaka region and the Ansongo district in southern Gao last year, while foreign fighters reportedly became more interested in traveling to Wilayat Sahel, the group's self-styled 'Sahel Province.' Elsewhere, [Islamic State] 'provinces' in Somalia and Mozambique have taken over various towns in the Puntland and Cabo Delgado regions [in early 2024], further destabilizing the area and in some cases jeopardizing important natural gas projects."[41] There is the risk that "if left unchecked, they could threaten U.S. and Western interests in the future."[42]

The trendline of attacks conducted by Islamic State Sahel (also known as the Islamic State in the Greater Sahara) since 2017 is illustrative of the rise of activity, and the development of operational capacity for key affiliates on the continent.[43] It also provides an

[f] This is a departure from a little more than a year ago when the United Nations Monitoring Team assessed: "While the previously well-developed external operations capability of both the ISIL (Da'esh) and Al-Qaida core groups remains diminished and largely constrained." See "Thirty-second report of the Analytical Support and Sanctions Monitoring Team," United Nations, July 2023.

[g] The Iranian government has also blamed the group for an attack in 2023. See Maziar Motamedi, "Iran blames ISIL for shrine attack, arrests foreign nationals," Al Jazeera, August 14, 2023.

[h] It is possible that the 2023 attack was also executed by ISK. See "Tajik National Behind Deadly Attack On Shah Cheragh Shrine In Iran, Regional Chief Justice Says," RFE/RL, August 14, 2023.

important counterpoint to the activity of ISK, which has placed more emphasis on external actions than local and regional ones.

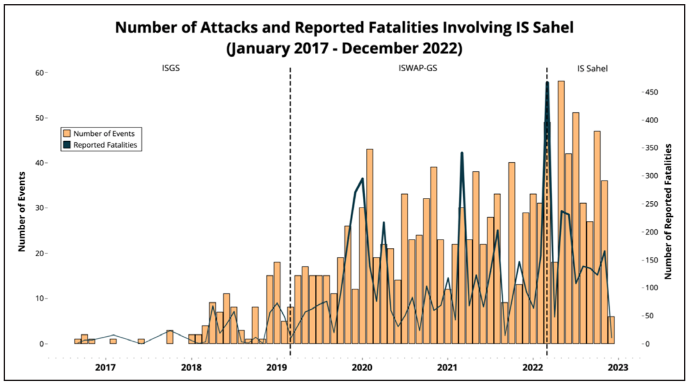


Figure 5: Temporal ACLED Data Illustrating Islamic State Sahel Attacks[44]

Like ISK, Islamic State-Somalia "is a study in contrasts. At home, [in Somalia] its impact is limited. It appears, however, to play an outsize, if still vague, role in the Islamic State's global operations."[45] When it comes to transnational terrorism, there is growing concern about the network. As noted by Caleb Weiss and Lucas Webber in this publication, "Over the last three years, the Islamic State's Somalia Province has grown increasingly international, sending money across two continents and recruiting around the globe. There are also growing linkages between the group and international terrorist plots, raising the possibility that Islamic State-Somalia may be seeking to follow in the footsteps of Islamic State Khorasan in going global."[46] While not a global threat today, that same possibility could extend to other Islamic State affiliates in Africa at some point in the future, too.

Assessment: Differences exist across various Islamic State components, but when these data points are viewed in aggregate, the Islamic State's overarching power to attack and destabilize is up across local, regional, and global levels. Over the past two years, the Islamic State has not been able to conduct an attack in the United States—an important win, but the movement's external operations capabilities are arguably more developed than they were two years ago, a dynamic that places the U.S. homeland at greater risk.

Power to Command and Enable

It is difficult to assess the Islamic State's ability to command and enable through open sources, as internal documents produced by the Islamic State and its affiliates and communications within and across the movement's nodes likely provide much more granular insights about this issue.

One high-level window into the Islamic State's power to command is the composition of the movement's global network of affiliates, and whether the number of formal affiliates has grown, reduced in size, or remained steady across time. This is because if the central leadership element of the Islamic State was viewed as not capable or not a useful partner, one would expect various affiliates to be less embracing of the movement and its brand. While the composition of Islamic State affiliates has changed at key periods, the most active and influential regional Islamic State nodes have maintained the affiliation and remained outwardly loyal. This is not to suggest that there have not been disagreements or points of friction between affiliates and the 'center'[i] but rather that the number and quality of formal Islamic State partners has remained mostly stable.

In July 2023, the United Nation's Monitoring Team held the view that "the trend of counter-terrorist pressure prompting ISIL ... to adopt flatter, more networked and decentralized structures has continued," and that this provided affiliated groups with more operational autonomy.[47] The report also assessed that the role of the Islamic State's "overall leader has become less relevant to the group's functioning." At the time, member states had "little evidence of command and control of the affiliates from the core leaderships."[48] While that view may have been true in 2023, it is less clear if the same can be said today. However, despite the lack of reporting and public clarity about the role the 'center' has recently played in guiding affiliate activity, the United Nations also assessed it had "not had an impact on the level of violence perpetrated by the affiliated groups and their perceived success."[49] Or, in other words, command and control dynamics did not appear to have meaningfully affected affiliate attack campaigns and how those are viewed.

This may be partly because the Islamic State has adapted and made changes in its structure and approach that appear designed to mitigate counterterrorism pressure effects.[50] A key lens into these dynamics is the Islamic State's General Directorate of Provinces (GDP).[51] The primary role of the GDP has been to serve as a "bridge between the Islamic State's central leadership and its various provinces," with it functioning as a core mechanism through which leaders can "issue orders on how provinces should organize their economic institutions, handle their finances, and pursue their military strategy." But, as noted by Tore Hamming in this publication, the GDP's importance and influence has also evolved over time, and it "now allegedly occupies a central position in the execution of external terrorist operations." Purported internal Islamic State documents covering the 2015-2020 period released online showed that the GDP "has tremendous institutional power within the Islamic State and directs how provinces are organized and set up."[j]

These adjustments were not just administrative; they appear to have also been underpinned by key geographic changes. As noted by Aaron Zelin, while the GDP "has previously been based in Syria ... new information suggests ... at least at the highest levels ... [that] it might now have centrality in Somalia."[52] This view is tied to recent reporting that the Islamic State had anointed the leader of its affiliate in Somalia, Abdulqadir Mumin, as its overall leader—the global 'caliph.'[53] Various terrorism researchers are skeptical of the claim, and some have put forward the theory that Mumin may have been appointed to serve as the emir of the GDP instead.[54] But regardless of which theory may be correct, they both suggest that the Islamic State is continuing to adapt its organizational structures and approach in response to repeated senior leadership losses

[i] One example highlighted by the United Nations: "With Omar's death and the relative silence from Abu Yasir Hassan (S/2023/549, para. 13), who has sought to disassociate ASWJ from ISIL following fundamental disagreements over reporting lines, finance, and leadership issues." See "Thirty-third report of the Analytical Support and Sanctions Monitoring Team," United Nations, January 29, 2024.

[j] While the collection of documents reviewed by Hamming provided insights into the dynamics of center and periphery relationships during the 2015-2020 period, the author is not aware of similar documents covering the 2020-2024 period having been made public.

that have affected the core network in the Levant. The survival implications of these changes seem clear. As noted by Zelin: "In many ways, the key aspects that animate the Islamic State as an organization (governance, foreign fighter mobilization, and external operations) remain, they have just moved from primarily being based out of or controlled by its location of origin in Iraq and Syria to being spread across its global provincial network."[55] The elevation of Mumin, given his geographic location, speaks to this. The critical role played by other Somalia-based Islamic State leaders, such as Bilal al-Sudani who according to the Department of Defense "was responsible for fostering the growing presence of ISIS in Africa and for funding the group's operations worldwide, including in Afghanistan" speaks to it as well.[56] Other reporting also suggests that the Islamic State's dispersion strategy is not limited to leadership dynamics but also involves efforts to "diversify … some of their combat power to Africa, to Central Asia."[57]

Over the short term, decentralization and dispersion provide depth and are likely to help the Islamic State to enhance its resilience, especially if counterterrorism pressure against other key dispersed command and control nodes remains limited. But, as al-Qa`ida's experience highlights, over the longer-term decentralization and dispersion could also introduce, or compound existing risks for the group.

ISK's power to virtually enable, guide, and in various cases direct radicalized individuals located abroad has also evolved into a growing problem.[58] Evidence of this is seen in the steady stream of ISK-linked arrests, plots, and attacks over the past two years that involved ISK members providing some form of remote instruction, including its devastating attack in Moscow.[59]

Assessment: The lack of data inputs makes this power area difficult to assess. CT pressure has degraded the ability of the Islamic State's core element based in Syria and Iraq to command and enable across the broader Islamic State enterprise. But despite the pressure, other Islamic State elements have generally been able to maintain their operational pace and capacity. In addition, ISK's ability to enable remote plotters has not diminished; it has arguably grown. The Islamic State also appears to be adapting its organizational structures and posture to limit the impact of CT pressure, reconstitute capabilities, and build resilience across its movement.

Power to Inspire

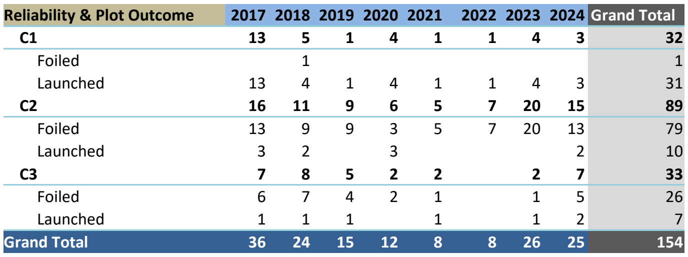
As noted earlier, a VEO network's power to inspire can be measured by its ability to offer a compelling vision and market itself, to recruit members, and to inspire individuals located abroad to engage in operational activity—either in direct partnership with the group or on behalf of it.

The Islamic State's loss of its territorial caliphate in Syria and Iraq has diminished its allure and its ability to inspire the masses of recruits, especially foreigners, that the core node in the Levant achieved during its heyday. But the ability of various Islamic State nodes to maintain or increase their local and regional attacks speaks to the capacity of those nodes, and the Islamic State generally, to remain attractive and to successfully recruit. While far from what it used to be, even the Syria-based fighters of the Islamic State have been able to enhance their operational capacity over the past year, a feat which requires committed recruits. Despite reported challenges in some areas,[k] manpower does not appear to be a broad issue for the movement.

The Islamic State's ability to virtually motivate distantly located individuals to align themselves with the movement, to seek formal connections, to reach out for operational guidance, or to conduct acts for the movement (or on its behalf) has also picked up over the past two years.

This is particularly evident in Europe. A critical resource in this regard is FFI's Jihadi Plots in Europe Dataset (JPED).[l] The JPED includes data on launched and foiled terror plots in Western Europe since 1994, and results are organized into three reliability categories based on the level of documentation that supports each case.[m] The most reliable and best sourced cases are C1 and those that are more dubious and not as well sourced are C3. Table 2 below provides a summary of Islamic State-linked plots from 2017 to early September 2024 organized by reliability measure. While C1 cases paint a more measured picture, the broad trend across all data categories is that Islamic State-linked plots have risen in Western Europe over the past two years from a lower period of activity (2020-2022) that coincided with the coronavirus global pandemic. When all C3 cases are excluded, the trend still holds. The collection of cases includes plots tied to single individuals and small groups, a considerable number of cases involving minors, plots with connections to ISK and the Islamic State—some of which involved remote contact and directions being provided, and plots where direct contact with Islamic State nodes or personnel was not publicly apparent.[n]

Table 2: Islamic State-Linked Plots (Launched and Foiled), 2017-September 2024



Reliability & Plot Outcome	2017	2018	2019	2020	2021	2022	2023	2024	Grand Total
C1	**13**	**5**	**1**	**4**	**1**	**1**	**4**	**3**	**32**
Foiled		1							1
Launched	13	4	1	4	1	1	4	3	31
C2	**16**	**11**	**9**	**6**	**5**	**7**	**20**	**15**	**89**
Foiled	13	9	9	3	5	7	20	13	79
Launched	3	2		3				2	10
C3	**7**	**8**	**5**	**2**	**2**		**2**	**7**	**33**
Foiled	6	7	4	2	1		1	5	26
Launched	1	1	1		1		1	2	7
Grand Total	**36**	**24**	**15**	**12**	**8**	**8**	**26**	**25**	**154**

[k] One example is Islamic State-Somalia, as according to the International Crisis Group: "Sustained recruitment in Somalia has proven a challenge, due both to Al-Shabaab's strength and IS-Somalia's narrow clan base." "The Islamic State in Somalia: Responding to an Evolving Threat," International Crisis Group, Briefing 21 / Africa, September 12, 2024.

[l] The author would like to thank Petter Nesser, who kindly shared a copy of JPED dataset, and helpful information about its features and limitations. The version of the JPED shared includes case information up to early September 2024, and it is more up to date than the version and data that Petter Nesser and Wassim Nasr used for their June 2024 *CTC Sentinel* article. For background on JPED, see Petter Nesser, "Introducing the Jihadi Plots in Europe Dataset (JPED)," *Journal of Peace Research* 61:2 (2023). See also Petter Nesser and Wassim Nasr.

[m] As explained by Nesser: "It classifies JPED's plots into three categories based on documentation. For an incident to be included we need documentation that the perpetrator is jihadi. Secondly, we need documentation that an attack was launched, or in the making (e.g. bomb-making). Last, we need documentation about targeting. If all aspects are well documented, the case is category 1 (C1). If two aspects are well documented, it is category 2 (C2). If there are uncertainties regarding two or more aspects, the case is defined as category 3 (C3). The purpose is to avoid generalizing from dubious (C3) cases." Nesser.

[n] The coding of plot connection type can be challenging. As noted by Nesser, "open sources seldom can specify connection type with a high degree of certainty. And it is very difficult to follow and update cases as investigations move along." Author correspondence with Nesser, November 2024.

U.S. Army soldiers prepare to go out on patrol from a remote combat outpost on May 25, 2021, in northeastern Syria. (John Moore/Getty Images)

The central 'glue' that appears to be enabling these plots is the Islamic State's propaganda combined with its virtual activity and remote enabling. As noted by MI5 head McCallum, "it's hard to overstate the centrality of the online world in enabling today's threats."[60] Data from the Washington Institute's Islamic State Worldwide Activity Map situates the central importance of online activity for the group: "Since March 2023, the IS Activity Map has tracked 470 relevant legal cases in forty-nine different countries. Of these, 103 cases featured some type of IS-related attack plot, *88 involved social media activity or other propaganda*, 55 involved financial transfers or fundraising, 42 were related to foreign fighters, and 38 involved recruitment activities."[61]

A core element of the Islamic State's virtual activity involves the use, and weaponization of, encrypted communication apps, with emphasis placed on platforms such as Telegram. For example, "in at least 44 percent of the 57 virtually directed Islamic State plots between 2014 and 2020," that researcher Rueban Dass studied "Telegram was used as a method of communication."[62] Further, according to Aaron Zelin: "A lot of Islamic State Khurasan Province-related external operations plotting has more to do with recruitment and inspiration online and guidance through encrypted applications than an individual traveling abroad to gain fighting and training experience and then returning home to plot. While this model is not new, it's the first time we've seen it be successful while a group is not in control of territory and shrinking in its local capabilities."[63]

The recent plot trends observed in Europe and the evolution of the Islamic State's virtual approach present threat implications to other areas, including the United States. That issue has not been lost on senior U.S. government CT leaders. For example, in October 2024 Acting Director of NCTC Brett Holmgren noted how "recent attacks and disrupted plots in Austria, Belgium, France, Germany, Italy and Sweden are manifestations of the threat we're worried about here at home—young, vulnerable lone actors or loosely formed groups, often only connected virtually, drawing inspiration or guidance from ISIS to radicalize online and plan attacks."[64]

That worry is well placed because "violent extremists who are not members of terrorist groups remain the most likely to successfully carry out attacks in the United States."[65] Indeed, since 9/11 homegrown violent extremists "have conducted 41 of the 49 terrorist attacks in the United States."[66]

According to the Washington Institute's Islamic State Worldwide Activity Map, which tracks inspired, directed, and guided plots and attacks linked to the group, there was one case in the United States in 2023. In 2024, as of mid-November, there have been five, a considerable rise.[67] [o]

Assessment: The Islamic State's ability to inspire, and the way it does so, varies across its components, but in aggregate

[o] The author would like to thank Aaron Zelin for this data input.

the movement maintains its ability to inspire. This capability is being reconstituted and for some affiliates such as ISK, which has leveraged virtual means and modalities to translate inspiration into more plots and operational attempts, it has grown. When it comes to CT pressure, this is a key area that deserves more strategic thought and attention.

Power to Regenerate

The Islamic State's power to regenerate is a two-sided coin. One side reflects steps the Islamic State and its partners take to regenerate capabilities. The other side reflects the will and posture of governments and coalitions to continue to apply meaningful forms of pressure to degrade the Islamic State over the short, mid, and longer terms. The regenerative outcome is highly dependent on how the two sides of the coin interact, and how they influence each other.

Like the power to command and enable, it is difficult to study a VEO's power to regenerate using open sources. This sub-section evaluates the Islamic State's regenerative capacity in relation to key resources (e.g., manpower and finances), operational capacity (i.e., how it makes use of those resources), and challenges and opportunities that could help the movement to rebuild.

As noted earlier, existing manpower does not appear to be an issue for the Islamic State generally. In certain locations like Syria, there also remains a lot of additional manpower potential that the group could tap into and use to either expand or intensify activity if not managed carefully. This includes some "9,000 Islamic State fighters [who] remain in jails across northeastern Syria." As reported by *The Wall Street Journal*:

> *The group has made no secret of its intention to free its comrades so they can return to the battlefield. Twice this year, insurgents have tried to stage breakouts from detention facilities. In one case, an Islamic State suicide bomber tried to breach the gate of a Raqqa jail in a three-wheeled auto rickshaw filled with explosives. There are also some 43,000 Syrian, Iraqi and other displaced people living in camps in northeastern Syria, including many wives and children of jailed Islamic State fighters whom the SDF and U.S. see as potential recruits for the next generation of militants.*[68]

So, on the manpower side—at least in Syria—there is a lot of latent potential, especially if counterterrorism pressure is lifted. These dynamics could also be heavily influenced by changes made to the U.S. mission in Syria, the plan to end the "U.S.-led coalition's military mission in Iraq … by September 2025,"[69] and the contours of the future bilateral U.S.-Iraqi defense relationship.

On the financial side, the Islamic State in its former core operating area in Iraq and Syria has not been able to regenerate, but it has been making do with far less resources than it had during its heyday.[70] In August, the CTC published a broad assessment by Jessica Davis on the financial future of the Islamic State. It found:

> *The future of the Islamic State's financial infrastructure is networked, resilient, and adaptive. The network has achieved this by focusing local groups on finance and governance and combining new and old methods of moving funds. The network also has redundancies: Revenue-sharing between groups and provinces allows the redistribution of funds to weaker groups or those that have suffered disruption, either because of between-group competition in their areas of operations or because of state or international CTF (countering the financing of terrorism) activities. As a result, countering the financing of the network will be an international coordination challenge, exacerbated by the great power division in some of the institutions for combating terrorism like the U.N. Security Council (and associated monitoring teams), and the expulsion of Russia from the Financial Action Task Force.*
>
> *There are currently insufficient kinetic counterterrorism efforts being applied to disrupt the territorial control of Islamic State sub-groups. Without a sustained and effective kinetic counterterrorism approach, the group's revenue-generating taxation and extortion activities will remain operational. Further, cash storage sites used by these groups will continue to amass funds, helping to sustain groups (and the broader network) over the long term. The current lack of investigative capacity to disrupt terrorist financing activities (through investigations and arrests) of terrorist financiers also remains a challenge for CTF and means that many Islamic State financiers and financial facilitators can operate with impunity. This is true for both the areas where Islamic State sub-groups operate directly, but also for their support areas outside direct conflict zones.*

So, even if the Islamic State has not been able to regenerate its financial resources, it has adapted. It also appears to have 'runway' in various locales around the world to continue to acquire and pull resources into the movement without much resistance.

The Islamic State's operational capacity varies across countries and regions. In Syria, the group has been making regenerative strides. In Iraq, in 2024 the group has conducted fewer attacks than in 2023, potentially a sign that it has less capacity.[71] In Africa, the operational capacity of the Islamic State's affiliates is generally trending up.

Assessment: The Islamic State's core network in the Levant has not regenerated to levels observed during the 2014-2017 period—far from it—but the core network has been making regeneration strides. Other Islamic State affiliates have been helping the movement to adapt, bolster its resilience, and regenerate in a more collective way as a system.

The scores from the four VEO powers paint a not-so-great picture, as the Islamic State's power is up or increasing in at least three of the four areas (power to attack and destabilize, inspire, and regenerate) from what it was years prior. The Islamic State's ability to command and enable is split. Its power to command appears to be down, but it has made gains in its ability to enable since the loss of the movement's physical caliphate.

The layered defense and degradation in depth framework also holds evaluative potential. For example, the June arrest of the eight Tajiks who gained entry to the United States and who were suspected of having ties to Islamic State members was touted by the Biden administration as a success because these individuals were identified, apprehended, and a potential plot was thwarted. The case is a good news story because nothing happened, and it was held out as a model to demonstrate how the "systems we have built and refined since 9/11 to keep the Homeland safe are working."[72] The efforts by U.S. government personnel to monitor and apprehend the eight individuals were a success, but there were also failings. When the ability of eight foreign nationals with suspected ties to a key terrorist group are evaluated in relation to the prevent entry action area included in the framework, it highlights how the system caught these individuals on the last line of defense—after they were already in the United States. So, while the detention of the eight suspects was a partial and important success, the case also illustrates how some of the United States' defense mechanisms failed even while the overall layered system of defense succeeded. Identifying how and where defenses fall short is important so those deficiencies can either be addressed or approaches can evolve.

Conclusion

When it comes to counterterrorism, the United States has been living through an inflection point. It wants to focus less on terrorism, but key terrorist adversaries remain committed. The terrorism environment has also been evolving, and the United States and its partners need to contend with a terror landscape that is "more diverse, decentralized, and complex"[73] than it used to be, which presents its own set of challenges. This includes threats posed by mainstay salafi-jihadi networks, such as the Islamic State and al-Qa`ida and their affiliated offshoots, but also inspired or loosely connected individuals, actors motivated by other ideologies and grievances, and the rise in state-sponsored or state-supported terror, as typified by the devasting attack on Israel on October 7, 2023, and the rise of the Houthi threat. Changes in the environment share connective tissue with, and are being driven by, adaptations—and adaptive strategies—that have been embraced by terror networks. The Islamic State's operationalization of its virtual enabling model is an important case in point.

Some of these adaptations have likely been initiated as a way to evolve around counterterrorism pressure. As a result, approaches to counterterrorism need to evolve along with them or adapt to better shape these adversarial changes in the first place. This article provided context and frameworks to help counterterrorism practitioners and strategists to understand and evaluate the power of VEOs and how CT pressure efforts or campaigns to degrade such entities could be approached and assessed from a strategic perspective. The Islamic State case study included at the end of this article highlighted how counterterrorism pressure has shaped the trajectory of that movement and made things much more difficult for its key node in the Levant. But that case study also drew attention to the limits of existing CT pressure approaches, the need for flexible and responsive approaches, and how additional thought and consideration should be given to the where, when, and how of CT pressure—so CT gains can be maintained, and so CT approaches can evolve to stay ahead of the threat. CTC

Citations

[1] Jim Garamone, "Defeat-ISIS Group Adapts to Continue Pressure on Islamic State," DoD News, October 11, 2024.

[2] "Beware, global jihadists are back on the march," *Economist*, April 29, 2024.

[3] Catherine Belton and Robyn Dixon, "Terrorist attack in Russia exposes vulnerabilities of Putin's regime," *Washington Post*, March 24, 2024.

[4] Adrian Blomfield, "The Return of al-Qaeda and Islamic State," *Telegraph*, October 12, 2024.

[5] Aaron Zelin, "Islamic State on the March in Africa," Washington Institute, March 1, 2024.

[6] Adam Goldman, Eric Schmitt, and Hamed Aleaziz, "The Southern Border, Terrorism Fears and the Arrests of 8 Tajik Men," *New York Times*, June 25, 2024.

[7] Ibid.

[8] Graham Allison and Michael J. Morell, "The Terrorism Warning Lights Are Blinking Red Again," *Foreign Affairs*, June 10, 2024.

