COMBATING TERRORISM CENTER AT WEST POINT

CTCSENTINEL

OBJECTIVE · RELEVANT · RIGOROUS | NOVEMBER/DECEMBER 2025 · VOLUME 18, ISSUE 11

FEATURE ARTICLE

Terrorism Risk: Theory, Practice, and Evolution

Don Rassler, Nicholas Clark, and Sean Morrow

A VIEW FROM THE CT FOXHOLE

Admiral Frank Bradley

Commander, U.S. Special Operations Command

Contents

FROM THE EDITORS

Our cover article focuses on how we measure risk in the terrorism field, a task that is increasingly important in a resource-constrained environment. It "makes that case that if the United States is to remain serious about 'risk-based' counterterrorism, then terrorism risk assessment itself" should "be modernized conceptually, institutionally, and technologically to match the complexity and dynamism of the threat it seeks to understand."

Our interview is with U.S. Special Operations Command (SOCOM) Commander Admiral Frank Bradley who describes a dynamic and changing threat landscape and how SOCOM has been evolving to meet and stay ahead of that challenge.

In the first analysis article, we take stock of the changing character of terrorism and U.S. counterterrorism today, evaluating how changes across the spread, structure, scale, and speed of terrorism are challenging the CT community in novel ways and at a time when CT resources are in shorter supply.

Daniel Milton examines why some Islamic State affiliates have failed to thrive and are currently "repressed." He identifies potential causes for their decline—from military counter-responses to in-group conflict to an inability to gain traction among local populations.

Iselin Brady and Daniel Byman consider the realities of burden-sharing with non-traditional CT partners. "Because the United States is reluctant to deploy large numbers of its own forces to fight terrorists everywhere around the globe," they write, "it will continue to rely on local actors, and this will often lead to strange bedfellows."

In looking at the threat from foreign terrorist fighters, Kim Cragin finds "current trends are worrisome but not alarming." She concludes: "If governments continue to … devote resources toward mitigating foreign fighter flows, the threat should remain in stasis."

Finally, Michael Knights examines how Iraq's "telecommunications industry is attracting the attention of U.S.-designated terrorist groups" in order "to generate threat finances and to control and monitor data" in the country.

Don Rassler and Kristina Hummel, *Editors-in-Chief*

CTCSENTINEL

Editors-in-Chief

Don Rassler

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.

Cover: A police officer stands guard outside Scotland Yard, central London, on July 1, 2007. (Simon Dawson/AP Photo)

Danger Zone: Terrorism Risk – Theory, Practice, and Evolution

By Don Rassler, Nicholas Clark, and Sean Morrow

As U.S. counterterrorism strategy has shifted toward "risk-based prioritization" in an environment of constrained resources, terrorism risk assessment has become more critical, as the efficient allocation of resources becomes more crucial the margins for error decrease. Yet, existing approaches to risk assessment remain fragmented in both theory and practice. This article offers a primer and a bridge. It synthesizes a diverse literature on terrorism risk and provides a perspective on the strengths, limitations, and practical utility of various approaches, models, and concepts. Turning to practice, it provides a case study of the Department of Defense's Joint Risk Analysis Methodology (JRAM) and proposes an operational Bayesian risk framework that integrates analyst priors, observable indicators, feasible courses of action, and explicit loss functions. This is complemented by a discussion focused on how data standards, automation, and modest AI applications can support rather than replace expert judgment. The conclusion outlines a future research agenda emphasizing bridges between individual and network-level risk instruments and systemic evaluation of past U.S. government risk assessment cases. It makes that case that if the United States is to remain serious about 'risk-based' counterterrorism, then terrorism risk assessment itself must be modernized conceptually, institutionally, and technologically to match the complexity and dynamism of the threat it seeks to understand.

The assessment of terrorism risk has always been important to U.S. counterterrorism strategy, especially since 9/11. But over the past several years, as the United States has been navigating a shift in counterterrorism as a priority—a move that has affected U.S. CT posture abroad and the resources available for CT—the issue of terrorism risk has become even more central. An important reflection of this change is found in National Security Memorandum 13 (NSM-13), the Biden administration's central CT strategy document, which employed "a risk-based prioritization framework to inform policy decision-making and resourcing to ensure focus on our highest-priority CT objectives."[1] The shift has also been highlighted in statements made by senior counterterrorism officials. For example, in 2023, Nicholas Rasmussen, who was then serving as the Department of Homeland Security's Counterterrorism Coordinater, noted how: "As a result of diminished forward-deployed resources and government attention, the counterterrorism strategy focuses more on risk management and risk mitigation."[2] In early 2025, senior CT officials in the Trump administration called attention to similar dilemmas: how the "threat from global jihadists has expanded significantly, although the resource to counter them have declined."[3] In practice, this has meant that the United States has needed to be even more careful, calculating, and deliberate in terms of how it evaluates terrorism risk, as the diminishment of CT resources and focus has narrowed the margin of error. It has also meant, at least in some cases, that the United States has had to be more risk accepting.

Despite the central, and growing, importance risk assessment plays as a pillar of U.S. CT strategy, there is not a lot of developed work that discusses how the U.S. government, and specific components, approach terrorism risk in practice. Indeed, while the literature is strong in theory, it offers much less insight into the real-world tradeoffs and limitations of key models, how they can be practically implemented, and how they can evolve to meet and keep pace with today's complex and dynamic terror threat landscape.

This article aims to enhance understanding of terrorism risk and advance conversations about the practice, and evolution, of terrorism risk approaches. It is part primer and part bridge, as it tries to show how theory connects, or at least intersects, with

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

COL(R) Nicholas Clark, Ph.D., is an Associate Professor in the Department of Mathematics at the University of St. Thomas (Minnesota). Prior to joining St. Thomas, COL(R) Clark served as an Associate Professor at the United States Military Academy at West Point from 2016 to 2024, where he founded and led the Applied Statistics and Data Science Program. In 2021, he created a curriculum in data literacy that is now the widest adopted program in the U.S. Army. Prior to his academic appointments, COL(R) Clark served as an intelligence officer for multiple units with U.S. Special Operations Command (SOCOM).

*Colonel Sean Morrow has served as the Combating Terrorism Center'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_*

practice. It starts—in Part 1—by taking high-level stock of the literature. It offers a perspective of what practitioners should take away from the literature, including a discussion of key concepts and models and related strengths and weaknesses of different approaches. Part II bridges to practice and includes a short case study of the primary and strategic approach that the Department of Defense uses to evaluate risk: the Joint Risk Analysis Methodology. Part III contains a discussion of how Bayesian risk calculations can be operationalized and used to assess terrorism risk, and how different sources of data, artificial intelligence, and automation can also be integrated into that type of approach. The article concludes with thoughts about next steps—future areas of research and how terrorism risk approaches can evolve in the future.

Part I: Terrorism Risk in Theory – Definitions, Key Approaches, and Takeaways

This section provides a general overview of the terrorism risk literature with emphasis placed on categorizing the corpus, highlighting important findings, and discussing key models, concepts, and approaches that have been developed to evaluate terrorism risk. This latter part, which is the focus of the second half of Part I, includes a discussion about the general utility, strengths, and limitations of key approaches for practitioners in today's environment.

The Terrorism Risk Literature – Collections, Areas of Coverage, and Key Findings

The terrorism risk literature base is a corpus of work that includes more than 60 articles and reports that the authors identified and reviewed. While this corpus includes different perspectives on how terrorism risk should be defined, the literature orients around terrorism risk being defined as a function of threat, consequence, and vulnerability. A core pillar of the corpus is the presentation of methods to model and evaluate terrorism risk, and debates about various approaches, which are explored in the next sub-section.

Articles in the corpus explore different types of terrorism risk. One important dividing line is the unit of analysis. For example, many articles explore terrorism risk through the lens of groups or networks.[4] This includes a subset of articles that examine risk through the lens of specific types of terror organizations or extremists motivated by different ideologies.[5] An important finding from a study of the behavior of nearly 400 terror groups active between 1968-2008 found that "the production of violent events tends to accelerate" as groups increase in size and experience.[6] As noted by the authors of that study:

> *This coupling of frequency, experience and size arises from a fundamental positive feedback loop in which attacks lead to growth which leads to increased production of new attacks. In contrast, event severity is independent of both size and experience. Thus larger, more experienced organizations are more deadly because they attack more frequently, not because their attacks are more deadly, and large events are equally likely to come from large and small organizations.*[7]

This group-level view is contrasted by a developed sub-field, represented by a cluster of articles that focus on the risks posed by individual extremists or lone-actor offenders. This collection of articles has a strong practical orientation, as these works either present frameworks or use real-world data to examine the utility of instruments that have been developed to identify individual radicalization and terrorism risk mobilization factors.[8] For example, the literature discusses at least nine risk and threat assessment instruments developed for violent extremism.[9] Articles in this collection evaluate various instruments, such as the Extremism Risk Guidance 22+ (ERG22+) formulation tool, which was developed to assess "risk and need in extremist offenders;"[10] the Terrorist Radicalization Assessment Protocol-18 (TRAP-18), "an investigative framework to identify those at risk of lone actor terrorism;"[11] and the Detention of Violent Jihadists Radicalization (DRAVY-3), an instrument that was designed "to assess the risks of violent jihadist radicalization in Spanish prisons."[12] The latter study, for example, evaluated a "pilot form of the DRAVY-3 … [that] was filled in, in April–May 2021 in fifty-six Spanish penitentiary centres" including data on 582 inmates involving 63 indicators: 20 for violence, 21 focused on radicalization, nine oriented around changes in habits, seven ethnographic considerations, and six other variables.[13] These data-driven studies complement other academic research[14] and efforts by governments[15] and technology platforms[16] to better understand the behaviors of individuals involved in terrorism, to surface extremist content, and to refine risk and mobilization indicators. Insights and lessons learned from the development to practical implementation of these various instruments would also likely be useful inputs to help evolve group and network focused terror risk approaches.

Another important dividing line in the literature is the distinction between articles that examine terrorism risk through a more general lens versus those that focus on specific dimensions of terrorism risk. For the latter category, this includes articles that explore terrorism risk through specific types of targets, such as commercial aviation[17] or critical infrastructure,[18] or specific weapons or types of terror attacks, such as terror incidents that involve use of chemical agents.[19] It also includes articles focused on terrorism risk insurance programs and specific types of events, such as large scale—similar to 9/11—terror attacks that, while more rare, can generate more devastating consequences.[20] These types of rare but extremely high severity events can be hard to anticipate and predict, and they complicate the scope of what a terror risk model needs to consider and cover.

A collection of the more focused articles explores temporal terrorism risks, spatial dynamics, or contextual factors through the lens of a specific geographic area (e.g., a region, country, or city).[21] For example, the collection includes an article that empirically examines the dynamics of terrorism risk in three Southeast Asian countries;[22] articles that provide separate data-driven profiles of Israel[23] and Pakistan;[24] a study on radicalization risk factors in the United States;[25] a comparative evaluation of terrorism in the United States, United Kingdom, and Ireland;[26] and a study that examined how "country characteristics affect the rate of terrorist violence."[27] Geography is also a key point of orientation for a terrorism risk assessment of historic urban areas in Europe.[28]

These more granular studies provide some helpful takeaways about the temporal and geographic determinates and dynamics of terrorism risk. For example, an empirical study of terror attacks in Israeli from 1949-2004 found—perhaps not surprisingly—that terrorists were "more likely to hit targets more accessible from their own homebases and international borders, closer to symbolic centers of government administration, and in more heavily Jewish

areas."[29] An examination of "waiting time between attacks" also revealed that in the Israeli context, long "periods without an attack signal lower risk for most localities, but higher risk for important areas such as regional or national capitals."[30] The quantitative study of terror incidents in Indonesia, the Philippines, and Thailand examined "patterns of terrorist activity in terms of three concepts: risk, resilience and volatility," and it did so by leveraging a self-exciting model: how "the occurrence of a terrorist event "excites" the overall terrorist process and elevates the probability of future events as a function of the times since the past events."[31] These concepts could be used by the United States and other governments to refine and better model terrorism risk, especially in select areas.

The literature can also be broken down and organized by method or an article's purpose. This includes four primary categories. First, the majority of articles in the corpus focus on theoretical frameworks and debates about how to approach and model terrorism risk. These range from discussions about more common approaches, such as probabilistic risk assessment, to a model designed to help prioritize anti-terrorism measures, to more boutique approaches. Articles that assess terrorism risk approaches or that aim to evaluate specific terrorism risk mitigation initiatives or programs are a second category. RAND has been a principal player in this space since the early 2000s. While RAND's work covers different aspects of the topic, it has done a considerable amount of work focused on the intersection between homeland security and terrorism risk.[32] A third category are articles that examine terrorism risk through case studies.

The final category are articles that discuss how technology, computational approaches, or artificial intelligence can be used to inform or augment terrorism risk approaches. This final category included, for instance, an article focused on the use of Natural Language Processing (NLP) to evaluate "whether the language used by extremists can help with early detection of…risk factors associated with violent extremism."[33] Another important article discussed "the challenges and opportunities associated with applying computational linguistics in the domain of threat assessment."[34] While not directly focused on terrorism risk, another contribution advances efforts to develop "automated, accurate, and scalable [terror attack] attribution mechanisms" by leveraging terrorism incident data to evaluate the performance of "ten machine learning algorithms models and two proposed ensemble methods" focused on the task.[35] These studies highlight how artificial intelligence approaches and tools can be used to derive new or additional insights from different types of data—and do so at both scale and speed.

Key Theories, Concepts, and Approaches

The literature also introduces and discusses key theories, models, and concepts that are used, or could potentially be used, to evaluate or understand terrorism risk. This subsection explores key approaches and concepts that are discussed and debated in the literature, with emphasis placed on their strengths, limitations, and practical utility. This discussion is not meant to be an exhaustive list of ideas and methods, but rather an overview of concepts and approaches that the authors believe are important to highlight.[36]

Foundations: Explaining the Statistical Definition of Risk

Along with the empirical notion of risk, there is also a statistical definition that is germane to the discussion of terrorism risk.

The Homeland Security Advisory System is pictured in April 2007. (Courtesy photo/U.S. Department of War)

In statistical decision theory, risk is defined as the average loss that is incurred based on the decisions that you would make. To accurately measure this, we would need to understand how the data manifests given a parameter, what our possible action space would be, and how we will measure loss.[37] For the purposes of calculating terrorism risk, we can think of the parameter as representing the various states of nature that may be true. For instance, one state of nature might be that there is an inactive sleeper cell in a country, another state is that the cell has already begun to plan attacks, and another may be that there is no threat at all in the country. Note that the mathematical or statistical notion of risks seeks to optimize the best action to take—that is, when we discuss risk, we are not talking about threat but rather talking about residual threat given we decide to act in a variety of ways.

To put this in more concrete terms for a terrorism analyst, to accurately measure risk, we would need to understand what we would expect to observe in a location at a given terrorist threat level. For a statistician, this would be the probability distribution given a parameter, or in other words how the data would manifest given a parameter. We would next need to understand what our possible responses to the situation could be. For example, some actions could be, surge ISR assets, increase soldier presence, or simply do nothing. For a statistician, this would be defining the action space. The final piece that would be necessary is an understanding of what the possible loss would be. For instance, if we think that we are in an area of high terrorist threat and we choose to do nothing, our expected loss would be higher than if we are in an area of low terrorist threat and choose to do nothing. This, for a statistician, would be the loss function.

While this framework is relatively straightforward, the most important distinction is that a risk function is defined for an action,

not for a location. We measure risk according to the average loss for a given action not for a location. Further, to accurately assess risk it is necessary to accurately define the probability of events occurring at different threat levels, capture the action space of possible responses, and quantify the loss for various actions at given threat levels. While the mathematics behind these calculations are relatively straightforward, properly quantifying these measures are often not.

With a few exceptions, the vast majority of the mathematical literature focuses on addressing only a subcomponent of what is needed to measure risk. Typically, the literature addresses the probability of an action occurring. While this is a necessary step in calculating risk, as detailed in Part III it is not sufficient.

Probabilistic Risk Assessment

Probabilistic risk assessment is similar to the mathematical definition of risk in that it seeks to quantify the likelihood of an event and the consequence of that event occurring. The formula is Risk = Probability X Severity.[a] While the formula is referred to as probabilistic risk assessment, the risk calculation does not return an actual probability. However, risk can be quantified and different regions can be compared by using this calculation. As opposed to the mathematical definition of risk, the probabilistic risk assessment does not take into account the observer's actions. That is, risk in this context is assumed to exist regardless of what mitigating measures may be employed. This formula, though, is likely appealing to many operational units as it is simple to construct and easily explained. The simple nature, though, hides a multitude of assumptions or questions that must be answered. Specifically, how is the probability of an event occurring calculated and what is meant by severity. While often severity is calculated through loss of human lives or monetary cost, the probability of an event occurring is typically either handled through an analyst's "best guess" or obfuscated through a further complex mathematical formula that hides other assumptions. Some criticism of PRA has focused on the inadequacy of PRA to hedge against the different probabilities that attackers may eventually act upon. That is, attackers may make a choice to attack in a manner that is unexpected, simply because that manner of attack is unexpected.[38] While this certainly could be true, this also would assume that the attackers knew how the defenders, or the analysts, were assigning probabilities in the first place. The argument then becomes tautological, leading to a conclusion that no probabilities should be calculated. Typically, this line of thought ends in a qualitative risk assessment; however, we argue the qualitative risk assessment is nothing more than an informed prior distribution, leading to the conclusion that we should leverage more Bayesian methods in our risk calculations.

Bayes Risk

As alluded to above, the issue with a strict probabilistic risk assessment is that the data is often not available to quantify the likelihood of an event occurring. So, analysts often make their best-informed guess on the likelihood of an event occurring. However, if the probability of an event occurring is calculated through an analyst's best guess, or prior belief before data convinces them otherwise, the formula really then belongs in the class of Bayesian risk calculations. A Bayesian risk calculation is a subset of a probabilistic risk assessment where the concept of mathematical risk as defined above is extended through incorporating an analyst's prior belief. This allows for calculations to occur in the absence of data but also updates when data becomes available. This has made Bayesian risk approaches useful, as when "the situation changes, they are easy to update; as the evidence changes, the posterior probability changes."[39] Bayesian networks also hold utility for risk communication, as "they show all the prior and marginal probability distributions of the risk results."[40] Bayes approaches have been used "in the development of anti-terrorism modeling" and "to predict distribution for lethal exposure to chemical nerve agents such as Sarin."[41] While Bayesian inferential techniques have been criticized as relying on the availability and completeness of data,[42] these techniques do naturally blend qualitative analysis (in the form of a prior belief) and can still provide insight when data are limited as is sometimes the case in assessing terrorism risk.

Mathematically, a Bayesian risk calculation incorporates a prior probability that is placed upon the parameter that is used in the classic risk calculation. The formula for Bayes Risk of an action is calculated through summing up the loss occurring if the action is performed given the various states of nature are true times the likelihood the various states of nature are true times the prior belief that that state of nature is true.[b]

Game-Theoretic Approaches

Another method discussed in the literature is game theoretic approaches, which provide a way to study "multi-agent decision problems."[43] Approaches informed by game theory have been proposed because terrorism is shaped by interactions between players, especially a terror network and a CT entity,[44] and game theory can help model how terror attackers—an intelligent adversary—may adapt to counterterrorism actions.[45] The motivation has also been driven by the view, expressed by some, that "probability is not enough" to measure terror risk.[46] But instead of game theory being viewed as the central tool to evaluate terrorism risk, the literature primarily discusses how game theoretic approaches could be useful as a "decision tool in counterterrorism risk assessment and management,"[47] and as a way to improve "current risk analyses of adversarial actions."[48]

Security-focused games have been utilized for "many real world applications," which intersect with the problem of terrorism. For example, "game-theoretic models have been deployed" to support: "canine-patrol and vehicle checkpoints at the Los Angeles International Airport, allocation of US Federal Air Marshals to international flights, US Coast Guard patrol boats, and many others."[49]

While game-theoretic approaches appear to hold some promise for terrorism risk assessment, their use is also complicated by limitations and tradeoffs. For example, a "major challenge" in

a When it comes to terrorism risk, different U.S. government agencies use different risk calculation formulas. For example, the Department of Homeland Security has defined terror risk as a function of threat, consequence, and vulnerability, while the Department of Defense has viewed strategic terror risk as being a function of threat and consequence.

b Risk of taking Action A = Loss if Action A is taken given state of nature 1 is true * likelihood that state of nature 1 is true given we observe data on the ground * Analysts prior belief that state of nature 1 is true + Loss if Action A is taken given state of nature 2is true * likelihood that state of nature 2 is true given we observe data on the ground * Analysts prior belief that state of nature 2 is true + etc.

models used "is their reliance on complete information and full rationality assumptions, which may not hold in practical security settings where attackers operate under uncertainty and defenders face information asymmetries."[50] Unfortunately, the 'world' of information asymmetries is usually the environment that CT practitioners need to live and act in. So, while "game theory will tell you how the game should be played," it might not tell you "how it will actually be played."[51] As noted by Ezell et al., the use of game theory may thus "lead an analyst to gain some unexpected and interesting insight into the terrorism problem, which other techniques fail to provide," but a key danger is that insight "could be for the wrong game in the first place."[52]

Richardson's Law and Power Law Distribution

Famous English mathematician and scientist Lewis Fry Richardson found that the "relationship between the severity of war, measured by battle deaths, and the frequency of war"[53] followed a Power law distribution. This type of probability distribution is considered a heavy-tail distribution and is used to model situations where large events are rare while small events are common. It has been used to model and describe a diverse mix of extreme events such as earthquakes, solar flares, and stock-market collapses,[54] and to understand 'black swan' events.

It has also been used to describe, and explain, certain dynamics of terrorism. For example, research by Aaron Clauset, Maxwell Young, and Kristian Skrede Gleditsch, found that the "apparent power-law pattern in global terrorism in remarkably robust"[55] and that it "persists over the past 40 years despite large structural and political changes in the international system."[56] Clauset and Ryan Woodard have used Power law to evaluate the historical and future probabilities of large terror events, such as 9/11.[57] Research by Stephane Baele also suggests that "heavy-tailed, power-law types of data distribution" are ubiquitous "in all major dimensions of digital extremism and terrorism."[58]

Hawkes Point Process Model

Another important concept discussed in the literature is the Hawkes Point Process Model.[59] The Hawkes process is a self-exciting point process. In the context of terrorism, "self-exciting models assume that the occurrence of a terrorist event 'excites' the overall terrorist process and elevates the probability of future events as a function of the times since the past events."[60]

This idea is intriguing as it may help to model a key aspect of dynamism that influences terrorism today: how some acts of terrorism by individuals or groups help to 'spark,' 'ignite,' or provide motivation for other acts of terrorism. This is not a theoretical problem. Indeed, as noted by White, Porter, and Mazerolle, "although terrorist attacks might appear to occur independently at random times, a sizeable body of theoretical and empirical research suggests that terrorist incidents actually occur in non-random clusters in space and time."[61] While these three researchers use the Hawkes process to evaluate terrorism patterns in three Southeast Asian countries, research by other scholars highlight where a 'self-exciting' dynamic appears to be playing an important role. For example, an examination of vehicular terror attacks found "the demonstration effect created by high-casualty vehicle-ramming attacks has in the past seemingly produced a surge in copycat attacks."[62] More concrete evidence can be found in the world of far-right terrorism. For years, researchers have documented a pattern of behavior, what has been framed as the 'cumulative momentum of far-right terror': how individual terror attackers are influenced by, and seek to build off the momentum, sparked by prior attacks, with the 2019 deadly terror attack in New Zealand being a key catalyst.[63]

While the 'self-exciting' dynamic exists in some areas, additional research illustrates how it does not appear to exist in others. For example, a data-driven study of terrorist suicide-attack clusters "did not uncover clear evidence supporting a copycat effect among the studied attacks."[64] This suggests that while the Hawkes process holds some utility to understand the modern dynamics of terrorism risk, its utility may also be limited to certain types or categories of threats.