[9] See "Chapter 8 – The System Was Blinking Red," 9/11 Commission Report, July 22, 2004.

[10] Don Rassler, *The Compound Era of U.S. Counterterrorism* (West Point, NY: Combating Terrorism Center, 2023).

[11] Paul Pillar, "The Instruments of Counterterrorism," *U.S. Foreign Policy Agenda* 6 (2001).

[12] Rassler.

[13] Pillar.

[14] For background, see "Counter-terrorism Strategy (CONTEST) 2023," UK Home Office, July 18, 2023.

[15] "National Strategy for Counterterrorism of the United States of America," The White House, October 2018.

[16] The literature of leadership decapitation suggests this is a key issue to consider. For background, see Bryan C. Price, "Targeting Top Terrorists: How Leadership Decapitation Contributes to Counterterrorism," *International Security* (2012) and Jenna Jordan, "When Heads Roll: Assessing the Effectiveness of Leadership Decapitation," *Security Studies* 4:18 (2009).

[17] Ellen Nakashima, "Israel, at behest of U.S., killed al-Qaeda's deputy in a drive-by attack in Iran," *Washington Post*, November 14, 2020. See also Assaf Moghadam, "Marriage of Convenience: The Evolution of Iran and al-Qa`ida's Tactical Cooperation," *CTC Sentinel* 10:4 (2017) and Cole Bunzel, "Why Are Al Qaeda Leaders in Iran?" *Foreign Affairs*, February 11, 2021.

[18] For background, see Andrew Zammit, "Operation Silves: Inside the 2017 Islamic State Sydney Plane Plot," *CTC Sentinel* 13:4 (2020). See also Mette Mayli Albæk, Puk Damsgård, Mahmoud Shiekh Ibrahim, Troels Kingo, and Jens Vithner, "The Controller: How Basil Hassan Launched Islamic State Terror into the Skies," *CTC Sentinel* 13:5 (2020).

[19] Zammit.

[20] Ibid.

[21] Albæk, Damsgård, Ibrahim, Kingo, and Vithner.

[22] Zammit.

[23] Ibid. Andrew Zammit's article also provides insight into how the plot was disrupted.

[24] Haroro Ingram, "The Cascading Risks of a Resurgent Islamic State in the Philippines," United States Institute of Peace, January 9, 2024.

[25] Ellen Mitchell, "US military carried out 95 counter-ISIS operations in last 60 days," Hill, November 4, 2024.

[26] Ibid.

[27] Blomfield. For additional context on Iraq data, see Charles Lister, "CENTCOM says ISIS is reconstituting in Syria and Iraq, but the reality is even worse," Middle East Institute, July 17, 2024.

[28] Ibid. See also Michael Phillips, "In Syria's Hinterlands, the U.S. Wages a Hidden Campaign Against a Resurgent Islamic State," *Wall Street Journal*, August 12, 2024.

[29] Lister.

[30] Blomfield.

[31] Blomfield. For full context of quote, see "Director General Ken McCallum gives latest threat update," MI5, October 8, 2024.

[32] Data in Table 1 is from Aaron Zelin, "The Islamic State's External Operations

are More than Just ISKP," Washington Institute, July 26, 2024. See also Amira Jadoon, Abdul Sayed, Lucas Webber, and Riccardo Valle, "From Tajikistan to Moscow and Iran: Mapping the Local and Transnational Threat of Islamic State Khorasan," *CTC Sentinel* 17:5 (2024).

[33] Analysis of ACLED data for the period. See also Jadoon, Sayed, Webber, Valle.

[34] Zelin, "The Islamic State's External Operations are More than Just ISKP."

[35] For background on early attacks, see Aaron Zelin, "The Islamic State Attacks the Islamic Republic," Washington Institute, October 31, 2022.

[36] See Aamer Madhani, "US warned Iran that ISIS-K was preparing attack ahead of deadly Kerman blasts, a US official says," Associated Press, January 25, 2024, and Jadoon, Sayed, Webber, and Valle.

[37] Aaron Zelin, "A Globally Integrated Islamic State," War on the Rocks, July 15, 2024.

[38] For background, see Petter Nesser and Wassim Nasr, "The Threat Matrix Facing the Paris Olympics," *CTC Sentinel* 17:6 (2024); Javed Ali, "The Islamic State's Afghanistan-based affiliate is emerging as a global menace," Defense One, March 26, 2024; Zelin, "The Islamic State's External Operations are More than Just ISKP;" and Jadoon, Sayed, Webber, and Valle.

[39] "NCTC Director Christine Abizaid, Statement for the Record, Senate Committee on Homeland Security and Government Affairs," October 31, 2023. For background on recent ISK plots and attacks, see Nicolas Stockhammer and Colin P. Clarke, "Learning from Islamic State-Khorasan Province's Recent Plots," Lawfare, August 11, 2024. See also Aaron Zelin, "The latest ISKP arrest in Germany is now the 21st external operations plot/attack . . .," X, March 19, 2024.

[40] "Beware, global jihadists are back on the march."

[41] Zelin, "Islamic State on the March in Africa."

[42] "Remarks by Acting Director of the National Counterterrorism Center at Cipher Brief Threat Conference," Cipher Brief Threat Conference, October 6, 2024.

[43] For background on Islamic State Sahel, see Héni Nsaibia, "Newly restructured, the Islamic State in the Sahel aims for regional expansion," ACLED, September 30, 2024.

[44] Ibid.

[45] "The Islamic State in Somalia: Responding to an Evolving Threat," International Crisis Group, Briefing 21 / Africa, September 12, 2024.

[46] Caleb Weiss and Lucas Webber, "Islamic State-Somalia: A Growing Global Terror Concern," *CTC Sentinel* 17:8 (2024).

[47] "Thirty-second report of the Analytical Support and Sanctions Monitoring Team," United Nations, July 25, 2023.

[48] Ibid.

[49] Ibid.

[50] Zelin, "A Globally Integrated Islamic State."

[51] For background, see Tore Hamming, "The General Directorate of Provinces: Managing the Islamic State's Global Network," *CTC Sentinel* 16:7 (2023).

[52] Zelin, "A Globally Integrated Islamic State."

[53] For background see Austin Doctor and Gina Ligon, "The Death of an Islamic State Global Leader in Africa?" *CTC Sentinel* 17:7 (2024). See also Weiss and Webber.

[54] Doctor and Ligon.

[55] Zelin, "A Globally Integrated Islamic State."

[56] Eric Schmitt and Helene Cooper, "Senior ISIS leader in Somalia killed in U.S. special operations raid," *New York Times*, January 26, 2023.

[57] Phil Stewart, "At 10-year mark, US and allies weigh future of Islamic State mission," Reuters, October 17, 2024. See also "The Islamic State in Somalia: Responding to an Evolving Threat."

[58] Tom Winter, Ken Dilanian and Julia Ainsley, "ISIS-K behind foiled Election Day terrorism plot, U.S. officials say," NBC News, October 15, 2024.

[59] See Rueben Dass, "Islamic State-Khorasan Province's Virtual Planning," Lawfare, May 19, 2024.

[60] "Director General Ken McCallum gives latest threat update."

[61] Aaron Y. Zelin and Ilana Winter, "One Year of the Islamic State Worldwide Activity Map," Washington Institute," March 20, 2024; emphasis in quote added by the author.

[62] Dass.

[63] Zelin, "A Globally Integrated Islamic State."

[64] "Remarks by Acting Director of the National Counterterrorism Center."

[65] "Calibrated Counterterrorism: Actively Suppressing International Terrorism," *CTC Sentinel* 16:8 (2023).

[66] "Remarks by Acting Director of the National Counterterrorism Center."

[67] For background on the Islamic State Worldwide Activity Map, see Aaron Zelin, "Introducing the Islamic State Select Worldwide Activity Map," Washington Institute, March 21, 2023.

[68] Phillips.

[69] "U.S.-led coalition mission in Iraq to end by September 2025," Reuters, September 27, 2024.

[70] For background, see Jessica Davis, "The Financial Future of the Islamic State," *CTC Sentinel* 17:7 (2024).

[71] Lister.

[72] "Remarks by Dr. Liz Sherwood-Randall for the Soufan Center's Global Summit on Counterterrorism and Political Violence," The White House, September 3, 2024.

[73] "Remarks by Acting Director of the National Counterterrorism Center."

A View from the CT Foxhole: General Bryan Fenton, Commander, U.S. Special Operations Command

By Sean Morrow and Don Rassler

General Bryan P. Fenton is a career Special Forces (Green Beret) Officer. He currently serves as the 13th Commander of U.S. Special Operations Command (USSOCOM) where he oversees all Special Operations for the U.S. Department of Defense. Before assuming command of USSOCOM, General Fenton served as the Commander of Joint Special Operations Command (JSOC). Prior to that, he was the Senior Military Assistant for two U.S. Secretaries of Defense.

General Fenton's other general officer assignments include: Deputy Commander of U.S. Indo-Pacific Command; Commander of U.S. Special Operations – Pacific; and Deputy Commanding General of the U.S. Army's 25th Infantry Division in Hawaii.

CTC: U.S. CT has been going through a more intense evolution over the past five years and the 'Global War on Terrorism' is a thing of the past. What are the top lessons you learned, and that you believe the CT community should take away, from the 'Global War on Terrorism' period?

Fenton: We have certainly seen an evolution in countering terrorism as we rebalance the needs of the country, but within the SOF [Special Operations Forces] enterprise, the CT mission is alive and well. As the adage goes, you may not be interested in terrorism, but terrorism is interested in you. While pressure on VEOs is crucial, we have learned that kinetic action alone is not enough to deter and defeat a radical ideology and that our actions must be informed by the root causes and needs of those who might be attracted to political violence.

Defending the homeland is still and will always remain the number-one priority for the Department; this is complementary to strategic competition and integrated deterrence. I view this as twofold: First, CT allows national attention to remain on the pacing threat without distraction, while directly supporting our teammates at DHS, FBI, and State to protect the homeland; second, CT allows us to continue valuable work with our international partners, while we protect our citizens abroad and carry the best practices forward into the future. This is especially the case with the threat of lone wolf attacks. One of the ways we couch our remit for CT and crisis response globally is that SOF helps our national leaders preserve the strategic focus for the future of the Joint Force, Department, and nation.

There has been a lot of incredible work done to protect our homeland through cooperation with partners domestically and internationally. Think about the monumental, international effort of securing a city like Paris for the Olympics this past summer; what a phenomenal effort. None of this happens magically or in isolation—there's a reason we call it a community—because it takes all of us. SOF works in concert with conventional forces, the intelligence community, our interagency partners, and of course, our allies and partners to make these gains. Terrorists intend to surprise by nature, as demonstrated by attacks from Israel to Iran and Russia. Just as CT is the ultimate team sport, the biggest change is that we've shifted from an away to a home game. We must work faster, collectively—all to stay a step ahead of those who are willing to risk everything to do us harm.

Our forward deployed posture has changed and will continue shift, which can alter our ability to get after bad guys and creates opportunities for VEOs to evolve. Afghanistan, Somalia, and Yemen showcase what happens absent CT pressure; the Sahel offers another example. In an era of online knowledge transfer among unlikely terror groups, the need to innovate and stay ahead of VEO adaption is paramount. Our community must recognize the evolving nature of the threats, while also continuing to evolve ourselves. I firmly believe this evolution is centered on our people, and it can't be done alone. The global SOF community must be on the cutting edge of technology and artificial intelligence. Our partners in academia are also critical to our evolution.

CTC: You previously served as the Deputy Commander of INDOPACOM and as the Senior Military Assistant for two Secretaries of Defense. After a long career conducting tactical operations with strategic impacts, did the experience at the COCOM and OSD change how you viewed the use and application of Special Operations Forces in CT or in other mission sets? How did it inform your views of SOF in strategic competition?

Fenton: I think, if anything, it reinforced that global problems require global solutions. I also learned that in pursuit of these solutions, the entire spectrum of special operations was just so critical to success. The experiences in OSD reinforced my understanding of how SOF are built for competition in a unique way. When you take a strategic view of the global security environment, it becomes quickly apparent that the threats, as outlined in the National Defense Strategy, are rapidly converging. In addition, the character of war is rapidly changing. SOF maintains unique placement and access to conduct our CT remit globally; however, this placement and access are also vital in building partnerships and relationships that underpin SOF's DNA. I see the application of SOF in both CT and competition as complementary efforts. In other words, it's actually okay to walk and chew gum at the same time. The fruits of the CT mission set in places like Ukraine, Colombia, the Philippines, and Central Asia have paid dividends over time in terms of tangible progress in strategic competition. Ultimately, both of these missions sets, when done right, require a whole-of-government approach, which is why our most senior national level leaders see many of these problem sets as intertwined across regions, elements of national power, and geopolitical divides. These global problems will require global solutions. SOF are postured

“We have to realize that while we are ready to win now, when we talk modernization, what we really mean is, ‘What do we need to be able to win tomorrow?’ That’s what modernizing is really about: Winning in the future.”

in more than 80 countries worldwide and perfectly positioned to operate across the elements of national power.

Since you brought up my time at INDOPACOM, I also want to speak specifically about that problem set. In terms of deterrence associated with a Taiwan scenario, USSOCOM takes a conditions-based approach to our day-to-day campaigning—we call it “What Winning Looks Like”—through which we increase our relative influence vis-à-vis our adversaries, deter them in the gray zone, and build warfighting advantages should deterrence fail. By taking such an approach, we can identify the way by which SOF—often with and through our allies and partners—can contribute to creating a *fait accompli* where the PRC has no choice but to accept the status quo with Taiwan and operate within the rules-based international order. We are using this “What Winning Looks Like” construct to communicate how SOF contributes to the Joint Force in competition especially—and as a way to share the “best use of SOF” globally to our fellow Combatant Commands.

I know I went a bit beyond CT here, but I think it’s important to show how SOF are taking the lessons from the past 20 years and applying them to the future while staying true to our historical roots in irregular warfare. Essentially, my time in INDOPACOM demonstrated the value of SOF to the nation across CT, crisis response, and strategic competition; all at the same time, and often integrated and intertwined. The fruits of these missions not only appeared as SOF shaped the operational environment, but also demonstrated the outsized role of SOF in relationship development with allies for the United States.

CTC: Over the past several years, the U.S. CT enterprise rebalanced and evolved so that the United States can focus more resolutely on strategic competition and prepare for threats posed by very capable state adversaries. This has pushed the U.S. CT community to place greater emphasis on the prioritization of terror threats, and to figure out ways in which it can optimize or do more with less. Given the persistence of terrorism, and the diversity of today’s terrorism landscape, navigating this shift has not always been an easy thing for the U.S. CT enterprise to do. What are some challenges and opportunities you see for this period of U.S. CT? When it comes to SOCOM’s CT efforts, which areas is the Command placing optimization emphasis on?

Fenton: I already briefly touched on it, but the operational environment is changing, as are our partners and presence globally. In an increasingly complex and contested world, how we maintain I&W [indicators and warning] matters immensely. Who and how we enable our partners will similarly become the coin of the realm because we cannot be everywhere all the time. With that said, we need to ensure we have the right expertise at the right time. It calls into mind—the First SOF Truth—that people are more important than hardware, and building incredible teams inside the department and across the interagency and across the globe will help us succeed. We must hyper-enable our people to continue to deliver winning results for our nation. These teammates remain focused on the National Defense Strategy—our North Star for prioritization—and deliver SOF capacity to counter the PRC and Russia, while still keeping VEO threats at bay. How do we do this? By choosing the best people, then providing them with the best training and technology.

We have to realize that while we are ready to win now, when we talk modernization, what we really mean is, ‘What do we need to be able to win tomorrow?’ That’s what modernizing is really about: Winning in the future. Ultimately, AI will also play a significant role in helping us to understand and disrupt the terrorist threat with a small group of dedicated professionals, freeing up the bulk of the force, including SOF, for the challenges of integrated deterrence and state conflict. Data acquisition and processing is a huge challenge. We know we won’t have the same level of fidelity on the terrorist threat that we did when [we] were postured directly against those threats, but through leveraging technology, SOF can continue to be a small force that delivers outsized impacts for the DoD. To do so, we must be more creative in our data acquisition strategies and leverage what the private sector is doing in terms on data analysis. This means creating algorithms to quantify risk, prioritize targets, and coordinate between multiple departments, agencies, and foreign partners. SOF, as always, is at the forefront of technological innovation, making us the perfect community to experiment with the power of AI.

CTC: Part of the success of U.S. CT efforts has been sustained pressure. As resource and priorities adjust, can the U.S. CT enterprise maintain the same global pressure? How can we mitigate risk in places perhaps where groups might not have external operations capability, or where violent extremist organizations pose a threat of violence but not a threat to U.S. national security interests or those of our allies?

Fenton: Yes, we absolutely can maintain pressure on VEOs. We just have to take a different approach than we did during the height of the GWOT. To accomplish this, our SOF global posture is vital to detect and mitigate prioritized threats and keep a pulse on rising regional threats. We rigidly scrutinize our SOF posture to ensure that we influence meaningful locations at the appropriate times. Additionally, we must get better at predictive analysis, anticipate the next locus of homeland threats, and provide timely warning.

One of the greatest keys to success in the C-VEO space is our partnerships. You’ll hear me say this a lot in this interview. Our partners in the interagency, in the intelligence community, in academia, and around the world came together in an unprecedented fashion post-9/11. Those relationships are forged in sacrifice, remain strong, and continuously refine capabilities to ensure operations are more efficient, tech enabled, and almost always partnered. Nowhere is this more pronounced than in Operation Gallant Phoenix (OGP)—a U.S. interagency and multinational C-VEO initiative. Now in its 10th year, OGP has enabled international and interagency partners to share information from battlefield captures

General Bryan Fenton

to asymmetrically disrupt 16 distinct al-Qa`ida and ISIS groups in FY 2023. Coupled with counter-threat finance authorities and analytical expertise, operations like OGP provide expanded and cost-effective ways to disrupt illicit financing and deter activities. Operations for U.S. and OGP partners contributed to more than 1,500 investigations, more than 6,000 foreign disclosure releases, and support to partners repatriating more than 60 individuals in 2023. DoD counter-threat finance analysts also supported numerous Treasury designations against VEO finances and facilitators. The OGP model could apply further to countering coercive activities and deterring aggression. We have to scale and expand this model, because terrorism is an enduring problem.

CTC: You came of age in the CT community when the joint and interagency boundaries were coming down and collaboration and sharing improved significantly. How can we continue to improve on what was built? As we reduce the forward operating bases and joint operations centers around the world, how can we avoid the tendency to go back to our corners?

Fenton: At SOCOM, we seek improvement and innovation; it's inherent in our SOF DNA. This is how we continue to improve and help everyone across the CT community, joint force, and interagency. To improve upon the foundation that's been laid, we have a responsibility at the highest levels of DoD to elevate these discussions related to our posture, footprint, and military agreements. We are the canary in the coalmine for all things VEO; if that means advocacy for authorities or funding for combat support agencies and having hard conversations about emerging threats, that's part of our job as the global coordinating authority.

We held a CT Risk Conference in 2022 and 2023 with the interagency when the cumulative cuts in CT resourcing started rippling across an interdependent community. We wanted to make sure we weren't creating too much risk in any one area. And you know what we found? The CT enterprise had become a Gordian Knot of interdependencies between departments and agencies. We couldn't untangle it if we wanted to, and the continuation of sharing people, LNOs, interns, and others among agencies is critical to sustaining these relationships. The best we can do is be circumspect about the effects our decrements have on other agencies when the Department cuts CT programs, many of which the interagency relies on as the foundation for their own capabilities. We've continued the tradition of the CT Risk Conference, and we'll have our third annual event next month. Every year, unity of effort is a key theme of the conference.

CTC: CT is an activity aimed at a specific threat, but it is also an operational design that focuses on the human element of the enemy's capabilities. What lessons learned from CT can we take into the strategic competition and conflict space? Are there ways in which the CT operational design can play a part in irregular deterrence? If so, how do you see personality-based targeting playing into future conflicts?

Fenton: We spent years in the CT fight learning how to understand organizations and the networks of humans that comprise those organizations. This type of targeting is universal; it applies to a government, a gang, a terrorist group, a private firm, etcetera. We continue to see the relevance of personality-based networks for kinetic and non-kinetic opportunities. Who makes the decisions, who influences those decisions, how do they perceive us, how do they see themselves? We've also learned a great deal about how we communicate, deliver, and shape the information as part of the operational design.

Ultimately in conflict, whether it is CT or peer conflict, the fight is largely won or lost in the human domain. This is the domain of SOF. The Navy thinks in terms of ships. The Army thinks terms of maneuver. SOF, we think about humans; it's our stock and trade. We continue to see the relevance of personality-based targets in places like Ukraine, and I suspect HVI targeting will have some role in most future conflicts. That isn't to say this type of approach should always be kinetic. It may not be, but it's critical that we consider our enemy's human terrain. Our capabilities in this arena provide one of the United States' greatest assurances to our allies. We remain the best in the world at direct action, and our forces still retain tremendous combat experience that our allies value.

After we assure our allies, we must deter our adversaries. And then when you talk about deterrence, we can deter by denial, making the enemy believe there is a small likelihood of success and also deter by punishment. All the tools for CT, both kinetic and non-kinetic, can work on any organization composed of humans, including state governments, both to cause enemy mission failure and make their actions very costly.

SOCOM is pioneering several concepts within the framework of irregular deterrence. Most of these concepts are not related to CT, but they are all done the SOF Way: irregular, asymmetric, asynchronous, and indirect.

Another great lesson from the CT fight that has tremendous applicability in the strategic competition arena is the need to dominate the information space. This goes in both directions. First, we must ensure our messages are fast, truthful, and delivered with purpose to achieve intended effects. Next, we must remain ahead of misinformation and disinformation spread by our adversaries. We protect the homeland physically, but we also protect the homeland from the threats posed by the information operations of malign actors.

CTC: When it comes to technology, and tech innovation, what types of technologies concern you the most when it comes to future terrorism threats? What types of technologies do believe will be important, or more important, for U.S. CT in the near future?

Fenton: The ability to strike and the risk to the force, even from a terrorist perspective, is concerning. With AI and aerial unmanned and uncrewed systems, the threat is evolving in creative ways. I think investment in these systems, as well as defensive capabilities against such systems, is paramount not only in the near future but today. Our unique acquisition authority at USSOCOM is enabling us to move with greater speed to meet the needs of our people.

The Russo-Ukrainian War is doing more than displaying the battlefield upon which the joint force will have to operate; it is also giving us a glimpse into the future of both terrorism and CT. The proliferation and technological leaps in one-way attack drones, first-person view drones, and long-range uncrewed systems are both available to terrorist groups and put our deployed forces and forward installations and facilities at risk.

It's no secret that uncrewed systems are no longer limited to the large, remotely controlled, heavily armed "unmanned aerial systems" of the past. The future is all-domain, remotely controlled, *and* autonomous, and in mass. While the services are doing a great job investing in these systems at scale, we see SOF's role as the mechanism to ensure these systems can get on target. In that way, we are investing in and experimenting with our command, control, and communications networks to test how best to get targeting data to this lattice of uncrewed systems.

Anti-access, area denial is another concept that is not solely in the realm of great powers and applies directly to CT. As we look globally to the places from which external operations threats may emanate, they are often in areas that require penetration of sophisticated integrated air defense and electromagnetic spectrum systems. Our research and experimentation with penetrating those networks and operating in a comms-degraded or denied environment for CT has direct applications to warfighting. If we can punch a hole in the A2/AD bubble to conduct a CT strike or raid, then we can do the same to open a window for the Air Force to get a long-range anti-ship missile off the rails and onto target.

Finally, we need to improve our digital intelligence collection and analysis capabilities to make up for the loss in posture. The role of space and cyber in this arena cannot be overstated. SOCOM has several initiatives to do just that and has made tremendous progress. However, we still have a long way to go. We are working with the private sector to improve our capabilities at the speed of innovation.

"We are always working to do things better and faster, and we're not afraid to fail fast and try again. The close coordination between SOCOM and industry enables movement at a pace we haven't seen before."

CTC: How do you balance the innovation requirements for integrated deterrence with counterterrorism? Are you seeing overlap, for example, in areas such as remote operations? How do you ensure CT is equipped with the technology it needs for posture-less operations without detracting from the critical innovation for peer conflict?

Fenton: Operationally, this occurs through the TSOCs. These Theater Special Operations Commands have the best feel for the needs of a region and serve as advisors to the Combatant Commanders. In support of these commanders, SOF capabilities must span the full-spectrum range of operations, so innovation efforts will focus primarily on SOF's role in large-scale combat operations against a peer adversary. This emphasis allows SOF to modernize to the most dangerous threat environment, mindful of further potential operations other than major conflict. Therefore, SOF will focus on creating multi-functional capabilities that address more than one mission area to cover the range of military operations. For the most part, we have seen that the changing nature of warfare affects all missions sets, and therefore, the innovations we've made in LSCO [large-scale combat operations] capabilities have translated well into the irregular warfare arena, including CT mission sets. The CT mission set is a key component of integrated deterrence and is an essential tool for developing partnerships and allies. There is no magic formula for balancing the innovation focus. It is both an art and a science, but we have found that innovation gains are often beneficial across the SOF mission spectrum.

CTC: USSOCOM has made important investments in liaison officers to Silicon Valley, Austin, Boston, and Washington, D.C., for acquisition, technology, and logistics. What have we learned from consistent exposure to these innovation hubs? How can our acquisition systems improve to keep up with the speed of technology?

Fenton: As SOF, we're needy—some would say discerning—and we're never satisfied. We are always working to do things better and faster, and we're not afraid to fail fast and try again. The close coordination between SOCOM and industry enables movement at a pace we haven't seen before. We are blessed to have talented officers in innovation hubs around the United States to forge partnerships and to learn from the fastest innovators in business and technology. Our connections with venture capital companies through our Defense Innovation Unit helps government learn how to move from idea to implementation in a way that's not typical for federal entities.

Thanks to congressional foresight, one of the hallmarks I mentioned before is that we have our own acquisition system. We don't have unique authorities in SOCOM, but we use the ones we have in a unique and more rapid fashion. A major USSOCOM acquisition advantage is our acquisition executive's well-developed culture of risk identification and management at the appropriate level, which is also enabled by our organizational scale and structure coupled with proximity to our warfighter. The warfighter, through interaction with our components and TSOCs are included in all our acquisition and development programs. Additionally, efforts like SOFWERX and leveraging the nation's network of service and national laboratories, FFRDCs, and UARCs are key to rapidly innovate and allow small start-ups to get their foot in the door.

CTC: Israel has demonstrated an astounding capability in its kinetic targeting over the past two months. How do you think the decapitation of Hezbollah and Hamas leaders will impact the conflict in Israel in the near term? What long term implications might it have for the larger CT fight?

Fenton: Let me start with the long view of the impact of the Israeli crisis. First off, the impact of the Hamas October 7th attack remains to be seen, as we typically expect roughly two years after an event for effects to manifest. With that said, we know VEOs are exploiting the crisis, while groups previously unaligned with Gaza have increasingly rallied against the West. Second, this event has renewed interest in jihad like we've not seen since the Arab Spring. The crisis in Gaza will continue to galvanize those susceptible to radicalization, creating a larger pool of recruits for local operations and inspired or enabled attacks inside Western homelands. VEOs continue to advance their anti-Western ideology in media platforms criticizing U.S. and Western support of Israel, while calling for attacks in the Middle East and beyond.

CTC: We are several years into, for lack of a better term, our 'over the horizon' model of CT. What is working? What is harder?

Fenton: It's always harder when you're not on the ground, but 'over the horizon' has helped us to examine the challenge differently and develop other tools to see and sense, and where necessary, strike anywhere around the globe. We've had to get a lot better at prioritizing targets, and we'll have to get even better still as we continue to lose posture. SOF has long had the ability to reach out and interdict threats anywhere in the world. So, I think, with sufficient will, that we can conduct any OTH scenario. My worry is more about "OTH sensing"—do we know what targets are of sufficient national import to initiate an OTH operation, and do we have enough fidelity to target them? I think we have more work to do on the front end of OTH, but when the balloon goes up, I think we are confident in our abilities. SOF forces are executing OTH with tremendous success due to the innovation of our teammates, atypical partners, new forms of ISR, and well-earned trust with traditional partners.

CTC: When you look to the future of U.S. counterterrorism—a future that the SOCOM enterprise and other partners are working to build—what does that future look like? How, if at all, will it be different than what U.S. counterterrorism looks like today?

Fenton: The future often looks a lot like the past, in that we will still conduct relentless pursuit of those who would do us harm. How we do it and who we pursue may look different. State-sponsored terrorists and proxies, while not new, increasingly offer plausible deniability to behave outside international norms. The information environment and the role of public perception continue to prove pivotal, and the challenge to be first with the truth, while meeting democratic ideals, will continue to challenge us. Terrorists, like private military firms, will continue to adapt and complicate the operational environment. Pay close attention to the convergence of adversaries.

We should not underestimate the terrorists' ability to innovate. From rapid knowledge transfers online to the use of satellite phones and imagery, the enemy will always capitalize on cheap, fast tech. We have benefited from valuable cyber targeting and disruption; however, we anticipate tech-savvy terrorists will reduce our advantage in the future. These innovations will also help us to dominate the information space, which will be a task for all of us from the tactical to the strategic levels.

"We talk about a SOF renaissance: What's old is new again. In other words, I don't see that our emphasis or necessity with partnerships will change. I do see opportunities for us to expand and evolve those partnerships from bilateral to multilateral. We will need to think differently about these because the security environment is global and demands it."

CTC: Narrowing that question down, when you think about the future of CT through the lens of partnerships, what does that picture look like? Can you share some examples of what you think might look the same, as well what might look different?

Fenton: We talk about a SOF renaissance: What's old is new again. In other words, I don't see that our emphasis or necessity with partnerships will change. I do see opportunities for us to expand and evolve those partnerships from bilateral to multilateral. We will need to think differently about these because the security environment is global and demands it.

As for differences, there are several. We expect more activity to fall under multilateral partnerships. Things that may have been NOFORN in the past will become YESFORN in the future as the reliance on partners becomes more critical to every campaign. We also expect to spend more time moving back and forth between CT and integrated deterrence and in the spaces where they overlap.

CTC: When we walk into the Pentagon, the SOF wall shows incredible photographs of operators in action. While those operators continue to do amazing work around the globe, there is a new generation of warriors in the data, cyber, and information space who are bringing a lot to the fight. As

capabilities evolve, how has your leadership style changed or evolved along with it?

Fenton: First, that's a good reminder that at every level, an appreciation for the total team is so important, and the diversity of skills and experiences only gets vaster at echelon as you move from platoon to battalion on up to joint and international operations. Relentless improvement across our formation is paramount. We are early adopters, and it starts with the knowledge and emphasis of our leaders on developing the skills and talents necessary to win today and in the future. We continue to educate ourselves and seek opportunities to gain greater experience based on new adaptations and evolutions that occur from generating new capabilities. Take cyber and information operations, for example. As leaders, we must understand the capabilities and capacity of specific skill sets within each of these communities. Much like a Special Forces Operational Detachment – Alpha is a conglomeration of individuals with various skills, so is a cyber mission unit or PYSOPS team. We have the institutional knowledge to understand the types of missions an ODA, SEAL platoon, or Marine Raider Detachment can perform and their capacity to do so. Our understanding of cyber, robotics, and other emerging capabilities is still nascent, and we are wrestling with how much we keep those capabilities as stand-alone teams versus integration with our traditional formations. The future of SOF leadership, from my level down to, perhaps, the O-5 or O-4 level will be both joint and multi-domain. It isn't enough that we are experts in our service-specific SOF missions; we must evolve as leaders to the reality of the challenges we face.

CTC: SOCOM and JSOC have long held the proponency for hostage recovery. While this threat has never gone away, the post-October 7th experiences have put renewed attention on the complexities of these operations. Can you share your insight on what SOF brings to the table for policy makers when they have to consider the critical task of hostage rescue in their development of response options?

Fenton: Hostage rescue is a wicked problem with strategic convergence. It is complex, politically sensitive, but above all, it is a no-fail mission. Our crisis response force is specially assessed, selected, and trained to provide this capability to our nation. They rehearse these missions over and over until the mindset is that they can never get it wrong. I come back to what we've been talking about: Success requires deep trust and assistance across the interagency and with partners and allies. It's what the American public expects from us. These mission sets, at their sharp end, provide policy makers with multiple options to solve the hardest problems.

CTC: When it comes to threats, what keeps you up at night?

Fenton: Always at the forefront of my mind is the question: What do we not know? What is the adversary doing that we have not anticipated? In short, blind spots keeps me up at night. We all have them, and they will always be out there. The risk to the homeland is increasing as reductions in CT operations, I&W, and posture have enabled VEOs space and time to regenerate disrupted leadership structures and communication networks. ISIS/AQ remain coordinated, transregional organizations capable of conducting and inspiring violent attacks against U.S./allied interests globally. I think professional anxiety is healthy because it keeps us both leaning forward, but also looking over our shoulder at the same time. Staying vigilant about the active, persistent threat is the challenge. There are plenty of strategic distractions that can take us off course. CT is not going away, and it is up to all of us, collectively, to maintain a trajectory that accepts it as a reality, but simultaneously and fundamentally, rejects it as an acceptable norm. USSOCOM works very, very hard to ensure we fill in gaps in knowledge to reduce the blind spots and to remain ahead of the threat. Our people, their talent, and their effort are what mitigate those concerns more than anything. CTC

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.

Convergence and the CT Return on Investment: A Framework

By Don Rassler and Sean Morrow

Since 2018, the United States has been trying to figure out what counterterrorism looks like during an era of strategic competition, and how it can maximize and optimize returns from its counterterrorism investments. There are important differences between these two national security priorities—strategic competition and counterterrorism—but if the United States wants to gain resource efficiencies, it should look across the gray space at how and where these two priorities interplay and converge. This is because a key part of the pathway to CT optimization lies in realizing how counterterrorism has evolved as a form of influence. This article introduces a conceptual framework to help the counterterrorism community situate the returns from CT investments, especially deployed CT force activity. It recommends that those returns be understood through two lenses: 1) those that are direct and oriented around threat mitigation and 2) those that are intersectional and oriented around influence. Interviews with three experts provide context to elements of the framework and highlight the interplay between counterterrorism and strategic competition in different regional areas.

The day after al-Qa`ida's surprise attack on 9/11 was the beginning of a new era for the United States. It usually takes time for the U.S. national security apparatus to pivot—the analogy that is often used to describe this process is the turning ability of an aircraft carrier, which can only make movements in a slow and deliberate manner due to its size. But on September 12, 2001, the United States made an immediate and hard shift in its priorities, and for a considerable period, it did not look back. During those early days, it was as if resources did not matter. As outlined by Eliot Ackerman: "At a joint session of Congress on September 20, 2001, U.S. President George W. Bush announced a new type of war, a 'war on terror.' He laid out its terms: 'We will direct every resource at our command-every means of diplomacy, every tool of intelligence, every instrument of law enforcement, every financial influence, and every necessary weapon of war-to the disruption and to the defeat of the global terror network.'"[1] For a period, time mattered little as well, as the 2002 U.S. National Security strategy outlined the war on terror as being "of uncertain duration."[2]

That environment is long gone, and for good reason. In November 2011, President Obama announced the U.S. "Pivot to Asia,"[3] that kicked off a long aircraft-carrier-like turn across the U.S. government to emphasize what today it characterizes as strategic competition. The rise of the Islamic State in 2014 derailed that shift. But by 2017 when the Islamic State was on the ropes in Syria and Iraq, the United States expressed it was ready to chart "a new and very different course,"[4] a course that was formalized in the 2018 U.S. National Defense Strategy, which identified "inter-state strategic competition, not terrorism" as the primary concern.[5] Since that time, the United States has been slowly turning round the mechanics of government so that focus and resources align with national security priorities. To achieve that end, the United States has been working to 'optimize' and 'calibrate' its approach to counterterrorism, to prioritize terror threats more, and figure out where it is comfortable accepting risk—to figure out what counterterrorism looks like during the era of strategic competition. That has not been the easiest thing to do, as while the United States would like to spend less time and fewer resources combating terrorism, America's terrorist adversaries are committed; they also get a vote.

As a result, over the past several years the U.S. counterterrorism enterprise has been navigating two truths and trying to find a sustainable path through them. First, the threat of terrorism is persistent. It will ebb and flow over time, but it is not going away. Second, the counterterrorism fight will no longer receive the funding or resource prioritization it once did. Adding to the challenge is that elected leaders and the American public still expect (and in many ways demand) similar CT success from a CT enterprise that is operating with fewer resources. Thus, in today's environment, it becomes paramount that every resource spent on people, dollars, and time must go further than it has in the past—with emphasis placed on outcomes. That applies to counterterrorism *and* strategic competition, as well as the gray space between those two priorities.

This article introduces a conceptual framework to help the CT community frame the return on investment from counterterrorism investments, specifically those associated with deployed CT force activity. It takes a broad view, and it aims to provide insight into what those direct and intersectional returns are and how they

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

Colonel Sean Morrow has served as the CTC's director since January 2021. He has served in a variety of roles in the U.S. military including as Battalion Commander in the United Nations Command in Korea and a Battalion Operations officer and a Brigade Executive Officer for the 10th Mountain Division in southeastern Afghanistan.
*X: @SeanMorrow_*

could be considered and captured in relation to counterterrorism and strategic competition. It proceeds in two parts. Part I explains and provides context to the CT return on investment (CT ROI) framework. Part II explores the dynamics of the framework, and the interplay between counterterrorism and strategic competition, through different regional lenses and the perspectives of three specialists interviewed for this article.

Part I: Introducing the CT ROI Framework

The CT ROI framework (Figure 1) is a conceptual tool designed to help decisionmakers and their staff to understand and map returns from counterterrorism investments, and to situate how those investments intersect with and can provide value to strategic competition. An overriding goal of the framework is to break down how these two national security priorities—CT and strategic competition—are often analytically bifurcated or siloed in the U.S. context and are routinely viewed, prioritized, and resourced as two distinct priorities or problems. In many ways, that line of thinking is true: CT and strategic competition could not be more different, and the tools and approaches needed to address or be effective in each can differ greatly. But there are limits to that analytical view, and in some ways, it is not helpful. This is because there are important areas where the two priorities nest and intersect. There are also areas where counterterrorism can provide key value or entry points to strategic competition pursuits. Those opportunities are not always present, but it is important to identify and maximize them when they do exist. This is especially true during an era when the two priorities present very real challenges and when the United States and its partners are trying to pursue both priorities well against committed adversaries using limited resources. From a strategic perspective, identifying areas of synergy and integration between counterterrorism and strategic competition is the smart and efficient thing to do.

The CT ROI framework has two core pillars that interplay with one another. The first is how it conceptualizes the benefits and returns from counterterrorism. This is illustrated by the arrow at the top of the graphic that moves from left to right—from direct benefits (the start of the arrow) to benefits that are progressively intersectional and that provide more relevant value to strategic competition. The second pillar is how different key goals are conceptualized in relation to the direct and intersectional benefits they provide to counterterrorism and strategic competition. These are reflected by the goal categories in gray boxes that are presented from the top to the bottom of the graphic. These include degrade and disrupt, offset and sustainable CT build, understand and warn, deterrence, reputation and trust, and access and placement.

In the United States and other contexts, counterterrorism has fundamentally been viewed as being about the mitigation of threats against the homeland and against U.S. allies and interests abroad—a mission area that uses various instruments and tradecraft to put pressure on key terror threat actors and to degrade their capabilities. When it comes to how CT returns are understood, this view dominates. That makes sense because this is the area where returns from CT investments are most direct and clear. This would include, for example, the number of mid- to senior-level Islamic State leaders removed in Syria over the past two years, other outcomes tied to unilateral or partnered direct action CT operations, or additional degrade and disrupt pursuits (i.e., financial resources seized, plots disrupted, etcetera). For the United States, the primary point of emphasis and focus of returns

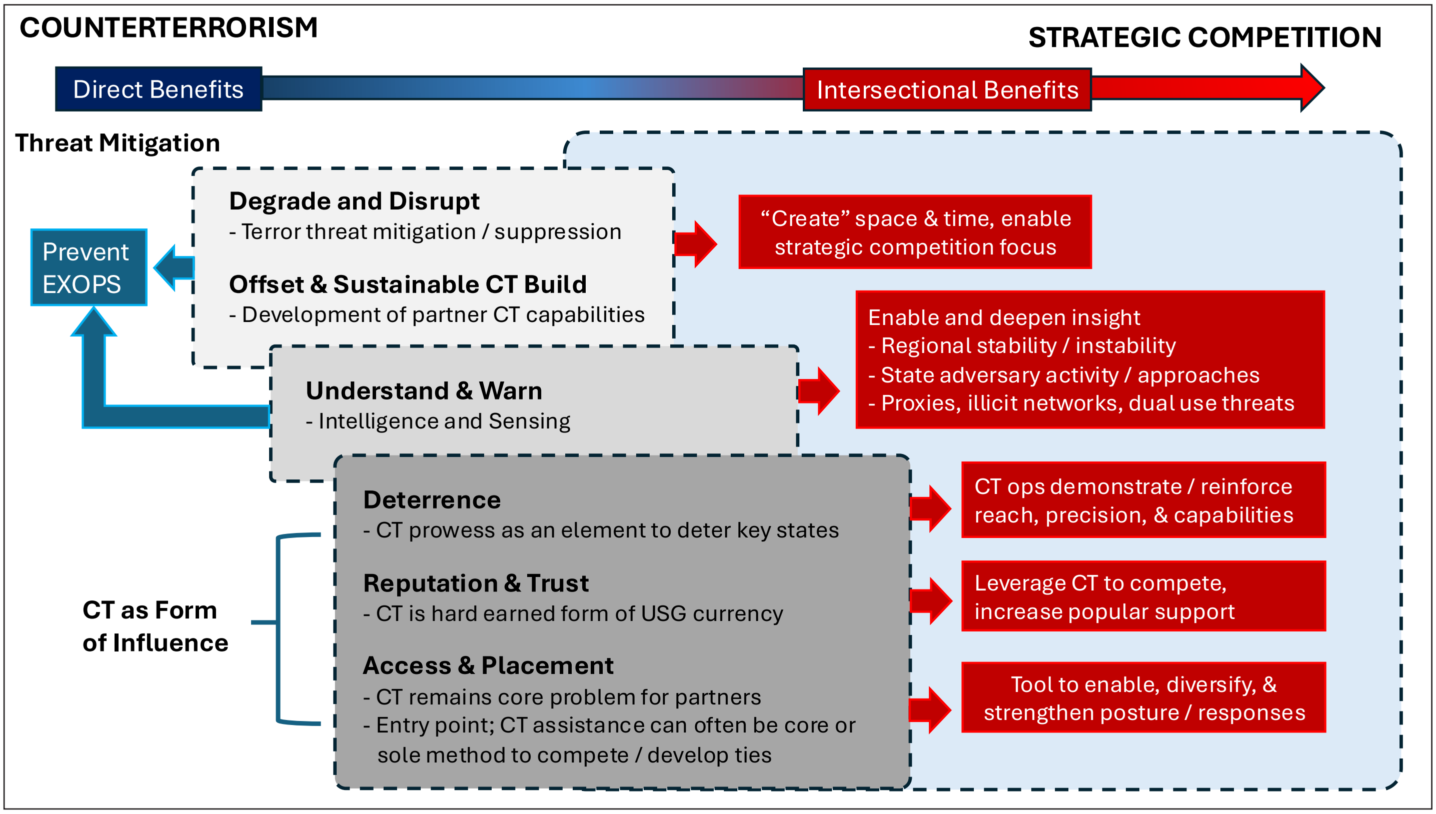

COUNTERTERRORISM
STRATEGIC COMPETITION
Direct Benefits
Intersectional Benefits
Threat Mitigation
Degrade and Disrupt
- Terror threat mitigation / suppression
Offset & Sustainable CT Build
- Development of partner CT capabilities
Prevent EXOPS
"Create" space & time, enable strategic competition focus
Understand & Warn
- Intelligence and Sensing
Enable and deepen insight
- Regional stability / instability
- State adversary activity / approaches
- Proxies, illicit networks, dual use threats
Deterrence
- CT prowess as an element to deter key states
CT ops demonstrate / reinforce reach, precision, & capabilities
Reputation & Trust
- CT is hard earned form of USG currency
Leverage CT to compete, increase popular support
CT as Form of Influence
Access & Placement
- CT remains core problem for partners
- Entry point; CT assistance can often be core or sole method to compete / develop ties
Tool to enable, diversify, & strengthen posture / responses

Figure 1: The CT ROI framework

has been on disrupting external operations.

Partners have been critical to U.S. efforts to mitigate terror threats, and they will remain critical given the scale and persistence of the threat. For the United States, the importance and centrality of partners is reflected in the progressive emphasis that has been placed on partnerships in different U.S. counterterrorism strategies across time and administrations.[6] "Build and Leverage Partner Capacity" is the second line of effort in the most recent strategic policy guidance, National Security Memorandum 13, and it notes how foreign "partnerships, already a key component of U.S. CT strategy and efforts, will take on increased importance."[7] This is because the United States views partnerships, and the development of effective and reliable partners, as a way to offset CT demands and to build a more sustainable approach to counterterrorism over time. For example, if U.S. efforts to develop the CT capacity and capability of partners are lasting, they can enhance a partner's ability to manage terrorism problems with less U.S. involvement (or on its own), which can create additional space and time for the United States to focus less on terrorism and more on strategic competition.

The second gray box—understand and warn—focuses on intelligence and sensing activity. Intelligence enables counterterrorism activity. It also enhances the United States' ability to understand how terrorism landscapes or specific threats are evolving, information that can be used to adjust CT priorities and to warn. But CT elements deployed in key countries also function as sensors that, by the virtue of their presence, can deepen insight into activity that is taking place in the area or region generally.[a] This could include, for example, the activity of state-supported proxies and illicit networks that state competitors may be leveraging or could one day weaponize, or the actions of state adversaries such as Iran.

In addition to threat mitigation, the second key value area that the framework advances is how counterterrorism can function as a form of influence. While not commonly used as a concept, this idea is not new.[8] But where the framework makes a unique contribution is in how it conceptualizes deterrence, reputation and trust, and access and placement as being three areas where CT activity can play an important influence role. For example, when it comes to deterrence, U.S. CT capabilities have demonstrated operational prowess, the ability to reach, deploy force, engage in surprise, and repeatedly remove hard-to-find leaders. That type of capability "makes you feared. It makes you respected."[9]

The development of the United States' counterterrorism capabilities over the past two and half decades is a hard-earned form of currency, and the CT assistance it provides to partners is a form of currency as well.[10] As noted by Matthew Levitt, "that currency buys goodwill and partnership on a wide array of other interests, including Great Power competition. The flipside is also true: if the United States declines to help other countries address their counterterrorism needs, it creates a vacuum that states like Russia and China, or Iran and Turkey, will fill."[11] Since terrorism mitigation is still a strategic priority for many of the United States' partners—and potential partners—counterterrorism can be an entry point to develop ties and build trust, to enrich both with existing partners, and to solidify or expand U.S. access and placement in key locations around the globe.

Indeed, the authorities and plans that go into the establishment of allied and partnered CT training and operations around the world can also be key to opening the door to the access, basing, and overflight that become so critical to potential conflict between major powers. CT operations help set the logistical and legal conditions to enable future operations in key areas.

The case of the Philippines is an important example. For more than two decades, counterterrorism assistance has been the keystone of the U.S.-Philippines defense relationship. That assistance has helped to develop the CT capacity of the Armed Forces of the Philippines (AFP) and the Philippine government to mitigate key Islamist terror threats in Mindanao over time. This includes, for example, key support provided to expel regionally affiliated Islamic State elements from the city of Marawi, which the Islamic State network laid siege to for five months in 2017, and to degrade the capabilities of that network.

Building partner capacity programs have also been a key mechanism through which U.S. and Philippine special operations force elements have built shoulder-to-shoulder level bonds and trust. During the Duterte period, the U.S.-Philippines alliance was tested, and its long-term viability was questioned and put in a precarious position. At the time, the Philippine president announced his "intent to 'separate' Manila from Washington, and declared his desire to scrap" the Enhanced Defense Cooperation Agreement (EDCA), a key agreement reached between the two countries in 2014.[12] In 2020, the Duterte administration also took steps to terminate the Visiting Forces Agreement, that helps to enable and provide protections for U.S. forces operating in the Philippines.[13]

The U.S.-Philippines defense relationship is largely viewed as having been a key protective element that helped the United States navigate through that period of turbulence and uncertainty. Duterte ended up reversing course, and the agreements stayed in place. In 2023, not long after the election of Philippine President Marcos, Jr. in 2022, the Philippine government expanded the number of EDCA sites in the country by four, bringing the total to nine[14]—a decision that has deepened U.S.-Philippine defense ties and enhanced U.S. access and placement in a strategic geographic area. Further, analysis of longitudinal polling data reveals that since 2000 Filipino trust in and satisfaction with the AFP has improved across time.[15] Filipino trust in the United States has also generally remained high.[16] While the Philippines case may be a unique one,[17] it underlines—perhaps most clearly—the intimate interplay between counterterrorism and strategic competition pursuits, and how CT can provide different benefits to the key goals outlined in the CT ROI framework.