Structured Professional Judgement

Another method, structured professional judgement (SPJ), is viewed by some researchers as "the current gold standard for assessing and managing violence risk"[65] and "the best practice approach for assessing terrorism risk."[66] As noted by Dean and Pettet:

> *The "SPJ" methodology arose as a compromise position between two disputing camps. The first camp, "unstructured clinical judgement," relies on professional expertise in collecting, aggregating, and interpreting data. The second camp, "actuarial assessment," "strives to achieve empirically accurate classifications by replacing clinical judgment with validated instruments and algorithms."*[67]

SPJ is an attempt to blend these two approaches. The result, at least in theory, "is an evidence-based approach that combines empirically grounded tools with professional judgment."[68] For example, this can take the form of experts being asked through a standardized process, such as a survey or checklist, to rate or score an individual or group in relation to defined risk factors or criteria and established risk level categories (e.g., low, moderate, high). To help standardize inputs, the assessor can "be trained in a "calibration" exercise … to ensure an adequate level of consistency is obtained in rating each risk indicator item."[69] After inputs are received, the professional judgements[c] from each expert can then be weighed and combined to provide a composite risk rating, which can be assessed in relation to a larger collection of responses to develop a summary risk score.

SPJ is widely used to assess the risk of violence in various areas, from terrorism and extremism, to stalking, domestic violence, and sexual violence.[70] SPJ, for example, informs and is used as a part of the Department of Defense's Joint Risk Assessment Methodology. It is also used as a part of the Violent Extremist Risk Assessment tool,[71] the TRAP-18 investigative framework,[72] ERG22+,[73] and other similar instruments.

One core challenge of SPJ is "how best to deal with the subjectivity inherently involved in professional judgement."[74] This is because SPJ tools are "not as 'objective' a process as some

c As noted by Dean and Pettet, "'professional judgement' is an amalgam of 'evidence base' and 'tacit knowledge,' which gets combined in the mind of the analyst to an unknowable extent and which in turn ends up as a final judgement call of the presumed 'risk level' a PoC" [person of concern] or group "may pose to the community." Geoff Dean and Graeme Pettet, "The 3 R's of risk assessment for violent extremism," *Journal of Forensic Practice* 19:2 (2017).

suggest."[75] While SPJ approaches provide a structured process that can help to control subjectivity, there will always be some "inherent 'subjectivity' of an analyst's professional judgement."[76] Dean and Pettet discuss 'controlling out' and 'controlling in' as two different approaches to try and manage this subjectivity challenge.[77]

SPJ-driven approaches are clearly valuable, but they should also be used with care. Integrating expert views into terrorism risk approaches is a source of strength, but SPJ approaches on their own do a poor job of highlighting individual or collective biases, and it seems prudent that it would be helpful to leverage other data to either validate expert views or to identify areas of divergence—so those can be explored.

Risk Terrain Modeling

Several researchers have used risk terrain modeling (RTM) to evaluate and better understand terrorism risk in specific locales, such as a city. Developed by Joel Caplan and Leslie Kennedy in 2009, RTM is a method to examine the spatial dynamics of crime, to "identify the risks that come from features of a landscape and [to] model how they co-locate to create unique behavior settings for crime."[78] [d] The approach has drawn the attention of some scholars because research "consistently demonstrates crime is spatially concentrated,"[79] and since terrorism is a type of crime, it is worthy of exploration.

There has been a small collection of academic studies that use RTM to evaluate the spatial dynamics of terrorism risk. This includes the use of RTM to evaluate how geographic space, risk factors, and terrorism intersect in places such as Istanbul, Belfast, and New York.[80] Research focused on RTM has been complemented by other work that centers 'place.' Two sets of scholars, for example, have developed frameworks to help navigate how acts of terrorism, and terror decision making, intersect with place. This includes the EVIL DONE terrorism risk framework "for assessing the desirability of targets based on eight criteria"[81] developed by Clarke and Newman and the TRACT framework, created by Zoe Marchment and Paul Gill, that identifies five factors that shape the spatial decision-making of a terrorist actor.[82]

Like other approaches, RTM has strengths and weaknesses. Two key strengths is that "RTM as an overall approach is relatively simple and user-friendly, and the associated RTMDx software provides an opportunity for practitioners to readily utilize the approach with minimal resources and time spent on learning new processes."[83] Another strength, according to a systematic review of the method by Zoe Marchment and Paul Gill, is that "RTM has been successful in identifying at risk places" for various crimes, including terrorism.[84] But, as Marchment and Gill also note:

> *A key limitation of RTM is that it does not address temporal variations in crime locations (over the course of day, duration of a week, over different seasons, etc.) Another limitation of RTM in general is that it may identify areas as being risky where crime may never emerge. It cannot be assumed that because a location is high in risk according to identified risk factors, that crime will always ensue—there can be numerous areas identified as risky, but no crime may actually occur in these defined risky areas.*[85]

The detailed data requirements of RTM would also limit its value and utility in various counterterrorism contexts, especially those focused on broader areas, remote locations, or under- or not-well governed terrain that do not have granular or reliable geolocated environmental or societal data.

Conjunctive Analysis of Case Configurations

The Conjunctive Analysis of Case Configurations (CACC) is another method that—like RTM—has its roots in criminology and crime prevention, but that has also been explored through the lens of terrorism.[86] CACC, a multivariate method, "is an analytical technique for identifying whether certain variables are causally related to an outcome while simultaneously accounting for other measures of interest."[87] It can also be used to test hypotheses and explore data patterns and causal relationships.[88] The method "begins by developing a data matrix, referred to as a truth table, consisting of all possible combinations, or interactions, of the variable attributes."[89] The truth table is then leveraged to create counts to "help identify key incident characteristics, their relationship with each other, and the frequency in which they are included in dominant configurations."[90] The method has been used to assess radicalization risk in the United States[91] and similarities between domestic types of terrorism in the United States, United Kingdom, and Ireland.[92]

When it comes to terrorism risk and terror prevention, scholars have argued that approaches like CACC and RTM are useful as they provide context and can be used to break down the dynamics of risk and the multitude of factors that help drive it in specific areas. Or put another way, the two methods can help to 'color in' the general picture of risk that statistical approaches offer. As noted by Jeffrey Gruenewald and his co-authors, CACC and RTM can elucidate terror opportunity structures and help to bridge this gap:

> *Another limitation of prior statistical research on risk of terrorism attacks occurring is the overreliance on statistical main effects models that tell us how single variables increase or decrease the likelihood of terrorism occurring. Useful in their own right, these approaches cannot capture complex spatial risk profiles of various terrorism-related activities, specifically the amalgamation of factors shaping opportunities situated within unique socio-political contexts that are more or less conducive for terrorists to reside, plan and prepare, and commit attacks.*[93]

But, like RTM, CACC requires developed, granular, and reliable data, which limits where and when it can be used.

By providing an overview of literature that focuses on terrorism risk, and highlighting key models, approaches, and concepts, Part I aimed to illuminate a set of options—aligned with empirical and theoretical research resources—for practitioners to examine and consider. The review of the diverse and scattered literature base revealed that there are primary approaches, such as probabilistic risk assessment and structured professional judgement, that are commonly used, and that hold broad utility to evaluate terrorism

d As noted by Jeff Gruenewald and his co-authors, "RTM relies on determining the spatial influence that risk factors have on the environment through two processes: proximity and density." See Jeff Gruenewald et al., "Innovative Methodologies for Assessing Radicalization Risk: Risk Terrain Modeling and Conjunctive Analysis," National Criminal Justice Reference Service, November 2021.

risks. The review also revealed several other methods that can be used for specific use cases or geographies, when there is a need to better understand and model offender-defender interactions, or to identify important contextual markers and/or the extremism and radicalization risk factors of individuals (and correlations of those factors). Key concepts, such as Power Law and Hawkins Point Process, also hold utility as they help to explain certain dynamics of terrorism, and related aspects of terror risk.

But the literature also highlighted divides and gaps. Indeed, one of the most interesting takeaways was the dividing line that exists between individual and group or network-based terrorism risk approaches, and how the instruments that have been developed to model and evaluate the risks posed by individuals are not only more developed—they also appear to be better evaluated. The comparative richness of the academic debate and discussion about those types of instruments and the dynamics of individual extremism risks was also quite stark. As for gaps in the literature, a primary one is how different risk assessment methods can be leveraged to complement one another and evolve terrorism risk as an area of practice.

Part II: Terrorism Risk in Practice: The JRAM as a Case Study

This section explores terrorism risk in practice through the lens of an approach—the Joint Risk Analysis Methodology, the JRAM—that has been used by the Departments of Defense.[94]

Before examining that approach, it is helpful to get a view of the role terrorism risk assessment plays in national strategy, and how approaches utilized by U.S. government agencies come together, or filter up, to affect that strategy. NSM-13, a key document that guided the Biden administration's CT approach, provides a useful window into the issue. That document outlined the strategic role that terrorism risk assessments play in guiding U.S. CT strategy. This can be seen in how NSM-13 committed the United States to using a "risk-based prioritization framework to inform policy decision-making and resourcing to ensure focus on our highest-priority CT objectives."[95] NSM-13 also revealed how terrorism risk was being assessed at a strategic level: It was defined "as a function of terrorist intent and capability (i.e., threat) to target the Homeland or persons or facilities overseas exposure or vulnerability and the willingness and capability of host-country governments to mitigate terrorist threats within their borders."[96] Another important detail discussed in the document is the cadence of terrorism risk reviews by senior U.S. government figures. NSM-13 outlines, for example, how the National Security Council-led Counterterrorism Security Group will meet quarterly to "assess and update, as necessary, prioritization guidance based on shifts in terrorism risk or other policy decisions."[97] While NSM-13 does not speak to these details, it seems likely that during those meetings, representatives from different U.S. departments discuss their agency's own terrorism risk findings, and any important changes that have transpired since the last meeting.

The JRAM, which is produced by the Joint Staff, is the central document that strategically guides the Department of Defense's approach to terrorism risk. The first version the JRAM was published in 2016 "to promote a common risk framework and lexicon to the joint force."[98] The JRAM include elements focused on risk appraisal, risk management, and risk communication. According to the JRAM, "effective risk assessment" should evaluate risk in relation to three elements: "harmful event, probability, and consequence."[99] While the JRAM defines risk as a function of those latter two elements—probability and consequence—it proposes that those two elements be viewed, and assessed, through the 'lens' of a harmful event.[100] This includes, as part of that process, the "identification of the source(s) and driver(s) or risk that may increase or decrease the probability or consequence."[101] For certain DoD components, sources or risk are identified through a threat survey, and drivers of risk are identified through an "OPS Survey," which both leverage the knowledge of experienced practitioners and experts.[102] Then, after the sources and drivers of risk have been identified, "the expected probability and consequence of the harmful event" are determined.[103]

The formula and approach used by one DoD component is as follows: the operations indicator (derived from the OPS Survey) is subtracted from the threat survey indicator. This leads to a heuristic value indicator defined by four categories:

Category 1: Operation pressure exceeds posed threats
Category 2: Operation pressure able to mitigate threat
Category 3: Threat exceeds operation ability to mitigate
Category 4: Threat overwhelms mitigation or is unchecked[104]

These categories are used to estimate probability. The probability (1-4) is then multiplied by a consequence value that is assessed in relation to four defined categories: 1) minor, 2) modest, 3) major, and 4) extreme.[105] Examples of terror events that would align with each category include 1) USS Cole bombing, 2) U.S. withdrawal from Lebanon after the Marine barracks bombing in 1983, 3) 9/11, and 4) an existential threat, such as a large scale WMD attack.[106] The multiplication of the assessed level of probability and consequence results in a risk value that ranges from 1-16 that associate with four baseline risk levels: low, moderate, significant, and high levels of risk.[107]

According to the JRAM, the final step in the risk characterization process is the plotting of the probability and consequence findings onto a risk contour that features the four baseline risk levels (see Figure 1 below for an example).[108] While the exact plotting of those findings on the risk contour is in part subjective, the contour is useful in that it helps to visualize the level of risk in a simple, easy to understand way.

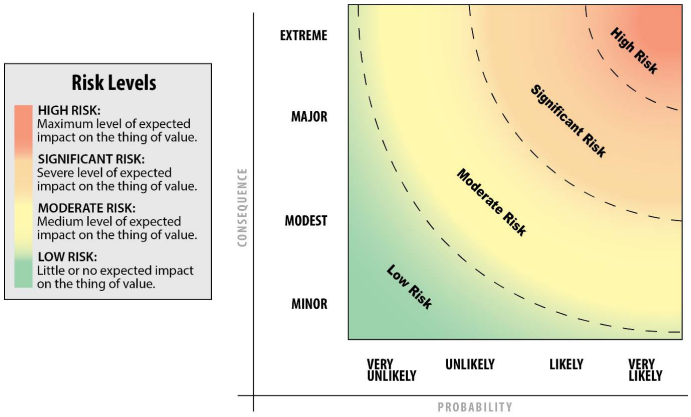

Figure 1: Baseline Risk Levels and Generic Risk Contour[109]

The JRAM approach is driven by structured professional judgement, and it has various strengths and limitations. The approach places emphasis on the experience and expertise of

practitioners to assess terrorism (and in different contexts other forms) of risk, and it quantitatively characterizes risk through a structured process that situates qualitative and subjective expert inputs within a quantitative risk categorization framework. In that way, as noted by the JRAM, "Risk appraisal is fundamentally a qualitative process incorporating and informing commander's judgment while quantitatively expressing probability and consequence when appropriate."[110] The JRAM's reliance on practitioner experience is a core source of strength, as specialists that 'live' the terrorism problem set on a daily basis, and who have access to different types of intelligence, especially granular data, are very well postured to understand and evaluate the types of risks that terror groups pose, and to identify changes in behavior. Another key strength lies in the structure and standardization that the JRAM provides to make sense of qualitative, expert inputs. This helps commanders and other decision makers to evaluate a collection of expert inputs as a whole or in relation to one another so areas of convergence or divergence can be identified and interrogated.

But the JRAM also has limitations and downsides. While the emphasis that the JRAM places on expert inputs is well placed, it is not clear how the JRAM process controls for—or attempts to minimize—subjectivity, including biases and assumptions. For example, as noted by Michael Mazarr: "What judgments, assumptions and outright guesses had to be made in order to produce a given level of risk? How many were close-run findings that could easily have gone the other way?"[111] The danger, as Mazarr highlights, is that:

> *Too often risk assessments have involved subjective judgments used to generate color-coded assessments without sufficient detail on their assumptions. Such singular verdicts ("moderate risk") can offer leaders the opportunity to close their minds when any good risk process ought to be doing just the opposite—be very clear about the assumptions and nuances behind the results to force senior leaders to discuss and debate key issues.*[112] [e]

These are not theoretical concerns. These challenges are also not limited to the individual level, the responses or views of one or a few individuals; they can manifest on a collective level as well, and lead to broader problems.[f] For example, an article featured in this publication last year examined how the U.S. intelligence community and CT enterprise failed to accurately assess, despite indicators, that al-Qa`ida in the Arabian Peninsula (AQAP) had the intent and was seeking to attack the United States, an oversight which led to the United States being surprised by AQAP's attempt to down an airliner over Detroit on Christmas Day in 2009. As noted by a government expert interviewed for that article: "We had assumptions about how a terror group [AQAP] operates. It was a major analytic failure."[113] In the view of another expert, the problem was not tied to lack of awareness of key indicators, but in how the evidence was interpreted and weighted.[114]

Another limitation is that terrorism is characterized by uncertainty and complexity. This poses challenges for terrorism risk assessments generally. For example, while terror groups will at times telegraph or demonstrate their intent and capabilities, they also often hide the same so they can engage in surprise or increase the likelihood that an operation will succeed. As a result, there will always be limits about what can be known about the activity and plans of terror networks, and the precise nature of the risk(s) they pose. This affirms the importance of identifying and being honest about gaps and assumptions and scrutinizing terror risk assessment findings through the lens of what we do not know.

The dynamic and evolving nature of today's information, security, and technology landscapes also make it challenging for governmental efforts that involve bureaucracy and coordination to keep pace with volatile terror threats. As noted by Kim Cragin, "The JRAM does not work well for dynamic risks like terrorism."[115] A key part of the challenge is that changes in terror risk can be driven by the actions of terror networks, by changing environmental conditions (e.g., a coup, economic shifts, etc.), by operations conducted by counterterrorism forces,[g] or by other factors. Approaches like JRAM need to be able to iterate at pace and strategically take stock of noteworthy developments and interactions, and how those changes may impact a prior terror risk assessment finding.

While the JRAM, and public information about the method, contain helpful reflections about how the approach leverages qualitative inputs, how the process makes use of quantitative data is not clear.[h] The issue is important to consider as analysis of quantitative terrorism and CT data and information about changing environmental conditions can be conducted at speed or automated, and that type of data can be leveraged to supplement, or enrich, the JRAM process, or to make it more dynamic and responsive. Automated analysis of these types of data could be used to identify, or alert, practitioners about important changes or anomalies, or to validate risk assessment findings or highlight areas where data and perspectives diverge. For example, terror incident data could be leveraged to baseline risk assessments or to alert analysts about key changes in the scale, frequency, focus, reach, and lethality of specific terror networks. Key environmental indicators, such as the Fragile States Index, could be used to identify if conditions in a certain country or region are getting worse or improving, dynamics

e In another publication, Mazarr expounded on this idea: "In a June 2012 article in the Harvard Business Review, Robert Kaplan and Anette Mikes suggested that the sort of hard-boiled confrontations so essential to real risk discussions are rare, and in fact an unnatural act for most human beings. They point to organizations that create rough-and-tumble dialogues of intellectual combat designed to ensure that risks are adequately identified and assessed. These can involve outside experts, internal review teams or other mechanisms, but the goal is always to generate rigor, candor and well-established procedures for analysis. The result ought to be habits and procedures to institutionalize what Jonathan Baron, professor of psychology at the University of Pennsylvania, has called 'actively open-minded thinking' – a combination of a thorough search for information and true open-mindedness to any possibility, while avoiding self-deception through rigorous consideration of alternatives." Michael J. Mazarr, "The True Character of Risk," Risk Management, June 1, 2016.

f They can also be further problematized by other human factors. For example, as also noted by Mazarr: "Risk failures are mostly attributable to human factors – things like overconfidence, personalities, group dynamics, organizational culture and discounting outcomes – that are largely immune to process." See Mazarr, "The True Character of Risk."

g Cragin proposed a strategic risk model to account for how the "iterative nature of counterterrorism" as reflected in strikes and raids impacts terrorism risk. The model defines strategic risk as risk to mission and risk to force divided by the number of previous strikes (or raids) plus one. See Kim Cragin, "A Better Way to Talk About Risk," Lawfare, July 6, 2025.

h According to one document that explains the JRAM, "most quantification serves to bound, not measure risk." "Joint Risk Analysis Manual Slides."

that have implications for terrorism. It is important to remember that food affordability and changes in the price of wheat are viewed as key factors that contributed to the rise of the Arab Spring, a huge development that led to violence and political change across North Africa and parts of the Middle East.[116] Structured data on counterterrorism operations, such as the number of strikes, raids or arrests, can be used in a similar way to provide a more up-to-date picture on the kinetic pressure placed against terror nodes, which has a bearing on their capabilities and near-term risk.

This short discussion highlights strengths and limitations of the JRAM and several important issues that are important to consider as the United States works to modernize its approach to terrorism risk. This includes the importance of surfacing biases and assumptions; creating pathways to integrate the perspectives of other experts, potentially even those outside of government, to refine views on risk or interrogate findings; and leveraging the power of different sources and types of data, especially quantitative data, and approaches (e.g., automation) to augment, enhance, facilitate iteration, or add dynamism to existing risk approaches.

Part III: Operationalizing Terrorism Risk for CT - A Case and Perspective

To make more concrete how alternative definitions of risk can be employed in the CT fight, we next consider a case study using Bayes risk to arrive at the optimal decision under uncertainty. The use of Bayesian risk calculations allows analysts to combine both subject matter expertise alongside a risk formula that is consistent with how mathematicians and statisticians understand and quantify risk. Here, we demonstrate not only how Bayesian risk can be employed but also highlight how proper data collection methods and understanding of the academic literature can help sharpen the necessary components of a risk model.

As previously discussed, a statistical definition of risk is not only a function of the threat; rather, it seeks to quantify the average loss that would occur if a unit takes a given decision. To a practitioner, this means that risk is not solely in the realm of the intelligence section for a unit, but a joint product derived from an understanding of the probability of events occurring, the action space of allowable responses, and the loss that would occur if you took that action.

In our hypothetical case study, we assume that intelligence analysts had been examining country X for some time and determined that there were three possible situations inside of the country. The first, which we will refer to as O_1 is that there are no insurgents that pose a threat to U.S. forces. The second, O_2, is that there are a few sleeper cells and in the presence of U.S. forces they will activate. The third, O_3, is that there is an active threat that is planning against the United State directly.

Based on the research that the analysts have conducted, they believe that the probability of O_1 being true is 30% (denoted as P(O_1)=0.3), further P(O_2)=0.5 and P(O_3) = 0.2. The analysts further assess that if O_1 was true, there is a 90% chance they will observe no vehicle traffic between two locations, and there is a 10% chance they will observe some vehicle traffic. For O_2 there is a 10% chance they will observe no vehicle traffic (90% chance they will observe some) and for O_3 there is a 50% chance they will observe no traffic.

The operations section then states that there are three possible actions: We should conduct a raid only if we observe traffic on the ground, we should raid either way, or we should continue to monitor. If we conduct a raid, but O_1 was true, we will incur a loss of 20 lives. If we do not conduct a raid but O_1 was true, no loss is incurred. Subsequently, if we raid and O_2 is true then we lose 100 lives, but if O_2 is true and we fail to raid then we would lose 200 lives. Finally, if we raid and O_3 is true we lose say 80 lives, but if we fail to raid and O-3 is true we would lose 300 lives.

So, we make the decision that we will raid only if we observe traffic on the ground. We then can calculate the risk surrounding that decision as:

R(raid only if traffic on ground) = P(O_1 is true given there's traffic on ground)*20 +
P(O_2 is true given there's traffic on ground) * 100 +
P(O_3 is true given there's traffic on ground)*80 +
P(O_1 is true given there's no traffic on ground)*0 +
P(O_2 is true given there's no traffic on ground)*200 +
P(O_3 is true given there's no traffic on ground)*300

To complete this calculation, we need to calculate P(O_i is true given there's traffic). To do this, we rely on Bayes theorem.

P(O_i is true given there's traffic) = P(Traffic given O_i)*P(O_i from analyst belief) / P(Traffic)

P(O_1 given traffic) = (.10 * .3) / (.10*.3 + .90*.5 + .5*.2) = 0.05
P(O_2 given traffic) = (.90 * .5) / (.10*.3 + .90*.5 + .5*.2) =0.77
P(O_3 given traffic) = 0.172

We can continue on to find:
P(O_1 given no traffic) = 0.64
P(O_2 given no traffic) = 0.12
P(O_3 given no traffic) = 0.24

In total, then, the risk associated with this decision is:
R(raid only if traffic on ground) = 187.76

We could then compare this to the decision to always raid regardless of what is on the ground:

R(raid either way) = P(O_1 is true given there's traffic on ground)*20 +
P(O_2 is true given there's traffic on ground) * 100 +
P(O_3 is true given there's traffic on ground)*80 +
P(O_1 is true given there's no traffic on ground)*20 +
P(O_2 is true given there's no traffic on ground)*100 +
P(O_3 is true given there's no traffic on ground)*80
Here the probabilities stay the same, however the loss functions differ as the action is different.

R(raid) = 135.76

Finally, we can look at the decision to not raid either way.

R(don't raid) = P(O_1 is true given there's traffic on ground)*0 +
P(O_2 is true given there's traffic on ground) * 200 +
P(O_3 is true given there's traffic on ground)*300 +
P(O_1 is true given there's no traffic on ground)*0 +
P(O_2 is true given there's no traffic on ground)*200 +
P(O_3 is true given there's no traffic on ground)*300

Again, the probabilities remain constant however the loss changes.

R(don't raid) = 301.06

The decision, then, that incurs the least risk would be to raid regardless of the actions on the ground. To summarize, in order to calculate risk, we need:

- Prior probabilities that analysts generate of different states of the world
  - In our example the probability of O_1, O_2, or O_3
- Understand the probability of observing different situations given the states of the world
  - The probability of observing traffic given O_1, O_2, or O_3 were true
- Finally, we need to know the actions we could take and the loss that we would incur given the different states of the world
  - The # of casualties incurred if we act or if we fail to act given all the states

While there are multiple calculations that need to be done throughout the process, the calculations are relatively straightforward and offer both analysts and decision makers to also generate ranges of risk based on uncertainty. For instance, if an analyst says there is about a 20-30% chance of O_1 being true, the calculations can be performed at each of these levels to provide a range in risk values.

While this example focuses on a tactical action, the same calculations can be performed at the operational or strategic level. Here, the states of nature (parameters) may focus more on strategic actors, and the actions would correspond to, say, moving forces into a region or employing a special operations task force.

The majority of the scientific literature appears to focus on properly quantifying the probability of outcomes occurring at different risk values, which is a necessary component, however it is insufficient to properly calculate risk. The key here is that risk should not be confined to a single staff section and should be calculated leveraging the subject matter expertise of analysts as well as the operational insight of others on the staff.

Critical in this too are consistent definitions of loss. In our toy example, we used human lives, which is a natural measure; however, other times financial loss or reputational loss would also occur depending on the action conducted. More emphasis, then, should be on formally defining what loss means for a given unit. It must remain consistent if different scenarios are analyzed.

While these calculations are perhaps more simplistic than some presented in literature, we propose that simplicity is preferable here. In communicating with a wide range of audiences, the typical risk calculations provided above are easily explained and argued. If an analyst feels that the prior probabilities are incorrect, anyone with a calculator can make the adjustment without relying on a black box algorithm that may be hiding unrealistic assumptions.

This is not to fully argue that automation and AI have no role in our risk calculations. Rather, as operational units define the probabilities of different outcomes occurring, a properly established data pipeline can update the components of risk in real time. Further, if units decide to change their loss functions or to change their situations that may arise from different states of nature, a properly configured algorithm should be able to automatically adjust.

However, the complex nature of risk does not necessarily require a complex algorithm to understand. Mathematics and probability can assist us in establishing the correct calculations for risk, but cannot replace the subject matter expertise that is needed to generate prior probabilities, define outcomes we would expect to see given states of nature, or generate the possible actions/losses that would occur at differing states of nature. Further, proper data can help us refine the various components that are necessary in computing the Bayes risk for a given action. Recall that Bayesian risk is a factor of knowing what the various states of nature could be (what the parameter space is), what analysts believes are the various probabilities of those states of nature (the prior beliefs), the likelihood of various actions given that the states of natures are correct (the likelihood function), and the cost of performing an action if we are correct or incorrect about our belief of the state of nature (the loss function). Here, we decompose these components and show how proper data collection and data management can assist in better sharpening these elements.

First, we focus on knowing what the various states of nature might be. That is, prior to any risk calculations we have to know the various possibilities for what may be occurring in a given region (or within a given network). To determine this, an analyst is limited by their creativity and historical knowledge. Here, it may be possible to leverage generative AI to assist in brainstorming the various possibilities in a given region. Note that at this stage, we do not seek to assign probabilities to these states of nature, but rather just to explore the possibilities.

The second aspect is to assign prior probabilities to these parameters. That is, based on the research that the analyst has performed, how likely are each of these outcomes to occur. This can be done in a variety of ways and often the risk calculations that exist in literature can be leveraged to assist in these calculations. For example, in Cragin, the author proposes using risk to mission * risk to force/(Previous Strikes +1) as a measure of risk. Here, if the parameter space is geographically focused, meaning one state of nature is there is an active threat against the United States in country A and another state is that there is an active threat in country B, the measure the author proposes could serve as the prior probabilities of the states of nature being true.

Perhaps the place that data and literature best serves is in the next component of the Bayesian risk calculation, the likelihood of various actions given that the states of nature are correct. Here, we need to not only define what data we might expect to see for various parameters, we also need to define how likely it is that we observe those data if the parameter is true. For instance, in the Hawkes processes defined above, structure can be placed on the background rate to determine what the causes are of violence emerging. That is, when a terrorist attack has happened in the past, what were perhaps socio-economic or other factors that may have suggested an attack was likely. These then could serve as the types of data that are collected. Once the data sources are determined that will be used to calculate the likelihood, it is imperative that the data remain consistent throughout the entire collection process. That is, all measurements should be standardized, and analysts should hesitate to modify the types or sorts of data that are being used in the calculations.

Historical data can also be leveraged to calculate the loss function. History can serve as a guide to help estimate the expected number of casualties or monetary loss should different actions be taken. Again, forms of generative AI can serve as a white board to assist analysts in determining what the possible actions and costs could be, but human oversight is necessary to ensure that only feasible courses of action are considered and also ensure that loss estimates are accurate.

After the various components of Bayes risk are established, data pipelines can be created to automatically update risk as new data gets observed. That is, as conditions change on the ground, the likelihood functions will change, which will modify the Bayes risk for all actions under consideration. These pipelines can be automated, allowing decision authorities a real-time updating of risk.

Clearly, the vast amount of literature on risk indicates that this is a sticky problem that is easy to conceptualize, but quite difficult to solve. However, there are several areas that an operational unit interested in quantifying risk should focus on. In particular, instead of relying on potentially esoteric statistical calculations, a unit should focus on ensuring the process that they use in quantifying risk is correct and consistent. To do this, we advocate for employing a Bayesian risk model that combines subject matter expertise of analysts along with the operational experience of other staff sections to derive the risk of courses of action under consideration. Further, data standards should be ruthlessly enforced, and automation should be leveraged to assist in establishing data pipelines. While AI undoubtedly has a role in assisting this process, it should focus on modest applications and be used primarily to assist in structuring information from key data piles.

Conclusion: Thoughts on Future Evolution

This article began from a simple but uncomfortable observation: At precisely the moment when U.S. counterterrorism strategy has leaned harder into "risk-based prioritization," our conceptual and practical tools for assessing terrorism risk remain fragmented, unevenly validated, and only partially aligned with how practitioners actually make decisions. NSM-13 and subsequent policy statements have elevated "risk" to a central organizing principle, even as counterterrorism resources, forward posture, and political attention have declined. That shift narrows the margin for error. It makes the quality of our risk assessments a critical component of national security, a component of CT with an importance on par with our collection and kinetic capabilities.

We argued that improving terrorism risk assessment requires both a clearer conceptual foundation and more disciplined practice. Part I mapped a wide-ranging body of literature, showing that despite definitional variation, most work converges on risk as some function of threat, vulnerability, and consequence. It highlighted a toolbox of approaches (probabilistic risk assessment, Bayesian methods, game theory, power-law, self-exciting processes, structured professional judgment, RTM, and CACC), each with distinctive strengths and blind spots. Part II then examined how one influential practitioner framework, the Joint Risk Analysis Methodology, translates some of these ideas into an institutionalized process that guides the Department of Defense. Part III proposed a way to operationalize terrorism risk using Bayesian risk models, not as a black-box replacement for expert judgment but as a disciplined framework to impose standardization and rigor to assessments regarding assumptions, tradeoffs, and loss.

A key takeaway from these sections is that process matters at least as much as tools or technology.[117] We are currently awash in data and surrounded by vendors promising AI-enabled solutions. Yet much of what is being sold concerns only one component of a proper risk calculation: estimating the likelihood of events. Our core claim is that without a coherent and transparent process for defining the states of nature, eliciting and updating prior beliefs, specifying a realistic action space, and rigorously defining loss functions, no volume of data or algorithmic sophistication will save us from mis-specified risk. A more modern terrorism risk posture must therefore begin with basics:

First, practitioners need to properly define the possible states of nature (parameters) relevant to a theater, network, or problem set. This step is inherently creative and interpretive. It can be supported by generative AI that helps analysts explore plausible scenarios and configurations. What AI can do here is expand the imagination; what it cannot do is decide which states of nature are strategically meaningful. The analyst must remain firmly in the loop.

Second, institutions need standardized processes for deriving and eliciting prior probabilities over those states of nature. This is where existing terrorism risk literature can and should be used more systematically to inform priors, rather than sitting on the shelf as an abstract academic exercise. Prior elicitation should be explicit, documented, and revisitable, rather than buried in unspoken assumptions or "gut feeling." It is also essential that analysts and experts have some degree of calibration when providing assessments and probabilities across different agencies or subcomponents of a command.

Third, risk assessment should move beyond J-2 centric conceptions of threat and be treated as a genuinely whole-of-staff product. Incorporating J-3 and J-5 perspectives is essential to properly defining the courses of action that are actually available and the loss functions associated with them. Risk is not a property of a place or a group alone; it is a property of actions taken under uncertainty. That reality is captured in a Bayesian risk framework, but it should be reflected in institutional practice, not just in equations.

Seen from this vantage point, one of the most striking gaps in the current ecosystem is the disconnect between individual-level and group/network-level terrorism risk assessment. Instruments designed to evaluate individual extremism and mobilization (including but not limited to TRAP-18, ERG22+, DRAVY-3, and related SPJ-based tools) are comparatively more developed, more systematically evaluated against real-world data, and are tightly coupled to operational decision-making. By contrast, tools focused on network or theater-level terrorism risk (such as JRAM-based processes) lean heavily on structured professional judgment without commensurate attention given to bias, calibration, or validation.

A key avenue for future evolution, therefore, lies in building conceptual and practical bridges between these two worlds. Network-level risk frameworks should learn from the methodological rigor and evaluation culture that has grown around individual-based instruments: clearer factor definitions, explicit rating guidance, calibration exercises, and structured feedback loops. Conversely, individual-level tools can benefit from the broader contextual insights generated by network- and place-based approaches. Terrorism risk today is jointly produced by networks, local opportunity structures, and individual trajectories;

our assessment approaches should reflect that fact rather than relegating these domains to separate silos.

A second consideration for future work is to develop a framework for assessment that incorporates public opinion, political will, and competing strategic priorities. Terrorism rarely poses a risk to the sovereignty of the nation—models that assess threats may eventually need to consider how much the populace cares, what the pressures would be on policymakers, and how tactical, operational, and strategic responses take away from competing priorities that may put at risk larger national security objectives. The models heretofore apply both mathematical science and social science to the assessment of terrorism risk; there is also a nuanced art to understanding the human nature involved in deciding how hard and how fast to respond when developing a deterrent in a resource constrained environment.

A third priority for future work is systematic evaluation of prior U.S. government terrorism risk judgments and scores. At present, we know relatively little about how accurate our institutional risk assessments have been, where they have consistently over- or under-estimated threats, or how biases and assumptions have played out over time. Retrospective studies that compare earlier risk ratings, JRAM outputs, or NSM-13-aligned prioritizations with subsequent attack patterns, plots, or operational outcomes would provide an empirical basis for refining both processes and models. Such work not only improves calibration; it may also build institutional humility and transparency about the limits of foresight in a domain characterized by strategic interaction and deep uncertainty.

Finally, we have suggested a role for automation and AI in the evolution of terrorism risk assessment. Rather than chasing comprehensive "AI solutions" to risk, operational units would do better to enforce rigorous data standards, build automated data pipelines that update key components of Bayes risk in near real time (likelihoods, relevant indicators, environmental indices, and data on CT operations), and deploy AI primarily as a tool for structuring information, identifying anomalies, and supporting prior elicitation. It should not, however, be the final arbiter of risk. This division of labor plays to the strengths of both humans and machines: analysts and operators define the problem, the states of nature, and the loss landscape. Humans also bring context, nuance and an understanding of outliers to the system. Algorithms help keep the inputs current, disciplined, and consistent.

The argument here is not that a Bayesian risk model, or any other single framework, can resolve the profound uncertainties that define terrorism. It is that risk assessment must be treated as an explicit, structured, and contestable process, one that transparently integrates subject-matter expertise, operational judgment, and the best available data and models. In a strategic environment where U.S. counterterrorism efforts are asked to do more with less, the way we conceptualize and calculate terrorism risk is no longer a secondary technical issue; it is a central determinant of where and how we choose to accept risk, and at what potential cost. The reality is the national security enterprise will do less with less, but these statistical models and proper use of data help us 'do less' better and with greater efficiency. If the United States is to remain serious about "risk-based" counterterrorism, then terrorism risk assessment itself must be modernized (conceptually, institutionally, and technologically) to match the complexity and dynamism of the threats it seeks to understand. CTC

Citations

1 Gia Kokotakis, "Biden Administration Declassifies Two Counterterrorism Memorandums," Lawfare, July 5, 2023.
2 Nicholas Rasmussen, "Navigating the Dynamic Homeland Threat Landscape," Remarks given at Washington Institute for Near East Policy, May 18, 2023.
3 Harun Maruf, "US counterterror official warns of growing global threat," Voice of America, February 15, 2025.
4 For example, see Aaron Clauset and Kristian Skrede Gleditsch, "The Developmental Dynamics of Terrorist Organizations," *PLoS ONE* 7:11 (2012).
5 See, for example, Ismail Onat and Zakir Gul, "Terrorism risk forecasting by ideology," *European Journal on Criminal Policy and Research* 24:4 (2018).
6 Clauset and Gleditsch.
7 Ibid.
8 For examples of broad-based and specific evaluations of some of these types of tools, see "Countering Violent Extremism: The Use of Assessment Tools for Measuring Violence Risk," RTI International, March 2017; Ghayda Hassanm et al., "PROTOCOL: Are tools that assess risk of violent radicalization fit for purpose?" Campbell Systematic Reviews, 2022; Adrian Cherney and Emma Belton, "Testing the reliability and validity of the VERA-2R on individuals who have radicalised in Australia," Report to the Criminology Research Advisory Council Grant: CRG 40/21–22, June 2024.
9 For an overview of these nine instruments, see Anna Clesle, Jonas Knäble, and Martin Rettenberger, "Risk and Threat Assessment Instruments for Violent Extremism: A Systematic Review," *Journal of Threat Assessment and Management* 12:1 (2025). See also Caroline Logan, Randy Borum, and Paul Gill eds., *Violent Extremism: A Handbook of Risk Assessment and Management* (London: University College London Press, 2023); Caitlin Clemmow et al., "The Base Rate Study: Developing Base Rates for Risk Factors and Indicators for Engagement in Violent Extremism*," *Journal of Forensic Sciences* 65:3 (2020).
10 Beverly Powis, Kiran Randhawa, and Darren Bishopp, "An Examination of the Structural Properties of the Extremism Risk Guidelines (ERG22+): A Structured Formulation Tool for Extremist Offenders," *Terrorism and Political Violence* 33:6 (2021).
11 Christine Shahan Brugh, Sarah L. Desmarais, and Joseph Simons-Rudolph, "Application of the TRAP-18 Framework to U.S. and Western European Lone Actor Terrorists," *Studies in Conflict and Terrorism* 46:2 (2023).
12 José Luis González-Álvarez et al., "A Theoretical, Empirical, and Methodologically Based Instrument to Assess the Risk of Violent Jihadist Radicalization in Prisons: The DRAVY-3," *Terrorism and Political Violence* 36:3 (2024).
13 Ibid.
14 For examples, see John Horgan, Neil Shortland, Suzzette Abbasciano, and Shaun Walsh, "Actions Speak Louder than Words: A Behavioral Analysis of 183 Individuals Convicted for Terrorist Offenses in the United States from 1995 to 2012," Journal of Forensic Sciences, 2016; Mary Beth Altier, Emma Leonard Boyle, Neil D. Shortland, and John G. Horgan, "Why They Leave: An Analysis of Terrorist Disengagement Events from Eighty-Seven Autobiographical Accounts," *Security Studies* 26:2 (2017): pp. 305-332.
15 "US Violent Extremist Mobilization Indicators," Office of the Director of National Intelligence, 2021 Edition; "Mobilization to Violence (Terrorism) Research: Key Findings," Canadian Security Intelligence Service, n.d.
16 T. G. Thorley and E. Saltman, "GIFCT Tech Trials: Combining Behavioural Signals to Surface Terrorist and Violent Extremist Content Online," Studies in Conflict and Terrorism, 2023.
17 Andrew R. Morral et al., *Modeling Terrorism Risk to the Air Transportation System* (Santa Monica, CA: RAND, 2012).
18 Xijun Yao et al., "Assessment of Terrorism Risk to Critical Infrastructures:

The Case of a Power-Supply Substation," *Applied Sciences* 10:7,162 (2020); M.G. Steward, M.D. Netherton, Y. Shi, M. Grant, and J. Mueller, "Probabilistic Terrorism Risk Assessment and Risk Acceptability for Infrastructure Protection," *Australian Journal of Structural Engineering* 13:1 (2012).

19 Rongchen Zhu et al., "Modeling and Risk Analysis of Chemical Terrorist Attacks: A Bayesian Network Method," *International Journal of Environmental Research and Public Health* 17:2,051 (2020).

20 For example, see Aaron Clauset and Ryan Woodard, "Estimating the Historical and Future Probabilities of Large Terrorist Events," *Annals of Applied Statistics* 7:4 (2013).

21 For an overview of, and perspective on, spatial approaches to terrorism risk, see Paul Gill et al., "Chapter 4: Advances in Violent Extremist Risk Assessment" in Derek M.D. Silva and Mathieu Deflam eds., *Radicalization and Counter-Radicalization* (Leeds, U.K.: Emerald Publishing, 2020).

22 Gentry White, Michael D. Porter, and Lorraine Mazerolle, "Terrorism Risk, Resilience and Volatility: A Comparison of Terrorism Patterns in Three Southeast Asian Countries," *Journal of Quantitative Criminology* 29:2 (2013). For another regional example, see Samrat Chatterjee and Mark D. Abkowitz, "A Methodology for Modeling Regional Terrorism Risk," *Risk Analysis* 31:7 (2011).

23 Claude Berrebi and Darius Lakdawalla, "How Does Terrorism Risk Vary Across Space and Time? An Analysis Based on the Israeli Experience," *Defence and Peace Economics* 18:2 (2007).

24 Shahid Imran, "Geographical spread analysis of terrorist attacks in Pakistan," GeoJournal, 2023.

25 Jeff Gruenwald, Grant Drawve, and Brent L. Smith, "The Situated Contexts of American Terrorism: A Conjunctive Analysis of Case Configurations," *Criminal Justice and Behavior* 46:6 (2019).

26 Joseph Gregory DeLeeuw and William Alex Pridemor, "The Threat from Within: A Conjunctive Analysis of Domestic Terrorism Incidents in the United States, United Kingdom, and Ireland," *Perspectives on Terrorism* 12:4 (2018).

27 Katherine A. Boyd, "Modeling Terrorist Attacks: Assessing Statistical Models to Evaluate Domestic and Ideologically International Attacks," *Studies in Conflict and Terrorism* 39:7-8 (2016).

28 Elena Cantatore, Enrico Quagliarini, and Fabio Fatiguso, "Terrorism Risk Assessment for Historic Urban Open Areas," *Heritage* 7 (2024).

29 Berrebi and Lakdawalla.

30 Ibid.

31 White, Porter, and Mazerolle.

32 For example, see Henry H. Willis et al., "Homeland Security National Risk Characterization," RAND, 2018.

33 Julia Ebner, Christopher Kavanagh, and Harvey Whitehouse, "Assessing Violence Risk among Far-Right Extremists: A New Role for Natural Language Processing," Terrorism and Political Violence, 2024.

34 Isabelle van der Vegt, Bennett Kleinberg, and Paul Gill, "Proceed with caution: on the use of computational linguistics in threat assessment," *Journal of Policing, Intelligence and Counter Terrorism* 18:2 (2023).

35 Gideon Mwendwa et al., "Deciphering terrorist attributions: a global terrorism data-driven comparison of machine learning models," *Social Network Analysis and Mining* 15 (2025).

36 For other perspectives, see Barry Charles Ezell et al., "Probabilistic Risk Analysis and Terrorism Risk," *Risk Analysis* 30:4 (2010) and Paul Gill, et. al., "Chapter 4: Advances in Violent Extremist Risk Assessment."

37 Mark J. Schervish, *Theory of Statistics* (New York: Springer, 1995).

38 Gerald G. Brown and Louis Anthony (Tony) Cox, Jr., "How Probabilistic Risk Assessment Can Mislead Terrorism Risk Analysts," *Risk Analysis* 31:2 (2011).

39 Ezell et al. For another perspective on this, see Andrea Molle, "The Mathematics of Political Mayhem: A Computational Model for Predicting Stochastic Violence," Terrorism and Political Violence, October 2025.

40 Jason Merrick and Gregory S. Parnell, "A Comparative Analysis of PRA and Intelligent Adversary Methods for Counterterrorism Risk Management," *Risk Analysis* 31:9 (2011).

41 Ezell et al. Other scholars also discuss and/or use Bayesian risk approaches in relation to terrorism risk(s). For examples, see Merrick and Parnell; Jesus Rios and David Rios Insua, "Adversarial Risk Analysis for Counterterrorism Modeling," *Risk Analysis* 32:5 (2012); Zhu et al.; and Molle.

42 Molle.

43 Ezell et al.

44 Ibid.

45 Ibid.

46 For example, see John Major, "Advanced Techniques for Modeling Terrorism Risk," Journal of Risk Finance, 2002.

47 Yao et al.; Henry H. Willis and Omar Al-Shahery, "National Security Perspectives on Terrorism Risk Insurance in the United States," RAND, 2014; Ezell et al.; John Major; Louis Anthony (Tony) Cox, Jr., "Game Theory and Risk Analysis," Risk Analysis, 2009.

48 Cox.

49 Stef Janssen, Diogo Matias, and Alexei Sharpanskykh, "An Agent-Based Empirical Game Theory Approach for Airport Security Patrols," *Aerospace* 7:8 (2020). See also Ezell et al.

50 Kjell Hausken, Jonathan W. Welburn, and Jun Zhuang, "A Review of Game Theory and Risk and Reliability Analysis in Infrastructures and Networks," *Reliability Engineering and System Safety* 261 (2025). See also Cox.

51 Ezell et al.

52 Ibid.

53 Yaneer Bar-Yam, "Concepts: Power Law," New England Complex Systems Institute, 2011.

54 Quirin Schiermeier, "Terror prediction hits limits," Nature, 2015.

55 Clauset and Woodard, referencing Aaron Clauset, Maxwell Young, and Kristian Skrede Gleditsch, "On the Frequency of Severe Terrorist Events," *Journal of Conflict Resolution* 51:1 (2007).

56 Clauset and Gleditsch.

57 Clauset and Woodard.

58 Stephane J. Baele, "Power-Law Online Terrorism and Extremism," *Perspectives on Terrorism* XIX:2 (2025).

59 Alan G. Hawkes, "Spectra of some self-exciting and mutually exciting point processes," *Biometrika* 58:1 (1971).

60 White, Porter, and Mazerolle.

61 Ibid.

62 Alexandre Rodde and Justin Olmstead, "Into the Crowd: The Evolution of Vehicular Attacks and Prevention Efforts," *CTC Sentinel* 18:2 (2025).

63 Amarnath Amarasingam, Marc-André Argentino, and Graham Macklin, "The Buffalo Attack: The Cumulative Momentum of Far-Right Terror," *CTC Sentinel* 15:7 (2022). See also Julia Kupper et al., "The Contagion and Copycat Effect in Transnational Far-right Terrorism: An Analysis of Language Evidence," *Perspective on Terrorism* 16:4 (2022).

64 Nicholas Farnham and Marieke Liem, "Can a Copycat Effect be Observed in Terrorist Suicide Attacks?" International Centre for Counter Terrorism, March 2017.

65 Kristin G. Schneider et al., "A Reference Guide for Counter-Insider Threat Professionals: Structured Professional Judgment Tools," OPA Report No. 2021-067, January 2022.

66 Geoff Dean and Graeme Pettet, "The 3 R's of risk assessment for violent extremism," *Journal of Forensic Practice* 19:2 (2017).

67 Dean and Pettet citing Paul R. Falzer, "Valuing structured professional judgment: predictive validity, decision-making, and the clinical-actuarial conflict," *Behavioral Sciences and the Law* 31 (2013), p. 40.

68 Schneider et al.

69 Dean and Pettet.

70 "Structured Professional Judgment Tools, White Paper Series, Issue #3," The Threat Lab, OPA Report No. 2020-099.

71 For background, see https://www.vera-2r.nl/instrument

72 Brugh, Desmarais, and Simons-Rudolph.

73 Powis, Randhawa, and Bishopp.

74 Dean and Pettet.

75 Ibid.

76 Ibid. For a discussion about bias in terror risk assessments, see Gill et al., "Chapter 4: Advances in Violent Extremist Risk Assessment."

77 Ibid.

78 Risk Terrain Modeling Overview at https://www.riskterrainmodeling.com/overview.html

79 Zoe Marchment and Paul Gill, "Systematic review and meta-analysis of risk terrain modelling (RTM) as a spatial forecasting method," *Crime Science* 10:12 (2021).