Benchmarks for each goal area—degrade and disrupt, offset and sustainable CT build, understand and warn, deterrence, reputation and trust, and access and placement—could be developed to enhance the practical utility of the framework, and track CT returns over time. This could take different forms. For example, terror threat mitigation efforts that are focused on key organizations in specific countries (e.g., al-Shabaab in Somalia) could evaluate the Global Terrorism Index ranking across time to identify high level changes in the threat environment. Al-Shabaab's operational capacity; ability to command, enable, and inspire; geographic reach; operational outcomes (e.g., lethality, ratio of

[a] As USSOCOM Commander General Bryan Fenton mentions in this issue of *CTC Sentinel*, the TSOCs are perhaps the best-placed elements to understand the environment and to advise the combatant commander.

completed to failed attacks, etcetera.), and other metrics could also be evaluated to provide a more granular picture of the network's temporal evolution. General and targeted survey and polling data could be leveraged to provide insights into reputation and trust. When available, this could include, for instance, data on public trust for rebel movements, armed groups, and terror networks in specific countries, with emphasis placed on whether that trust is improving or declining. Data that provides insight into public support and trust for partner security forces, CT campaigns, partner force trust in the United States, or country-level trust in the United States or the U.S. military could be leveraged in a similar way.

Part II: CT and Strategic Competition — Regional Views

The section explores the dynamics of the framework, and the interplay between counterterrorism and strategic competition, through different regional lens and the perspectives of three specialists who were interviewed for this article. These three individuals, and their areas of focus, include Christopher Faulkner (Africa), Michael Knights (Middle East, with emphasis placed on Iraq, Syria, and Yemen), and Magnus Ranstorp (Europe). The views shared by these experts help draw attention to key case studies, how CT and strategic competition dynamics manifest in different regions and where there are areas of commonality and divergence, and other issues, including challenges and opportunities, that are important to consider.

Africa – Christopher Faulkner

CT as Threat Mitigation in the African Context

I think how the United States views counterterrorism in the African context is still very much through the lens of threat mitigation—e.g., number of attacks thwarted, assessing the severity of attacks, considering if the location of attacks is spreading or becoming more concentrated, etcetera. Those things still very much matter, but—and this sounds cliché—an overreliance on traditional metrics of threat mitigation can miss the forest for the trees. To overgeneralize a bit, the United States should probably view CT in the African context through the theme of resilience—security force resilience, community resilience, regional cooperation (like regional economic communities or security architectures) resilience.

For African states, there is still a need to count traditional [threat mitigation] metrics, especially in locations where terrorism is thriving (i.e., the Sahel). But it is as important, if not more important, to think about a much broader spectrum of factors to gauge CT value/benefits. African states, in partnership with U.S. and European partners, would be wise to focus on assessing metrics more closely linked to the root causes of terrorism (e.g., poverty, lack of educational opportunities, poor governance, corruption, etcetera), which can lead to a more durable and comprehensive CT approach. Many groups exploit these conditions, tapping into personal agitation or financial stability as [a] means to recruit.

Another element African states might look to is regional security cooperation: number of troops trained, number of joint exercises, etcetera. These efforts are short of things like kinetic targeting but speak to security cooperation, interoperability, coordination, and resilience that can be important for mitigating enduring threats.

Lastly, community policing and engagement need to improve. I'm reminded of a blog post which reported on trust in police in Africa,[18] and the moral of the story is that trust in police is quite poor in many states. So, working to improve community policing, trust in police, and working with local leaders and community leaders can be critical for successful CT efforts.

CT's Relevance, or Irrelevance, to Strategic Competition in Africa

I think there are two schools of thought here. First is the idea that CT is directly relevant to strategic competition because it is 'in demand' by a number of African states and a necessary way to compete with strategic competitors like Russia who has emerged as an alternative security partner.

The second thought is that CT is irrelevant, or at least should be, because it treats African states as pawns in a competition between the United States and Russia. In other words, it runs the risks of failing to consider the agency of African partners because of the tunnel vision of competing with Russia—seeing CT as a way to 'beat' Russia and not as a means to support African partners. Some analysts have really equated the current environment as posing a strategic "trilemma," with the United States trying to balance "promoting democracy, combatting violent extremism, and engaging in great-power competition."[19] Though I'm cautious in suggesting a policy of democracy promotion, pushing it aside in favor of the latter two lines of effort can unintentionally undermine the United States over the long term.

Some of this might seem like semantics, but I think it matters. My take, as I've written elsewhere, is that CT has relevance to strategic competition and can be a valuable tool for the United States, but it must be a more comprehensive project, focused not exclusively on military means but instead on prioritizing non-military instruments of national power that can genuinely differentiate the United States from its strategic competitors like Russia, [which] is primarily focused on using the barrel of a gun, or China, [which] is primarily interested in economic/infrastructure investment which often comes off as predatory.

Another element that I think is important to keep in mind is that almost all critiques of the U.S. approach to CT in the Sahel and across Africa writ large is that even interagency programs can come off as overly militaristic because AFRICOM becomes a primary driver simply because it is better resourced than its interagency partners. Moreover, it isn't inherently true that African security forces lack capacity to combat terrorism, but there are serious governance challenges that can put the United States in a position where it is seen as reinforcing a corrupt government. Chad comes to mind as a case where U.S. pragmatism in not branding a coup a coup can be seen as delegitimizing for the United States by other African states.

The U.S. exit from Niger and pursuit of relationships with coastal West African states is an example where CT/strategic competition priorities intersect and the United States must be careful to marry traditional CT efforts (security force assistance and CT training/investment) with diplomatic investment, economic investment, promoting healthy democratic norms like respect for the rule of law, media freedom, electoral norms, and investing in civil society. The Biden administration's $100 million pledge in March 2023 for several littoral West African nations, including Benin, Ghana, Guinea, Cote d'Ivoire, and Togo,[20] was specifically designed to invest in stopping the spread of terrorism from the Sahel, but in implementation, it needs to have a whole-of-government approach to include DoD, State, USAID, Commerce, and so on.

Is CT as a Form of Influence a Useful Concept in the African Context?
Yes and no. There is a double-edged sword here. CT activity/assistance is arguably necessary as a means of yielding influence, especially because the trajectory of terrorism demands CT assistance. But the risk is that such provisions, in isolation, rarely if ever resolve the insecurity and then can unintentionally help contribute to anti-Western sentiment. As a result, the United States risks running afoul by using CT activity/assistance as a means of doing 'great power' or 'strategic competition' without considering the agency of African partners.

It's a truism that post-2001, the United States dramatically scaled up its CT operations globally, and one could argue that CT became a primary means of guiding U.S. strategy in Africa. In short, while there were some clear successes in CT as a form of influence to generate partnerships with African militaries, leading with CT, or rather doing it in isolation, is not a durable long-term strategy.

Still, the United States cannot abandon CT support as a form of influence in Africa. It might be limited on where it can do certain things, but simply withdrawing CT as a means for influence would only be playing into the hands of Moscow. How we do CT and putting African governments at the helm of crafting ideas and solutions for CT can be powerful for identifying long-term strategies. In other words, giving African states agency is going to be critical and necessary for long-term buy in. The United States can advise and guide, but enduring CT efforts are going to have to be organically developed and implemented (within reason). My two cents is that local actors are far better positioned to think through enduring solutions for local communities.

Strengths and Weaknesses of the CT ROI Framework
I think the framework has a lot of value, especially in suggesting that CT 'intersects' with strategic competition rather than framing CT as a way to 'do' strategic competition.

The overarching thing I like about the framework is that it's really about capacity building broadly construed. The three strongest pieces to me are the CT Build (top left box), the reputation/trust bullet, and the access/placement bullet.

On CT Build: It's going to remain necessary to build partner capacity so that the United States is helping African partners develop a comprehensive CT ecosystem both at the national levels and at the regional level.

On Reputation/Trust: CT can clearly be a way to build trust, but it can also be a way to lose it. Working with African militaries/police can build trust between these institutions and the United States, but it's important to consider the relationship between the military/police and local populations as training units that are widely unpopular or distrusted by local populations can be self-defeating.

On Access/Placement: I think this is a really strong point. CT as an 'entry point' is critical—maybe necessary in some cases— but it also needs to be complemented. For example, traditional ways of thinking about CT (kinetic approaches, security force assistance, etcetera) is that this is something the United States does well and it is in demand. So, the U.S. should not sacrifice its comparative advantage, but it should also do so in tandem with interagency investment to ensure it's attacking the immediate problem (terrorist threats) and the enduring problems (development, corruption, etcetera) that contribute to terrorism.

Middle East – Michael Knights

CT's Relevance, or Irrelevance, to Strategic Competition in the Middle East
The first thing is, who's the first world leader to call [President] George Bush and commiserate with him after 9/11? [Then Yemeni President] Ali Abdullah Saleh. He immediately recognized that it was going to be a huge boon to him potentially. So, one thing to point out is that there's a demand for our CT support.

It is important that we try and make sure we don't get suckered in that process because a lot of people will want our CT support in order to kill domestic opponents, to create death squads, and all that kind of stuff. But in great power competition, it is also important to strengthen partners.

Any kind of special forces and intelligence interaction with the partner, whether you call it CT or something else, is very intimate, very highly valued. For Ali Abdullah Saleh, from the first minute after 9/11, this was the future for him. It didn't actually end up working very well for him eventually. He saw us as an absolute goldmine, and when a partner country sees you as a gold mine, that's not a bad thing. That's a good thing.

China can talk a big fight when it comes to being a peer competitor to us. It can certainly provide very useful repression tools. But when it comes to actually hunting down terrorists, the U.S. brand is unrivaled and will probably remain unrivaled for a very long period of time.

A lot of people doubt our strategic acumen. They doubt our level of attention to their concerns. But they never doubt our ability to find, fix, and finish someone or something on the surface of the earth or under the surface now.

In terms of brand and competitive advantage and unique selling point, we are head and shoulders above anybody else. Everyone knows that we can do this stuff. That's very important in great power competition, to have a unique capability that everyone knows nobody else has really got. It makes you feared. It makes you respected. It makes you a fantastic partner to have if you're the Iraqis trying to root out ISIS. We're a must-have partner.

In 2014, the Obama administration basically said [to the Iraqi government], 'If you want our CT help, you're going to get rid of that guy [Prime Minister] Nouri al-Maliki, who in our view is counterproductive.' That's an interesting case study. In the battle of Tikrit in 2015, the Iraqi military said, 'If we have to choose between the Popular Mobilization Forces supported by Iran and the U.S.-led coalition, we're gonna choose the U.S.-led coalition.'

Likewise, when the Russians, Syrians, and Iranians opened the Quadrilateral Command Control Center in Iraq in 2015, we knew very quickly that it was just hollow, and [the] Iraqis knew very quickly it was hollow. It couldn't do anything. They brought a bunch of geriatric Russian generals in; there was no technical capability. There was nothing like our [setup].

So, whether it's a technical system, whether it's an entire find, fix, finish system, or whether it's the U.S. Marine Colonel who is in the Joint Operations Center – Iraq quarterbacking the Battle of Ramadi, that kind of support is extremely valuable.

I could keep talking and throw up bazillion ways that counterterrorism support gave us a seat at the table we otherwise wouldn't have had in Iraq, in Yemen.

Counterterrorism and Deterrence in Relation to Iran

First of all, anytime U.S. forces occupy a space, anytime we're in an environment, it makes it harder for Iran or Russia to be in that same environment physically, for instance, to cohabitate key headquarters. And that's important: As long as we're there, they're not there.

As bad as things are in Iraq, there's not going to be a Revolutionary Guard Quds Force tactical operations center in the prime minister's office in Iraq, purely because it's us or them when it comes to facility presence, and that's important I think. So, we deny space by continuing to operate in space.

When we removed the task force etcetera, from al-Anad in Yemen as the south of the country was falling in 2015, we lost a lot of interaction. We lost what could have remained in place. Not there, but it could have remained in place somewhere in Yemen essentially as our alternate and shadow embassy on the ground and a source of collection of all kinds of intelligence, including diplomatic intelligence.

So, if you look at how the [United Arab] Emirates used their special forces, which is a counterterrorism capability, they used it to essentially fill the gap while their diplomats were not there for a number of years.

We've done that, for instance, in northeastern Syria, too. If you look at it, that is not really the way it should be done, but it becomes—in a war environment—the next best thing to having an embassy or a consulate in place.

It is space filling. It's the same in Iraq right now. I mean, as we close down al-Assad perhaps, in the west of the country, one whole portion of the Iraqi population (i.e., the Sunnis) will say, 'We now have no direct contact with the Americans anymore.'

If we would have closed down our counterterrorism ops in northern Iraq, Kurdistan Region of Iraq, same thing would happen. If we do it in Syria, same thing. It creates a sense of abandonment. And who fills that? Obviously, the other side fills it. Wherever we leave, you can see they do vacuum-filling. Any of our opponents, the Russians and the Iranians, do vacuum-filling. [The] Chinese are a little bit different.

Let me [also] just say this on deterrence. A determined enemy will try and penetrate an environment, and I'll talk about here about the Iranians in Iraq. They will try and penetrate the environment because it really is a strategic priority for them. They are slightly deterred from taking certain actions due to the presence of our special operations and the importance the Iraqis place on having them remain in position, but it doesn't deter completely. They'll just work ways around it. They move slower essentially.

So, for instance, the way they've undermined the CTS [Iraq's Counter Terrorism Service], the way they've essentially done a very, very, very slow rolling coup in the country. It never hit the point where we recognized something urgently dangerous enough for us to turn to the Iraqis and say, 'Your CTS was surrounded, our advisors, we're ready to help you go remove these guys from the government district.' They've worked around us over time. We didn't deter them with our special force presence, but there's probably many acts that we are deterring with the Iranians by being at Al-Asad, let's say.

Now, if we give up that presence, which we probably will, what the U.S. government often doesn't realize is that just by being there, U.S. forces are stopping worse things from happening. They look at a placement, and they say, 'It doesn't seem to be having any effect.' But what it's doing is to put a floor on how bad things can get once it's gone.

Without the CT mission, there is no floor anymore. Whether its central African coups falling into Wagner, whether it's the way Iraq deteriorated 2011 through '14. Of course, we did have a CT presence there, but it just wasn't integrated with anything else.

That's a good example of a deterrence failure. We maintained our training presence with CTS in 2011, 2012 through 2014. It didn't prevent either the major penetration by the Iranians or the return of ISIS. There's something about that experience that should have worked better but didn't.

I think one of the reasons for it is probably because we powered down too much. In 2013, the Iraqis were saying, al-Maliki was saying, 'Please come back and drone strike. Drone strike in Anbar. Drone strike around Sinjar, please. Either give us Apaches, give U.S. drone strikes. Help more than you are right now. Get more active. Actually, get kinetic again. And we'll make it happen permissions-wise.' And we didn't do it. As a result, I think we missed a trick there. So, you could say it's a case study of failure, but that's probably because we ourselves didn't see the need to get a bit more muscular.

What's the point of us being in Iraq or Syria, Iraq particularly? It's very depressing because for the USA, a decisive strategic culture that likes to win, that likes to fight conflicts and then go home. The very Jominian decisive kind of warfare type model.[21] The reality is it's horrible for the serving members who are out there, that it's not necessarily that they're contributing much. But their absence will cause significant deterioration. So, we are holding a space, and we hate to hold a space and not decisively win or change things while we're there. But there is an important value to holding a space, and conventional forces don't cut it in that environment. CT is what's still important, and it always will be.

CT as a Form of Influence

First of all, when you got a good product and you *do* have a good product, when it comes to CT support, you have to make maximum use of that in strategic competition.

Sometimes it can feel a little distasteful, particularly to the diplomats. For instance, what is America good for—killing your enemies, killing your Sunni jihadis in Iraq, let's say. We are those guys you bring in to help you dig people out from under rocks and kill them.

For diplomats there, if you listen to the way they're framing it in Iraq, they're saying, 'We want a 360-degree relationship with Iraq. It's not just about military.' And the Iraqis are like, 'Yeah, yeah, yeah, but does the CT still come?' You know, they're trying to sell them something that we're crap at, which is investing in their country. We're not gonna do that. You know all this stuff that State and the broader machine wants to sell, but the reality is what they want is our CT. That's a reality that we will be unwise to not recognize. We are good at finding [and] killing people, and it's something we're known for worldwide. We might want to be more than that, but it's one of the only things we do that works properly when we try and export it, and some of our military hardware, too, but some of that's too complicated and we don't want to release it. It's more than they need.

To me, when I look at us being able to mentor the special forces of countries around the world, what I'm looking at [is] us being able to basically develop the countercoup force in that country.

Supporting CT forces is vital because such elite military leadership tends to move sideways into the conventional leadership structure.

So, CTS—that was the effort in Iraq—this was the force that might prevent a militia takeover or Iranian takeover. This was the force that, under the worst circumstances, might hold civilian government open in a guarded military role. This is the force that we could always count on to protect our technology and our training.

Now, unfortunately, it's going wrong as we speak. It has been allowed to atrophy and to be politicized, and the best example of what we will try to do with CT is starting to fall apart, sadly, in Iraq. It's a good case study of what you must not let happen.

So, I am not suggesting we need School of the Americas 2, but I am suggesting that special forces leadership tends to become very significant leadership within the country. And they provide a safety catch, and they provide an ultimate force for cooperation. Or where a government has gone badly wrong, they provide an ability to fix the problem and restore some kind of system of government that works. So, they're critical to have. Look at all these coups in central Africa.

Europe – Magnus Ranstorp

CT as Threat Mitigation in the European Context

Maybe the best example is the U.K. one, which has become sort of standard all across Europe, and that is, if you look at the four 'P's—prevent, pursue, protect, and prepare—you have a holistic framework, whereby the CT bits in relation to 'pursue'—which also involves the military dimension, security services, etcetera—is only one set of a whole framework where you have either 'prevention' or 'pursue' or 'prosecute.' Then you have the other two Ps—'protect' and 'prepare'—which are helpful when you have a terrorist incident and how quickly you can come back from it. Here, I take my cue from Sir David Omand, who really was the principal architect of this [the United Kingdom's four 'P' approach]. He said that all counterterrorism needs this strategic framework because it is essential to bounce back to normalcy as quickly as possible once terrorism occurs. So, strategic communication becomes very important to how you control the narrative once something happens—crisis communication, strategic communication, etcetera after an event.

There are also communicative elements in how different security services in Europe have different levels of openness in relation to the public. If I just take my own, the Swedish security service, they were very closed before because they were more directly involved in counterintelligence against the Russians, but gradually when CT came around with 9/11, the value of strategic communication was understood—communication about the threat, communication about the intersection of threats and deterrence, a kind of signaling to the adversary that they are in focus.

We also have hybrid threats. A good example is the fact that the Iranians and particularly the Islamic Revolutionary Guards Corps (IRGC) have sent agents to Sweden to assassinate leaders of the Jewish community, and they're also using criminal groups as a sort of cheap, proxy wars; they don't need to use Hezbollah in the same way, which also creates plausible deniability. Now, the security services are out communicating this threat—calling the Iranians out, calling the network out—and that is an important part of creating deterrence, accountability, and that there is a cost. It also creates political pressure because now there are calls for classifying the IRGC as a terrorist entity within the European Union. Sweden is calling for that actively.

CT's Relevance, or Irrelevance, to Strategic Competition in the European Context

This can be seen in different areas. First of all, we have the listings of terrorist groups, and there, you have different states taking different approaches. We have the U.K., the Netherlands, Germany, and, of course, other Five Eyes countries, they all have designated Hezbollah, the entire entity, which only makes sense as it is under one command. So, you have had a gradual slide towards an understanding that you cannot isolate these different things [non-state and state level threats]. For example, you cannot speak about Hezbollah without speaking about Iran due to their intertwined operational cooperation.

Of course, these hybrid threats with Iranians behind actions in Europe has meant that the Iranians are more offensive, but also that European counterterrorism efforts are correspondingly responding to this threat more assertively. The fact that you have criminal groups acting on behalf of terror states is quite a new and important development in terms of potentially classifying the IRGC Revolutionary Guards Corps as a terrorist entity, or individuals within that organization. This is not new to the U.S. It's not new to Canada and others.

The 7th of October [attack] also comes to mind. I think the financial architecture, but also the U.S. listings, the Treasury listings, etcetera, also have a massive impact on Europe, forcing Europe also to adhere to the sanctions lists. These lists, particularly U.S. Treasury lists, lists of the State Department, have a massive impact on shrinking the space for different groups in the financial arena and actually changing behavior. A good example is the Nordic Resistance Movement, and the U.S. listing, and the linking of that movement to a state actor [Russia].[22] Nordic Resistance Movement leaders cannot have bank accounts or travel without the fear of being subject to U.S. rendition.

In many ways, the United States is the CT conductor, which is welcome, and they are particularly effective in the financial space, that's where it really bites. Because without the financing, terrorist groups have difficulty operating, and the U.S. sanctions regime has huge consequences for banks and other financial institutions because if you do not adhere, banks may be sanctioned themselves. This is a huge instrument.

What we need in Europe is working [in a] more focused [way] on tackling the financial architecture of terrorist groups and networks, and particularly when terrorist groups use humanitarian causes, using fronts as covers, as a method of collecting massive amounts of money.

We've been very slow tackling the financing of all these different groups. A good example right now, there's the case of [Amin] Abu Rashid in the Netherlands,[23] who has been accused of financing Hamas within Europe. He [was allegedly] using the European Palestine Conference as a means to generate funding, etcetera. So, I think that there's a sort of change in mood after the 7th of October, especially in relation to what is happening with Hezbollah and Hamas and their support infrastructure in Europe, which is starting to be tackled more. However, E.U. states need to move faster and more offensively against this.

Members of the Iraqi Counter-Terrorism Service (CTS) are pictured with the Islamic State's flag in the Old City of Mosul in Iraq on July 2, 2017, during the offensive to retake the city from the group's fighters. (Ahmad al-Rubaye/AFP via Getty Images)

<u>*Counterterrorism and Deterrence in the European Context*</u>

To be honest, the first thing I think of is the Israelis—of course, what they are doing now to reestablish deterrence, to reestablish dominance. Their incredible intelligence operations against Hamas and Hezbollah signal that they can reach anyone, anywhere, anytime.

[There is often] a five-grade scale. In Sweden and Denmark, the threat level is [currently] at a 4 (out of 5). So, [through these systems] you're trying to communicate to the public, but you're also communicating to states that they may also be consequences for states using states' sponsorship.

Highlighting the actors, this also becomes part of deterrence. The U.S. has been doing this, of course, a long time, but I think the Europeans are waking up more to this hybrid threat of warfare, which involves Russia and the Iranians particularly.

There is also the basic issue of having the adversary spend more time thinking about their own security than plotting and planning. There are European services that have a more offensive reputation. Denmark, for example, has been extremely offensive, and over a period of time, it became very clear that extremist groups or terrorist groups, etcetera didn't want to base themselves in Denmark because they were intercepting and disrupting their activity either earlier or in a much more forceful way.

So, you have counterterrorism as signaling—that if you are based in a particular territory, you will face pressure. [The] U.K. is another example. The U.K. has a reputation for being a bit lenient on certain groups, has been traditionally. This is, of course, historically why the French were complaining about Londonistan etcetera, that they allow groups to function. As a result, you have different spaces across Europe.

Belgium is another example where you have, until the [2015] Paris and [2016] Brussels attacks, a sort of recognition that the Belgian CT community needed to step up. So, you have differences all across Europe in relation to how you deal with this threat. The Italians, as soon as they detect any threat—extremists, etcetera—they expel them to North Africa and normally this wouldn't happen in other [European] countries. It wouldn't happen the farther north you get. The more sort of risk averse [a country is], the more conservative the response may be in relation to some actions that may be taken against particular organizations and groups.