80 Onat and Gul; Ismail Onat, "An analysis of spatial correlates of terrorism using risk terrain modeling," *Terrorism and Political Violence* 31:2 (2019); Zoe Marchment, Paul Gill, and John Morrison, "Risk factors for violent dissident republican incidents in Belfast: A comparison of bombings and bomb hoaxes," *Journal of Quantitative Criminology* 36:3 (2020); Jeff Gruenewald et al., "Innovative Methodologies for Assessing Radicalization Risk: Risk Terrain Modeling and Conjunctive Analysis," National Criminal Justice Reference Service, November 2021. For additional details, see Christine H. Neudecker, *Terrorism Risk Assessment* (Newark, NJ: Rutgers Center on Public Security, 2021); RH Hagan, "Filling Terrorism Gaps: VEOs, Evaluating Databases, and Applying Risk Terrain Modeling to Terrorism," Pacific Northwest National Laboratory, August 2016.

81 Rachel Monaghan, Bianca Slocombe, David McIlhatton, and John Cuddihy,

"Examining the relevance of 'EVIL DONE' to the current terrorist threat landscape in the United Kingdom," *Behavioral Sciences of Terrorism and Political Aggression* 17:3 (2025). For original framework, see Ronald V. Clarke and Graeme R. Newman, *Outsmarting the Terrorists* (Westport, CT: Praeger Security International, 2006).

82 Zoe Marchment and Paul Gill, "Spatial Decision Making of Terrorist Target Selection: Introducing the TRACK Framework," *Studies in Conflict and Terrorism* 40:10 (2022).
83 Marchment and Gill, "Systematic review and meta-analysis of risk terrain modelling (RTM) as a spatial forecasting method."
84 Ibid.
85 Ibid.
86 For example, see DeLeeuw and Pridemor.
87 Gruenewald et al.
88 Ibid.
89 Ibid.
90 DeLeeuw and Pridemor.
91 Gruenwald, Drawve, and Smith.
92 DeLeeuw and Pridemor.
93 Gruenewald et al.
94 For a review of how DHS has approached risk analysis, see "Review of the Department of Homeland Security's Approach to RISK ANALYSIS," National Academies Press, 2010.
95 Kokotakis.
96 Ibid.
97 Ibid.
98 Bryan Groves, Jerad M. Rich, and Kaley Scholl, "Risky Business Using the Joint Force's Framework for Managing Risk," *Joint Forces Quarterly* 111 (4th Quarter 2023).
99 "Joint Risk Analysis Methodology," CJCSM 3105.01B, December 22, 2023.
100 Ibid.
101 Ibid.
102 "Joint Risk Analysis Manual Slides," in possession of the author, undated.
103 "Joint Risk Analysis Methodology."
104 "Joint Risk Analysis Manual Slides."
105 "Joint Risk Analysis Methodology;" "Joint Risk Analysis Manual Slides."
106 "Joint Risk Analysis Manual Slides."
107 "Joint Risk Analysis Manual Slides;" "Joint Risk Analysis Methodology."
108 "Joint Risk Analysis Methodology."
109 Ibid.
110 Ibid.
111 Michael J. Mazarr, "Rethinking Risk in Defense," War on the Rocks, April 13, 2015.
112 Ibid.
113 Brian Dodwell, Don Rassler, and Paul Cruickshank, "Show and Tell: Expert Perspectives on Indicators and Warning Approaches for External Terror Ops," *CTC Sentinel* 17:10 (2024).
114 Ibid.
115 Kim Cragin, "A Better Way to Talk About Risk," Lawfare, July 6, 2025.
116 "Did Food Prices Spur the Arab Spring?" PBS, September 7, 2011; Tom Gjelten, "The Impact of Rising Food Prices on Arab Unrest," NPR, February 18, 2011.
117 The importance of placing emphasis on process was also reflected in a key survey of violent extremism risk approaches. See Gill et al., "Chapter 4: Advances in Violent Extremist Risk Assessment."

A View from the CT Foxhole: Admiral Frank Bradley, Commander, U.S. Special Operations Command

By Don Rassler

Admiral Frank M. Bradley has been the Commander of U.S. Special Operations Command (USSOCOM) since October 2025. Originally from Eldorado, Texas, ADM Bradley is a 1991 graduate of the United States Naval Academy. He has commanded at all levels of special operations, including Joint Special Operations Command, Special Operations Command Central, and Naval Special Warfare Development Group. He has multiple tours in command of joint task forces and was among the first to deploy into Afghanistan following the attacks of September 11, 2001.

CTC: You have been working CT for more than two decades. When you reflect on how the United States engaged in CT when you first became a SEAL to how the United States engages in CT today, what stands out to you?

Bradley: The increased cooperation between our integrated interagency and our allies and partners is quite remarkable. That increased cooperation was driven by our failure to see and disrupt the 9/11 attacks, but I believe this cooperation, coupled with the vigilance of our local and federal law enforcement enterprise is the reason there has not been a repeat attack of that nature. A second clear distinction is the increased trust/reliance that our elected and appointed civilian leaders have in the integrated interagency and SOCOM team. That trust is now empowered with a deeper understanding and knowledge of the art of the possible. We are more effective today at accomplishing our CT mission than we ever have been.

CTC: What is the toughest CT issue or challenge you have had to navigate through over the course of your career?

Bradley: The importance of truly working "By, Through and With" the local security forces of a region to defeat a terrorist organization is an important challenge. In the early years of the CT campaigns, we levered indigenous elements to support our largely unilateral efforts. Over time we realized that—to accomplish our mission—we would have to turn the territory over to that indigenous element to hold the security we had established. After a decade, the D-ISIS campaign in Iraq and Syria (2014-2019) and the C-al Shabaab efforts in Somalia (2010-2015) demonstrated an approach that was both illuminated and successful. The organizational inertia against "letting go" and trusting a partner force to own the solution was no small challenge. I am proud of our leaders who came to recognize the importance of this priority and those who led through it to achieve today's sustainable CT approach—with our allies and partners in the lead. Our empowerment and occasional acute action to render a particularly dangerous threat will remain a part of that sustainable approach, but it is far more economical—and effective—than it ever has been.

CTC: There is an idea that JNIM and/or al-Shabaab could potentially be encouraged to follow a path or model similar to the Afghan Taliban or new Syrian government, which could limit the type of regional and extraterritorial threats that these two movements pose in the future. What do you think of this idea?

Bradley: JNIM and al-Shabaab are ideologically salafi-jihadist terror groups with clear political goals including territorial control and governance of their countries. If they are willing to prioritize those tangible political goals over salafi-jihadist terrorism and agree to renounce violence as their principal approach to governance, there could be opportunity to address the terror threat through engagement or diplomacy. The new Syrian government rejected ideological hostility to the West, providing more room for cooperation. Before JNIM or al-Shabaab can follow the same path as the Taliban or the al-Sharaa government in Syria, the groups would need to reconsider their relationships with the wider salafi-jihadist movement.

CTC: The issue of adversarial convergence has been a Department of War area of concern, and there are unfortunately a lot of examples where we see concerning interactions and cooperation between America's state and non-state adversaries. Which areas concern you the most? Is there a vignette that stands out?

Bradley: Adversarial convergence challenges us when it creates a simultaneity problem—forcing the U.S. to prioritize limited resources against multiple facets of disparate, multi-domain threats. Additionally, alignment enables an adversary to offset their own shortfalls, which may then challenge us with new capabilities. For example, the Houthis, enabled by Iran, presented a threat to freedom of navigation in the Red Sea. Then, the Houthis began providing advanced weaponry and training to al-Shabaab. This further complicates freedom of navigation, threatens the safety of global commerce and U.S. military operations, all while increasing the demand for limited forces in the same region. The Russian/Iranian interdependencies are of interest as well. On the one hand, the Iranians have buttressed the Russian inadequacies on the battlefields of Ukraine, and though the Russians continue to lose their soldiers at an astounding rate, the mass of low-cost weapons the Iranians are providing them has allowed the Russians to remain active. Meanwhile, the Iranians have mortgaged their people's future and prosperity by funding the Russian's military adventure. While the short-term nature of these cooperative activities is prolonging the suffering of millions—on the battlefield and off—it is also providing the most stark example of the failures of their governance models. Ultimately, this collaboration will hasten their collective strategic failure.

CTC: What terrorist groups concern you the most today and what groups do you see having the potential to emerge as a homeland threat in the future?

Bradley: VEOs and terrorism remain a consistent and persistent threat, and both ISIS and al-Qa`ida are improving their ability to attack U.S. interests. At least two affiliates—al-Qa`ida in Yemen and ISIS-Khorasan—have the potential to emerge as a homeland threat and continue to seek to inspire, enable, and direct attacks. Both groups maintain strong ideological motivations to attack the United States and are drawing on ample recruits and funding while becoming more technological savvy.

Outside of VEOs, transnational criminal organizations (TCOs) and drug trafficking organizations (DTOs) in Mexico, Latin America, and South America represent an escalating threat to the homeland as well. These organizations are seeking to expand their revenue streams and tighten their grip on critical smuggling routes to the U.S. to deliver drugs that are killing Americans at an alarming rate. To do this, they use violence, coercion, and bribery to undermine governments and the rule of law.

CTC: The United States and its partners continue to place a lot of pressure on Islamic State networks in Syria and Iraq, and in Somalia. For example, in mid-September U.S. forces along with Iraqi counterparts, killed Omar Abdul Qader, who served as the Islamic State's head of operations and external security. How would you characterize the current state and threat posed by the Islamic State ecosystem, and how the United States has been trying to combat it?

Bradley: Both the current state of and the threat from the Islamic State is degraded compared to when it held territory … but it is a persistent one. While the physical caliphate was eliminated, as you note, ISIS continues to adapt. Progress against ISIS in one area is often undermined by ISIS expansion in another. For example, the loss of Omar Abdul Qader left ISIS in Iraq severely weakened and our Iraqi allies are effectively degrading its remnants. Unfortunately, the Islamic State is also expanding into West Africa, which then allowed another affiliate to assume a greater leadership role for the Islamic State enterprise. In other areas, like Afghanistan and Pakistan, the DRC, Mozambique, Somalia, and Syria, we see ISIS affiliates that endure episodic periods of increased CT pressure, and then immediately begin to regenerate lost capability when that CT pressure wanes. While not all those regions pose direct threats to the U.S., they are all still working together as part of a common enterprise and we do see them providing each other mutual support to various degrees. While not every Islamic State affiliate has the intent to attack the homeland, they all work together to provide those groups who do with access to more resources and capability than they would have had otherwise.

CTC: One of the first things that President Trump did once in office was designate six Mexican cartels as Foreign Terrorist Organizations (FTOs). This has raised questions about the potential role of special operations forces to combat them. How is the SOF enterprise thinking about this issue? What are some of the key considerations we need to navigate? What advantages does SOF bring to bear if used in the fight against these entities and how can SOF lead the CT enterprise through this new challenge?

Bradley: The designation of Mexican cartels as Foreign Terrorist Organizations (FTOs) by President Trump has sparked significant discussions about the role of SOF in combating these entities. One key consideration is the need for a comprehensive approach that integrates intelligence, direct action, and support to local forces. This approach was exemplified in the U.S. Plan Colombia, where SOF played a crucial role in training and advising Colombian military and police forces, enhancing their capabilities to combat drug trafficking and insurgent groups. Plan Colombia yielded significant outcomes, including a substantial reduction in coca cultivation and cocaine production, as well as the weakening of major insurgent groups like the FARC (Revolutionary Armed Forces of Colombia).

The success of Plan Colombia demonstrates the advantages SOF can bring to bear, such as specialized training, operational flexibility, and the ability to build strong partnerships with host nation forces. By leveraging these strengths, SOF can effectively contribute to the counterterrorism enterprise in addressing the threats posed by these newly designated cartels.

CTC: Increasingly, we are seeing the proliferation of drone use as a weapon in asymmetric conflict by terrorist groups against their adversaries—from Islamic State West Africa Province (ISWAP) fighters targeting the Nigerian military[1] and Houthis striking inside Israel[2] to their use recently by a drug-trafficking militia in Colombia in downing a police Blackhawk helicopter.[3] From your vantage point, how do weaponized drones in the hands of non-state actors and terrorist groups change the calculus for special operations? What concerns do you have about overcoming this threat vector?

Bradley: The proliferation of weaponized drones to non-state actors and VEOs presents a significant challenge for special operations forces. Weaponized drones provide non-state actors and VEOs a new capability that holds U.S. protection at risk and gives the enemy battlefield advantages never seen before. Until very recently, the ability to exploit the aerial domain and leverage it for a range of missions, including surveillance and attack, was limited to nation-states. Now, someone with a few thousand dollars and access to the internet can order a drone that takes high-resolution images and modify it to drop explosives. These drones also give threat groups the ability to pose a more significant threat to a wider target set in their operating areas. For example, the recent disruptions to airport operations in Europe demonstrate the ability of even unarmed drones to pose a real challenge.

SOCOM recognizes the critical need to stay ahead of such evolving threats and prioritizes innovation to counter these challenges. By fostering a culture of innovation and leveraging cutting-edge technology, SOCOM aims to maintain a strategic advantage over VEOs and non-state actors alike. A key aspect of this strategy involves working closely with partners to find

Admiral Frank Bradley

effective solutions. Events like SOF Week[a] play a crucial role in this collaborative effort, bringing together military leaders, industry experts, and international allies to share knowledge, develop new technologies, and enhance interoperability. By emphasizing partnerships and collective problem-solving, SOCOM ensures that it remains at the forefront of countering the threats posed by weaponized drones.

CTC: Technology is revolutionizing warfare and lowering barriers to entry to key types of tech—from drones to artificial intelligence, and 3D printing—and capabilities for terrorist groups and radicalized individuals. How is the U.S. CT community evolving and modernizing to meet the threat and enhancing or developing new CT capabilities to stay ahead of these challenges?

Bradley: We need to operationalize the notion of disruptive technology and use it to deter future war. We need to recreate a team of industry, academia, defense, warfighters, and the various ecosystems inside the United States. We need to recognize that to deter war today and avoid a future war, we must be able to meet those challenges of the day. Technological change is outpacing our procurement cycles. Our markets are innovating faster in many important areas than the pace of our contracting offices or of those acquisition cycles. Information is no longer the guarded property of governments alone. It is ubiquitous, crowdsourced, and exploitable by anyone with a will to look. Our adversaries in many cases adapt in weeks, leveraging the state of the market, not the state of the art.

While we transform over years with our traditional acquisition approach, those gaps, that gap in time and in pace of innovation, is a risk that can become existential. The time for us to evolve this system is now. Our challenge is to adapt before that existential threat presents itself and evolves into a crisis. We have to evolve ahead of the threat, ride the wave of technological change, and not be overrun by it.

CTC: Less resources have been devoted to CT over the past several years. This has meant that key resources or some tools that have been used for CT are now more focused on other problems and priorities. One area where this has been felt is the domain of intelligence, surveillance, and reconnaissance (ISR),[4] which has been a core aspect of modern CT operations. This has pushed the CT community to prioritize, innovate, and get more creative, but in some ways the issue remains a key constraint, as legacy ISR platforms still hold a lot of utility. How do you think about this dilemma and the pathway through it?

Bradley: The reduction in resources devoted to CT over the past several years has followed the reduction of the scope of the terrorist organizations. Airborne ISR has and always will be a key part of our tool kit, but increasingly, we are able to leverage the virtual domain to help us understand terrorist intent, plans, and coordination activities. With less resources being devoted to CT, SOCOM seeks to empower our partners and allies to achieve shared security objectives through their own use of both the increasingly available small UAS physical domain ISR as well as their own exploitation of the virtual domain as well. We accomplish this through platforms such as Operation Gallant Phoenix, which brings together military and law enforcement personnel of 32 countries to better understand and respond to current and evolving CT threats.

CTC: When you look forward and scan the near-term horizon to the future of terrorism, what are you concerned about? What gives you hope?

Bradley: Looking forward, I'm concerned that the underlying conditions that allowed groups like al-Qa`ida and ISIS to emerge still exist across much of the world. In many regions, the conditions don't just persist, they're getting worse, further exacerbated by world events like the Gaza crisis and poor governance driven by the Iranian influence across the Middle East. This creates a large and growing population susceptible to radicalization. Advanced technologies like cheap smart phones also make it easier for extremist groups to connect with these vulnerable populations and then direct them at us. As the world changes, my greatest concern is the rapidly accelerating ability of bad actors to connect and enable individuals with the capabilities to do outsized damage. My balancing hope is in the ever-resilient Western alliance of freedom-loving peoples who are more interconnected and complementary than ever. We are stronger together, and our cooperation is the bulwark against the ills of instability. CTC

a "Held in Tampa, Florida, Special Operations Forces (SOF) Week is an annual conference for the international SOF community to learn, connect, and honor its members. Jointly sponsored by USSOCOM and the Global SOF Foundation, the 2025 edition attracted over 19,000 in-person attendees." See https://sofweek.org/

Citations

1 Abiodun Jamiu, "Nigeria: ISWAP Extremists Launching Attack Drones," Deutsche Welle, April 16, 2025.

2 Abby Rogers, "Suspected Houthi Drone Attack Strikes Israeli City of Eilat," Al Jazeera, September 18, 2025.

3 Juan Forero, "Police Helicopter Downed by Drone in Colombia, Killing 12," *Wall Street Journal*, August 21, 2025.

4 "Senate Armed Services Committee Hearing on Posture of USCENTCOM and USAFRICOM in Review of the Defense Authorization Request for FY24 and the Future Years Defense Program."

The Changing Character of Terrorism and U.S. Counterterrorism

By Don Rassler, Kristina Hummel, Brian Dodwell, and Ned Curry

The competition between terror movements and counterterrorism forces is an interactive and iterative game, as the actions taken by one side are designed to defeat, circumvent, or shape the activity taken by the opposing players. To better understand these interactive dynamics, it is important to evaluate how terrorism and counterterrorism have been evolving. This article first takes high-level stock of how the spread, structure, scale, and speed of terrorism have been changing in recent years and highlights key challenges and implications for counterterrorism. It then evaluates the United States' ongoing effort to find a sustainable counterterrorism path, a journey that has been filled with challenges, benefits, dilemmas, and opportunities, and discusses how key factors have been shaping the direction, reach, and pace of change. An important takeaway from these reviews is that while the threat of international terrorism is not what it used to be, there is a lot of change occurring across the terrorism landscape. U.S. counterterrorism has also been undergoing some important shifts, and there are open questions about whether U.S. CT forces and assets will be spread further. If not managed carefully, change taking place across these two 'systems' could interact in ways that may disrupt CT progress.

In less than a year, the United States will mark 25 years since the terrorist attacks of September 11, 2001. The terrorism landscape today is markedly different than it was that morning, and even the elements that remain have evolved and adapted. The landscape has been impacted by various counterterrorism actions and world events that have affected states and non-state actors alike. There is perhaps no more critical time to take stock of the state of terrorism and counterterrorism and assess how the very character of both have changed.

This article proceeds in two parts. The first examines the current state of terrorism through the lens of four major categories: spread, structure, scale, and speed. While much has changed on the terrorism front over the last decade, let alone since 9/11, developments in these key domains over the past couple of years have been particularly acute. Identifying the global terrorism trends from these categories helps illuminate what might be in store in the coming years. The second part explores recent evolutions of U.S. counterterrorism and the United States' quest to find a sustainable CT path. It concludes with a review of key findings and implications.

The State of International Terrorism Today

Terrorism in 2025 presents a complicated picture. Across multiple dimensions—geographic spread, the organizational structure and alliances of groups, the scale and diversity of terror threat actors, and the speed of radicalization and mobilization—terrorism is both persistent and in flux. While the goal of the first half of this article is to describe the current state of terrorism today from a strategic vantage point, it is important to state plainly that such an endeavor could fill many volumes. Thus, the authors endeavor not to capture completely the current universe of threats, but rather to outline the broad contours of the threat landscape, selecting specific examples that elucidate the most pertinent trends and aspects of change.

It is also important to note that while the authors have organized these trends into four broad categories—spread, structure, scale, and speed—for ease of analysis/explanation, these should not be viewed as distinct or static categories in reality. Indeed, evolutions in one category can and regularly do impact developments in another. For example, a terrorist group's spread into a new geographic area may impact its structure over time, as seen with the development of al-Qa`ida affiliates in the Sahel. Similarly, increases in the number of FTO designations by the United States may curtail or otherwise change the geographic spread of the implicated groups. The purpose of isolating the categories is to better situate and analyze key trends in the terrorism space in a manageable manner. It is hoped that by

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

Kristina Hummel is co-Editor-in-Chief of CTC Sentinel *and an Instructor in the Department of Social Sciences at the Combating Terrorism Center at the U.S. Military Academy.*

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.

Major Ned Curry teaches courses in terrorism and international relations in the Department of Social Sciences at the United States Military Academy. An Army Reserve Intelligence Officer, he previously worked for the Bureau of Conflict and Stabilization Operations at the State Department (2019-2025).

taking these four aspects of the phenomenon in turn, the whole can be understood more clearly.

Spread: The Geographic Span of Terrorism

The story of the geographic spread of terrorism today is one of both expansion and concentration—a difficult combination to confront. While more countries (66) experienced at least one terrorist incident in 2024 than in any year since 2018,[1] terrorist activity is also increasingly concentrated in a small number of countries: 86 percent of all terrorism-related deaths in 2024 occurred in just 10 countries.[2] [a] Seven of those countries are in Africa, five in the Sahel specifically.[3]

Where once the global terror threat was concentrated in the Middle East and North Africa, today it is centered in the Sahel, specifically in the tri-border region between Burkina Faso, Mali, and Niger.[4] Indeed, according to the 2025 Global Terrorism Index, the Sahel accounted "for over half of all terrorism-related deaths in 2024."[5]

The data shows that while countries such as Pakistan, Afghanistan, Syria, Somalia, and Nigeria have been largely steady when it comes to significant impact by terrorism over recent years, Sahelian countries (Burkina Faso, chief among them[6]) have experienced a steep increase.[7] In 2023 and 2024, Burkina Faso was most impacted by terrorism globally.[8] Simultaneously, high-fatality attacks have punctuated the terrorism landscape—from Kerman, Iran, in January 2024 (the deadliest terrorist attack in the country since 1978) to the Crocus Hall attack in Moscow in March 2024 (the country's deadliest terrorist attack in 20 years).[9] [b] It is notable that both strikes were perpetrated by Islamic State Khorasan (ISK). In short, while terrorist groups have found consistently favorable conditions in the Sahel to engage in terrorism, certain networks are still capable of conducting devastating attacks in countries elsewhere.

The picture in 2025 has been bleak, particularly for Africa and the threats from the Islamic State and al-Qa`ida there. Findings from ACLED reveal that "over two-thirds of the Islamic State's global activity in the first half of 2025 was recorded in Africa."[10] Meanwhile, according to the Africa Center for Strategic Studies, militant Islamist groups linked to al-Qa`ida affiliate Jama'a Nusrat ul-Islam wa al-Muslimin (JNIM) today "account for 83 percent of all fatalities in the Sahel."[11] These groups have found ample ungoverned or under-governed territorial space in the region to exploit, and there have been no signs of abatement this year. Not only are groups in the region maintaining (or exceeding) their attack tempo of recent years,[12] they are increasingly weakening what exists of central governments there. The situation in Mali is deeply emblematic of this trend, where a crippling fuel blockade imposed by JNIM in the country since September is impacting Bamako directly and threatening the military junta in power.[13] This "expansion of its strategic economic warfare," according to some experts, is JNIM's "most significant show of strength to date."[14] While, according to one long-term observer, JNIM alone would not be able to take over Bamako currently, it could if it formed a coalition with other opponents of the government.[15] These developments only underscore that the Sahelian challenge will continue into 2026.

Meanwhile, consistent focal areas on the terrorism map persist, although some have been quieter than in years past. For example, in Afghanistan more than two dozen terrorist groups operate inside the country today.[16] In 2025, however, ISK has conducted far fewer attacks than in recent years.[17] It remains to be seen if this trend holds into 2026. Conversely, regions elsewhere face entrenched or resurgent threats. Syria is illustrative in this regard. According to recent Syrian Democratic Forces numbers, "Islamic State militants staged 117 attacks in northeast Syria through the end of August [2025], far outpacing the 73 attacks in all of 2024."[18] At a time when the U.S. presence there is shrinking[19] and the new Syrian government is attempting to consolidate control over the country, this resurgent threat has the potential to complicate local and regional security in 2026 and beyond.

Finally, the geographic bounds of the threat landscape were expanded considerably in 2025 following the U.S. designation of several Latin American cartels and criminal organizations and four European Antifa groups as foreign terrorist organizations. These include entities based in Mexico, Venezuela, Ecuador, Haiti, Germany, Greece, and Italy.[20] This widening of the geographic aperture has implications for confronting terror threats globally, especially given finite resources dedicated to counterterrorism and the uneven/constrained level of intelligence sharing between the involved countries.

It is worth remembering that while terrorist groups are often conceptualized as geographically bound, those boundaries can be expanded through attack plotting from afar and through the operational deployment of long-range systems (e.g., drones). Terrorist groups and their adherents are inherently opportunistic and seek to exploit seams and vulnerabilities. Today, there are terror groups such as ISK that engage and place emphasis on external operations, but there are also other groups that—while remaining centered in one specific area—have shown signs they may engage in more far-reaching terror operations at some point in the future. Take, for example, the 2019 case of Cholo Abdi Abdullah, a Kenyan national who at the direction of senior leaders of Somalia-based al-Qa`ida affiliate al-Shabaab sought and "obtained pilot training in the Philippines in preparation for seeking to hijack a commercial aircraft and crash it into a building in the United States."[21]

In a more recent example, there is growing concern that Hamas—a group that has never conducted a successful attack outside of Israel, the West Bank, or Gaza—is developing external operations capabilities in Europe and may seek to depart from the group's prior *modus operandi*.[22] Additionally, the Houthis have deployed drones and missiles at longer, and impressive, distances over the past five years, even demonstrating the ability to strike Israel. The Houthis' ability to strike from greater distances, and in turn expand the geographic area over which they can threaten and project kinetic power, is a leading-edge indicator that range may become more accessible for other terror groups in the coming years. In short, as the terrorism threat concentrates and deepens in known areas, there are signs and indicators that—at least for some groups—they may be seeking to spread terror further afield.

Structure: The Evolving Forms of International Terror

The structure of terror threats and their alliances are critical

a Those countries are Burkina Faso, Pakistan, Niger, Syria, Mali, Nigeria, Somalia, Democratic Republic of the Congo, Cameroon, and Russia.

b These two attacks were among the 10 deadliest terrorist attacks of 2024. See "Global Terrorism Index 2025," Institute for Economics & Peace, 2025, p. 94.

features to examine when assessing the threat landscape today. In 2025, the two most prominent salafi-jihadi groups continue to operate, to varying degrees, as an affiliate model. With its presumptive leader, Saif al-`Adl, inside Iran, al-Qa`ida has relied on a dispersed, decentralized franchise model in recent years to sustain counterterrorism efforts against it and to "weather the Islamic State storm."[23] Today, al-Qa`ida has affiliates in the Arabian Peninsula, the Horn of Africa, the Sahel, and South Asia.[24] In the Sahel and Horn of Africa alone, its branches—JNIM and al-Shabaab, respectively—are powerful, well-funded, and gaining ground.[25] As Colin Clarke and Clara Broekaert have noted, however, the franchise approach "has watered down what al-Qa`ida actually stands for, having a deleterious impact on group cohesion and brand identity."[26] But the ability of al-Qa`ida affiliates to remain, and to operate in pockets around the world, particularly in areas, such as the Sahel, where the United States has limited on-the-ground capability or local partnerships to stem their activities, means that continued focus is required.

Alternately, the Islamic State administered a "province" model almost since its inception.[27] Today, over six years after the end of its physical caliphate, some of those affiliates still exist—Islamic State Khorasan, for one—but placed on top of the group's constellation of wilayat is its General Directorate of Provinces, a kind of "superstructure that now oversees the provinces themselves" and provides coherence and connection within the network.[28] Aaron Zelin has warned that overlooking the GDP and "viewing only one or two of [the provinces] as a threat misunderstands that the allocation of responsibility and resources within the group's global network has spread, providing longer-term resiliency."[29] Furthermore, as noted by one analyst, the external operations threat posed by the Islamic State has become more multi-vector.[30] One need only look to the attacks in Iran and Russia in 2024, recent disrupted plots in Europe,[31] and two thwarted plots to assassinate the new leader of Syria[32] to find evidence of the endurance of the Islamic State in 2025, and likely into the future.

A key complicating factor is that some terror networks inspire and encourage individual supporters to conduct attacks in the countries where they reside. It is well established that the Islamic State, in addition to directed and enabled external operations, has encouraged attacks by inspired supporters in their immediate locales for years.[33] To wit, readers will recall that it has been less than a year since a 42-year-old American conducted a terrorist attack in New Orleans in support of the Islamic State.[34] It has been less than a month since several young men were arrested in multiple states in the United States and charged for allegedly plotting an Islamic State-inspired terrorist attack in Michigan.[35]

A complementary issue to consider is that the overwhelming majority of terror attacks conducted in the United States are conducted not by groups, but by individuals; it is the primary threat. While some of these individuals are inspired by groups, many others are not. One study used START data to show that, in the United States, "the number of radicalized young people with no formal allegiances or ties to recognized extremist or terrorist groups has increased by 311% in the past 10 years alone as compared to the past 5 decades."[36]

The rise in importance of terror threats posed by individuals and small cells—who usually operate under 'looser' or more amorphous forms of structure, or with no defined or discernable form of structure at all—is reflected in statements by senior U.S. government officials. For example, when characterizing 'top terrorism threats' from 2020-2024, the FBI Director issued some variation of the following statement during congressional testimony each year: "The greatest terrorism threat to our homeland has been posed by lone actors or small cells of individuals who typically radicalize to violence online and use easily accessible weapons to attack targets."[37]

The key takeaway: The threat posed by individuals and small cells has been a persistent feature. Not only has it broadened the forms of structure that CT investigators need to consider in the United States, it has also complicated the geographic 'spread' of the threat *and* changed the dynamics of terrorism risk, highlighting how structure and spread intersect.

Tied closely to the structure of these groups themselves are the alliances they form with other groups, and even states, and how they lead to different types of adversarial convergence. This cooperation presents challenges, as it creates opportunities for terror groups to enhance or diversify their capabilities. It also blends threat vectors, obfuscates networks and sources of activities, and compounds the challenge of understanding and combating these groups. Some alliances are more opaque than others—for example, the relationship between al-Qa`ida and Iran, where senior leaders of the group have lived for decades, has been the subject of much speculation and debate over the years.[38] Developments on the alliances front in 2025 have been complex and varied; it is useful to conceive of adversarial convergence as falling into two major categories: between non-state groups and between a non-state group and state. Several topical examples are outlined next.

Houthis/AQAP/Al-Shabaab: In the non-state/non-state category, one critical case is the triangular confluence that has developed between the Houthis, al-Qa`ida in the Arabian Peninsula (AQAP), and al-Shabaab. According to Michael Horton, as the Houthis have sought to expand supply chains and funding beyond Iran, they have increasingly turned to AQAP in Yemen, which in turn "has opened new doors for the Houthis to interact with Horn of Africa-based militant groups such as al-Shabaab."[39] The United Nations' Panel of Experts on Yemen has called the relationship between the Houthis and AQAP an "opportunistic alliance ... characterized by cooperation in security and intelligence, offering safe havens for each other's members, reinforcing their respective strongholds and coordinating efforts,"[40] a relationship it says has continued throughout 2025 in the form of operatives training, arms trafficking, and smuggling, and an agreement to "wage a war of attrition against [Yemeni] Government forces."[41] In the case of the Houthis and al-Shabaab, in exchange for weapons, training, and expanded economic opportunities for the latter, the Houthis receive support from al-Shabaab in its "disruptive piracy activity in the Gulf of Aden and Western Indian Ocean as well as from more diversified supply arteries."[42] The U.N. panel on Yemen reported last month that cooperation between the Houthis and al-Shabaab has intensified, particularly when it comes to weapons transfers and training "in the manufacture of sophisticated improvised explosive devices and drone technology."[43] Furthermore, there is even evidence that the Houthis have collaborated with Islamic State Somalia, coordinating on intelligence and procurement of drones and technical training.[44] These disparate groups' willingness to collaborate and to continue to leverage insecurity along a vital global trade route[45] has injected new complexity into an already-fraught terror picture in the region.

Houthis/China: In the non-state/state category, the newer

and evolving case of the Houthis and China represents a highly transactional alliance centered on pain for common opponents and gain for respective priorities. According to reporting at the beginning of the year, the Houthis have received "Chinese-made weapons for their assaults on shipping in the Red Sea in exchange for refraining from attacks upon Chinese vessels."[46] More recently, China has been reportedly "providing the Houthis with dual-use technologies such as satellite imagery and drone components," similarly to safeguard its shipping interests in the Red Sea.[47] This comes on the heels of U.S. Treasury action against Houthi leader Mohamed Ali Al-Houthi, among others, for communicating with officials from China "to ensure that Houthi militants do not strike" Chinese vessels traveling in the Red Sea.[48] Furthermore, just last month, the U.S. Commerce Department announced it had added "15 Chinese companies to its restricted trade list for facilitating the purchase of American electronic components found in drones operated by Iranian proxies including Houthis and Hamas militants."[49] Regardless of Beijing's objectives in this case—pragmatism, reciprocity, economic advantage—this covert alliance is illustrative of how state/non-state actor cooperation complicates the terror threat landscape.

Iran/Criminal Proxies: A state/non-state alliance of significant concern is the Iranian government's increasing use of criminal proxies to conduct attacks in order to maintain plausible deniability. According to one analyst, over the past five years, Iran has conducted 157 foreign operations, of which 22 involved criminal proxies and 55 involved terrorist proxies.[50] The U.S. government is endeavoring to respond to this threat: In March 2025, the U.S. Treasury Department sanctioned the Sweden-based transnational criminal organization Foxtrot Network, which it says had "orchestrated an attack on the Israeli Embassy in Stockholm, Sweden, on behalf of the Government of Iran" in January 2024.[51] A joint statement by the United States, the United Kingdom, Canada, and 11 European countries followed this summer, condemning "the growing number of state threats from Iranian intelligence services" against their countries, stating that "these services are increasingly collaborating with international criminal organizations" to target their citizens.[52] From Hell's Angels gang members in Canada[53] to the Kinahan Cartel in Ireland,[54] the list of criminal entities Tehran is willing to work with is growing. Furthermore, while Iranian "pragmatism" in its use of criminal intermediaries is not new, one scholar finds Iran's "use of criminal intermediaries now reflects a more structured approach shaped by modern constraints" against it.[55] In short, these alliances continue to be sought out for their "efficiency, cover, and reach."[56]

Scale: The Number and Diversity of Terror Threat Actors

The scale of the terror threat today, in terms of the number and volume of attacks and diversity of threat actors, is a critical variable when considering change in the terrorism landscape. As mentioned earlier, more countries experienced a terrorist attack in 2024 (66) than in any other year since 2018, and the Sahel has borne the brunt of the deaths caused by terrorism.[57] In fact, terrorism deaths in the Sahel in 2024 were 10 times higher than in 2019.[58] According to the Global Terrorism Index, the Islamic State and its affiliates were the deadliest terrorist organizations in the world in 2024, responsible for 1,805 killed in 22 countries.[59] That is the largest number of countries affected by Islamic State attacks since 2020.[60] The major terrorist organizations operating in the world today—the Islamic State, JNIM, TTP, and al-Shabaab—caused 11 percent more deaths in 2024, operating in 30 countries.[61]

When data from Myanmar is excluded, there was an eight percent increase in the number of terror attacks globally from 2023 to 2024.[c] But the volume of terror activity varies according to place, and the data contains a mix of 'good' and 'bad' stories. For example, while Afghanistan has witnessed a general decline in the number of terror attacks since 2020, Pakistan has experienced the opposite. According to GTI data, in 2020 there were 172 terror incidents in Pakistan. In 2024, that number jumped to 1,099—a more than 500 percent increase.[62] In the Sahel, since 2020 the number of terror incidents in Mali, Burkina Faso, and Niger has remained high but fluctuated over that same span of time. The upward rise in the number of fatalities from terror incidents in Niger and Burkina Faso from 2020 to 2024 is particularly concerning as it demonstrates that the ability for terror networks in that region to inflict harm has escalated. In Niger, for example, fatalities steadily climbed year over year: 262 fatalities were recorded in 2020, but by 2024, that number had risen to 930.[63] The terror fatality numbers of Burkina Faso, which rose from 666 in 2020 to 1,532 in 2024, are similarly bleak.[64]

Data on terrorism-related attacks and arrests from the European Union provides another window into the issue of scale, and the trend over the last several years is sobering. Arrests increased each year—aside from a slight dip in 2022—which could be seen as a positive development that law enforcement is getting ahead of the problem but could also indicate a greater number of individuals involved in terrorist offenses who merit arrest. Meanwhile, when it comes to attacks (completed, failed, or foiled), the trend is more mixed. The overall number of attacks in 2024 was over triple the 2021 figure, over double the 2022 figure, but less than half of the 2023 figure. These high-level stats are a reminder about the ebb and flow of terrorism and how CT in the European context still requires a consistent, and potentially even growing, amount of investigatory resources.

Table 1: Terrorist attacks (completed, failed, foiled) and arrests for terrorist offenses in the European Union (2021-2024)[65]

Year	Attacks	Arrests
2021	18	388
2022	28	380
2023	120	426
2024	58	449

Data released by the FBI and statements made by two FBI directors—Kash Patel and Christopher Wray—provide insight into threat changes and the scale of effort, including time, resources, attention, that has been required since 2019 to 'hold the line' and keep the number successful terror attacks in the United States low. In 2019, Director Wray shared that the Bureau had "about 5,000 terrorism cases under investigation."[66] Out of that total

c If data from Myanmar is included, "the number of terrorist attacks dropped by three per cent" over the same time period. As noted by the Global Terrorism Index, that drop was "primarily driven by an 85 per cent reduction in Myanmar." "Terrorism is spreading, despite a fall in attacks," Vision of Humanity, March 4, 2025.

around 850 were focused on domestic terrorism while the rest had an international terrorism nexus, including "about 1,000 cases each of so-called homegrown violent extremism and Islamic State" and "thousands of other cases associated with foreign terrorist organizations like al-Qaida and Hezbollah."[67] During congressional testimony four years later in 2023, Director Wray noted how "the number of FBI domestic terrorism investigations has more than doubled since the spring of 2020."[68] Wray also shared that in November 2023, the FBI was "conducting approximately 2,700" domestic terrorism investigations, and in September of the same year, the Bureau was "conducting approximately 4,000" international terrorism investigations—totaling roughly 6,700 terrorism investigations.[69] Nearly two years after that, in September 2025, Kash Patel noted how the Bureau was working on "1,700 domestic terrorism investigations, a large chunk of which are nihilistic violent extremism (NVE)" and "3,500 international terrorism investigations"—5,200 terror investigations in total.[70] While the domestic and international terrorism case numbers shared by Patel have somewhat declined from those shared by Wray two years prior, they still speak to an active terrorism threat environment and an overall terrorism investigation case load that has remained fairly steady, and which likely demands a considerable amount of Bureau resources.

Another way to conceive of the scale of international terrorism as a problem set is to look at who and what the United States considers a terrorist group, namely which entities it has placed on its foreign terrorist organization (FTO) list. This is a helpful high-level measure as the FTO list includes organizations that meet specific criteria, one of which is that the entity threatens "the security of U.S. nationals or the national defense, foreign relations, or economic interests of the United States."[71] So, the FTO list reflects those foreign terror organizations about which the United States has national security concerns—the terror entities it wants to keep an 'eye on' to monitor and, in various cases, to combat. In that way, the FTO list provides insight into how the scale, as reflected by the number and type, of foreign terror groups that are of concern to the United States is changing. It also provides insight into how the United States' use of the FTO list as a signaling tool has been evolving, especially under the Trump administration.

The overarching change is that FTO list has expanded considerably in scale, scope, and group type. As of November 24, 2025, 24 FTOs have been added to the designation list in 2025.[72] That is the single largest increase in a year since 1997 when the list was created and 28 were added. Meanwhile, only one entity was removed in 2025: Hay'at Tahrir al-Sham, the terrorist organization formerly headed by the new leader of Syria.[73] While some entities have been removed over the years,[d] the number of organizations the U.S. government deems a foreign terrorist group is only growing, and substantially so over the past year.

The designation of the 24 new FTOs is a seismic shift, as not only has it dramatically expanded the scale of the FTO list in terms of numbers, but it has also broadened the types of networks and groups that the United States frames as being a part of the terrorism problem set. Table 2 organizes the 24 recently designated entities into threat type categories to highlight this broadening of who the U.S. government considers international terrorists.

Table 2: Foreign Terrorist Organizations Designated by the United States in 2025

Type	Group
Cartel, Transnational Criminal Organization, Gang	Mara Salvatrucha (MS-13) Tren de Aragua Carteles Unidos Cartel del Golfo La Nueva Familia Michoacana Cartel del Noreste Cartel de Jalisco Nueva Generacion (CJNG) Cartel de Sinaloa Gran Grif Viv Ansanm Los Lobos Los Choneros Barrio 18 Cartel de los Soles
Iran Threat Network Proxies	Ansarallah (Houthis) Kata'ib al-Imam Ali (KIA) Harakat Ansar Allah al-Awfiya (HAAA) Kata'ib Sayyid al-Shuhada (KSS) Harakat al-Nujaba (HAN)
Anti-Fascist	Antifa Ost Informal Anarchist Federation/ International Revolutionary Front Armed Proletarian Justice Revolutionary Class Self-Defense
Ethnonationalist	Balochistan Liberation Army (BLA)

While the United States is unlikely to devote significant resources to monitor or combat all of these groups, it has signaled that some of them—such as the Mexican and Venezuelan cartels—are, and will be, a strategic priority. Thus, today, under the framework of terrorism, the United States must contend with a broad and diverse constellation of threats, which range from mainstay threats posed by core salafi-jihadi networks, such as the Islamic State and al-Qa`ida movements, to threats posed by state-sponsored or state-supported entities, principally enabled by Iran, to the recently designated cartels, transnational criminal groups, and gangs, and to a domestic terrorism landscape increasingly committed to mixed and composite ideologies.

A cross-cutting challenge is the danger posed by individual extremists—so called 'lone actors'—who have complicated the threats posed by many of these group types over the past decade, and who also represent their own form of risk through the idiosyncratic motivations that push radicalized individuals to at times act on their own terms without ties to formal terror networks. This shift to individuals acting on behalf of groups has broadly dispersed the 'who' and 'what' counterterrorism practitioners need to monitor and investigate, which presents detection challenges and makes the task of identifying threats harder than ever before.

d Twenty-one entities have been delisted since the list's inception, though one of those is Ansarallah (the Houthis), which was designated in January 2021, delisted in February 2021, and subsequently redesignated in March 2025. See "Foreign Terrorist Organizations," U.S. Department of State, Bureau of Counterterrorism, n.d.

These dynamics have implications for how the United States will manage resources as well as prioritize attention across this universe of terrorism threats in the short-, mid-, and very likely long-term. Indeed, since each of these types of groups/threats require specialized knowledge, including geographic or other forms of domain expertise, one potential danger of the rise in the number and type of FTO groups designated is that it could stretch an already stretched U.S. CT enterprise thin. This could lead to new gaps and seams in depth of coverage, or compound existing ones, which could stress, or generate new blind spots and, by extension, vulnerabilities. It could also pose challenges or further complicate the United States' ability to deploy limited CT assets and forces to more dispersed geographic locations, or to maintain the necessary amount of pressure or cadence of strikes and operations designed to continually attrit threats posed by mainstay networks, such as those from key Islamic State nodes. These risks could become even more acute if the campaign against cartels becomes considerably more taxing for the U.S. CT enterprise.

Speed: The Pace of Radicalization and Mobilization

A final category of evolution in the terrorism threat is speed—specifically, how long it takes individuals to radicalize and mobilize to violence. There has been much discussion of late suggesting that the radicalization and mobilization process is happening more quickly in this current environment, as characterized by the growing scale and spread of activity, and by the rapid proliferation and prevalence of online communications. This trend is further complicated by the rise in individual-driven forms of terrorism as a modality. These developments mean that counterterrorism forces have less time to identify, react, and intervene to prevent the development of a threat which—given its individual nature—can also be more dispersed.

While determining radicalization timelines is a particularly fraught exercise given the limited data available on what is an inherently private process by individuals, a handful of studies have attempted to measure these timelines. These studies generally conclude that while the increased pace of radicalization feels like a recent evolution, it has, in fact, been steadily climbing over the past several decades, with a couple ebbs and flows during that timeframe.

A November 2016 study by Jytte Klausen estimated radicalization timelines in a population of 135 American jihadism-inspired homegrown terrorism offenders convicted or killed between 2001-2015.[74] This estimate measured the time between the first indication that an individual showed an interest in jihadi ideology and the time when an offender is incarcerated or engaged in a terrorism event.[75] Across the full study group, the median timetable for the radicalization process was 4.2 years. After removing some extreme outliers at the higher end of the spectrum, this value was 3.2 years.[76] However, the typical radicalization trajectory contracted significantly during the last five years of the study, with the radicalization process taking an average of 5.3 years during the pre-2010 period, while dropping to 1.5 years during the 2010-2015 timeframe.[77]

A more recent study conducted by the National Consortium for the Study of Terrorism and Responses to Terrorism (START) compiled a database of over 3,000 extremists of all ideological persuasions who radicalized in the United States between 1948 and 2021.[78] As part of this effort, researchers assessed the "radicalization to mobilization" timeframes[e] of extremists in the 2007 to 2021 timeframe. Similar to the Klausen study, START researchers noted an increase in pace in the 2010 to 2014 period. Between 2007 and 2010, the percentage of subjects in the dataset who proceeded through the radicalization to mobilization process in less than a year hovered between 15 and 20 percent. But this number then steadily rose to just under 40 percent by 2014. Interestingly, there was a decline back down to 20 percent by 2017, but then a marked increase up to almost 50 percent by 2021.[f] In sum, there is empirical support for the more anecdotal sense that this problematic process is occurring increasingly fast. Although, while there does seem to be a surge in recent years, the acceleration of radicalization began at least 15 years ago, if not earlier.