Different states also have different terrorism legislation. In some states, it can work as a form of deterrence: You can lose your citizenship if you get convicted. I testified in the Mullah Krekar case[24] in Norway [and] also in the Said Mansour[25] case in Denmark. Said Mansour was involved in the 2003 suicide bombing in Casablanca, Morocco, and was also the main Moroccan jihadist leader figure in Denmark who became a towering preacher like Abu Qatada or other such leaders. Mansour was prosecuted. And he had dual citizenship (Moroccan and Danish), and the Danish government brought charges for a relatively minor offense which [led to the withdrawal of] his citizenship and [his expulsion] back to Morocco. So, if you're dual national, withdrawing your citizenship or not granting citizenship to [individuals who pose] security threats [who have] sought asylum is actually a form [of] deterrence, because [the message is] then 'you will lose all your benefits. You won't be able to stay in the country.'

When it comes to deterrence, another weakness in counterterrorism in Europe is the listing system that we have. It's a bit antiquated. It needs to be updated, and it needs to be more developed along the lines of the United States, whose system involves individuals and entities, in addition to groups. The European framework could also be developed and updated much more often.

Conclusion

The CT ROI framework examines value through a convergent lens where counterterrorism and strategic competition can be mutually supporting and complementary activities. That is its starting point, and it may be the area where the framework proves most useful. That is because since 9/11, U.S. counterterrorism efforts have evolved into being more than activities focused on threat mitigation. For the United States, that is the core element of CT and it always will be, but over the past two and half decades, counterterrorism has also been a form of influence, a tool—and in some cases a strategic one—that the United States has leveraged to cultivate and enhance partnerships, to build trust, to offset direct time spent on CT, and to make progress toward other goals. This is why the CT ROI framework places emphasis on direct and intersectional CT returns.

The interviews featured in this article provide additional context and important color to how CT and strategic competition intersect generally and in specific regions—Africa, the Middle East, and Europe. The interviews highlight opportunities. They also offer cautions and provide insight into risks and other issues that need to be considered as the United States and its partners continue their quests to find what 'CT right' looks like in different regional areas.

As noted by Christopher Faulkner, it is also helpful to view "CT in the African context through the theme of resilience" as reflected in different ways.[26] He also stressed that CT only gets one so far: "It must be a more comprehensive project, focused not exclusively on military means but instead on prioritizing non-military instruments of national power that can genuinely differentiate the United States from its strategic competitions."[27] Leveraging CT as a form of influence in Africa can also be a "double-edged sword … [it is] arguably necessary as a means of yielding influence … [but] the risk is that such provisions, in isolation, rarely if ever resolve the insecurity and then can unintentionally help contribute to anti-Western sentiment."[28] Or to put it more simply, CT can provide short-term threat mitigation 'wins,' but if those gains are not lasting, it can help to create an environment that is less friendly to U.S. interests and lead to longer term 'loses.'

Michael Knights stressed that "counterterrorism support gave us a seat at the table we otherwise wouldn't have had in Iraq, in Yemen."[29] He also made the important point that "we deny space by continuing to operate in space," even if that is hard for Americans, who have a "decisive strategic culture that likes to win," to accept.[30] Drawing on the case of the Iraqi CTS, he offered cautions about partner success stories and the sustainment of capabilities: "It's going wrong as we speak. It has been allowed to atrophy and to be politicized, and the best example of what we will try and do with CT is starting to fall apart, sadly, in Iraq. It's a good case study of what you must not let happen."[31]

Magnus Ranstorp called attention to the intersection between terrorism and hybrid threats in Europe, how counterterrorism approaches are evolving on the continent, and areas that deserve attention and could be improved. "A good example" of hybrid threats "is the fact that the Iranians and particularly the Islamic Revolutionary Guards Corps (IRGC) have sent agents to Sweden to assassinate leaders of the Jewish community, and they're also using criminal groups as a sort of cheap, proxy wars."[32] Ranstorp viewed sanctions, and particularly financial sanctions, as being an area where Europe needs to work in a more focused way because "we've been very slow tackling the financing of all these different groups."[33]

Through all of this, there is also an underlying current of the importance of information and messaging. While several of the returns on CT investment have tangible outputs and can be cleanly measured, there are also many returns on investment that are psychological and can be difficult to quantify. These types of returns, more than others, require a deliberate dominance of the information space. The CT enterprise must rapidly combat misinformation and disinformation by adversaries and must ensure that allies and partners know when U.S. CT activity has resulted in a measurable disruption and defeat of an ongoing or planned attack. Information operations and strategic messaging help take the measurable outcomes and help translate them into the psychological effects. This is demonstrated by greater trust and confidence in U.S. CT forces, which translates to greater access and influence for U.S. diplomats and an increased likelihood of cooperation in the strategic competition environment.

The authors provided this framework as a starting point to developing a more adaptable and integrated model for investing in a resource (CT) that can provide direct and various types of intersectional returns. When used properly, the framework may have the ability to increase shared understanding regarding the broad utility of CT forces, their interoperability, their role in campaigning, and their ability to shape or build momentum for other pursuits in support of combatant commanders and the president. CTC

Citations

[1] Eliot Ackerman, "Winning Ugly: What the War on Terrorism Cost America," *Foreign Affairs*, September/October 2021.

[2] "The National Security Strategy of the United States of America," September 2002.

[3] Kenneth G. Lieberthal, "The American Pivot to Asia," Brookings Institution, December 21, 2011. See also "Fact Sheet: Advancing the Rebalance to Asia and the Pacific," The White House, November 16, 2015.

[4] "The National Security Strategy of the United States of America," December 2017.

[5] "Summary of the 2018 National Defense Strategy of the United States of America," 2018.

[6] For a perspective on the importance of CT partnerships during an era of strategic competition, see Matthew Levitt, "Rethinking U.S. Efforts on Counterterrorism: Toward a Sustainable Plan Two Decades After 9/11," *Journal*

of National Security Law & Policy 12:247 (2022).

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

[8] Paul K. Davis and Brian Michael Jenkins, *Deterrence & Influence in Counterterrorism* (Santa Monica, CA: RAND, 2002); Don Rassler, *The Compound Era of U.S. Counterterrorism* (West Point, NY: Combating Terrorism Center, 2023); Jason Warner, "The Counterterrorism-as-Influence Competition in Africa," Lawfare, October 5, 2024.

[9] Authors' interview, Michael Knights, October 2024.

[10] Brian Michael Jenkins, "The Future Role of the U.S. Armed Forces in Counterterrorism," *CTC Sentinel* 13:9 (2020).

[11] Matthew Levitt, "Harmonizing Counterterrorism and Great-Power Competition," *National Interest*, May 9, 2021.

[12] Mico A. Galang, "A Decade On: EDCA and the Philippines–US Alliance," RUSI, April 18, 2024.

[13] Ibid.

[14] See "Philippines, U.S. Announce Locations of Four New EDCA Sites," U.S. Department of Defense, April 3, 2023.

[15] Temporal analysis of polling data released by Social Weather Stations.

[16] Ibid. See also Janvic Mateo, "Poll: Pinoys trust United States the most; China least trusted," *Philippine Star*, April 29, 2024.

[17] Cases from different regions and countries are also explored in Levitt, "Rethinking U.S. Efforts on Counterterrorism: Toward a Sustainable Plan Two Decades After 9/11."

[18] Matthias Krönke, Thomas Isbell, and Makanga Ronald Kakumba, "In citizens' assessments, most African police forces come up short," Good Authority, March 22, 2024.

[19] John Chin and Haleigh Bartos, "Rethinking U.S. Africa Policy Amid Changing Geopolitical Realities," *Texas National Security Review* 7:2 (2024): pp. 114-132.

[20] For background, see Annie Linskey, "Kamala Harris Pledges $100 Million to West Africa Nations to Fight Extremist Threat," *Wall Street Journal*, March 27, 2023.

[21] For background, see Austin L. Bajc, "Improving Maneuver Warfighting with Antoine-Henri Jomini Warfighting Functions, the Single Battle Concept, and Interior Lines," Marine Corps University Press, September 15, 2022.

[22] Magnus Ranstorp and Filip Ahlin, "Från Nordiska motståndsrörelsen till alternativhögern En studie om den svenska radikalnationalistiska miljön," Swedish Defence University, 2020.

[23] For background, see "Netherlands court orders release of Palestinian activist Amin Abu Rashed," Middle East Monitor, May 16, 2024.

[24] For background, see "Norway extradites jihadist preacher Mullah Krekar to Italy," BBC, March 26, 2020.

[25] For background, see "Denmark strips man of citizenship over 'terror links,'" Al Jazeera, June 11, 2016.

[26] Author interview, Christopher Faulkner, October 2024; author correspondence with Christopher Faulkner, October 2024.

[27] Ibid.

[28] Ibid.

[29] Authors' interview, Michael Knights, October 2024.

[30] Ibid.

[31] Ibid.

[32] Author interview, Magnus Ranstorp, October 2024.

[33] Ibid.

Go Big or Stay Home? A Framework for Understanding Terrorist Group Expansion

By Daniel Milton

Terrorist organizations are not monolithic entities when it comes to many different aspects of their activities. Among other things, they may change goals, leaders, and tactics over time. This article focuses on one particular type of change: the decision by a terrorist group to geographically expand attack operations outside of its home base of operations. The article presents a discussion of what is meant by expansion and contends that expansion can be best understood in terms of the opportunity and willingness framework. It then turns to an application of this framework to two cases of expansion: the Liberation Tigers of Tamil Eelam (LTTE) and Islamic State Khorasan (ISK) into multiple countries.

In 2009, the United States Senate held a pair of hearings over concern that the terrorist group al-Shabaab might pose a threat to the U.S. homeland, even though up until that point, al-Shabaab's attacks occurred mostly in and around Somalia.[1] After the group's September 2013 attack against a shopping mall in Nairobi, Kenya, policymakers in the United States again expressed increasing concern that the group may turn its sights toward conducting attacks on the homeland of the United States. A few weeks after the attack, the Foreign Affairs Committee of the U.S. House of Representatives held a hearing titled, "Al-Shabaab: How Great A Threat?"[2] A few years later, on February 21, 2015, the concern of al-Shabaab expanding its reach from East Africa to the United States resurfaced when the group released a propaganda video calling for attacks on American and Canadian shopping malls.[3] Over the next several years, al-Shabaab carried out attacks against U.S. targets in and around Somalia, including the Camp Simba attack in Kenya in January 2020 that resulted in the deaths of three U.S. military personnel.[4] The group also directed at least two individuals to obtain flight training in preparation for operations in the United States similar to the September 11 attacks, although both were arrested in countries outside of the United States before those plots could be carried out.[5] Despite the concern of policymakers and the efforts of the group itself, at the time of this writing in November 2024, al-Shabaab cannot claim a successful attack on the U.S. homeland.

Daniel Milton, Ph.D. is a Professor of Transnational Security Studies at the George C. Marshall European Center for Security Studies. His work focuses on the dynamics of terrorist organizations, counterterrorism policy, and international security.
X: @Dr_DMilton

The views expressed in this publication are those of the author and do not necessarily reflect the official policy or position of the George C. Marshall European Center for Security Studies, the U.S. Department of Defense, the German Ministry of Defense, or the U.S. and German Governments.

Even though al-Shabaab has not carried out the attack in the U.S. homeland that many feared, the underlying question that drove the public hearings and continued concern remains an important one: What are the factors that drive some groups to expand their geographic reach and others to remain more locally focused? The importance of this question is even greater in today's environment in which a large number of terrorist groups remain committed to the use of violence against non-combatants in furtherance of political goals at the same time that many governments have decreased the resources available for counterterrorism.[6] The continued conflict in the Middle East, the disruption of recent terror plots in Europe over the past two years, and ISK's attack in Moscow in early 2024 have only served to underscore the reality of the threat.[7]

This article endeavors to provide a framework for analyzing the factors that lead to terrorist group expansion. The goal is not to provide a mechanism for perfect prediction—the factors impacting each terrorist group are too unique for this—but rather to offer increased structure to our understanding on this important question. It does so by first contextualizing the concept of expansion across two variables: the distance of the operation from the group's base and the amount of control the group has over the operation. Then, in seeking to explain why groups choose to expand, it utilizes the opportunity and willingness framework from the literature on international conflict. This framework is then briefly applied in two cases: the Liberation Tigers of Tamil Eelam's (LTTE) expansion into India and Islamic State Khorasan's (ISK) operational expansion into a number of theaters. The article concludes with a discussion of the implications of this for academics, policymakers, and practitioners.

What Is Expansion?

Although it may seem elementary, it is critical to first pause and consider what is meant by expansion. As it turns out, the term 'expansion' could be defined along several parameters. A terror group located in one state that takes advantage of the porous, hard-to-defend borders of a neighboring state to establish a safe haven may have expanded its area of operations, as was the case with al-Qa`ida and the Taliban in Pakistan in the time after the U.S. invasion of Afghanistan in 2001 or the Revolutionary Armed Forces of Colombia (FARC) in Venezuela at various points over the history of that conflict.[8] In a similar manner, the establishment of logistical supply routes or financial activities in distant countries might also be considered expansion, such as the activities of Hezbollah to raise funds or procure weapons in the United States.[9] Another way to answer this question would be to focus exclusively on the interests of a specific country. For example, a U.S.-centric answer to this question might simply focus on the possibility that a terrorist group can strike the U.S. homeland, but this view does not adequately consider the various avenues through which terrorist groups can threaten both U.S. and global security interests as their ability to attack outside of their normal area of operations increases. Another answer might emphasize expansion in terms of an escalating level of attacks from soft to hard targets (or vice versa) or the targeting by the group in its home territory or a foreign country's governmental or commercial facilities.

In sum, there is no single way to conceptualize 'expansion.' However, it is critical to select an approach to 'expansion' that captures the dynamic relevant to the analysis of interest. In the case of this article, the concern is with the ability of terrorist groups to conduct attacks across greater geographic distances. More specifically, an expansion involves a group carrying out operations beyond the theater of normal operation. Context is critical in making this determination, as a theater of operation might be a single country (or part of a country) for some groups, while for other it spans across several countries. Moreover, there is also a difference between expansion to the next state over as opposed to expansion that requires a group to cross many borders or even the ocean. The decision to focus on geography is made in part because one of the most dangerous capabilities posed by terrorist groups is their ability to intentionally carry out destructive acts of violence. Although the ability of terrorist operatives to cross borders in order to recruit, raise funds, or obtain weapons might be important conditions enabling violence, they are not the end or primary concern of interest here.

One additional conceptual issue to consider is whether a group should be considered as having 'expanded' because its ideology inspired someone in a distant country to carry out an attack, even though there may not have been any direct command-and-control exercised by the group over the operation itself. For example, when a 16-year old teenager in Las Vegas, Nevada, was arrested by authorities in November 2023, information was found in his possession that indicated that he supported Islamic State and referred to "Islamic State – Las Vegas Province."[10] At the time of this writing, no public evidence has emerged to suggest that the teenager communicated directly with or was personally directed by any other formal element of the group. Even if the plot had been successful, would it have been reasonable to say that Islamic State's operations "expanded" to Las Vegas? It is not clear that the answer to this counterfactual is no, but it also seems that there is a qualitative difference between a group providing inspiration for a plot as opposed to enabling it through the provision of instructions, funding, and so forth or exercising command and control over its execution.[a] A conclusive answer to this question is not provided here, but it merits additional thought and research.

The framework proposed here focuses on attacks as the primary outcome of interest and considers expansion as occurring along two different dimensions: the control that a terrorist group exerts over attacks and the distance of the attacks from the home location of the terrorist group.[b] Although each of these dimensions exists along a continuum, for the ease of presentation and discussion, Figure 1 depicts each with three separate values or categories. It also contains shaded coloring that accounts for the way in which groups that expand toward the upper-right of the figure represent a greater danger to global security.

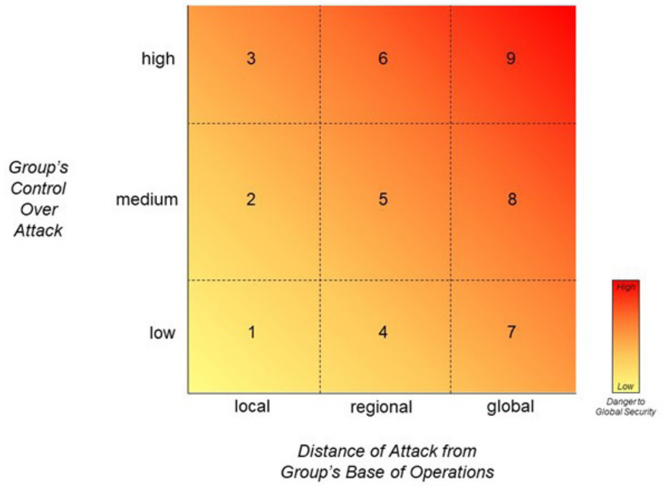

Group's Control Over Attack
high
medium
low
3
6
9
2
5
8
1
4
7
local
regional
global
Distance of Attack from Group's Base of Operations
High
Low
Danger to Global Security

Figure 1: Geographically Categorizing the Attacks of Terrorist Groups

Although expansion is a dynamic phenomenon whereby a group moves from one box to another, it may be beneficial for contextual understanding to provide a few examples of the types of attacks that fall into some of the categories that appear in Figure 1.

Categories 1-3 reflect a terrorist group of varying strength and capacity that has mostly local concerns, also referred to as a domestic terrorist group. Even though this group is local, it is important to note that it might be able to inspire others to carry out violence in service of its worldview, but without much direct involvement of the group itself (Category 1). It may also be the case that the group has the capability and control to be able to plan and execute local attacks on its own (Category 3). Groups with the capability to carry out local attacks may indeed pose a serious threat to the government or area in which they operate. And there is a potential

[a] There is seldom a cut-and-dry line between inspired and directed attacks. Islamic State's virtual planning model is a good example of this grey area, as some plots under this model approach a centrally directed attack while others appear to be slightly more than an inspired operation. Daveed Gartenstein-Ross and Madeleine Blackman, "ISIL's Virtual Planners: A Critical Terrorist Innovation," War on the Rocks, January 4, 2017.

[b] Note that, in this framework, expansion is very much a geographic phenomenon. A terrorist group choosing to attack a foreign embassy located within the group's already existing area of operation is not considered here, although, as mentioned above, it could certainly be considered expansion and is a dynamic worth examining in the future. Some scholars have already carried out work along these lines in the form of large-n studies focused on the targeting of Americans by foreign groups. Eric Neumayer and Thomas Plümper, "Foreign terror on Americans," *Journal of Peace Research* 48:1 (2011): pp. 3-17; Daniel J. Milton, "Dangerous work: Terrorism against U.S. diplomats," *Contemporary Security Policy* 38:3 (2017): pp. 345-370; Daniel Meierrieks and Thomas Gries, "'Pay for It Heavily': Does U.S. Support for Israel Lead to Anti-American Terrorism?" *Defence and Peace Economics* 31:2 (2020): pp. 160-174; Victor Asal, Christopher Linebarger, Amira Jadoon, and J. Michael Greig, "Why Some Rebel Organizations Attack Americans" in Khusrav Gaibulloev and Todd Sandler eds., *On Terrorist Groups: Formation, Interactions, Survivability and Attacks* (London: Routledge, 2023), pp. 72-89; Eugen Dimant, Tim Krieger, and Daniel Meierrieks, "Paying Them to Hate US: The Effect of US Military Aid on Anti-American Terrorism, 1968–2018," *Economic Journal* 134:663 (2024): pp. 2,772-2,802.

that they may, at some point, turn their gaze outward toward an expansion of attacks. However, when it comes to a global threat picture, it is the groups that are capable of both launching and inspiring regional and global attacks that generally create larger international security concerns.

Perhaps one of the most challenging type of groups are those with an attack portfolio somewhere in Categories 4-6, with the most concern for international security focused on Category 6. Some of the groups that carry out attacks in these categories have some level of capability and likely have some measure of staying power, yet they have not continued to expand their operations. Al-Shabaab, discussed in the opening to this article, is an excellent example of a group that falls into Category 6. It has demonstrated strong control over attacks both locally and regionally, and it continues to exist despite persistent international efforts to reduce its area of operations.[11] It is these groups in many cases that may pose the most perplexing challenges for security professionals, as they may appear to be on the cusp of expanding.

At the highest end of the threat spectrum is a group that is able to plan and execute a global attack directly (Category 9). Such a group would likely be well-resourced and experienced in the array of tradecraft necessary to carry out such operations. This is a terrorist group that likely poses a direct threat to many nations. Perhaps one of the most well-known examples of this type of attack is al-Qa`ida's 9/11 attacks in the United States, which demonstrated both a high level of control as well as distance from the group's known base of operations in Afghanistan.

A group's attack portfolio does not have to be constrained to one box alone, but may end up conducting operations across multiple categories in a given period of time. One example of this is the Islamic State in the 2015-2017 timeframe. Not only did the group exercise a high level of control over the attack in Paris (November 2015),[12] but its ideology also inspired the attacks in Barcelona (August 2017),[13] with little evidence emerging to suggest a more central role by the group in the planning or execution of that attack. Of course, during this period of time, the group carried out and inspired attacks in its home base of Iraq and Syria, but also in other locations around the world.[14] All of these attacks place the Islamic State's overall attack portfolio into a number of these categories depending on the specific moment at which the analysis occurs.

So, what then is meant by expansion? Based on the conceptualization presented in Figure 1, expansion can be best thought of as movement by a group horizontally or diagonally from the left to the right. In the former case, a group moving from Category 6 to 9 is expanding, while in the latter case a group moving from 6 to 7 would also be considered expanding. In more straightforward terms, when a group moves from carrying out operations locally to regionally to globally, it is expanding. That is the general type of expansion considered in this article. It is worth noting, however, one might also consider expansion have occurred if a group moves vertically (from the bottom to the top) in terms of their attack portfolio. This would not be geographic expansion, but more an expansion of operational control and capacity. However, this type of expansion is not discussed in this article.

Explaining Expansion

With a clearer understanding of what this article means when it refers to the expansion of terrorist groups, it now turns to address the important question regarding why these groups expand. To do so, it borrows from the literature on international conflict. In this literature, explanations regarding why nations go to war abound. While there are many useful explanations and frameworks for this purpose, some early research focused on the importance of opportunity and willingness to explain state decisions to go to war.[15] The idea is relatively straightforward. If a nation is going to go to war against another nation, a state seeking conflict must actually have the opportunity to do so. If two states never interact, it is unlikely they will go to war. If one state has no tanks or soldiers, it is unlikely that it will go to war with another that does. Moreover, opportunity is not sufficient. War will only occur if the state also has the desire, or willingness, to begin fighting. There must be some motivation on the part of the country's executive, legislature, military, or people to want to engage in combat.

A similar framework can be useful for thinking about the expansion of terrorist groups.[c] Just like the leadership in other organizations, the decision makers in terrorist groups have incentives for various courses of action but are also bound by constraints.[d] Decisions about where, when, and how to carry out attacks are not detached from considerations related to the opportunity to carry out such strikes and the willingness to do so given the group's motivations and goals. Terrorist organizations must navigate and balance factors such as the availability of operatives, the ability of operatives to travel using false documents or safehouses, leadership opinions regarding both the viability and desirability of expansion, and the potential response of the intended target with their overall objectives and goals.

The use of the word "balance" above deserves added discussion. Opportunity and willingness are not to be considered in isolation when attempted to explain expansion. A group may have all the opportunity in the world, but absent a motivation to mobilize that opportunity into an expanded pattern of attacks, the group itself will likely remain locally focused. On the other hand, a group may wish to carry out a worldwide campaign of violence in an effort to advance its political goals, but may not have the opportunity or willingness to do so. A lack of either factor will lead to an outcome in which a group is unable to carry out an expansion in terms of its attack portfolio.

One additional observation has to do with the use of the opportunity and willingness framework as opposed to a seemingly similar framework: capabilities and intent. Some may argue that the difference between these two frameworks is negligible, but the author prefers the former for three reasons. First, as it applies to "opportunity" as opposed to "capabilities," the author finds the latter term to be narrower and encourage a focus strictly on more tangible resources such as weapons and money. The reality is that the decision to expand is about more than just items. As will be discussed more below, it is also about intangible factors that may

[c] Although the author employs the "opportunity" and "willingness" framework here and prefers that terminology, other scholars have utilized a "push" and "pull" model imported from the study of organized criminal groups. Tin Kapetanovic, Mark Dechesne, and Joanne P. Van der Leun, "Transplantation theory in terrorism: an exploratory analysis of organised crime and terrorist group expansion," *Global Crime* 25:1 (2024): pp. 1-25.