Most assessments attribute the acceleration to the transformative development of online communication tools and social media applications. The Klausen study found a marked increase in the prevalence of the role of these tools occurring at the same time as the acceleration of the pace of radicalization. Of the offenders in their study who were radicalized before 2010, over 75 percent were assessed to have radicalized initially through personal contacts, while for those radicalized post-2010, it was nearly a 50-50 split between real-life sources and online inspiration.[79] This timing aligns fairly well with a George Washington University (GWU) study on online radicalization that highlights the emergence of a "second generation" of online radicalization in the mid- to late-2000s, one which carried forward to the late 2010s. This generation was

"Today, under the framework of terrorism, the United States must contend with a broad and diverse constellation of threats, which range from mainstay threats posed by core salafi-jihadi networks, such as the Islamic State and al-Qa`ida movements, to threats posed by state-sponsored or state-supported entities, principally enabled by Iran, to the recently designated cartels, transnational criminal groups, and gangs, and to a domestic terrorism landscape increasingly committed to mixed and composite ideologies."

e "Measured as the length of time between an individual's first exposure to extremist views and their date of arrest and/or criminal activity." "Profiles of Individual Radicalization in the United States (PIRUS)," Research Brief, START, University of Maryland, March 2023, p. 8.

f "Measured as the length of time between an individual's first exposure to extremist views and their date of arrest and/or criminal activity." "Profiles of Individual Radicalization in the United States (PIRUS)," Research Brief, START, University of Maryland, March 2023, pp. 8-9.

distinguished by the emergence of the large and public social media platforms, leading to a "more connected, user-generated internet."[80] Sharing extremist content across borders and directly linking to extremist content was revolutionary, leading one prominent analyst to claim, "Open social-media platforms changed the game."[81] As the study concluded regarding the "second generation," "The radicalization process now infiltrated every aspect of a subject's life, and a radicalizer could project influence into a living room or bedroom."[82]

The GWU study then identifies a "third generation" of online radicalization that aligns well with the surge in radicalization speed identified by Klausen as beginning in the late 2010s. This generation is characterized by decreased importance of organizations, increased ideological fluidity, more personalized motivations, and a more chaotic online environment.[83] As another study concluded:

Increasingly, the extremist landscape has fragmented into an ideologically diverse array of groups, movements, subcultures and hateful belief systems all simultaneously playing off one another. Facilitating this fragmentation is the increasingly central role of digital communications in extremist strategies, with movements using a broad range of mainstream and fringe digital platforms to organize, communicate, and plan in a decentralized fashion.[84]

In this most recent surge in radicalization acceleration, the dramatic proliferation of social media and the widespread use of encrypted communications tools present a dangerous combination. Social media platforms like TikTok offer ideological exposure, which can then lead to direct invitations to migrate to alternative platforms such as Instagram, Telegram, or Rocket.Chat, which offer more privacy and communication in closed or encrypted channels.[85] As a recent article in this publication noted, "Such 'safe spaces' provide fertile ground for harder to monitor indoctrination, ideological reinforcement, and even operational planning."[86]

Significantly, one of the other hallmarks of this latest generation of online radicalization is the increased prevalence of minors. The nature of this evolving information domain is tailor-made for the youth audience. As a recent study on the topic concluded, "Like no previous group, Generation Z have had their social and political life defined by social media and ubiquitous connectivity."[87] And this generation is notably tech-savvy, digitally native, and ideologically fluid.[88] As described by Nicholas Stockhammer, "Short-form videos, memes, and similar stylized imagery allow radical messages to be disguised in appealing formats, making them especially effective for engaging younger, digitally native audiences."[89] With extremist content proliferating on platforms such as TikTok and Discord, and with young online gamers reporting increasing encounters with extremist propaganda, the challenge of youth radicalization is only getting worse.[90] For example, German authorities have issued warnings that TikTok functions as a "radicalization accelerant" for vulnerable youth and labels the degree of this acceleration as "dramatic."[91]

There is evidence suggesting that age plays a factor in the pace of radicalization. For example, a study by the Canadian Security Intelligence Service determined that among a population of approximately 100 individuals who mobilized to violence in Canada, "young adults (under 21 years of age) and minors mobilize more quickly than adults. The mobilization process for youth, especially young travellers, is a relatively minimalist endeavour … Young adults and minors generally have fewer obstacles to overcome in their process of mobilization."[92]

But the issue of youth radicalization goes beyond the speed category. Circling back to the other categories of threat evolution discussed above, the perceived increase in extremist activity by children ties back to discussions about the scale, spread, and structure of the threat. Recent reporting is replete with stories about youth involvement in extremist activity. Some examples from just this month (November 2025) include:

- On November 7, a 17-year-old male student in Jakarta, Indonesia, reportedly detonated an improvised explosive device inside a mosque at a school located within a naval compound, injuring 96 people. In an interesting example of the ideological diffusion discussed above, initial reporting suggests the Muslim perpetrator was actually inspired by past white supremacist and/or nihilistic violent extremist attacks, although it is not yet clear if he subscribed to any specific ideology himself.[93]
- On November 7, German police announced the investigation of a 16-year-old suspect for sharing posts related to the Islamic State.[94]
- On November 6, Swedish prosecutors charged an 18-year-old Syrian-Swedish dual national who was identified during an undercover sting operation and accused of planning a suicide bomb attack on a Stockholm culture festival on behalf of the Islamic State. (The investigation began a year prior, when he was a minor.) He was also indicted, along with a 17-year-old boy, for planning a murder in southern Germany in 2024.[95]

These recent cases are indicative of what many analysts have highlighted as a new wave of extremism among children. The proliferation of this threat has not been isolated to one geographic region. For example, in the United Kingdom, police officials issued warnings in 2021 regarding what they saw as a new wave of extremists emerging among children in the country, citing the highest figures on record for the number of underage arrests for terror-related offenses.[96] By 2024, the Home Office reported that one in every five terrorist suspects in Britain was legally classified as a child.[97] Britain's youngest terror offender was sentenced in 2021 after recruiting members for a neo-Nazi group. He committed his first terror-related offense when he was 13 years old.[98] Across Europe as a whole, nearly two-thirds of Islamic State-linked arrests in 2024 involved teenagers.[99] This included the infamous August 2024 plot by three males aged 17 to 19 targeting a Taylor Swift concert in Vienna, Austria.[100] This youth trend also extended to Australia, where "counterterrorism operations exposed a network of youth who shared a 'religiously motivated violent extremist ideology' and were planning an attack."[101] As a result, "Australia elevated its terror threat level from 'possible' to 'probable,' citing a heightened vulnerability in its security environment due to emerging threats."[102]

The threats posed by the accelerating pace of radicalization and the disturbing rise in youth radicalization represent distinct trends in the evolution of global terrorism. These challenges, however, are tied together by the shared role played by the dramatic growth of digital communications in facilitating both trends. This is evidenced by how closely aligned the timelines of these trends are. And the fact that there is little evidence of a slowing down of the growing pervasiveness of online communication platforms suggests that both these challenges are likely to be present for the foreseeable future.

This reality poses significant challenges for the counterterrorism

community. First, the ubiquity of social media access and influence, especially among youth, poses numerous challenges for society that go far beyond just terrorism. But social media platforms do seem uniquely suited to the spread of propaganda and extremism due to the unrestricted global reach, low entry barriers, their capacity for anonymity, and their algorithm-driven content delivery.[103] It is essentially impossible for law enforcement to slow the spread of this material, as monitoring tools struggle to keep pace with the proliferation of messaging and content moderation efforts suffer from numerous limitations, both legal and practical. Second, the ease of access to end-to-end encrypted messaging tools by potential extremists make it increasingly difficult for counterterrorism practitioners to get inside terrorism plots and monitor the activities of radicalizing individuals. Finally, the increased speed of the radicalization process means that law enforcement and intelligence professionals are faced with an increasingly narrow window of time to overcome the increasingly difficult challenges just outlined.

The Changing Character of U.S. Counterterrorism

Since 2018, the U.S. CT community has been undergoing change and trying to identify what 'CT right' looks like. This period of transition has been characterized by "a shift in U.S. national security priorities; a complex, diverse, and ever-evolving threat landscape; and ongoing technological change that is transforming the worlds of extremism, terrorism, and counterterrorism."[104] A defining aspect of this period has been the prioritization of strategic competition as the leading U.S. national security priority, a shift which has led to a reduction in emphasis and resources devoted to counterterrorism. As a result, the U.S. CT community had to streamline; navigate tradeoffs; and innovate, modernize, and evolve. This transformation, which is still underway, has not always been easy, as it has been challenged by several points of tension.

U.S. CT in Transition: Key Considerations, Benefits, Drawbacks, and Tensions

The section examines how the United States has been trying to 'right size' CT over the past several years; how key factors have been shaping the direction, reach, and pace of change; and how dilemmas and points of tension have complicated and challenged the U.S. efforts to optimize CT and find a sustainable CT path.

In Search of Sustainable CT

Since at least 2018, the U.S. national security enterprise has been grappling with a key overarching question: What does a sustainable CT posture and commensurate level of CT resourcing look like and how can that be achieved?[105] The United States recognizes it needs to spend less time and resources focused on counterterrorism so that it can prioritize more strategic and capable threats, such as the pacing threat that China poses to the United States in various areas. This recognition led to what was arguably an overdue shift in 2018, whereby terrorism was identified in the National Defense Strategy (NDS) as a secondary, but still important and persistent, national security priority.[106] Since that time, the U.S. CT community has been trying to figure out what 'CT right' looks like during this era, and what level of resourcing, focus, and CT activity is required to sufficiently degrade and keep the threats posed by the Islamic State, al-Qa`ida, Iran and its proxy network, and other actors with international terrorism ambitions at a low enough level.

This has not been the easiest thing to do in practice. At a base level, there have been different views and debates about just how much CT matters given the nature and scale of threats posed by a rising China and other state adversaries. For example, 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."[107] While those distinctions can at times be helpful, they have also challenged U.S. efforts to look across these two priorities to identify "how and where these two priorities interplay and converge," so investments in each priority can be optimized and service the other when appropriate.[108]

Some of the United States' most vexing national security challenges involve the deep blending of both priorities—whether that is how Iran instrumentalizes terrorism as a core part of its foreign policy; how terrorism has been a key driver of violence and instability across the Sahel and West Africa; or how CT assistance has been a longstanding pillar of the United States' defense alliance with the Philippines, a nation whose strategic location would be important for any Taiwan or China-related contingency.

In these pages last year, one of the authors introduced the CT Return on Investment (CT ROI) Framework: 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."[109] A primary contribution of the framework is that it illustrates how CT activity functions as a form of threat mitigation *and* how it has also "evolved as a form of influence" that the United States can leverage to shape or achieve strategic competition goals.[110] For example, while the United States would like to move on from terrorism, for many partners—or potential partners—terrorism remains a preeminent security concern. Over the past two decades, the United States has developed a considerable amount of hard-earned CT currency, and it should leverage that currency to achieve other goals. It would be a mistake not to do so.

The United States is still living through and learning lessons about how prior policy decisions may have overlooked the ways in which CT and strategic competition nest. For example, in September 2025, President Trump made headlines after stating the United States wanted to get Bagram airfield in Afghanistan back from the Taliban. For two decades, Bagram functioned as a key logistical hub for U.S. CT activity in the country. According to *The Wall Street Journal*, Trump administration officials "are in discussions with the Taliban about re-establishing a small U.S. military presence at Afghanistan's Bagram Air Base as a launch point for counterterrorism operations."[111] The push is reportedly a "potential component of a broader diplomatic effort to normalize relations with the Taliban,"[112] but comments made by President Trump hint at other strategic motivations. In talking about Bagram, for example, President Trump noted how: "It's an hour away from where China makes its nuclear weapons" and "where they make their missiles."[113] From a strategic competition perspective, Afghanistan is a key location for U.S. forces and assets to be postured for missions that involve Iran and China.

The quest to find the right balance—a sustainable U.S. CT posture—has been a work-in-progress, and it has been complicated by various factors. For example, while the United States has been eager to make the shift and fully transition international terrorism into being a less resource-demanding problem, key terror networks also unfortunately get a say. Over the past decade, terror networks have found ways to disrupt the shift, and strategically distract the

U. S. Air Force Tech. Sgt. Jacob Kozlowski marshals in a C-130J Super Hercules at AB 101, Niger, on February 9, 2023. (Master Sgt. Michael Matkin/U.S. Department of War)

United States, even if only for limited periods. The tragic terror attack on October 7, 2023—a single event that ignited tensions and broader regional conflict in the Middle East, the repercussions of which still reverberate today—is an important case in point. As noted by Christine Abizaid, the former NCTC Director, the disruptive impact of the attack for the United States was profound:

> *We spent a lot of time trying to narrow our focus to only those most urgent threats to Americans. If a group wanted to conduct attacks against Americans, they were going to go to the top of our list. And yet, a group that wasn't necessarily interested in attacking Americans set off a chain of events in the Middle East that caused one of biggest strategic challenges for us as a country over the last couple of years.*[114]

Another key complicating factor has been fluctuations across administrations about *how* CT challenges should be handled—the approaches, instruments of power, and tools that should be prioritized, and at what levels. For example, in 2023, Nicholas Rasmussen—President Biden's DHS CT Coordinator—remarked that the United States was "in a place where we are less reliant on a strategy where we will be using aggressive direct action in the overseas environment to deal with counterterrorism threats."[115] That shift was reflected in National Security Memorandum 13 (NSM-13)—a key document that strategically guided the Biden Administration's CT approach—in which "Narrowly Focus Direct Action CT Operations" appeared as Line of Effort 4 after "Strengthen Defenses," "Build and Leverage Partner Capacity," and "Strengthen Capacity to Warn."[116] To help support Line of Effort 1—"Strengthen Defenses"—the Biden administration placed emphasis on domestic terrorism prevention as an important component of its strategy. Since January 2025, the Trump administration has prioritized other CT approaches by placing greater emphasis on offensive direct action, border security,[117] and illegal immigration; less emphasis is given to terrorism prevention programs. While some level of change in how the United States engages in CT is expected across time, and is the prerogative of any administration, the fluctuations and lack of consistency across time make it hard for the U.S. CT enterprise to mature efforts and develop efficiencies.

Not long after the release of the 2018 NDS, the United States started to scale back the level of resourcing for CT so more personnel and assets could be redirected to the China mission set and other priorities. Across time, this has "meant that there have been less resources across the U.S. government for counterterrorism."[118] It has also meant that the U.S. "counterterrorism enterprise and community [has had] to make harder choices about where resources can be devoted."[119]

The reduction in resources has had several positive benefits. Overall, it has been a good forcing function to initiate and drive change across the U.S. CT enterprise. It has pushed the United States to be more rigorous about how it prioritizes international terrorism threats, and what networks or threats require, or are

"CT resource constraints have pushed the United States to explore and get more comfortable with tradeoffs, including by investing in non-traditional CT partnerships."

more deserving of, U.S. CT attention, which is in more limited supply. As part of that effort, it has also pushed the United States to focus "on disrupting and degrading only the most dangerous VEOs (those demonstrating intent and capability to attack the U.S. homeland), while allocating fewer resources toward disrupting and monitoring VEOs which present a regional and/or local threat to U.S. interests."[120] The United States cares about these other terrorism threats, but at the end of the day, what matters most is protecting the U.S. homeland and the American people.

Less resources devoted to CT has also pushed the United States to identify and minimize areas where resources were not aligned with core CT priorities, where CT efforts were ineffective, or where the U.S. interagency had unnecessarily redundant, or overlapping, capabilities. The concern about CT 'bloat' and duplication of effort has been highlighted by researchers[121] and been a subject of congressional testimony. In 2018, during his nomination to be the next NCTC Director, Vice Admiral (Ret) Joseph Maguire fielded questions driven by concerns about redundancies and the growth and size of different NCTC directorates.[122] While some level of redundancy can be helpful,[123] these efficiency initiatives have generally helped to streamline and optimize the U.S. CT enterprise. But, at the same time, there have been concerns that some of these initiatives may have gone too far, as some have argued that they have eroded important CT capabilities.[124] Meanwhile, the reduction in manpower devoted to CT has also given new urgency to data and other modernization initiatives.

The CT resourcing environment has pushed the United States to lean more on partners to burden-share, by asking, or requiring, them to do more or take more ownership of localized terrorism challenges. As noted in NSM-13: "Foreign partnerships, already a key component of U.S. CT strategy and efforts, will take on increased importance."[125] This "will help to spread the CT resource burden" and enable the United States—at least in theory—to "leverage complementary CT capabilities and efforts, and produce more enduring results by empowering partners to assess, prevent, and mitigate terrorism threats in their own countries and regions."[126] Overall, the increase in emphasis placed on burden-sharing as a pillar of U.S. CT strategy during the Biden and Trump administrations is designed to offset the management of risk and "make U.S. counterterrorism efforts more sustainable."[127]

While the theory of CT burden-sharing has emerged as an important pillar of U.S. CT strategy, the track record of U.S. CT burden-sharing efforts have been more mixed in practice. Part of the reason, as noted by Christopher Maier, former Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict, is because:

> *There's a balance between being able to be proximate enough to be able to mitigate some of these threats and being able to do that with our partners and allies. In many cases, we're talking about partners who are not that capable, often dealing in a semi-permissive, if not permissive environment, for these non-state actors or CT problems because there's fundamentally not a lot of governance in these places.*[128]

In many cases, this has made it hard for the United States and its varied CT partners to translate tactical gains into strategic and sustainable gains. While areas of success are apparent—for example, the United States' partnership with the SDF was critical to the territorial defeat of the Islamic State in Syria and is largely viewed as an overarching CT success—challenging, or more mixed cases, are also easy to find. While the United States developed effective CT units and partners that achieved important tactical gains in Afghanistan and Iraq, the capacity and willingness of both governments to progressively manage and take broader ownership of the CT fight, and to translate tactical gains (along with the United States) into strategic wins was limited. In the Afghanistan case, the result was a collective security failure and the collapse of the Afghan government. In Iraq, the results have been more nuanced. The poor performance of Iraq's security forces was a key factor that led to the rise and territorial expansion of the Islamic State in 2014, but Iraq's CT forces were also a key partner that helped to enable the defeat of the network and to generally contain the Islamic State's violence in Iraq since.

CT resource constraints have pushed the United States to explore and get more comfortable with tradeoffs, including by investing in non-traditional CT partnerships. The United States' CT cooperation with the new Syrian government[129] and areas where the Taliban regime and United States have shared threat concerns[130] speak to this. The environment has also helped the United States to strengthen ties and cooperation with other mixed record partners, such as the Pakistani government, to attrit and degrade the capabilities of groups such as ISK where there is mutual interest.[131]

But the reduction in resources for CT has also had downsides, as it has created, or compounded, various challenges. One high-level impact is that it has led to less manpower and bandwidth devoted to CT, which has affected the number and type of threat networks the U.S. CT community can monitor, or at least monitor closely with less tradeoffs. The danger is that this could create blind spots, especially for groups such as Hamas or Lashkar-e-Taiba that are primarily driven by local and regional interests, but that have also explored and taken steps toward international terrorism.[132] It could also limit the United States' ability to monitor, evaluate, and keep close tabs on other known risks such as the detention of ~10,000 Islamic State prisoners in northeast Syria.[133]

The erosion of expertise—which has been driven by multiple causes including retirements and natural attrition, the movement of personnel to other priorities, and CT manpower cuts—has compounded the challenge. Today, not only are there less people working in CT, but there are also less seasoned experts still working on this complicated and evolving problem set. A danger is that this could lead to gaps in knowledge, inefficiencies, and vulnerabilities especially as the number and type of terror groups that the United States needs to monitor expands.

Importantly, the reduction in resources has led to changes in the posture of U.S. CT and how the United States assesses and accepts terrorism risk. As noted by Matthew Levitt: "By definition, shifting away from two decades of counterterrorism premised on an

"While the full impact of multi-year cuts to the U.S. CT enterprise is not yet known, there are ongoing debates about what CT 'right' looks like. One concern that has been expressed is the danger of overcorrection, as recent goal line saves in the United States and Europe illustrate how there is not much room for error."

aggressive forward defense posture and toward one more focused on indicators and warning means assuming some greater level of risk."[134] The shift has had practical impacts, which have complicated the ability of the United States to 'see' and make sense of key threat environments, and develop options for CT activity. For example, as noted by Russ Travers in 2019: "As we draw down military forces we will have less human intelligence and intelligence, surveillance, and reconnaissance capability in theater. There will be less liaison with on the ground partners."[135] In addition to affecting collection strategies, this has meant that terrorism risk assessments, which have always been an important part of U.S. CT strategy during the post-9/11 era, have become even more important. The enhanced emphasis placed on risk is reflected in NSM-13 and in statements by senior U.S. CT officials. In 2023, for instance, the DHS Coordinator for CT noted how the Biden administration's "counterterrorism strategy focuses more on risk management and risk mitigation."[136] It also was oriented around a more "defensive counterterrorism strategy" that had "much less margin for error."[137]

It was a shift that the United States did not always get right at the time, as there were some close calls. The most noteworthy case was the arrest in 2024 of eight Tajik nationals over terrorism concerns and suspected ties to Islamic State members after they had entered the United States through its southern border.[138] According to *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."[139] The incident raised alarm bells in the counterterrorism community because even though nothing tragic happened, the layered system that the United States has constructed to prevent acts of terror only caught the individuals "on the last line of defense—after they were already in the United States."[140]

These types of close calls have also been an issue in Europe. For example, in the United Kingdom between 2017 and 2024, "Police and security services … [in the U.K.] stopped 43 late-stage terror plots …, three of which were in [2024] … with some of these being 'goal line saves.'"[141] These dynamics highlight the persistence of the terrorism threat and how shifts in focus, resources, and risk tolerance have been stressing on the ability of CT elements to detect and disrupt threats at earlier stages of planning.

Shifts in resources have also led to other important changes in U.S. CT orientation and capabilities. For example, in 2021, the focus of Joint Task Force Ares—a key Cyber Command task force that was created in 2016 to degrade and disrupt Islamic State and other terrorist activity online—changed its primary point of orientation. As noted by the commander of U.S. Cyber Command at the time: "We are also shifting JTF-Ares' focus (though not all of its missions) from counterterrorism toward heightened support to great power competition, particularly in USINDOPACOM's… area of responsibility."[142] Resourcing shifts away from tacking online dimensions of the terror threat have been compounded by cuts and a similar general reduction in focus across the private sector. For example, Adam Hadley, executive director of Tech Against Terrorism, recently noted that online terrorist content is no longer a major focus at tech companies.[143]

Decisions about CT resourcing have also been challenged by changing security conditions and the actions of adversaries in key areas that affect the conduct and logistics of U.S. CT. One area where this has been felt is airborne ISR. As noted by Christine Abizaid, the former Director of NCTC, during an interview in this publication in 2025:

> *We have limited airborne ISR, we have limited strike capacity that can reach various parts of the world, we have a range of threat actors and associated plotting against the United States, and so this also becomes a cost-benefit analysis of how you use your precious resources to best effect when you're dealing with a diverse array of threats.*[144]

Global events have certainly challenged and stressed this limitation even more. For example, in 2024, the Department of Defense lost access to a key military base in Niger "5 years after building a $110 million drone base" in the country.[145] The impact was that the United States' "ability to conduct ISR within the Sahel … has been severely degraded."[146] It has also been reported that during Operation Rough Rider, the Houthis downed at least seven MQ-9 Reaper drones, "a loss of aircraft worth more than $200 million."[147] These are not insignificant losses, and they likely have a bearing on where and how the United States can engage in CT.

Another downside of CT cuts is that modernization is not a switch. It takes time and considerable resources to build, test, and refine new systems and pipelines, and to integrate and educate the force about new processes and technologies developed for CT.[148] It also requires the right type of talent. This has arguably led to a point of tension: The U.S. CT enterprise needs to modernize and accelerate existing modernization efforts so it can optimize; but it is not clear, given the resource environment for CT, that it has the appropriate level of resources and time to do so at the scale and speed needed.

While the full impact of multi-year cuts to the U.S. CT enterprise is not yet known, there are ongoing debates about what CT 'right' looks like. One concern that has been expressed is the danger of overcorrection,[149] as recent goal line saves in the United States and Europe illustrate how there is not much room for error. There is also the need to avoid, and fight against, complacency; a self-initiated threat that always lurks. In the months and years ahead, the United States' quest to find the right balance will also need to contend with the broadening of CT priorities and focus areas under the Trump administration, and how that impacts the work of the CT community in practice. As noted in the first section of this article, not only are there now more FTO-designed groups that the U.S. CT enterprise needs to monitor, but the different types of groups represented require different forms of expertise and the potential,

broader geographic spreading of limited U.S. CT assets, capabilities, and manpower.

As others have noted, for the United States, part of the pathway forward to sustainable CT lies in recognizing that while there have been challenges and failures, "what we have built works, and it's not broken … it's important to identify and reinforce the successes we've had in the CT sphere."[150] Thus, while embracing change and evolving U.S. CT are critical parts of the way forward, those factors should be balanced against consistency and "a sustainable investment in a community of professionals whose only job is to focus on CT and to tell policymakers when it's time to take action against our worst terrorist adversaries."[151]

The future of U.S. CT will also need to contend with other important shaping factors. For example, compared to a decade ago, today's CT landscape contains a broader and more diverse mix of "stakeholders or 'players' who either have been meaningfully shaping, or have a role in, the world of counterterrorism and how specific counterterrorism actions or responses take place."[152] This includes states such as Turkey, Qatar, and the United Arab Emirates that are playing more assertive and in some cases central roles in the CT arena, and also nations like China and Russia that are leveraging CT as a form of influence in key areas to achieve their own interests, or to contest, counter, or provide an alternative to U.S. presence and access in strategic areas. It also includes the rise and development of commercial counterterrorism as a sector, and how non-state actors and private companies, such as technology platforms, have been shifting who "designs, manages, owns, and has access to, or influence over, specific platforms and approaches."[153] For instance, when it was founded in 2017, the Global Internet Forum to Counter Terrorism had four private sector members; by 2025 that number had grown to 33. Thus, a core driver of the future of U.S. CT is going to lie in how the United States situates itself and leads, or does not lead, in this more complicated CT landscape that is more saturated with equities, opportunities, competitive dynamics, and risks.