[d] The opportunity and willingness framework could also be applied to individual decision-making processes regarding radicalization and carrying out attacks, but that level of analysis is not what is being examined here. This is focusing on the strategic decision of the group to expand and is an organizational-level analysis.

be beyond the group's control that create the space for expansion to occur. Focusing only on "capabilities" may lead scholars and analysts to miss critical factors. Second, although "intent" is not as limiting in the author's view as "capabilities," it conveys a level of agency and calculation that might overemphasize leadership choice at the expense of broader environmental factors at play. Intent also seems difficult to assess, relying more on the internal processes of individual thought-making rather than other observable factors.

Although terrorist organizations differ from states in many respects, the overarching framework in which they make decisions at times displays similar rationales.[16] Space here does not permit a full examination of the reasons identified by scholars that impact decision-making by terrorist organizations, but some of this work, together with other factors necessary for expansion, can be modified and distilled down into factors that fall under the opportunity and willingness framework described above. What appears below is a simple categorization of the factors that might fall under opportunity and willingness when considering the organizational decision to expand.

- **Opportunity**
    - » Factors under control of the group
        - Access to and/or availability of self-procured resources[17]
            - Financial: funding, ability to transfer money to cells in new locations
            - Human: useful operatives, returning foreign fighters[18]
            - Logistical: falsified documents, external support networks
            - Weapons
    - » Factors not under group control
        - Existence of a diaspora community[19]
        - Safe haven[20]
        - Anti- and counter-terrorism activities and policies
        - Resource support from a state sponsor
        - Geopolitical events
- **Willingness**
    - » Factors under control of the group
        - Expansive or transnational ideology/goals[21]
        - Seeking international attention or support[22]
    - » Factors not under group control
        - Direction from a state supporter/terrorist ally[23]
        - Internal or external counterterrorism pressure[24]
        - Lack of constituent support in home area[25]
        - Geopolitical events

This list of factors provides some possibilities when it comes to reasons for expansion, but is not intended to be an exhaustive explanation for each case. As noted above, it is critical to state that even if a factor is listed twice (state sponsorship and geopolitical events), this does not mean that the same mechanism is at play. For example, consider the October 7 attack on Israel and the subsequent Israeli response. Some analysts have noted that it has provided a boost to terrorists when it comes to human resources. One senior U.S. intelligence official noted that October 7 "was, is and will be a generational event that terrorist organizations in the Middle East and around the world use as a recruiting opportunity."[26] But in addition to helping the opportunity side of the equation, it may also be the case that October 7 and subsequent events have also encouraged terrorist groups to increase their willingness to target Israel and those viewed as being supportive of it.[27] One scholar noted that, "A U.S. military confrontation with Hezbollah could spark terrorist attacks on American targets abroad and domestically."[28] In other words, it might increase the willingness of Hezbollah to act.

Most terrorism experts are familiar with the fact that there is no individual profile when it comes to an individual's radicalization pathway. The same logic applies here. There is no one-size-fits-all solution or explanation for the reason a group chooses to expand its area of operations. Despite this, the opportunity and willingness framework can still be useful in understanding and structuring an examination of the decision to expand. Although each individual case might deserve its own article or book length treatment, a few brief examples are useful for illustrating the framework in action.

The Expansion of the Liberation Tigers of Tamil Eelam (LTTE) to India

In 1983, after years of acrimony between the Sinhalese majority and Tamil minority in Sri Lanka, frustrations exploded into a full-blown civil war between the Sri Lankan government and a number of non-state militant groups. One of these was the Liberation Tigers of Tamil Eelam, also known as the Tamil Tigers or LTTE. The LTTE's violence against both government and civilian targets included a wide array of tactics, including suicide bombings.[29] Eventually, the group's nearly 40-year reign of violence ended in 2009 when the Sri Lankan government claimed victory after an intense military campaign, but not until tens of thousands were dead, wounded, or otherwise unaccounted for.[30]

During the LTTE's history, there is an interesting transition that happens during the conflict. Using the Global Terrorism Database (GTD) from the University of Maryland's National Consortium for the Study of Terrorism and Responses to Terrorism, the first attributed incident for the LTTE is in 1975 in Sri Lanka.[31] The GTD reports 279 LTTE attacks up through 1990, all occurring in Sri Lanka. But then, something changes. In 1990, 1991, and 1992, the GTD contains a total of five attacks carried out by the LTTE in India. Looking at Figure 1, it seems that the LTTE changed from being a well-coordinated, locally operating group (Category 3) to a well-coordinated, regionally operating group (Category 6). How do we explain the decision by the LTTE to expand the geographic area of its operations to India in 1990? The opportunity and willingness framework provides a template for doing so.

Opportunity

In terms of opportunity, geographic proximity certainly seems to have made expansion easier in the case of the LTTE, if not likely. The two countries are, at their closest point, merely 25-35 miles away from each other, albeit separated by a body of water.[e] When it comes to India specifically, there was and is a fairly large population of Sri Lankan Tamils living there, to say nothing of the broader population of Tamil Nadu.[32] The close geographic and ethnic ties might have provided some of the opportunity for expansion, although such factors exist in many different contexts, so it is hard to ascribe too much weight to them.

[e] Given the close distance, it may be argued that the LTTE attacking in India does not even represent an expansion. However, such a change in the attack portfolio, even over a short distance, is likely a deliberate choice, given that not a single attack had occurred outside of Sri Lanka's borders prior to 1990.

Smoke rises from the Westgate mall in Nairobi, Kenya, on September 23, 2013, during an attack by al-Shabaab. (Carl de Souza/AFP via Getty Images)

That said, the LTTE arguably had a safe haven in Sri Lanka in which they could plan to expand their portfolio of attacks. Even though they were under pressure from the very beginning of the conflict by the Sri Lankan military, those military efforts had decidedly mixed results at best.[33] And even if the northeastern part of Sri Lanka had not been a safe haven, not far away LTTE fighters were trained in India to fight against the Sri Lankan government—an irony given that LTEE would eventually embark on a regional expansion of operations against India.[34] In essence, LTTE had benefit of the resources and knowledge of a state sponsor (an important consideration on the opportunities side of the equation) and then later expanded its operations against that very state sponsor.[35] Additionally, some analysts have argued that LTTE did not attract significant international censure early on in its operations.[36] Moreover, refugees fleeing the violence in Sri Lanka have helped establish a worldwide diaspora community that enabled fundraising and political support from abroad, although this was more limited earlier on.[37]

The LTTE also seems to have had healthy amounts of resources in order to coordinate, finance, and staff an expansion. On the financial front, it is harder to pin down the yearly earnings of the group. Some estimates have suggested, however, that the group brought in large amounts of money every year, ranging from tens to even possibly hundreds of millions of dollars each year.[38] Regardless of the actual amounts, it is clear that financial constraints to an expansion did not seem to exist. And the group had significant human capital as well, with an estimated 10,000 fighters at the pinnacle of its power.[39]

In sum, it seems that the LTTE had proximity, some level of safe haven, and a sufficient amount of resources working in its favor as far as the opportunity component necessary for expansion. However, as noted above, opportunity in and of itself is not a sufficient explanation. It must be considering in tandem with the willingness factor.

Willingness

Examining the ideology of the group, in this case, does not appear in and of itself provide any added impetus for expansion. The LTTE was largely a secular group oriented toward fighting for the independence of the Tamil minority living in Sri Lanka, in other words, for a geographic homeland on the island of Sri Lanka.[40] Of course, the fact that the group was willing to carry out acts of violence in this effort certainly showed a strong resolve to do whatever was necessary for the cause. However, the key point is that, absent either a change in the group's ideology or some other factor, the willingness to engage in an operational expansion remained low.

Nor does a loss of public support seem a useful explanation. As other scholars have noted, early on the conflict, the LTTE not only managed to eliminate rivals for leadership of the Tamil cause, but also seemed to enjoy some level of public support among Tamils, especially because of the group's tactical successes and ability to provide some level of protection to population.[41] Whether this "support" came by virtue of the LTTE being the only player left on the field or true belief in the group's goals, ultimately it does not seem to be a factor in explaining the group's expansion to India.

What more likely explains the expansion of LTTE's terrorist attacks into India is the introduction of Indian peacekeeping forces into Sri Lanka in July 1987 under the leadership of Indian Prime Minister Rajiv Ghandi. These troops, known as the Indian Peace Keeping Force (IPKF), entered Sri Lanka as part of an effort to reduce the violence between the Tamil minority and the Sri Lankan government following the conclusion of the Indo-Sri Lankan Accord. The reasons for the IPKF's deployment are many, but here it is sufficient to highlight the intended purpose of disarming Tamil militants and ensuring the separation of the warring sides. Soon after its arrival, however, the IPKF found itself targeted by an LTTE that had not been fully supportive of the accords and that felt the IPKF either never had or had lost its impartiality.[42] Violence between the IPKF and the LTTE escalated, and eventually the IPKF withdrew in 1990.[43]

There is dispute over whether the LTTE ever really supported the peace agreement and introduction of the IPKF. Regardless, it is clear that the LTTE came very quickly to view the IPKF as ineffective, biased, and ultimately a roadblock to the LTTE's objectives. It is perhaps not surprising, then, that part of the LTTE's operational expansion included deploying a suicide bomber to assassinate former Prime Minister Rajiv Gandhi at a campaign event in southeastern India in May 1991.[44] One scholar observed that the LTTE's feelings for India and Ghandi were shown most comprehensively in a propaganda publication called *The Satanic Force*, which highlighted what the group saw as the shortcomings of the IPKF.[45]

In the end, it seems that the best explanation for the regional expansion of the LTTE's attack profile is the implementation of counterterrorism/counterinsurgency efforts of the IPKF. Regardless of their legitimacy or shortcomings, the LTTE and its leadership clearly saw India generally, and Gandhi specifically, as an adversary for which a greater response was merited. The decision to expand appears to have been taken, not because the LTTE's ideology or worldview had changed in any substantive way, but rather because India's actions brought it into greater conflict with the LTTE. Hindsight prediction is far easier than in the moment prediction, but it does seem that there was escalating rhetoric on the part of LTTE regarding frustration and enmity toward Indian involvement in Sri Lanka that signaled a desire on the part of the LTTE to expand their operations.

Examining the case of the LTTE using the opportunity and willingness framework demonstrated that the willingness piece of the equation was critical for understanding expansion. Although more historical than current, one benefit of discussing the LTTE case is that there is a fair amount of information available in the public space given that the incidents described here occurred more nearly 30 years ago. A more relevant, but also more challenging, example in which this framework might be applied is the case of Islamic State Khorasan (ISK).

The Expansion of Islamic State Khorasan (ISK)

When the group known as the Islamic State declared itself the legitimate (at least in its own view) caliphate in June 2014, it also called for pledges of allegiance of individuals and groups from around the world.[46] Within short order, individuals and small parts of other groups around the world began to align themselves with the Islamic State. This included terror threat networks in Afghanistan and Pakistan. Although the Islamic State's central group did not immediately acknowledge an official branch of its group in the region following the initial pledges of allegiance, it did not take long for official recognition to come. In January 2015, the Islamic State's official spokesperson released an audio recording in which he formalized the establishment of a province in the Afghanistan-Pakistan region, known as Islamic State Khorasan,[f] or ISK.[47] Since that point, ISK has carried out a large number of operations, but according to the GTD, all of its initial operations were within the group's geographic home base of operations: Afghanistan and Pakistan.[48]

Pinpointing the exact moment that ISK expanded its operations is not straightforward. According to the GTD, a series of attacks connected to ISK outside of Afghanistan and Pakistan occurred in India in 2017.[g] Regardless of the specific timing or location, it is clear that the group began conducting operations outside of its home area on or around this time, with plots and attacks turning up in several locations over the next several years, including India, Iran, Maldives, Qatar, Tajikistan, and Uzbekistan. Activity in these particular locations, if conducted with centralized direction from the leadership of ISK or the central Islamic State core group, would qualify as expansion from local (Category 3) to regional (Category 6).

Not too long after these regional plots started to pick up, ISK was also implicated in carrying out attacks and plots in a number of countries outside of the regional sphere, including Austria, France, Germany, Turkey, and Russia.[49] In 2020, the Islamic State and possibly ISK may have been involved in the plot to bomb U.S. military bases in Germany.[50] Its largest attack during this phase, on March 22, 2024, against the Crocus City Hall in Moscow, killed nearly 150 people and wounded 551.[51] This attack, which demonstrated that ISK could carry out attacks far from its home base with high levels of coordination, was an example of global expansion (Category 9).

While the LTTE's expansion from one country to the next was easier to understand, ISK's expansion to a wide array of both regional and global targets is a bit more complicated. One approach would be to offer a nuanced analysis of each new country of expansion. While there may be similar factors in the opportunity/willingness framework that help explain the group's decision to carry out attacks in each of these countries, there are also likely some differences. Another approach, implemented here, is to discuss more generally about how the opportunity/willingness framework might be useful in explaining the overall phenomenon of expansion as it applies to ISK.

[f] The term Khorasan means "rising sun" and refers to a historical region generally, though not exactly, in the same area as where ISK operates. Adrija Roychowdhury, "Why Islamic State in Afghanistan harks on the concept of Khorasan and what it means for India," *Indian Express*, September 25, 2021.

[g] Attribution for these individual events is challenging to say the least. Some of the attacks attributed to ISK appear to be attributed not because of a formal claim of responsibility, but at times on the word of "security sources." Other times, the attribution is based on the activity of an Indian cell with the name of "Khorasan," even though there is no indication that the actual ISK group had any involvement. "ISIS linked militant killed in Lucknow," LeadPakistan, March 9, 2017.

The GTD does include an earlier attack/plot attributed to ISK on October 1, 2016. However, that same attack/plot was also attributed to Maoists operating in the country. Ultimately, the author's own research led to a conclusion that the nature of the incident was more consistent with other Maoist operations.

Opportunity

On the opportunities side of the framework, the availability of human resources is always an important factor to consider. The Islamic State benefited from an international appeal that allowed it to attract individuals from a wide array of countries around the world, enabling expansion should the group so choose.[52] Although ISK's appeal is not as broad, several of the recent high-profile ISK attacks and plots have highlighted the presence of a number of individuals with Central Asian heritage, especially Tajikistan, including the attacks in Moscow and a recent investigation that resulted in the arrest of eight Tajiks in the United States.[53] Their presence in ISK attacks and plots makes sense, as some reporting has suggested that as many as half of ISK's members are from Tajikistan.[54] The presence of a large number of recruits from one country does not necessarily explain the expansionary push, but it does enable it in terms of manpower.

The fact that the eight Tajik men arrested in the United States had claimed asylum at the border highlights how ISK has potentially been exploiting the global migration crisis. Political instability, economic challenges, and conflict have forced many people to flee from their homes and seek refuge abroad. A 2024 UNHCR report showed that, in 2023, the number of people worldwide who had been forcibly displaced from their homes grew to 117.3 million, up from just under 60 million in 2014.[55] The number of asylum seekers grew from 1.2 million in 2014 to 6.9 million in 2023.[56] To be very clear, the point is not that asylum seekers and refugees are all potential terrorists. Rather, it is that terrorist organizations can take advantage of the flow of humans as an opportunity to move operatives, should they so desire.[h] After the ISK attack on Moscow, at least one analyst encouraged greater concern regarding the migrant flows from Tajikistan into Russia.[57] And, in addition to the eight men arrested at the U.S. border in 2024 mentioned above, an earlier plot in Germany in 2020 also highlighted the way in which the Islamic State (and possibly ISK) might have exploited human migration flows.[58]

Another point that is clearly an opportunity factor in the ISK case that did not exist for the LTTE in the early 1990s is the prevalence of easy to use, secure, widely available communications technologies that enable groups to coordinate much more easily with operatives in the field. A number of scholars have noted the existence of a multi-tiered structure used by a small number of groups, including ISK, to direct, guide, and inspire attacks from abroad.[59] These approaches, such as the failed effort of a Toronto man to carry out an attack on behalf of ISK, involve encrypted channels, online chat groups, and other similar venues.[60]

A related point is that technological advances have not only facilitated a greater ability of groups to communicate, but also to raise and transfer funds necessary to carry out attacks. Now, instead of relying on traditional bank transfers or the less formal *hawala* system, money can be sent to operatives abroad in order to carry out attacks. ISK, among other groups, has certainly taken advantage of various financial platforms for financing purposes.[61] Although there remains much uncertainty surrounding the Moscow attack, some information suggests that ISK used cryptocurrency to transfer money to the perpetrators.[62]

Finally, it is important to note that ISK's expansion of attacks in the past few years has coincided with a decreased amount of counterterrorism pressure against the group.[63] Not only did U.S. and other international troops withdraw from Afghanistan in August 2021, but many critical intelligence resources that accompanied them diminished as well.[64] In place of resources on the ground, U.S. security and intelligence officials have articulated an ability to transition to an "over-the-horizon" counterterrorism capability.[65] However, this capability has some notable challenges that have only increased in scrutiny.[66] According to U.S. Central Command Commander General Michael Kurilla, "lack of sustained pressure allowed ISIS-K to regenerate and harden their networks."[67]

Not only did a reduction in U.S. pressure in Afghanistan potentially increase the opportunity of ISK, but it appears that so too did a lack of counterterrorism capability (or, at the least, a perception of such) among some of the nations that were ultimately targeted by ISK. In the case of the attacks against both Iran and Russia in 2024, it was later revealed that U.S. intelligence had previously warned both countries of potential ISK attacks, but that those warnings were not effectively acted upon.[68]

When it comes to opportunity, the above discussion does seem to indicate that there has been sufficient opportunity for ISK to expand. And although that opportunity appears to have increased after the U.S. withdrawal in 2021, there were certainly indicators of increasing opportunity prior to that point.

Willingness

Shifting to an analysis of the willingness side of the framework, there are several contributing factors. First, the Islamic State itself has an expansionary ideology, both in terms of geography and the need to attack adversaries who oppose it. In its propaganda, the group focused on painting the nations of the world as legitimate targets, not only for attacks but also for conquering.[69] As an affiliate of the parent organization, ISK has, on some level, the same worldview in its DNA.[70] Of course, it is important to understand that the group is not a monolith, and the impact of these forces can differ from time to time.[71] Nevertheless, there is nothing constraining external expansion of operations in the group's ideology. Absent this feature, ISK might be more like a more nationally focused group such as the Taliban.[72] But with a worldwide and expansionary ideology, theoretically the willingness of the group to strike abroad has existed from the beginning of the organization. Given that, it is hard to suggest that the increasing number of regional and global attacks can be attributed totally to ideology. Another way to think about it is that the ideology of ISK does contribute to its willingness to conduct an expansion, but it does not really help explain the timing of that expansion.

Another factor in the willingness part of the equation may be ISK's desire for payback, either for the oppression of Muslims around the world and/or the more targeted counter-Islamic State efforts of nations around the world. On this latter front in particular, there seem to be plenty of threats levied by the Islamic State and ISK against a wide range of enemies. The Global Coalition Against Daesh has 87 members, not to mention those outside of the coalition who have fought against the Islamic State. This makes assigning the reason for ISK's expansion on a desire for revenge against nations

[h] This is not a new phenomenon. Regular human flows have aided the movement of operatives previously. The September 11 hijackers used a combination of business, tourist, and even one student visa to enter the United States. Thomas R. Eldridge, Susan Ginsburg, Walter T. Hempel II, Janice L. Kephart, and Kelly Moore, *9/11 and Terrorist Travel* (Washington, D.C:. Staff Report of the National Commission on Terrorist Attacks Upon the United States, 2004).

that have fought against the group seem a bit unfulfilling, although it would also be hard to argue that participation in activities against the Islamic State (either in the past or currently) does not raise the risk to some degree.[73] Consider two examples from Moscow and Iran.

In the wake of the Moscow attack, Russia's history of abuses against Muslims in Chechnya and its support of the Assad regime in Syria were both mentioned in news reporting as potential reasons for ISK's focus on the country.[74] But, as early as 2015, Russia had also previously fallen into the crosshairs of the Islamic State (ISK's parent organization) because of its involvement in the Syrian civil war, with the downing of a Russian airline in the Sinai Peninsula and several small-scale inspired attacks in Russia.[75] More recently, ISK has gone after Russia in its propaganda because of Russia's support for the Taliban.[76] This rationale also likely played a role in a suicide bombing attack on the Russian embassy in Kabul in September 2022.[77] In the group's Voice of Khurasan publication issued in April 2023, one article attempted to redirect violence from the Russia-Ukraine conflict toward Russian troops fighting against Muslims around the world and in Russia.[78]

Iran's historical involvement in Syria led it to deploy military forces earlier in the Syrian conflict. That fact, combined with the Islamic State's hatred of Shi`a adherents, led to Iran being a target of Islamic State propaganda, with efforts being made by the group to offer Persian translations of its material.[79] It is not known exactly when the baton was passed from Islamic State core to ISK, but by late 2022, both the Islamic State and the Iranian government reported the involvement of Afghans, Azeris, Tajiks, and Uzbeks in attacks and plots, followed by the claim of an arrest of a key ISK leader in Iran in May 2024.[80] Then, in January 2024, after ISK attacked a funeral in Iran for Qassem Soleimani, largely seen as the architect of Iran's involvement in Syrian civil war, one rationale given by observers in the press was that the attack was retribution for the Soleimani's role in that campaign.[81] Given its consistent messaging and efforts, it seems clear that ISK had been increasingly targeting Iran for years in some part for that reason.

Although ISK's expansion of operations outside its normal operating territory pre-dates the U.S. withdrawal from Afghanistan in August 2021, there does seem to be a connection between its increased expansion of operations and the presence of a new ruler in the Taliban. Several scholars suggested that the group's willingness to expand operations may be due to ISK's desire to maintain relevance as it weathers the Taliban's efforts to destroy it.[82] It is worth noting that these efforts to destroy ISK have proven to be unsuccessful, even if there have been some successes by the Taliban.[83] Another suggestion is that ISK's willingness to expand may also reflect an effort to embarrass the Taliban by showing that it cannot prevent transnational attacks from emanating from Afghanistan.[84] In other words, regardless of whether the motivation to expand is due to one, or a combination, of these arguments, the Taliban in charge does seem to have provided some accelerant to the geographic expansion of ISK attacks.

This brief examination of some of the willingness factors has suggested that there were both longstanding and recently emerging forces at play when it comes to ISK's expansion. On one hand, the group's adherence to Islamic State ideology provided a broad set of potential targets and adversaries. On the other hand, the recent departure of the United States left ISK as one of the primary actors still in opposition to the Taliban, a fact which may have altered its strategic calculus. Given the recency of ISK's expansion, it may be the case that more information will emerge that helps provide a clearer picture of its expansion efforts and helps apportion the weight that should be given to each of these factors.

Conclusion

The purpose of this article was to provide a simple framework while exploring the rationales that might help explain why terrorist organizations expand the geographic scope of their attacks. In doing so, it posited that expansion requires a combination of both opportunity and willingness factors. These two factors are not linear, as, for example, a group may possess the desire but be hamstrung by a lack of adequate resources. It may also be the case that a well-funded, large terrorist organization does not expand because it has no motivation or reason to do so. Expansion is not inevitable or desired by all groups, which is part of what makes this line of inquiry important.

This article also applied the opportunity and willingness framework in the context of two cases: the LTTE and ISK. Neither of these two brief case studies in this article should be considered exhaustive in terms of the evidence or authoritative in capturing the reasons for expansion. However, the point remains that the opportunities/willingness framework can be useful for categorizing the factors leading to expansion after the fact, but may also prove useful for purposes of ex-ante analysis. As policymakers and practitioners seek to understand the threat environment, studying the factors that groups have in both the opportunity and willingness categories may potentially provide indicators and warnings, tripwires, and other useful information in understanding the expansion process.

Admittedly, this article has been a short treatment of a complicated subject, about which additional research can and should be conducted. Such research might profitably add more substance to the opportunity and willingness framework outlined above, teasing out the factors that matter as opposed to those that do not seem to matter. Another avenue for investigation would be to conduct additional case studies and even large-n quantitative work to explore the dynamics of expansion to a greater number of groups and scenarios. Finally, the timing of expansion remains a key area for investigation, and probably one of the most difficult to pin down. Even if the opportunity and willingness factors matter, *when* they reach a critical boiling point is a key issue for policymakers and practitioners alike. Answering this question with specificity will likely require in-depth examination of primary sources that provide greater light on the internal decision-making processes of these groups.

Finally, this framework also has implications for the counterterrorism efforts that countries may seek to conduct. While reducing some of the contributing factors that lead to opportunity or willingness is not necessarily an incorrect approach, even the brief case studies above highlighted how multiple opportunity and willingness factors interacted and, in some cases, overlapped to create conditions that were fully ripe for expansion. Counterterrorism efforts should take note of this and be careful about designing a successful policy based on one factor alone. Although additional research is needed to assess how the opportunity and willingness approach fares when it comes to counterterrorism, there is reason to suggest that a more holistic policy will be more effective than a limited one. CTC

Citations

1 "Eight Years After 9/11: Confronting the Terrorist Threat to the Homeland," U.S. Senate Committee on Homeland Security and Governmental Affairs, September 30, 2009; "Violent Islamic Extremism: Al-Shabaab Recruitment in America," U.S. Senate Committee on Homeland Security and Governmental Affairs, March 11, 2009.

2 "Al-Shabaab: How Great a Threat?" U.S. House of Representative Committee on Foreign Affairs, October 3, 2013.

3 Faith Karimi, Ashley Fantz, and Catherine E. Shoichet, "Al-Shabaab threatens malls, including some in U.S.; FBI downplays threat," CNN, February 21, 2015.

4 "Camp Simba: Three Americans killed in Kenya base," BBC, January 5, 2020.

5 "Kenyan National Indicted for Conspiring to Hijack Aircraft on Behalf of the Al Qaeda-Affiliated Terrorist Organization Al Shabaab," U.S. Department of Justice, December 16, 2020; Benjamin Weiser, "Kenyan Planned 9/11-Style Attack After Training as Pilot, U.S. Says," *New York Times*, December 16, 2020; Tara Suter, "Man convicted in 9/11-style plot to kill Americans," Hill, November 5, 2024.

6 Graham Allison and Michael J. Morrell, "The Terrorism Warning Lights Are Blinking Red Again," *Foreign Affairs*, June 10, 2024; Catrina Doxsee and Lauren Adler, "Asked and Answered: Global Terrorism Threat Assessment 2024," CSIS, February 9, 2024.

7 "Germany: Islamist terror poses 'persistently high' risk," Deutsche Welle, August 12, 2024; Mike Corder, "The Dutch counterterror agency has raised the national threat alert to the second-highest level," Associated Press, December 12, 2023.

8 Luis R. Martinez, "Transnational insurgents: Evidence from Colombia's FARC at the border with Chávez's Venezuela," *Journal of Development Economics* 126 (2017): pp. 138-153; Rohan Gunaratna and Anders Nielsen, "Al Qaeda in the Tribal Areas of Pakistan and Beyond," *Studies in Conflict & Terrorism* 31:9 (2008): pp. 775-807.

9 Matthew Levitt, "Hezbollah's Procurement Channels: Leveraging Criminal Networks and Partnering with Iran," *CTC Sentinel* 12:3 (2019): pp. 1-9.

10 David Charns, "Las Vegas teenager plotted ISIS-inspired terror attack, built bombs in room: documents," 8 News Now, August 20, 2024.

11 "Somalia: UN official reports on electoral progress, ongoing security challenges," United Nations, October 3, 2024.

12 Guy Van Vlierden, "Profile: Paris Attack Ringleader Abdelhamid Abaaoud," *CTC Sentinel* 8:11 (2015): pp. 30-33.

13 Fernando Reinares and Carola Garcia-Calvo, "'Spaniards, You Are Going to Suffer:' The Inside Story of the August 2017 Attacks in Barcelona and Cambrils," *CTC Sentinel* 11:1 (2018): pp. 1-11.

14 Tim Lister, Ray Sanchez, Mark Bixler, Sean O'Key, Michael Hogenmiller, and Mohammad Tawfeeq, "ISIS goes global: 143 attacks in 29 countries have killed 2,043," CNN, February 12, 2018.

15 Harvey Starr, "'Opportunity' and 'willingness' as ordering concepts in the study of war," *International Interactions* 4:4 (1978): pp. 363-387.

16 Jacob N. Shapiro, "Terrorist Decision-Making: Insights from Economics and Political Science," *Perspectives on Terrorism* 6:4-5 (2012): pp. 5-20.

17 Gabriel Koehler-Derrick and Daniel Milton, "Choose Your Weapon: The Impact of Strategic Considerations and Resource Constraints on Terrorist Group Weapon Selection," *Terrorism and Political Violence* 31:5 (2019): pp. 909-928; Tin Kapetanovic, Mark Dechesne, and Joanne P. Van der Leun, "Transplantation theory in terrorism: an exploratory analysis of organised crime and terrorist group expansion," *Global Crime* 25:1 (2024): pp. 1-25.

18 Angela Dalton and Victor Asal, "Is It Ideology or Desperation: Why Do Organizations Deploy Women in Violent Terrorist Attacks?" *Studies in Conflict & Terrorism* 34:10 (2011): pp. 802-819.

19 Victor Asal, Justin Conrad, and Peter White, "Going Abroad: Transnational Solicitation and Contention by Ethnopolitical Organizations," *International Organization* 68:4 (2014): pp. 945-978.

20 Elizabeth G. Arsenault and Tricia Bacon, "Disaggregating and Defeating Terrorist Safe Havens," *Studies in Conflict & Terrorism* 38:2 (2015): pp. 85-112.

21 Koehler-Derrick and Milton.

22 Andrew Silke and Anastasia Filippidou, "What drives terrorist innovation? Lessons from Black September and Munich 1972," *Security Journal* 33 (2020): pp. 210-227; Victor Asal and Aaron M. Hoffman, "Media effects: Do terrorist organizations launch foreign attacks in response to levels of press freedom or press attention?" *Conflict Management and Peace Science* 33:4 (2016): pp. 381-399; Gabriel Weimann, "When the theatre of terror emerged," *Israel Affairs* 28:4 (2022): pp. 553-572.

23 Asal, Conrad, and White.

24 Kapetanovic, Dechesne, and Leun.

25 Asal, Conrad, and White.

26 John Hudson, "Gaza war a recruiting boon for terrorists, U.S. intelligence shows," *Washington Post*, July 5, 2024.

27 Catherine Herridge and Nicole Sganga, "Intel bulletin says terror groups are calling on supporters to target U.S., Israeli interests amid Israel-Hamas conflict," CBS News, October 18, 2023; Mark Berlin, Sara Harmouch, and Vladimir Rauta, "The Extremist Domino Effect of October 7," Irregular Warfare Initiative, November 14, 2023; Ilana Winter, "Islamic State's Response to October 7," Washington Institute for Near East Policy, February 9, 2024.

28 Brian Michael Jenkins, "The Israel-Hamas War Has Upended the Terrorist Threat Matrix," RAND Corporation Commentary, November 22, 2023.

29 W. Alejandro Sanchez Nieto, "A war of attrition: Sri Lanka and the Tamil Tigers," *Small Wars & Insurgencies* 19:4 (2008): pp. 573-587.

30 Sameer P. Lawani, "Size Still Matters: Explaining Sri Lanka's Counterinsurgency Victory over the Tamil Tigers," *Small Wars & Insurgencies* 28:1 (2017): pp. 119-165.

31 The GTD is a publicly searchable database containing terrorist attacks from 1970-2020. See https://www.start.umd.edu/gtd

32 Sarah Wayland, "Ethnonationalist networks and transnational opportunities: the Sri Lankan Tamil diaspora," *Review of International Studies* 30 (2004): pp. 405-426.

33 Robert N. Kearney, "Sri Lanka in 1984: The Politics of Communal Violence," *Asian Survey* 25:2 (1985): pp. 257-263; Rone Tempest, "Rebels Shift Targets as Sri Lanka Military Shapes Up," *Los Angeles Times*, April 18, 1987; Marshall R. Singer, "New Realities in Sri Lankan Politics," *Asian Survey* 30:4 (1990): pp. 409-425.

34 Rohan Gunaratna, "Internationalisation of the Tamil conflict (and its implications)," *South Asia: Journal of South Asian Studies* 20:1 (1997): pp. 119-152; Giacomo Mantovan, "Becoming a Fearless Tiger: The Social Conditions for the Production of LTTE Fighters," *Conflict and Society* 9:1 (2023): pp. 37-54.

35 Daniel Byman and Sarah E. Kreps, "Agents of Destruction? Applying Principal-Agent Analysis to State-Sponsored Terrorism," *International Studies Perspectives* 11:1 (2010): pp. 1-18.

36 Ravinatha Aryasinha, "Terrorism, the LTTE and the conflict in Sri Lanka," *Conflict, Security & Development* 1:2 (2001): pp. 25-50.

37 Cécile Van de Voorde, "Sri Lankan Terrorism: Assessing and Responding to the Threat of the Liberation Tigers of Tamil Eelam (LTTE)," *Police Practice and Research: An International Journal* 6:2 (2005): pp. 181-199.

38 Wayland; Peter Chalk, "The Tigers Abroad: How the LTTE Diaspora Supports the Conflict in Sri Lanka," *Georgetown Journal of International Affairs* 9:2 (2008): pp. 97-104.

39 "The history of the Tamil Tigers," Al Jazeera, April 28, 2009.

40 Van de Voorde.

41 Kate Cronin-Furman and Mario Arulthas, "How the Tigers Got Their Stripes: A Case Study of the LTTE's Rise to Power," *Studies in Conflict & Terrorism* 47:9 (2024): pp. 1,006-1,025.

42 Kumar Rupesinghe, "Ethnic Conflicts in South Asia: The Case of Sri Lanka and the Indian Peace-Keeping Force (IPKF)," *Journal of Peace Research* 25:4 (1988): pp. 337-350; Alan Bullion, "The Indian peace- keeping force in Sri Lanka," *International Peacekeeping* 1:2 (1994): pp. 148-159.

43 Eric Ouellet, "Institutional Analysis of Counterinsurgency: the Case of the IPKF in Sri Lanka (1987–1990)," *Defence Studies* 11:3 (2011): pp. 470-496.

44 Manoj Joshi, "On Razor's Edge: The Liberation Tigers of Tamil Eelam," *Studies in Conflict & Terrorism* 19:1 (1996): pp. 19-42.

45 Michael Roberts, "Killing Rajiv Gandhi: Dhanu's sacrificial metamorphosis in death," *South Asian History and Culture* 1:1 (2009): pp. 25-41.

46 Daniel Milton and Muhammad al-`Ubaydi, "Pledging Bay`a: A Benefit or Burden to the Islamic State?" *CTC Sentinel* 8:3 (2015): pp. 1-7.

47 Catrina Doxsee, Jared Thompson, and Grace Hwang, "Examining Extremism: Islamic State Khorasan Province (ISKP)," *Center for Strategic & International Studies,* September 8, 2021; Amira Jadoon, Abdul Sayed, and Andrew Mines, "The Islamic State Threat in Taliban Afghanistan: Tracing the Resurgence of Islamic State Khorasan," *CTC Sentinel* 15:1 (2022): pp. 33-45.

48 See https://www.start.umd.edu/gtd

49 Aaron Zelin, "ISKP Goes Global: External Operations from Afghanistan," Washington Institute for Near East Policy*,* September 11, 2023; Amira Jadoon, Abdul Sayed, Lucas Webber, and Riccardo Valle, "From Tajikistan to

Moscow and Iran: Mapping the Local and Transnational Threat of Islamic State Khorasan," *CTC Sentinel* 17:5 (2024): pp. 1-12.

[50] Nodirbek Soliev, "The April 2020 Islamic State Terror Plot Against U.S. and NATO Military Bases in Germany: The Tajik Connection," *CTC Sentinel* 14:1 (2021): pp. 30-40.

[51] Andrew Roth and Pjotr Sauer, "Four suspects in Moscow concert hall terror attack appear in court," *Guardian*, March 24, 2024; "Number of those injured in Moscow terrorist attack revised upward to 551," TASS, March 30, 2024; "Russia says Islamic State behind deadly Moscow concert hall attack," France 24, May 24, 2024.

[52] The geographic and human diversity of this appeal was highlighted in primary source documents leaked about the inflow of foreign fighters to the group. 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).

[53] Adam Goldman, Eric Schmitt, and Hamed Aleaziz, "The Southern Border, Terrorism Fears and the Arrests of 8 Tajik Men," *New York Times*, June 25, 2024.

[54] Neil MacFarquhar and Eric Schmitt, "An ISIS Terror Group Draws Half Its Recruits From Tiny Tajikistan," *New York Times*, April 18, 2024.

[55] UNHCR, *Global Trends: Force Displacement in 2023* (New York: United Nations, 2024).

[56] Ibid. UNHCR, *UNHCR Mid-Year Trends 2014* (New York: United Nations, 2014).

[57] Marlene Laruelle, "A New Recruiting Ground for ISIS: Why Jihadism Is Thriving in Tajikistan," *Foreign Affairs*, May 14, 2024.

[58] Soliev.

[59] Daveed Gartenstein-Ross and Madeleine Blackman, "ISIL's Virtual Planners: A Critical Terrorist Innovation," War on the Rocks, January 4, 2017.

[60] Allan Woods, "The return of ISIS: How a Toronto case fits into the global resurgence of a terror group we thought had been defeated," *Toronto Star*, September 15, 2024.

[61] Animesh Roul, "The Rise of Monero: ISKP's Preferred Cryptocurrency for Terror Financing," GNET Insights, October 4, 2024.

[62] Jessica Davis, "The Financial Future of the Islamic State," *CTC Sentinel* 17:7 (2024): pp. 32-37; Roul. Stronger allegations of this connection have been made by Russian officials, but the veracity of these stronger claims is unclear.

[63] Jadoon, Sayed, Webber, and Valle.

[64] Tore Hamming and Colin P. Clarke, "Over-the-Horizon Is Far Below Standard," *Foreign Policy*, January 2, 2022; Meghann Myers, "Post-withdrawal, no 'over-the-horizon' strikes in Afghanistan," *Military Times*, May 12, 2023.

[65] David Vergun, "U.S. to Maintain Robust Over-the-Horizon Capability for Afghanistan if Needed," DOD News, July 6, 2021.

[66] Asfandyar Mir, "Commentary: No Good Choices: The Counterterrorism Dilemmas in Afghanistan and Pakistan," *CTC Sentinel* 16:10 (2023): pp. 40-55; R. Kim Cragin, "The Elusive Promise of 'Over-the-Horizon' Counterterrorism," *Studies in Conflict and Terrorism* (online), 2024.

[67] "Commander of U.S. Central Command General Michael Kurilla, Testimony before the U.S. Senate Armed Services Committee," March 7, 2024; Katherine Brucker, "On the Terrorist Attack at the Crocus City Hall in Moscow," U.S. Mission to the Organization for Security and Co-operation in Europe, April 11, 2024.

[68] Natasha Bertrand, "US secretly warned Iran before ISIS terror attack," CNN, January 25, 2024; Aamer Madhani, "US warned Iran that ISIS-K was preparing attack ahead of deadly Kerman blasts, a US official says," Associated Press, January 25, 2024; Shane Harris, "U.S. told Russia that Crocus City Hall was possible target of attack," *Washington Post*, April 2, 2024.

[69] Muhammad al-`Ubaydi, Nelly Lahoud, Daniel Milton, and Bryan Price, *The Group That Calls Itself a State: Understanding the Evolution and Challenges of the Islamic State* (West Point, NY: Combating Terrorism Center, 2014); Haroro J. Ingram, "An analysis of Islamic State's Dabiq magazine," *Australian Journal of Political Science* 51:3 (2016): pp. 458-477.

[70] Amira Jadoon, Nakissa Jahanbani, and Charmaine Willis, "Challenging the ISK Brand in Afghanistan-Pakistan: Rivalries and Divided Loyalties," *CTC Sentinel* 11:4 (2018): 23-29.

[71] Amira Jadoon, *Allied & Lethal: Islamic State Khorasan's Network and Organizational Capacity in Afghanistan and Pakistan* (West Point, NY: Combating Terrorism Center, 2018).

[72] Ayesha Sikandar, "Assessing ISKP's Expansion in Pakistan," South Asian Voices, September 25, 2023.

[73] See https://theglobalcoalition.org/en/

[74] Kevin Doyle, "Moscow concert hall attack: Why is ISIL targeting Russia?" Al Jazeera, March 23, 2024.

[75] Brian Glyn Williams and Robert Souza, "The Consequences of Russia's 'Counterterrorism' Campaign in Syria," *CTC Sentinel* 9:11 (2016): pp. 23-30.

[76] Lucas Webber, "The Islamic State's Anti-Russia Propaganda Campaign and Criticism of Taliban-Russian Relations," *Terrorism Monitor* 20:1 (2022): pp. 7-10.

[77] Christina Goldbaum, "Suicide Attack Hits Russian Embassy in Afghanistan, Killing 2 Employees," *New York Times*, September 5, 2022.

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

[79] Golnaz Esfandiari, "IS Propaganda Increasingly Targeting Iran And Its Sunnis," Radio Free Europe, June 6, 2017.

[80] These events were all referenced in Aaron Zelin's Islamic State activity tracker between 2022 and 2023. Aaron Y Zelin, *The Islamic State Activity Interactive Map*, Washington Institute for Near East Policy, accessed October 10, 2024. See "Attack on Shia Shrine in Shiraz, Iran," "Ten Arrested for Attack on Shah Cheragh Shrine in Shiraz, Iran," "Two Islamic State Cells Arrested in Iran," and "Leader of Khurasan 'Province' Operational and Media Network Arrested in Fars, Iran."

[81] Leila Fadel and Peter Kenyon, "An Afghan branch of ISIS claims responsibility for a deadly attack in Iran," NPR, January 5, 2024.

[82] Abdul Sayed and Tore Refslund Hamming, "The Growing Threat of the Islamic State in Afghanistan and South Asia," *Special Report: United States Institute of Peace* 520 (2023): pp. 1-28; Haroro J. Ingram and Andrew Mines, "From Expeditionary to Inspired: Situating External Operations within the Islamic State's Insurgency Method," ICCT Analysis, November 23, 2023.

[83] Jadoon, Sayed, Webber, and Valle.

[84] Sayed and Hamming.

Feature Commentary: Organizing for Innovation: Lessons from Digital Counterterrorism

By Brian Fishman

Digital platforms were slow to build robust teams to counter threat actors, but today, many of those corporate teams have robust processes, specialized tools, and innovative approaches to countering highly adaptive adversaries. They operate in a tremendously dynamic environment where their adversaries can innovate at low cost, primarily because of the nature of the digital "terrain" where the conflict occurs. And while the actions these teams take are not kinetic, as those sometimes utilized in geopolitical conflict, the cat-and-mouse game between Trust & Safety teams and threat actors online suggests lessons that are increasingly relevant to the national security community. This article explores five factors that were key to facilitating innovation in Facebook's approach to countering the Islamic State—and that I argue are more generalizable. They are: people, organization, legitimacy, tools, and collaboration. It also identifies lessons that can be learned from that experience. For example, we did not prioritize using a particular technology or focus experimentation in some bespoke "innovation center." Rather, we succeeded because we were made responsible for a critical mission, were unencumbered by past process, and had the right team structured to reduce external dependencies for innovation. Basic technological innovation can occur in an ivory tower, but applied innovation requires proximity to real-world missions. You cannot expect dramatic innovation without failure and iteration in an environment of real responsibility. Fundamentally, that means that innovation requires accepting risk. The structures and incentives of Silicon Valley cannot and should not simply be grafted on to our national security infrastructure. The rewards and costs of failure are different. But military organizations should shoulder the risks associated with innovation and study the lessons of corollary efforts in Silicon Valley and the private sector more broadly.

Over the past 30 years, technology companies built the modern internet—and with it a slew of new methods for communication and commerce. In doing so, they also inadvertently constructed new digital terrain for threat actors to exploit. In order to safeguard the communities and commerce that emerged online, and under significant pressure from governments and civil society, these companies belatedly built mechanisms to identify, disrupt, and deter those threat actors. Collectively, those activities are a key element of what professionals call Trust & Safety.[a] Trust & Safety is a practice of adversarial adaptation mediated by technology that often results in punitive action. And while the actions taken by Trust & Safety teams are not kinetic, the technology, organization, and centrality of technological adaptation necessary for Trust & Safety offers lessons for military leaders now and in the future.

The fundamentally adversarial nature of Trust & Safety drives innovation by attackers and defenders. When I arrived to lead Facebook's efforts against the Islamic State in the spring of 2016, the prevailing instinct among engineers was to build AI-driven classifiers to find content supporting the group. But I understood how the Islamic State's propaganda operation functioned, both on and off Facebook. There was a more straightforward, intelligence-driven way to disrupt the group's formal propaganda operation, which was our initial goal. So, we used vendors to collect emerging Islamic State propaganda on Telegram; established pipelines to triage, label, and hash it quickly; and then were able to detect that propaganda as soon as it was uploaded to a Facebook server.[b] I asked for entirely new ways to measure operational success—built around time rather than scale—and eventually, we regularly ran that process more quickly than Islamic State supporters could upload the first instance of a piece of propaganda to Facebook.

This was a good, creative win, but it was also only a single blow in a much longer cat-and-mouse game. Predictably, the Islamic State

[a] The Digital Trust & Safety Partnership defines Trust & Safety, broadly, as: "The field and practices employed by digital services to manage content- and conduct related risks to users and others, mitigate online or other forms of technology facilitated abuse, advocate for user rights, and protect brand safety." "Trust & Safety Glossary of Terms," Digital Trust & Safety Partnership, July 2023.

[b] A perceptual hash is a method to convert a file into a series of numbers. This digital fingerprint can then be algorithmically compared to other such fingerprints to identify media that is similar. Hash-matching is a common method to identify to child sexual abuse material (CSAM), terrorist propaganda, and non-consensual intimate imagery (NCII).

Brian Fishman is a co-founder of Cinder, which builds an orchestration platform for Responsible AI and Trust & Safety. He previously led Facebook's work to counter terrorism, hate groups, and large-scale criminal organizations. Prior to Facebook, Fishman served as the director of research at the Combating Terrorism Center at West Point; ran Palantir Technologies' disaster relief program; worked in-house at New America, a think-tank; and worked on Capitol Hill. Fishman authored The Master Plan: ISIS: al-Qaeda, and the Jihadi Strategy for Final Victory *(Yale University Press), which was built on a pathbreaking course he taught at West Point in 2008 about the Islamic State's plan to govern.*

innovated: by speeding up their process, editing core material to confound detection tools, and eventually operating on Facebook in more informal ways. The lesson is neither that AI classifiers are too clunky (they are, in fact, very useful) nor that lower-tech solutions produce partial victories. Rather, it is that technology must fit the mission and that every victory is fleeting against innovative opponents, especially online where the cost of iterating is low.

So, how do you build systems able to innovate and integrate technology into complex, adversarial missions so that you can strike not just one blow but an entire campaign? In my experience, five factors stand out: people, organization, legitimacy, tools, and collaboration. In short, successful innovation requires the right people, which are sometimes atypical for your organization; the right organizational structures and disposition; mechanisms and leadership to establish and maintain the legitimacy of new processes; technical tools designed for flexibility, innovation, and impact (not point solutions or flashy demos); and a commitment to use technology to improve collaboration across organizations and sectors.

Before exploring those five factors in depth, this article briefly describes the history of Trust & Safety and notes unique features of this sort of digital contestation. The purpose of the article is to suggest mechanisms to enable technological innovation, but, perhaps counterintuitively, most of the recommendations regard traditional issues of personnel, organization, and leadership. That is because applied innovation is more a matter of adapting workflows to capitalize on emergent technology more than it is advancing raw science or operating on the bleeding edge of what can be achieved with physics or biology. Applied innovation requires openness to cutting edge technology, but fundamentally, it is about matching technology and organization to the mission—and preventing legacy processes from getting in the way.

Background & Key Concepts

Trust & Safety has a longer history than generally understood and some key features that shape how the competition between threat actors and Trust & Safety professionals plays out.

History of Trust & Safety

Trust & Safety efforts began in earnest in the late 1990s when companies such as eBay organized to counter fraud, counterfeits, and other disruptions to their digital marketplace.[1] Social media companies like Facebook and YouTube were slow to develop robust Trust & Safety teams, but have since built some of the most sophisticated operations for building and implementing private policy anywhere in the world.[c]

At the significant risk of oversimplification, Trust & Safety practices can be bucketed into two intertwined categories: community management and threat disruption. Community management governs how people engage each other on a platform, so the rules vary from one site to another. For example, a platform built for discourse might allow more contentious political speech or sexualized content. Conversely, a site for buying and selling vintage T-shirts might decide it is not the place for such content. In both cases, community management generally requires delineating rules, communicating them to users, and aiming to correct bad behavior before taking irrevocable enforcement actions.