How the United States approaches partnerships will be an important barometer to watch, as while the United States has spent the last several years streamlining its own priorities and optimizing how the interagency engages in the practice of counterterrorism, there are a lot of opportunities for the United States to learn from, to enhance, to integrate with, and to optimize how it engages with and makes strategic and operational use of private sector partners. It can even be argued that the future evolution of U.S. CT will be conditioned on how the United States optimizes these types of relationships, as the potential they hold could unlock and radically transform the speed and efficiency of counterterrorism, and better position the United State to respond and deal with the challenges posed by the evolving spread, structure, and scale of terrorism noted earlier.

Conclusion

U.S. CT must contend with changes and complexity associated with the spread, structure, scale, and speed of terrorism threats. This is not an easy task because over the past several years, the U.S. CT enterprise has been determining what CT 'right' looks like during an era with less resources and lower prioritization. As the United States continues that quest, it is important that it evolves intentionally in relation to key changes and trends affecting the terrorism threat environment. This is important because changes across the four terror threat factors—spread, structure, scale, and speed—could either complicate U.S. CT efforts or demand greater U.S. leadership and attention in the future.

"The steady number of terrorism cases in the European Union and United States over the past several years also highlights how considerable resources are required to 'hold the line' and keep the number of terror attacks at low levels, despite core al-Qa`ida and the Islamic State having been significantly degraded and diminished."

When it comes to spread, the United States and its partners have had to contend with a geographic shifting of terrorism to other regions, such as the Sahel, over the past several years—a dynamic that has expanded the portfolio of threat networks that need to be understood and more closely monitored. This shift has created other geographic concentrations, fronts where affiliates of older mainstay jihadi networks have found space to control sizable amounts of territory, threaten local governments and regional stability, and conduct operations across borders. In the Sahel, an area where the U.S. government has less knowledge, influence, and reliable partners, it appears—absent some type of arresting mechanism—that JNIM is poised to expand its area of influence, consolidate areas of local control, or both, a dynamic which is likely to further complicate the trajectory of terrorism in the region, and potentially beyond, in the near- to mid-term.

The evolving structure of extremism and terrorism presents similar challenges. It can be argued, as some researchers have, that the Islamic State has evolved its own structures in response to CT pressure. That is an important win. But it is also important for the United States to take stock of those changes and reflect on where additional shifts may be needed to counter those Islamic State movement adaptations, especially when they pertain to external operations, which are increasingly multi-vectoral. The fact that the primary terrorism threat that the United States has had to contend with over the past several years is attacks from individuals and small cells similarly illustrates just how far the United States has come in fracturing the capabilities of key terror organizations, primarily al-Qa`ida and the Islamic State. Yet, there are lessons to be learned on this front, too, as while the Islamic State's general dependence on inspiring—and to a lesser extent enabling—radicalized individuals to conduct acts of terror on its behalf is a sign that things have been 'working,' the persistent ability for the Islamic State to remain an attraction and a source of inspiration highlights how the fight is far from over. The evolving ways in which terror networks have been looking past ideological distinctions and practically collaborating with other terror networks, criminally motivated individuals and entities, and states is also an issue that has been affecting the character and structure of threats, and it seems likely that it may also be a driver that shapes its future evolution and form.

One seam that may need tightening is how offensive and defensive aspects of CT are synchronized. For example, it is important that

kinetic pressure placed against key international terror networks abroad is disrupting key nodes generally, but that it also diminishes their ability to engage in 'reach' online and to inspire, enable, and shape the actions of sympathizers back 'home' and in other nations. It is ironic that at a time when the Islamic State needs to rely on its online presence more, U.S. and international efforts focused on terrorism activity in this domain do not appear to be as strong as they have been in the past.

To improve security, it is also important that offensive 'away' CT activity be bolstered by stronger defensive CT measures that lean forward in a similar way. The domestic legal frameworks that guide counter small unmanned aerial systems activity is one area where stronger defense capabilities and measures are not just appropriate but needed and would likely go a long way in complementing U.S. CT efforts to mitigate the threat abroad.

Public-private partnerships hold a lot of potential and are a key area where U.S. CT activity can be further optimized to enhance or evolve existing approaches; better tackle areas, such as terror activity online or drone countermeasures, where additional assistance would likely be helpful; and develop new methods. The embrace of these forms of collaboration and partnering will likely lead to more efficient CT; it could also lead to new CT structures and changes in how the U.S. government organizes itself for CT.

The scale of today's terrorism threat, as reflected by the number of attacks and diversity of terror networks that want to harm the United States, has meant that U.S. efforts to prioritize terrorism threats—where and when it can devote time and resources—are more important than ever. The steady number of terrorism cases in the European Union and United States over the past several years also highlights how considerable resources are required to 'hold the line' and keep the number of terror attacks at low levels, despite core al-Qa`ida and the Islamic State having been significantly degraded and diminished.

It is still too early to know how the addition of 24 new entities to the foreign terrorist organizations list by the Trump administration in 2025 will affect the issue of scale. Also unknown is how it may impact the spread and deployment of U.S. CT forces, or how it may divert U.S. CT attention from other terrorism threats over the short- to mid-term.

To help manage the challenge of scale and offset terror risk, the United States has placed greater emphasis on CT burden-sharing, with a mixed record of success. In some cases, this has required that the United States get more comfortable with tradeoffs and prickly alliances oriented around common threats. For example, the United States' CT cooperation with the new Syrian government has thus far been productive, and depending upon how it evolves, it may end up being a key model that it looks to emulate elsewhere.

In today's environment, thanks to the transformative impact of technology, speed effects nearly everything, and it has created challenges and opportunities for terrorism and CT. The U.S. and global CT communities are still navigating how to deal with the increased speed of radicalization and the shortening of time it appears to be taking for radicalized individuals to mobilize. The trend, which seems likely to continue, has made it harder for CT investigators to identify who presents a threat from a broadening sea of 'noise' and respond at commensurable speed. Technological change has also lowered the barriers to entry and made it easier for youth and minors to access and engage with extremist content, which has led to an unfortunate rise in terrorism cases involving minors in many nations.

While not fully here yet, speed also lurks as an operational terrorism threat vector. It is not hard to find evidence, from the accessibility of capable fast-moving FPV drones that can be purchased readily online to tactical knowledge about how drones are being operationally used and weaponized in Ukraine, to see that drones moving at speed will shape the future of terrorism too. But, if the United States embraces and wields technology right and leads with vision, speed can also be a force multiplying asset and help the United States to optimize the structure, scale, and spread of its response to the complex and varied terrorist threats it will face tomorrow and further into the future. CTC

Citations

1 "Global Terrorism Index 2025," Institute for Economics & Peace, 2025, p. 2.
2 Ibid., p. 12.
3 Ibid., p. 2.
4 Ibid., pp. 4, 34.
5 Ibid., p. 2.
6 Ibid., p. 21.
7 Ibid., p. 21.
8 Ibid., p. 21.

9 Ibid., p. 94.
10 Ladd Serwat, Héni Nsaibia, Miriam Adah, Peter Bofin, and Mohamed, "Q&A | The Islamic State's pivot to Africa," ACLED Data, September 4, 2025.
11 "Africa Surpasses 150,000 Deaths Linked to Militant Islamist Groups in Past Decade," Africa Center for Strategic Studies, July 28, 2025.
12 Priya Sippy and Jacob Boswall, "How an al-Qaeda offshoot became one of Africa's deadliest militant groups," BBC, July 6, 2025.
13 Rachel Chason, "Islamist extremists have taken this country to the brink," *Washington Post*, October 21, 2025; "Mali's economy near standstill amid JNIM fuel attacks," RFI, November 5, 2025.
14 Chason.
15 Wassim Nasr, "Jihadists' fuel blockade squeezes Mali's military rulers," France 24, November 4, 2025.
16 "Thirty-fifth report of the Analytical Support and Sanctions Monitoring Team submitted pursuant to resolution 2734 (2024) concerning ISIL (Da'esh), Al-Qaida and associated individuals and entities," United Nations, February 6, 2025, p. 16.
17 "The Islamic State in Afghanistan: A Jihadist Threat in Retreat?" International Crisis Group, July 16, 2025.
18 Sudarsan Raghavan, "Islamic State Rises Again in Syria, Filling a Void Left by U.S.," *Wall Street Journal*, October 22, 2025.
19 Christopher M. Blanchard, "Syria: Transition and U.S. Policy," Congressional Research Service, updated September 5, 2025.
20 "Foreign Terrorist Organizations," U.S. Department of State, Bureau of Counterterrorism, n.d.; "Designations of Antifa Ost and Three Other Violent Antifa Groups," U.S. Department of State, November 13, 2025.
21 "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.
22 Matthew Levitt, "Hamas Plots in Europe: A Shift Toward External Operations?" *CTC Sentinel* 18:10 (2025).
23 Colin Clarke and Clara Broekaert, "The Global State of al-Qa`ida 24 Years After 9/11," *CTC Sentinel* 18:9 (2025).
24 Ibid.
25 Ibid.; "Al-Shabaab's 2025 Offensive and the Unraveling of Somalia's Federal Counterinsurgency," Soufan Center, July 24, 2025; Rachel Chason and Adrián Blanco Ramos, "A powerful, opaque al-Qaeda affiliate is rampaging across West Africa," *Washington Post*, June 8, 2025; "Annual Threat Assessment of the U.S. Intelligence Community," Office of the Director of National Intelligence, March 2025.
26 Clarke and Broekaert.
27 Caleb Weiss, Ryan O'Farrell, Tara Candland, and Laren Poole, "Fatal Transaction: The Funding Behind the Islamic State's Central Africa Province," Program on Extremism at George Washington University, 2023, pp. 14-15.
28 Aaron Y. Zelin, "A Globally Integrated Islamic State," War on the Rocks, July 15, 2024.
29 Ibid.
30 Authors' correspondence, Lucas Webber, November 2025.
31 Sune Engel Rasmussen, "Teenage Terrorists Are a Growing Threat to Europe's Security," *Wall Street Journal*, May 4, 2025.
32 Timour Azhari and Mahmoud Hassano, "Exclusive: Syria foiled Islamic State plots on President Sharaa's life, sources say," Reuters, November 10, 2025.
33 Don Rassler, *The Compound Era of U.S. Counterterrorism* (West Point, NY: Combating Terrorism Center, 2023).
34 Leah Sarnoff, "FBI releases timeline of suspect Shamsud-Dim Jabbar's New Orleans attack," ABC News, January 5, 2025.
35 Kwasi Gyamfi Asiedu, "Two Michigan men charged with Halloween Islamic State-inspired terror plot," BBC, November 3, 2025; Sarah Boxer, "Terror plot arrests reveal 'more dangerous' online pathway to ISIS radicalization in America," CNN, November 16, 2025.
36 Isabel Jones, Jakob Guhl, David Leenstra, Jacob Davey, and Moustafa Ayad, "Young guns: Understanding a new generation of extremist radicalization in the United States," Institute for Strategic Dialogue, 2023, p. 6.
37 "Statement of Christopher A. Wray, Director, Federal Bureau of Investigation, Before the House Judiciary Committee, United States House of Representatives," July 24, 2024; "Statement of Christopher A. Wray, Director, Federal Bureau of Investigation, Before the Committee on the Judiciary, United States Senate," December 5, 2023; "Statement of Christopher A. Wray, Director, Federal Bureau of Investigation, Before the Committee on the Judiciary, United States Senate," August 4, 2022; "Statement of Christopher A. Wray, Director, Federal Bureau of Investigation, Before the Committee on the Judiciary, United States Senate," March 2, 2021; "Statement of Christopher A. Wray, Director, Federal Bureau of Investigation, Before the Committee on Homeland Security and Governmental Affairs, United States Senate," September 24, 2020.
38 Daniel L. Byman, "Unlikely Alliance: Iran's Secretive Relationship with Al-Qaeda," Brookings Institution, July 31, 2012; Bruce Riedel, "The Mysterious Relationship Between Al-Qa`ida and Iran," *CTC Sentinel* 3:7 (2010); Fatemeh Aman, "Will Iran turn to al-Qaeda to combat Islamic State?" Middle East Institute, September 23, 2022.
39 Michael Horton, "Looking West: The Houthis' Expanding Footprint in the Horn of Africa," *CTC Sentinel* 17:11 (2024).
40 "Final report of the Panel of Experts on Yemen established pursuant to Security Council resolution 2140 (2014)," United Nations, October 11, 2024, p. 11.
41 "Final report of the Panel of Experts on Yemen established pursuant to Security Council resolution 2140 (2014)," United Nations, October 17, 2025, p. 19.
42 "Expanding Al Shabaab–Houthi Ties Escalate Security Threats to Red Sea Region," Africa Center for Strategic Studies, May 28, 2025.
43 "Final report of the Panel of Experts on Yemen established pursuant to Security Council resolution 2140 (2014)," United Nations, October 17, 2025, p. 18.
44 Ibrahim Jalal and Adnan al-Jabarni, "Dhows, Drones, and Dollars: Ansar Allah's Expansion into Somalia," Carnegie Endowment for International Peace, March 14, 2025; "Continued U.S. Airstrikes in Somalia Demonstrate Relentless Nature of the Threat," Soufan Center, May 6, 2025.
45 "Expanding Al Shabaab–Houthi Ties Escalate Security Threats to Red Sea Region."
46 "China Arming Houthi Rebels in Yemen in Exchange For Unimpeded Red Sea Passage," Foundation for Defense of Democracies, January 2, 2025.
47 Mohammad Salami, "China Sends Houthis Dual-Use Technology to Boost Influence and Undercut the US," Stimson Center, August 12, 2025.
48 "Treasury Targets Houthi Leaders Involved in Smuggling and Procuring Weapons," U.S. Department of the Treasury, March 5, 2025.
49 Karen Freifeld, "US targets Chinese companies over drone components used by Hamas, Houthis," Reuters, October 8, 2025.
50 Matthew Levitt, "Tehran's Homeland Option: Terror Pathways for Iran to Strike in the United States," *CTC Sentinel* 18:8 (2025).
51 "Treasury Sanctions Swedish Gang and Leader Serving Iranian Regime," U.S. Department of the Treasury, March 12, 2025.
52 "Joint Statement on Iranian State Threat Activity in Europe and North America," U.S. Department of State, July 31, 2025.
53 Janatan Sayeh, "Iran's ties to Western organized crime networks," FDD's Long War Journal, March 17, 2025.
54 John Mooney, "Kinahan cartel: hunt for gang now linked to Iran and Hezbollah," *Sunday Times*, May 13, 2023.
55 Ardavan M. Khoshnood, "The Islamic Republic of Iran's use of criminal intermediaries for extraterritorial assassinations and covert violence: a gray zone strategy of outsourced repression," Small Wars & Insurgencies, August 19, 2025, p. 4.
56 Ibid., p. 10.
57 "Global Terrorism Index 2025."
58 Ibid., p. 2.
59 Ibid., p. 2.
60 Ibid., p. 16.
61 Ibid., p. 11.
62 Authors' analysis of annual GTI data for these two countries. For data, see https://www.visionofhumanity.org/maps/global-terrorism-index/#/
63 GTI data.
64 GTI data.
65 "TE-SAT Terrorism Situation and Trend Report 2024," European Union, EUROPOL, 2024, p. 11; "TE-SAT Terrorism Situation and Trend Report 2025," European Union, EUROPOL, 2025, p. 13.
66 Masood Farivar, "FBI Scrutinizes Over 2,000 Cases Tied to Foreign Terrorist Organizations," VOA News, October 31, 2019. For a similar data point from 2018, see Luke Barr, "FBI director says bureau is investigating 5,000 terrorism cases across the world," ABC News, October 10, 2018.
67 Farivar.
68 "Statement of Christopher A. Wray Director Federal Bureau of Investigation Before the Committee on the Judiciary United States Senate," U.S. Senate, December 5, 2023. For additional insight into this issue, see Michael Gabriel Hernandez, "FBI chief says domestic terrorism cases spike to 2,000," Anadolu Ajansi, March 3, 2021.
69 "Statement of Christopher A. Wray Director Federal Bureau of Investigation Before the Committee on the Judiciary United States Senate," U.S. Senate, December 5, 2023.
70 "Director Patel's Opening Statement to the Senate Committee on the Judiciary," FBI, September 16, 2025.

71 "The Foreign Terrorist Organization (FTO) List," Congressional Research Service, September 11, 2025.
72 "Foreign Terrorist Organizations," U.S. Department of State.
73 Ibid.
74 Jytte Klausen, "A Behavioral Study of the Radicalization Trajectories of American 'Homegrown' Al Qaeda-Inspired Terrorist Offenders," Office of Justice Programs, National Institute of Justice, U.S. Department of Justice, August 2016.
75 Ibid., p. 17.
76 Ibid., p. 18.
77 Ibid., p. 16.
78 "Profiles of Individual Radicalization in the United States (PIRUS)," Research Brief, START, University of Maryland, March 2023, p. 1.
79 Ibid., p. 39.
80 Jacob Ware, "The Third Generation of Online Radicalization," Program On Extremism at George Washington University, June 2023, p. 10.
81 J.M. Berger, "The Strategy of Violent White Supremacy Is Evolving," *Atlantic*, August 7, 2019.
82 Ware, p. 11.
83 Ibid., pp. 17-28.
84 Jones, Guhl, Leenstra, Davey, and Ayad, p. 4.
85 Nicolas Stockhammer, "From TikTok to Terrorism? The Online Radicalization of European Lone Attackers since October 7, 2023," *CTC Sentinel* 18:7 (2025).
86 Ibid.
87 Jones, Guhl, Leenstra, Davey, and Ayad, p. 5.
88 Ibid., p. 4.
89 Stockhammer.
90 "The Online Radicalization of Youth Remains a Growing Problem Worldwide," Soufan Center, September 9, 2025.
91 Stockhammer.
92 "Mobilization to Violence (Terrorism) Research: Key Findings," Canadian Security Intelligence Service, 2018, p. 7.
93 Ananda Teresia, "Suspect in Indonesia mosque bombing was inspired by past mass killings, police say," Reuters, November 11, 2025.
94 "[Search in Nottuln: Münster Police investigate violation of weapons law]," Münster Police, November 8, 2025.
95 "Swedish prosecutor charges man over planned Islamic State attack in Stockholm," Reuters, November 6, 2025.
96 Ceclia Polizzi, "Youth Radicalization: A New Frontier in Terrorism and Security," Global Terrorism Index 2025, p. 86.
97 Ibid., p. 86.
98 Lizzie Dearden, "Children forming 'new generation of extremists' in UK as terror threat shifts, Cressida Dick warns," *Independent*, September 13, 2021.
99 Polizzi, p. 86.
100 See Nicolas Stockhammer and Colin Clarke, "The August 2024 Taylor Swift Vienna Concert Plot," *CTC Sentinel* 18:1 (2025).
101 Polizzi, p. 86.
102 Ibid., p. 86.
103 Stockhammer.
104 Rassler, *The Compound Era of U.S. Counterterrorism.*
105 For deeper context of this issue and other perspectives, see Matthew Levitt, "Rethinking U.S. Efforts on Counterterrorism: Toward a Sustainable Plan Two Decades After 9/11," Journal of National Security Law and Policy, 2021; Stephen Tankel, "Doing More with Less: How to Optimize U.S. Counterterrorism," War on the Rocks, May 22, 2018; Stephen Tankel, *A Resource-Sustainable Strategy for Countering Violent Extremist Organizations* (Washington, D.C.: Center for New American Security: 2020); Stephen Tankel, "Making the U.S. Military's Counter-terrorism Mission Sustainable," War on the Rocks, September 28, 2020.
106 "Summary of the 2018 National Defense Strategy of the United States of America," U.S. Department of Defense, May 18, 2020.
107 Don Rassler, "Convergence and the CT Return on Investment: A Framework," *CTC Sentinel* 17:10 (2024).
108 Ibid.
109 Ibid.
110 Ibid.
111 Lara Seligman and Michael R. Gordon, "U.S. in Talks With Taliban on Returning Counterterrorism Forces to Afghan Base," *Wall Street Journal*, September 19, 2025.
112 Ibid.
113 Chantal Da Silva, "Why Trump wants the U.S. to 'get back' the Bagram Airfield from the Taliban," NBC News, September 19, 2025.
114 Sean Morrow, Don Rassler, and Briar Bundy, "A View from the CT Foxhole: Christine Abizaid, Former Director, National Counterterrorism Center," *CTC Sentinel* (18:5): 2025.
115 Ibid.
116 Gia Kokotakis, "Biden Administration Declassifies Two Counterterrorism Memorandums," Lawfare, July 5, 2023.
117 "Protecting the United States from Foreign Terrorists and Other National Security and Public Safety Threats," The White House, January 20, 2025.
118 "The Global Terrorism Landscape with the Acting Director of the National Counterterrorism Center," CSIS, November 12, 2024. For other reflections, see Russ Travers, "Counterterrorism in an Era of Competing Priorities," Washington Institute for Near East Policy, November 8, 2019. Similar statements were made by Christine Abizaid. See "Prehearing Questions for Christine S. Abizaid upon her nomination to be the Director of the National Counterterrorism Center," Select Committee on Intelligence, U.S. Senate, n.d.
119 Nicholas Rasmussen, "Navigating the Dynamic Homeland Threat Landscape," Counterterrorism Lecture Series Washington Institute for Near East Policy, May 17, 2023.
120 "Senate Armed Services Committee Advance Policy Questions for Vice Admiral Frank M. Bradley, USN Nominee to be Commander, United States Special Operations Command," U.S. Senate, n.d.
121 For example, see Katherine Zimmerman, "Fragility and Failure: A Better Foreign Policy to Counter New Threats," American Enterprise Institute, October 2020. See also Levitt, "Rethinking U.S. Efforts on Counterterrorism."
122 "Open Hearing: Nominations of Vice Admiral Joseph Maguire USN (RET.) to be Director National Counterterrorism Center and Ellen M. McCarthy to be Assistant Secretary for Intelligence and Research," U.S. Department of State, July 25, 2018.
123 Ibid.
124 Hannah Allam, "Killing Grants That Have Saved Lives: Trump's Cuts Signal End to Government Work on Terrorism Prevention," ProPublica, March 20, 2025.
125 Kokotakis.
126 Ibid.
127 Stephen Tankel, *With Us and Against Us: How America's Partners Help and Hinder the War on Terror* (New York: Columbia University Press, 2018), p. 58.
128 Sean Morrow, Don Rassler, and Kristina Hummel, "A View from the CT Foxhole: Christopher Maier, Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict," *CTC Sentinel* 17:2 (2024).
129 "U.S., Syrian Leaders Meet in Damascus," U.S. CENTCOM, September 12, 2025; "U.S. Forces Kill Syria-Based ISIS External Operations Planner," U.S. CENTCOM, September 19, 2025.
130 "Joint Declaration between the Islamic Republic of Afghanistan and the United States of America for Bringing Peace to Afghanistan," February 2020.
131 "Joint Statement on U.S.-Pakistan Counterterrorism Dialogue," Media Note, August 12, 2025; Umair Jamal, "Pakistan-US Counterterrorism Cooperation Takes Big Strides Forward," Diplomat, August 19, 2025; Sarah Zaman, "US-Pakistan capture of 'top terrorist' signals deep counterterrorism cooperation despite cold ties, experts say," Voice of America, March 5, 2025.
132 For LeT example, see "American Terrorist," Frontline, April 21, 2025; for Hamas example, see Levitt, "Hamas Plots in Europe."
133 Leila Molana-Allen, "Prisons holding ISIS members in Syria a breeding ground for radicalization, officials say," PBS, May 3, 2024.
134 Matthew Levitt, "Re-Budgeting for a Right-Sized International Counterterrorism Posture," Washington Institute for Near East Policy, Policy Analysis, March 18, 2021.
135 Travers.
136 Rasmussen, "Navigating the Dynamic Homeland Threat Landscape."
137 Ibid.
138 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.
139 Ibid.
140 Don Rassler, "Smart Pressure: Conceptualizing Counterterrorism for a New Era," *CTC Sentinel* 17:10 (2024).
141 Daniel Sandford, Maia Davies, and Hafsa Khalil, "Threat against UK 'smouldering', top counter terror officer warns," BBC, December 18, 2024.
142 Mark Pomerleau, "Cyber Command shifts counterterrorism task force to focus on higher-priority threats," C4ISRNET, May 4, 2021.
143 Don Rassler, "A View from the CT Foxhole: Adam Hadley, Executive Director, Tech Against Terrorism," *CTC Sentinel* 18:7 (2025).
144 Morrow, Rassler, and Bundy. For another view of this issue, see "Committee on Armed Services United States Senate to Consider the Nominations of Vice Admiral Frank M. Bradley, USN, . . .," U.S. Senate, July 22, 2025.
145 Alison Bath, "Pentagon completes pullout from Niger, 5 years after building a

$110 million drone base," Stars and Stripes, August 5, 2024.
146 "Committee on Armed Services United States Senate to Consider the Nominations of Vice Admiral Frank M. Bradley, USN, . . ."
147 Lolita C. Baldor, "Houthi rebels have shot down 7 US Reaper drones in recent weeks," Military Times, April 25, 2025.
148 For a perspective on this, see Levitt, "Rethinking U.S. Efforts on Counterterrorism."
149 Seth Loertscher and Nick Kramer, "A View from the CT Foxhole: Chris Costa, Former Special Assistant to the President and Senior Director for Counterterrorism," *CTC Sentinel* 13:7 (2020).
150 Ibid.
151 Morrow, Rassler, and Bundy.
152 Rassler, *The Compound Era of U.S. Counterterrorism*.
153 Ibid.