"Platforms shape the digital terrain itself, not just the countermeasures they use against threat actors. This is a powerful, but limited, advantage."

Threat disruption is different. It is focused on identifying and disrupting actors engaged in deeply problematic behavior, sometimes offline: terrorists, child predators, organized criminal networks, and nation-states. Most platforms have policies that prohibit these actors, but many lack the resources to enforce them aggressively, which requires defining, identifying, investigating, acting against, and then defending against their shifting tactics. These actors are often the worst of the worst, but they are also less common. So threat disruption requires finding needles and networks in immense haystacks of data.

Scale, Terrain, Account Regeneration, and the Villain Use Case

The conflict between threat actors and Trust & Safety professionals has some unique features. The first is scale. A large-scale Trust & Safety operation makes millions of decisions daily about individual pieces of content and accounts. In Q2 2024, Meta removed 7.5 million pieces of content just for violating its rules around terrorism.[2] This means that both human and automated systems must be built to process very large amounts of information and that even a low error rate, whether false positives or false negatives, can result in a large number of bad decisions. In a highly scrutinized space, those errors can draw regulatory pressure and alienate users.

It is tempting to conclude that the scale and sensitivity of these choices creates a simple operational tradeoff: the scale of these decisions requires automation, but their sensitivity demands the thoughtfulness of human decisions. That tradeoff does exist, but the basic version is over-simplified. The reality is that human decision-making at scale is extremely error-prone. Even before the current explosion of AI tools, AI systems at Facebook (and other methods of automation) were regularly as accurate as human beings at many Trust & Safety tasks. But they could also be expensive to train and made mistakes that were stranger and more inexplicable than those made by humans. It is not just the scale of the mistakes AI and automation can make; it is the nature of those mistakes that can make them more problematic, even unacceptable. Nonetheless, it is important not to assume that humans do all jobs more accurately (in aggregate) than AI and automation more generally.

The second feature of the conflict between threat actors and Trust & Safety professionals is that the platforms shape the digital terrain itself, not just the countermeasures they use against threat actors. This is a powerful, but limited, advantage. Platforms build the algorithms that surface content, determine how easy it is to find new accounts to engage, and decide how much privacy to build into a digital system. Trust & Safety teams often advise on these systems to highlight potential risks. But just as the walls of a medieval city might be constructed both for security and to enable

[c] While this discussion primarily draws on lessons from the largest and most sophisticated Trust & Safety efforts, it is important to note that smaller teams face related challenges and sometimes innovate extremely effectively as a result.

everyday life and commerce, digital platforms are not constructed solely, or even primarily, to hinder the behavior of threat actors. Platforms are often designed to allow likeminded people to find one another; buyers to find sellers; and a range of users to engage with various levels of privacy and broadcast functions. The ability to shape this terrain gives platforms a huge advantage—both in terms of designing for safety and in gathering intelligence. But that advantage is not fully utilized, even by well-meaning platforms, because the same systems exploited by threat actors are also used by productive users—creating both a commercial tension for platforms and one of general social utility.

The third feature of the threat actor versus Trust & Safety contest is that threat actors can regenerate capacity online, often at minimal cost. This means that threat actors can iterate and experiment tactically and operationally at a scale that is simply not feasible offline. If their accounts are removed, they can recreate them. If a particular content type is discovered, they can move to another. Sophisticated platforms can make this innovation less fruitful, but they cannot eliminate the process. Viewed from the perspective of Trust & Safety, the physical world can represent a safe haven for digital threat actors, even when their ultimate aim is harm in the real world.

The internet beyond the 'walls' of a particular platform also serves as a safe haven. Cross-platform collaboration against threat actors remains nascent. When Facebook disrupted Islamic State operations, its supporters could (and did) plot and plan on Telegram to circumvent those techniques. There are some cross-platform coordination efforts—addressing child sexual abuse material (CSAM), non-consensual intimate imagery (NCII), terrorism, and disinformation—but they are not systematic enough. At the same time, a platform's only ability to impact a threat actor in the offline world is to inform relevant law enforcement authorities. There are very impactful examples of this kind of collaboration working, but such mechanisms are limited given the global nature of the internet, law enforcement capacity, and the unreliability of law enforcement in some jurisdictions.

Finally, every digital tool is dual-use, even those developed to mitigate harm. Product managers sometimes imagine a 'hero use case,' which essentially reflects an ideal user that fully embraces a product to get the most out of its functions. But for every hero use case, there is a villain use case, whereby some actors use the same tool for harm. For example, early in my tenure at Facebook, user reports of terrorist material on the platform were erroneous more than 90 percent of the time. Some of these reports represented overzealous users with generally good intent, but others were deliberately reporting benign content as terrorism in the hope that Facebook would be more likely to remove it. Every technical system that creates capability also creates new attack surfaces.

People, Organization, Legitimacy, Tools, and Collaboration

There is no silver bullet to create innovative systems. But the five factors of people, legitimacy, organization, tools, and collaboration are critical.

People

The mission of Trust & Safety teams is ultimately to make a platform safe and thereby inviting for the majority of users. In that respect, it is deeply aligned with the commercial mission of most technology companies. But the process of highlighting risks, expelling some users, and embracing paranoia as a professional virtue is non-standard in generally optimistic Silicon Valley. Unsurprisingly, Trust & Safety attracts a mélange of professionals somewhat different than the Silicon Valley workforce as a whole—and one that is more focused on the risks of a platform rather than the potential benefits to the wider community.

"Highly process-driven organizations often resist innovation because individuals in them are rewarded for implementing that process rather than achieving mission-altering outcomes."

It is treacherous to synthesize complex personalities into typologies. Nonetheless, I like to think about three basic "personas" in Trust & Safety: 'tech do-gooders,' 'the ones who know,' and 'hunters.' Tech do-gooders believe in the general social value of technology and that to realize those benefits the risks and costs associated with technology must be mitigated. These folks often have engineering, product, or design skills and would have a place in tech companies even if they were not working on Trust & Safety. The-ones-who-know have seen first-hand the downsides of technological innovation. They often come from marginalized communities at-risk online and have linguistic, cultural, and lived experiences far more diverse than technology companies writ large. For example, Trust & Safety as a discipline has more women in leadership roles than tech generally, and Trust & Safety includes incredibly diverse groups of people that speak the languages and understand the cultures of global communities. Finally, there are the hunters. These are folks who relish the fight against bad actors. They often think of themselves as protectors. Many now come from law enforcement and intelligence communities and sought roles at tech companies because technology is now a key terrain for the threat actors they pursued elsewhere. Yet, the tech community has grown some of these people internally; they often grew up fighting spam and fraud.

All three of these personas are necessary for Trust & Safety to succeed. The tech do-gooders often understand technology best and can imagine ways to utilize cutting edge tools. The-ones-who-know understand how those new techniques will work and can apply them in various contexts. Although Trust & Safety tends to embrace diversity, these people are often the most junior members of a team. Nonetheless, they are often where the rubber meets the road and regularly are sources of the on-the-ground knowledge that is necessary to keep pace with adapting adversaries. Finally, the hunters have the experience and skillset to target the worst-of-the-worst actors. They think in terms of networks, organization, and the nodes that have an outsized impact. For innovation to work in an adversarial setting, all three personas are necessary, and that means that technology companies have to recruit people that do not fit their standard profile.

Organization

Highly process-driven organizations often resist innovation because individuals in them are rewarded for implementing that process rather than achieving mission-altering outcomes.

To incentivize innovation, organizations should limit process, reconsider personnel assessment, and embrace experimentation, despite the reality that it will inevitably lead to some failure. Crisis often enables such structures, but they can be implemented without crisis by leaders willing to accept the risks.

Many of these factors were present when I joined Facebook, and they contributed to an environment I was able to utilize effectively. The Islamic State was (belatedly) seen as a true crisis; we had a cross-functional team whose participants were unusually independent of their 'home' bureaucracies; and resources were plentiful. Finally, we had leadership clarity, meaning both that Facebook's most-senior executives supported the work and that I, as the operational leader—a relative outsider with subject matter expertise and the credentials to prove it (not the same things; both important)—had unusual credibility and leverage to try new things.

Innovation in conflict is difficult because the importance of the mission can lead to an ethos where failure is inconceivable and unacceptable. That notion is sometimes necessary, particularly at a tactical level. But failure and iteration are critical to applied technological innovation. Organizations, and the leaders that guide them, must facilitate experimentation and celebrate productive failure. If not, they will disincentivize the risk-taking that is necessary for new ideas, technologies, and procedures to emerge.

When I arrived at Facebook, the community management elements of the Trust & Safety effort were generally divided into three major bureaucratic components: policy, operations, and engineering. These teams worked together, but individuals within those verticals were accountable to their own leadership. Leaders of those teams sought unity, but that intent could break down because distinct organizational perspectives were codified not just in mission prioritization from leadership but in bespoke personnel assessment standards which were not turned primarily to the success of the cross-functional group.

The Dangerous Organizations and Individuals (DOI) team that built a renewed campaign against the Islamic State operated differently. For starters, it was extremely well-resourced, more than 300 people strong. Moreover, the DOI operations team had its own technical capacity—data scientists and engineers who could explore new ideas quickly and without cross-functional handwringing. Finally, the engineers seconded to work with this DOI cross-functional group were also 'graded' (especially early in my tenure) by their own organization based on the importance of the work rather than compared on narrow metrics, which was more standard within the engineering organization.

It was ultimately valuable to have technical capacity both embedded in the operations team and engineers seconded from the engineering team. The former allowed us to iterate quickly and test new ideas with minimal friction; the latter emphasized scalable process and quantitative success metrics. Notably, the traditional engineering teams were paid more and generally 'better' engineers. Their processes and products were generally more rigorous. But in an innovative, adversarial environment workable is better than perfect—and so the technical creativity of the operations engineers pointed the way toward solutions that could subsequently be scaled.

Legitimacy

Leadership is critical in an organization innovating with technology in an adversarial environment. Process-derived legitimacy is too slow and outcomes can take time, particularly when the adversaries adjust. Leadership is therefore critical, both at the strategic and operational level. The strategic leader must generate resources and space to break standard procedures, including over prosaic issues such as personnel assessment; and tolerate missteps and imperfection. The operational leader must generate clear priorities; insulate the operational team from inevitable bureaucratic politics; and ensure that operational wins can be translated into strategic ones. The art of the innovative operational leader is that they must direct the team when necessary and enable innovation to bubble up organically.

"Leadership is critical in an organization innovating with technology in an adversarial environment. Process-derived legitimacy is too slow and outcomes can take time, particularly when the adversaries adjust. Leadership is therefore critical, both at the strategic and operational level."

Sheryl Sandberg, then the chief operating officer of Facebook, created the strategic space for Facebook's campaign against the Islamic State, and I was the operational leader tasked with designing and executing it. Fairly or unfairly, my legitimacy as a *credentialed* expert on the Islamic State was critical. Before my arrival, Facebook already had analysts that understood the Islamic State; it had relevant linguistic and cultural expertise rivaling any intelligence agency; and it had tremendous engineers with more data than they knew what to do with. But my knowledge of the group coupled with credentials, ability to communicate at a senior leadership level, and willingness to accept personal responsibility and risk for new techniques was key to unlocking that latent capability.

Coalescing the cross-functional team to execute those plans was primarily my responsibility, but managing the complex bureaucracy of a major corporation is no small task. This only worked because my leadership coached me on how to engage Facebook's top-level decision makers. Moreover, they avoided the mistake of many leaders in a crisis-driven organization, which is to reward folks for reacting well to crises, but failing to reward people for preventing crises in the first place.

This set-up worked. In just over a year, Facebook went from finding almost zero Islamic State material proactively to identifying 99 percent of the terrorist material it removed via automated systems.[3]

Legitimacy is critical for generating innovation, but maintaining that legitimacy is more difficult than it appears. The reason is that innovation fundamentally requires failure. This ethos is built into the bones of Silicon Valley, where the "power law" of venture capital stipulates that most financial returns will be concentrated in a small percentage of startups. Others will break even, and many will fail completely. The "power law" means that even the people supposedly best at identifying innovative concepts and teams recognize that they will fail most of the time. They still win big because a single major success can outweigh numerous small failures. Such a pattern is not easily applicable to military affairs or geopolitical issues more generally. It is rare that occasional big victories compensate for repeated failures. Nonetheless, innovative military organizations must allow for mission-relevant experimentation if they are to produce a culture that enables groundbreaking ideas and innovation.

This will be extremely difficult to achieve. For strategic leaders, it will mean carefully selecting missions where higher-risk, higher-reward approaches can be tested. It also means adjusting communication patterns to prepare stakeholders for risk. Innovative operational leaders must communicate clearly with superiors about risks, and those superiors must not only accept, but champion, them. Combatant commands must communicate up the chain and political leaders in the executive and legislative branches ultimately need to bless experimentation. Publicizing experimentation is important as well. Failure costs money, time, and in some awful cases, lives. But failure is not always a scandal—if the risks are well-considered, the mission critical, and innovation necessary. Innovators should engage the media and related stakeholders early, educate them on the risks, and explain that adversarial shifts demand creative approaches that will inevitably be imperfect, especially initially.

Tools

The most visible manifestations of innovation are not necessarily the most important. Over and over again at Facebook, we identified internal tools that failed to provide accurate information, conflicted with other tools, or were built for static challenges, not dynamic ones. Innovation requires fast iteration and adaptation, and that means building core tooling capabilities that enable operational and tactical creativity. Innovation means expecting obsolescence from technologies and processes—so you should emphasize core technical platforms that are easily updated, extensible to a wide range of other technologies, and modular enough to facilitate process and technological dynamism.

In 2016, Facebook had some dynamic systems but not others. For example, Facebook had incredibly powerful tools to query immense datasets and map entities related to one another. These systems were relatively easy to use and accessible to many people in the company. That meant that frontline data scientists could query information and test hypotheses almost as quickly as I could generate them, which allowed us to quickly identify promising concepts to disrupt Islamic State activities. At the same, Facebook did not have good tools to visualize networks, enable non-technical subject matter experts to reliably fanout through them, or quickly construct new enforcement procedures. In some cases, it could be difficult to understand how or why a particular enforcement action had been taken - in part because there were multiple, sometimes conflicting systems for gathering that information. We had very powerful AI systems, but they took too long to retrain and deploy.

That meant that we could not always update actual enforcement systems as quickly as the Islamic State could adjust—and when we did, it was often by updating human-driven processes as opposed to technical ones, so we did not systematically capture data on their adversarial responses to our improved process. Those data limitations might have been damning in Facebook's traditionally metrics-driven decision processes, but the unique organizational and leadership structure of the DOI XFN meant that during key time periods we could adapt regardless.

Nonetheless, that was a poor substitute for having better, more dynamic systems to begin with. Improved basic tooling was critical to long-term innovation. Large bureaucracies cannot scale innovation forever based on the credibility of individual leaders. So, Facebook invested. Better mapping software powered network-level takedowns of terrorist material. Improved AI training meant classifiers could better keep up with current trends. Consolidating competing tools that sometimes produced divergent information reduced confusion and ensuing decision slowdowns.

Notably, most of this innovation was focused on capturing and understanding signals, rather than innovating the sort of actions we took against the Islamic State. Improving our own decision-making was more important than improving the precise actions we took against threat actors. (It is worth noting that other teams did innovate more in the actions they took against other threat actors, but this was less impactful in the DOI context.) The success was primarily tooling and innovation built to derive understanding from data, to drive decision-making, and to build components of operational systems that could be easily rearranged in response to changing operational and tactical demands.

Collaboration

Like other harmful actors that operate online, the Islamic State does not simply use one platform. It might coordinate internally on Rocket.chat, advertise propaganda on Telegram, recruit on Facebook, and store content on Dropbox. A single digital operation might span five or six platforms. As a result, improving Facebook's defenses has had a limited impact on the group as a whole and left key elements of its digital network intact. This means that, as in traditional geopolitical competition, coalitions are a key part of confronting harm online. These collaborative spaces are also a venue for technical innovation, but they pose unique challenges.

First, innovation is a full-time job. Time-bound efforts deployed in a 'hackathon'-style environment might generate new ideas, but they are unlikely to produce products that can be used over time. It is possible to build joint organizations with generic mandates to innovate, but the distance of such bodies from tactical realities will limit their understanding of the adversarial environment and reduce their urgency to innovate. Innovative joint (and combined) organizations must maintain staffing for an extended period. Seconded personnel should access tactical leaders from their home organizations to generate ideas and vet progress, but if those seconded personnel are not exempted from the typical personnel reviews of their home institutions, they will likely be less innovative.

Second, some coalition partners will represent best practices in any coalition and will likely have existing tools that can be appropriated for new purposes. At Facebook, I helped build the Global Internet Forum to Counter Terrorism (GIFCT), a coalition of tech companies dedicated to sharing tools and processes to counter terrorist activity online. One of GIFCT's core tools is a database of hashed terrorist propaganda. Participating companies upload hashes of terrorist material so that others may download them to identify that material on their own platform. This basic idea was originally used to counter child sexual abuse material (CSAM) and the technical platform used for GIFCT hash-sharing was originally built to share hashes of malware. But an enterprising engineer at Facebook recognized we could repurpose that tool (called Threat Exchange), and I was able to convince internal stakeholders and other companies to use it for a new purpose. Sometimes, technological innovation is simply recognizing that an existing tool can be used for a different mission. This may not energize engineers and those excited by using cutting edge technology, but this is particularly useful when the mission is elevating the baseline capability of a coalition.

Third, building innovative shared resources does not mean that coalition partners will use them. Facebook had the resources to integrate its internal tools for detecting media hashes to the GIFCT database. Facebook could both push and pull those hashes seamlessly. But many smaller companies did not have the resources to integrate with the shared database nor, perhaps, even the ability to store and match hashes on their own systems. Building shared tools is only valuable if less-capable partners can use them. It is no surprise that Meta has subsequently open-sourced a hashing protocol and is releasing an open-source system for maintaining internal hash databases on a platform's internal systems.[4] Innovative tools are meaningless unless they connect practically to the tools and systems needed to deploy them.

Conclusions

Adversarial innovation is dirty business. When the stakes are high, innovation is dangerous. The positive impact is rarely immediately clear, and it will produce new modes of error. Inaction is often less risky for individuals in a bureaucracy but poses more dangers to a long-term mission against an adaptive adversary. There is no greater lesson from Trust & Safety than that cycles of adversarial adaptation occur faster today than ever before.

Based on my experience in Trust & Safety, Commands should consider a variety of practical steps to enhance innovation:

Expect obsolescence. Innovation in an adversarial setting is never done. Expect that every process, technology, and framework will become outdated. Iteration and innovation happen incredibly quickly online because the cost of failure for attackers is low. But this dynamic exists elsewhere, and it is accelerating in many areas of military conflict. The cost of experimenting with new drone techniques is lower than with manned aircraft. Electronic warfare systems can be deployed, deprecated, and updated quickly by a determined adversary.

Hire unusual talent. Talent is destiny in technology. Find the introverts, the folks with blue hair, the ones who can rebuild an engine from scrap, and the people who are skeptical of working with the government. Show them that the mission matters and set them loose. Many of these people will not live in Tampa. Build Centers of Excellence in New York, Los Angeles, and San Francisco. That's hard for the government, but that is not an excuse. It is also hard in the private sector. OpenAI originally wanted all hires in its San Francisco office. But all the talent they needed was not where they wanted it, so they had to open offices elsewhere. If innovation is a top priority, the government must position itself to hire innovators where they live.

Build innovation around real problems. Generic innovation centers will not work to develop applied solutions. Applied innovation requires proximity to and responsibility for real, meaningful missions. Some missions are not well-suited to risky innovation, but you cannot de-risk entirely and expect new ideas. To that end, give your innovators real, practical problems. Assign responsibility for a critical mission to that innovation center - or simply demand innovation from a unit assigned a particular problem. You cannot innovate in a vacuum; you must feel pain and failure and risk to do it right.

> **"Talent is destiny in technology. Find the introverts, the folks with blue hair, the ones who can rebuild an engine from scrap, and the people who are skeptical of working with the government. Show them that the mission matters and set them loose."**

Cross-functional organizations innovate better. Give an innovative team what it needs to try new ideas by embedding appropriate cross-functional resources within it. Do not make them beg a bureaucracy for resources and expect them to innovate quickly. Unleash this cross-functional team from dependencies on service-provider organizations, including by decoupling personnel seconded to that team from traditional rating processes.

Align strategic and operational leaders. Operational flexibility and dynamism are critical to success. Strategic leaders will rarely have the right answers; even dynamic, expert operational leaders must primarily empower bottom-up ideas within their teams rather than drive it top-down. How do you do this? Hire non-traditional operational leaders, empower them by emphasizing the importance of their mission and resourcing their efforts, and offer grace if (when) they fail productively. If your operational leaders learn and adapt quickly from failure, embrace that effort. Do not disincentivize experimentation by punishing failure and risk-taking. Expect that operational leaders with a healthy disregard for standard operating procedure will innovate more effectively.

Prioritize mission, not process. Crisis is useful because it creates urgency around the mission. At its most basic, innovation is what occurs when a mission is given primacy over an established process. This is why innovation is fundamentally disruptive to an organization: If it is not painful, it is not systematic. It is possible to empower innovation in sub-units of an organization, but to do so, strategic leaders must emphasize the imperative of their mission and offer the leverage to upend the process in order to achieve it. Expect this to be unpopular in other parts of the organization.

Better tools enable new process. The limitations of existing tools regularly shape the operational processes of organizations. They destroy creativity. Fight this every day. Imagine an optimal process to advance your mission—and envision the tools that would facilitate that reality.

Innovation exists throughout the stack. Innovation is not always sexy. The most important innovations do not necessarily occur at the point of the spear where action is taken against an adversary. Understanding that technological innovation is inextricably tied to process change helps illustrate the links between upstream changes and mission outcomes. Both strategic and operational leaders must understand the entire chain of information gathering, decision-making, and execution that leads to positive outcomes in order to prioritize the most impactful innovations.

Use tools that facilitate innovation. Tools (and contracts) that lock you into specific operational processes impede innovation.

Emphasize core tooling that can be reconfigured quickly for various roles and missions, and that can operate as a platform for time-bound or experimental efforts. As a practical matter, this means tooling that can be configured easily by non-technical staff and makes data easily accessible for use with new tools and processes. Tools that lock-in data impede innovation and undermine your mission. The companies that sell them are prioritizing their revenue rather than your mission. Do not use them.

Do not assume human-driven processes are more accurate. Automated systems have shortcomings, but modern AI regularly beats human decisionmakers at many scaled tasks. Expect automation to make unpredictable errors and consider when such mistakes are acceptable to your mission. But do not assume that human beings will be better in the aggregate. Measure both and compare.

Collaborative innovation often just means sharing the basics. Collaborative work in coalitions is incredibly difficult—and the political hurdles to cooperation are often more important than the technical elements. A key lesson is that collaboration is not just about creating a shared resource; it is also about ensuring that every collaborator is able to effectively use that shared resource. This seems obvious, but it is an easy mistake for highly resourced organizations working with less capable entities.

It is an age-old question: Does art imitate life, or does life imitate art? An updated version might ask: Does digital conflict imitate real-world conflict or does real-world conflict imitate digital conflict? The answer, of course, is that these processes are bidirectional, symbiotic, and deeply intertwined. But if the digital conflict managed by Trust & Safety teams has lower stakes, on average, than real-world conflict, it also faces a faster pace of innovation because the costs of iteration are lower. The most successful Trust & Safety teams embrace this challenge. They cannot match their adversaries' pace, but they can get faster, shape the digital terrain, and use myriad other advantages to achieve their mission.

Innovation is what happens when the mission really, truly comes first. Not an existing process. Not long-standing culture. Not bureaucracy. That is why building innovation around a real, critical mission is central to success. Technological innovation should drive process and decision-making changes. That likely means pain for someone in the organization. Managing and overcoming the prevarication that pain will engender demands leadership—humble, audacious leadership. CTC

Citations

[1] Josh Boyd, "In Community We Trust: Online Security Communication at eBay," *Journal of Computer-Mediated Communication* 7:3 (2002).

[2] "Facebook Community Standards Enforcement Report – Q2 2024 Report," Meta, August 2024.

[3] See "Dangerous Organizations: Terrorism and Organized Hate" in "Community Standards Enforcement Report – Q2 2024 Report."

[4] See https://github.com/facebook/ThreatExchange/blob/main/README.md