The Best of Times, the Worst of Times: The Repressed Islamic State Affiliates

By Daniel Milton

It has been more than 10 years since Abu Bakr al-Baghdadi ascended the pulpit in the al-Nuri mosque to announce that the group known as the Islamic State had, at least in its own eyes, fulfilled the requirement to become a caliphate. In doing so, he opened an era of expansion for the Islamic State in which it welcomed numerous affiliates into its fold from all over the world. While some of those affiliates remain to this day, others appear to have faded away, at least when it comes to carrying out operations. This article explores these "repressed" affiliates in an effort to provide a brief overview of potential reasons behind their decline. The stories of each of these affiliates contain both similarities and differences. The repression of Islamic State affiliates seems to be the result of a combination of factors, ranging from military power of external actors to in-group conflict to an inability to gain a foothold among a target population. The importance of nuanced counterterrorism efforts, as opposed to a one-size-fits-all approach, is the main takeaway of this analysis.

When the group known as the Islamic State announced itself as a new caliphate in the summer of 2014, it did so with a call to groups and individuals from around the world to join its cause.[1] Many groups and individuals responded, creating a perception that the Islamic State had established a large network of affiliates committed to its cause, one that would also serve as a test of the group's overall success or failure.[2] Indeed, even as the group began to experience increased military pressure from local and international forces in late 2014, it released its flagship propaganda product, Dabiq, with the bold headline of "Remaining and Expanding," suggesting that its network of affiliates demonstrated its staying power. In the many years since this period, even as a number of caliphs have been killed, the group has continued to rely on this network of affiliates to reaffirm its relevance and presence, as demonstrated by the fact that the group highlights all of the affiliates who release statements confirming their allegiance to the newest caliph.[3]

Of course, public pronouncements of support are not the only source of support that affiliates provide to the Islamic State's global brand. Unfortunately, some of these affiliates have proven themselves to be incredibly capable of carrying out tremendous acts of violence, both inside the borders in which they have their base of operations as well as beyond those same borders. For example, the Islamic State's affiliate in the Lake Chad basin, known as Islamic State – West Africa Province (ISWAP), carried out a deadly attack on a village in Nigeria that left as many as 170 residents dead.[4] When it comes to attacks beyond the affiliate's home base, perhaps the most prolific example is Islamic State Khorasan (ISK), which has carried out several high-profile attacks beyond the borders of Afghanistan and Pakistan.[5]

However, the activity of some of the Islamic State's affiliates should not obscure the reality that several of the group's other affiliates appear to be incredibly limited in their ability to carry out attacks. Yet, despite the potential lessons to be learned from examining the cases in which affiliates have struggled, there has been comparatively less work at these affiliates as an analytic category. The author argues that these affiliates that have struggled are important to study and can potentially provide insight into what strategies may ultimately be effective in fighting against these types of organizations or whether their reduction in operational activity appears to be out of the control of counterterrorism efforts. Additionally, there is value in looking at the examples in which the Islamic State affiliates have effectively disappeared from the public mind in terms of attacks, if for no other reason than to remember that, despite some of its successes, the Islamic State, even with a large network of affiliated organizations, is neither inevitable nor invincible.

In what follows, the author first discusses the methodology used to identify the Islamic State affiliates that make up the population of study in this article. These are referred to as "repressed" affiliates in an effort to indicate that their operational activity has significantly declined or ceased according to some metrics. Then, the author proceeds to discuss each affiliate in terms of four categories: brief summary, reflections on current status, counterterrorism activities, and other considerations. It is important to explicitly state upfront that the goal of these examinations of each group is not to provide an exhaustive or comprehensive account of their history. Many other scholars, experts, and practitioners are better qualified and positioned to do this type of valuable work. Instead, the goal here is to prime conversation and thought about select factors and issues worth considering when it comes to the decline of these affiliates. After the discussion of each of the individual affiliates, the article concludes with an overview of the commonalities and differences that stood out between the circumstances surrounding the decreased activity of each of the affiliates.

The Repressed Islamic State Affiliates

As noted above, the Islamic State's network includes activities

Daniel Milton, Ph.D., is a Visiting Professor of Political Science at Brigham Young University. His work focuses on the dynamics of terrorist organizations, counterterrorism policy, and international security. X: @Dr_DMilton

Screen capture from a video titled "The Failed Confrontation" and released by Islamic State – Sinai in March 2018

carried out by core groups located in the group's original stronghold of Iraq and Syria (referred to here as the Islamic State – Core or ISC), affiliates, and individuals who view themselves as operating in the group's interest although they are not formal members of the core or affiliates. The study here focuses on the second group, the affiliates. Obtaining a count of the total number of affiliates is difficult, in part because affiliation may be extended by a group, but not accepted by ISC. Moreover, ISC has in some cases had distinct entities that it and others have referred to under a lump entity. For example, when Abu Bakr al-Baghdadi announced the establishment of the group's affiliate in Libya, he did so by designating three provinces: Barqa, Fezzan, and Tripolitania.[6] Yet, after time, most analysts simply referred to these three entities as the Islamic State in Libya, even though the entity itself still utilized separate province names from time to time.[7] Then, in one of the affiliates' communications in support of a new Islamic State caliph in 2022, the propaganda product referred to Libya alone, with no other geographic distinction.[8]

Though issues like these make a total count of affiliates, past and present, difficult, the relevant point for this article is that there are more than just one or two prominent affiliates, and that not all of them appear to be equally active when it comes to operations or other activities. The goal here is to identify a group of what the author refers to as "repressed" affiliates, which is taken to mean an affiliate that has been formally recognized by the group, but which, despite carrying out attacks in the name of the group previously, has been unable to do so for a length of time. One may wish to call these affiliates "failed" or "inactive," but such nomenclature is dangerous when applied to affiliates. Because they are clandestine, it can be difficult to measure when they have truly ceased to exist, especially when relying on open-source information. The danger in declaring a terrorist group to have ended, failed, or to be inactive based on a lack of visible attacks, comes in the case where a lull in attacks may simply be a strategic move by the group to avoid scrutiny in an effort to rebuild and launch future attacks. As will be demonstrated below, there are cases in which a lack of claimed attacks may not tell the full picture regarding an affiliate's potential.

Recognizing these challenges, this article avoids labeling affiliates with a designation that conveys a sense of finality and instead refers to the sample of interest as "repressed" affiliates. The intuition behind this label is that it suggests demonstrated diminished level of operational activity, but does not necessarily indicate that an affiliate has gone out of existence. To determine whether an affiliate is repressed or not, the author first takes the list of affiliates as contained in Islamic State's public claims of responsibility for activity as contained in the group's Al Naba weekly periodical. Al Naba contains, among other things, interviews, written articles, and, most importantly for this study, a list of incidents that the group has claimed throughout its network. Using this text as the source, the author then identified affiliates for which the group has not reported any operations for at least 12 months prior to the end of the data collection (August 2025).[a] Those affiliates that meet these criteria are as follows: Algeria, Caucasus, India, Libya, Saudi Arabia (which consists of the Islamic State's affiliates in Hijaz and

a Al Naba has continued to be released since August 2025, but the data collection for this article stopped at that point in time. However, it was felt that the 12-month window was a defensible, if arbitrary, cut-off point that provided a long amount of time in which an affiliate that was not "repressed" could feasibly plan and carry out another operation. The author wishes to thank Muhammad al-`Ubaydi for conducting and sharing the data collection. As with many projects, they would not have been possible without his diligent work.

Najd), Sinai, and Yemen. Table 1 provides an overview of these groups, including the month and year in which Al Naba last claimed an operation on behalf of the group.

Table 1: Islamic State Repressed Affiliates as of August 2025

Islamic State Affiliate Name	Last Claimed Attack in Al Naba
Algeria	February 2020
Caucasus	December 2020
Hijaz (Saudi Arabia)	November 2020
India	July 2022
Libya	April 2022
Najd (Saudi Arabia)	April 2019
Sinai	January 2023
Yemen	July 2022

Relying on Al Naba claims of responsibility for operations is not without potential weaknesses or shortcomings. The first is that it is difficult to know how reliable it may be as a source, whether as a result of strategic underreporting by the group due to counterterrorism concerns, difficulties in communication between various elements of the group (ISC and the affiliates, for example), or due to other intra-group conflict dynamics.[9] For example, even though Al Naba has been released with a fair amount of consistency for many years, the network of individuals that contribute to and produce it may be faced with counterterrorism or other pressures that lead to disruptions in the timing and scope of their individual reporting. The second is that this data might not contain failed plots or other indicators of group activity, which can lead to a biased analysis.[10] These are all important points to keep in mind and further support the decision not to label affiliates as failed based off of Al Naba reporting alone. Moreover, to mitigate some of these concerns, other forms of data (including government reports and media reporting) are included in the subsequent analysis in an effort to avoid privileging the Islamic State's own reporting. Although Al Naba reporting provides the initial list of affiliates and those with diminished operational activity, it is not the sole source of data in this article.

Islamic State in Algeria

Brief Summary

On September 14, 2014, media reports emerged that a group of fighters had left al-Qa`ida in the Islamic Maghreb (AQIM), formed a new, but distinct group, and then pledged allegiance to Abu Bakr al-Baghdadi.[11] Less than two weeks later, a video emerged in which the Algerian branch of the Islamic State executed a French tourist, Hervé Gourdel, who had been hiking in the region.[12] Despite carrying out several other operations after this point, the group quickly declined in numbers and in activity, only carrying out sporadic attacks, including four in 2017, one in 2019, and then its last claimed operation as reported in Al Naba in February 2020.[13] In the other words, the operational pace of the Islamic State's Algerian affiliate had slowed down long before 2020.

Reflections on Current Status

Very little has been heard from the Islamic State - Algeria since its last attack 2020. Despite the silence, there have been a few indicators from other sources that the group may still be operational. In a 2023 report by the U.S. government on terrorism in Algeria, it was noted that "ISIS's Algeria branch, including the local group Jund al-Khilafah in Algeria, remained in the country – though in ever-smaller numbers, as they have been unable to attract new recruits or significant new resources."[14] Two years later, in a U.N. report, it was noted that Algerian security services had resulted in "the detention of ISIL (Da'esh) supporters involved in propaganda."[15] Even though minimal, these statements are somewhat surprising, especially given the fact that the affiliate has not claimed an operation for several years. Still, reports from Algeria recently claim arrests of "terrorists," though they are vague and do not tie the individuals publicly to any group or ideology.[16]

Counterterrorism Activities

To explain this decline, several analysts have pointed to the forceful and sustained operations carried out by the Algerian government against the Islamic State affiliate, which also appears to have dealt similarly with AQIM in the country.[17] Of particular note, in December 2014, merely a few months after Gourdel's execution, the Algerian government's counterterrorism operations resulted in the death of the leader of the Islamic State affiliate, Abdelmalek Gouri.[18] The subsequent year, 2015, the U.S. State Department reported that the Algerian government had killed or arrested 157 terrorists during the year, although it did not provide a breakdown of how many might have been associated with the Islamic State as opposed to other terrorist groups.[19] Subsequent reports from the U.S. government did not identify specific numbers of arrests or deaths as a result of Algerian efforts, instead only noting that terrorist groups, including the Islamic State's Algerian affiliate, "were under considerable pressure."[20] For its part, the Algerian government, again without distinction, claimed to have reduced the ranks of terrorists by 500 from 2015-2018.[21] These efforts have been supported by the U.S. government, which has engaged in intelligence sharing and military support with Algeria.[22]

Relying on military and law enforcement is only a part of Algeria's counterterrorism strategy, which also utilizes other measures designed to limit both the supply of potential recruits for the Islamic State as well as the demand for their ideology. On the supply side, one focal point of the Algerian strategy has been to increase its ability to monitor and control the border, especially given the instability that exists in Libya, its neighbor to the east.[23] On the demand side, Algeria has sought to employ a whole-of-government approach that includes "prevention and deradicalization."[24] The effort to address extremism in religious spaces and to promote more moderate interpretations of Islam seems to have had, at least in part, the desired effect.[25] Despite the seeming success of these efforts, some have criticized the Algerian government's prevention and deradicalization programs as being little more than an effort to control religious messaging in favor of the regime.[26] While an assessment of these claims is beyond the scope of this article, the need to consider how efforts made in pursuit of security may potentially have unintended consequences is a theme in each of the countries featured in this article.

Other Considerations

Interestingly, although Algeria has prioritized its counterterrorism efforts, there are additional factors to consider. Political instability

has gripped the country for many years, yet this has not seemed to further increase the willingness of individuals to join groups such as the Islamic State. One explanation for this is that there is also the long history of violence in Algeria, which may have changed the way that Algerians think about all forms of political activism. During the Algerian civil war, the 1990s is known as the "dark decade," during which an estimated 150,000 people lost their lives.[27] During the beginning days of the Arab Spring, the scar of past political violence was one reason some used to explain Algeria's more limited response.[28] Another expert has referenced this same period as a potential reason for AQIM's struggles in Algeria.[29] Thus, it may be the combination of the country's history with extremism and counterterrorism activity that help explain why it has not seen as much domestic support for Islamic State and why fewer foreign fighters came from within its borders than that of its neighbors.[30]

Islamic State in the Caucasus

Brief Summary

The Caucasus region, which includes Chechnya, Dagestan, and Ingushetia, has long been the focal point of intense conflicts between a variety of groups. Fighters from the region appeared among early recruits to groups in the Syrian civil war, including the Islamic State.[31] Perhaps the most prominent was former member of the Georgian military Abu Omar al-Shishani, who rose in the Islamic State hierarchy to become a top leader in the war ministry.[32] By late 2014, the popularity of the Islamic State made it an attractive banner under which fighters in the Caucasus region could unite, eventually resulting in the declaration of an Islamic State province several months later.[33] The group's first attack came shortly thereafter in September 2015 against Russian military forces.[34] The violence continued, with the affiliate launching approximately 30 operations between 2015-2020 and carrying out its last reported operation in December 2020.[35]

Reflections on Current Status

The current status of the Islamic State's affiliate in the Caucasus is unclear. The affiliate was not mentioned in the 2023 U.S. State Department report on terrorism in Russia.[36] The Caucasus region was mentioned in the most recent U.N. report on Islamic State activity around the world, but only in the context of providing fighters to the Islamic State's affiliate in Khorasan, known as ISK.[37] Despite this lack of officially claimed activity, Russian security services have continued to arrest individuals in the North Caucasus, though the official narrative is more that they have links to "banned" terrorist groups, but does not name the actual group or motivating ideology.[38] In others, it deliberately misattributes the ideological connection, even though connections to Islamist groups seem apparent to other analysts.[b] Taken together with what appears to be an encroachment of ISK on the same territory, it makes it hard to say what the status of the Caucasus affiliate is (see more discussion on this topic below in the "Other Considerations" section). Regardless of whether the affiliate itself is active (and not claiming credit), the attacks are being carried out with the support of ISK, or these attacks are inspired by the group's ideology, it does seem to be the case that violence inspired by jihadism is not a thing of the past in the region.

Counterterrorism Activities

The Russian approach to dealing with this affiliate, at least according to its own reporting, includes a mix of approaches to both kill and detain terrorists, as well as efforts to seek to undermine support for terrorism. When it comes to operations that breakup terrorist cells or otherwise disrupt terrorist plots, Russia reported a decent amount of counterterrorism activity from 2018-2022, as seen in Table 2. Data for later periods is not available, but this data is still useful in the context of this affiliate because it overlaps with the time during which the affiliate's self-reported operational activities declined and then stopped altogether.

Table 2: Russian Counterterrorism Activities, 2018-2022

Year	Cells Disrupted	"Supporters" Arrested	Attacks Prevented	Militants Killed
2018	70	777	---	---
2019	49	679	39	32
2020	55	753	41	49
2021	62	926	32	---
2022	68	---	64	---

Source: U.S. State Department's Country Reports on Terrorism; Media Reporting

Any interpretation of these figures requires a fair amount of caution, in part because they are provided by the Russian government and hard to independently verify. One additional complication is that, at least in 2021, there appears to have been a distinct change in the nature of the Russia governments reports, shifting from focusing on arrests of those associated with jihadi groups to those more connected to Ukraine. Indeed, beyond 2021, media reporting suggested that a surge of "terrorism-related criminal cases" occurred in 2024, although some of the description suggests these arrests might be related to Ukraine, not necessarily to an Islamic State-affiliated group.[39] Another cautionary note is that these figures are for all of Russia, not just the territory covered by the Islamic State's affiliate in the Caucasus.[c] Still, these figures do show consistent activity and some measure of success in disrupting terrorist plots in Russia prior to 2021, a time in which there was a concerted effort by Russia to deal with the growing threat posed by the Islamic State. The fact that there may have been a shift in Russian reporting of these figures in 2021, which is around the time that the Caucasus affiliate seems to have gone silent, may just be a coincidence.

b The June 2024 attacks that killed more than 25 in Dagestan are an excellent example, as they demonstrate that there are likely incentives for the Russian government to (1) downplay the threat of the Islamic State to avoid looking weak or incompetent and (2) to hype up the threat from Ukraine. In this particular case, the Russian government claimed Ukraine was responsible, but others suggested the attack has Islamist ties. Henri Astier and Laura Gozzi, "Twenty dead in attacks on churches and synagogue in southern Russia," BBC, June 24, 2024. Some analysts even attributed this attack to the Caucasus affiliate, though only ISK seemed to acknowledge the attack as having been carried out by "brothers in the Caucasus." "Russian region of Dagestan holds a day of mourning after attacks kill 20 people, officials say," Associated Press, June 24, 2024.

c Another concern with these numbers is the fact that they likely include actions against individuals/groups that Russia defines as extremist, but that would likely not qualify on a more objective standard.

Additionally, even though there were no claims of responsibility in Al Naba for the Caucasus affiliate's operations after 2020, media reporting indicated that dozens of Islamist-related arrests were still being carried out by Russia in the Caucasus region from 2021 until as late as August 2024.[40] Unfortunately, in many of these cases, the specific affiliation of those arrested is unknown, making it impossible to say if these were affiliate members, inspired sympathizers, or potentially part of another Islamic State affiliate that has taken over responsibility for this region. Regardless, this information does indicate that utilizing law enforcement has been and continues to be the primary counterterrorism method for the Russian government in the Caucasus.

On the side of preventing or countering extremism, reports include efforts aimed at extremism in general, including outreach to religiously oriented educational facilities, designed in part to control of the nature of the religious messages.[41] Various reports also indicate that Russia is proactively seeking to prevent and remove what it deems to be extremist or terrorist propaganda online and pass anti-terrorism legislation, although these types of programs and authorities are not only used against Islamic State-affiliated forces.[42] Yet, the root causes appear to remain. When the Islamic State first established a presence in the Caucasus region, several analysts pointed out that lack of opportunities, including for youth, led to support for militancy in general, but also for the Islamic State specifically.[43]

Other Considerations

One challenge in trying to identify the decline of the Islamic State's Caucasus affiliate is that, in the time since its last reported operation in 2020, ISK has carried out or attempted to carry out operations in Russia, the most prominent of which was the concert hall attack in Moscow in 2024 that resulted in at least 130 deaths.[44] This is territory that might have previously been seen as pertaining to the Caucasus affiliate, but there has been encroachment by ISK into the North Caucasus region as well.[d] Additionally, the July 2025 United Nations monitoring report on the Islamic State noted that ISK "continued to recruit both inside and outside Afghanistan, including among Central Asian States and *the Russian North Caucasus*" (emphasis added).[45] Taken together, these pieces of evidence suggest that ISK may be operating in territory that previously would have pertained to the Islamic State's Caucasus affiliate. However, it is unknown whether ISK subsumed the Caucasus affiliate and is now using the same infrastructure and members as the Caucasus group or if the Caucasus group has been disbanded and the area has been taken over by the Khorasan affiliate. To further complicate matters, a recording allegedly from members of the Islamic State's affiliate in the Caucasus emerged in April 2024, encouraging others to take up the cause of the group.[46] This raises the possibility that, at least for several years after the final operation of the Islamic State's Caucasus affiliate, it either remained a separate entity or the group wanted give the perception that it remained a separate entity.

d On April 10, 2019, the Caucasus province claimed responsibility for a bombing at an apartment building about 70 miles outside of Moscow. Aaron Y. Zelin, "Attack on Apartment Building in Kolomna, Russia," Islamic State Select Worldwide Activity Interactive Map, Washington Institute for Near East Policy, April 10, 2019.

Islamic State in Saudi Arabia (Hijaz and Najd)

Brief Summary

Given its geographic proximity to ground zero of the Islamic State, the fact that a large number of Saudis traveled to Iraq and Syria to fight for the group, and the fact that it has always had to deal with radical elements, it is not surprising that the Islamic State sought to establish itself in Saudi Arabia.[47] Eventually, the Islamic State would have two affiliates in Saudi Arabia, Hijaz and Najd, which will be discussed together in this section. The Islamic State accepted Najd into the fold in November 2014, and by May 2015, it claimed responsibility for its first attack, a suicide bombing at a Shiite mosque.[48] The Hijaz province announced itself a few months later in August 2015 when it claimed responsibility for a suicide bombing at a mosque that resulted in the death of more than a dozen security services personnel who were worshipping there.[49] After this point, the attack tempo of the affiliates remained relatively high for a year or so, but it soon started to change both quantitatively, with attacks decreasing, and also qualitatively, as operations seemed to result more from lone or inspired actors as opposed to a concerted effort by the affiliate itself. The last attributed attack came in November 2020, when the Saudi Arabian affiliate claimed responsibility for a bombing at a World War I commemoration event in Jeddah.[50]

Reflections on Current Status

Since that last attributed attack, there has been little public information about the current status of the Saudi Arabian affiliate. The 2023 U.S. State Department report on terrorism did not mention the affiliate is having any activity or presence.[51] The affiliate is similarly absent from the July 2025 U.N. report.[52] And whereas other affiliates released renewed pledges of allegiance in support of newly minted Islamic State caliphs, this did not appear to be the case from the Saudi Arabian affiliate.[e] This lack of reporting of any sort stands in stark contrast to many of the other repressed affiliates discussed in this article, suggesting that Saudi Arabia has either effectively stamped the group out or that it maintains a very tight level of control on news regarding its existence and activity.

Counterterrorism Activities

In considering the decline and disappearance of the Islamic State affiliate's formal operations in Saudi Arabia, one of the most important factors to point out is the persistence and efforts of the Saudi counterterrorism services in detecting, arresting, and prosecuting those suspected of participating in or otherwise supporting the affiliate's activities. For example, in 2014, the government publicized the arrest of 431 individuals affiliated with the Islamic State in a series of operations across the country.[53] Two years later in 2016, security services reported arresting 1,390 for terrorism ties, including at least 190 with connections to the Islamic State.[54] In 2019, a major attack was prevented when security services shot and killed four attackers targeting a government building, with subsequent operations resulting in the arrest of another 13 suspects.[55]

But Saudi Arabia's approach to dealing with the Islamic State,

e The author reviewed each of the post-November 2020 activities in Saudi Arabia as captured by the Washington Institute's Islamic State Worldwide Activity Map and found nothing in terms of arrests, plots, or operations, whether connected to the affiliate or otherwise.

and terrorism in general, is more than just law enforcement action. As one scholar noted, it has sought to approach the non-kinetic fight by targeting the terrorism lifecycle through efforts focused on prevention, rehabilitation, and minimizing the risk of recidivism.[56] Though the efficacy of these programs is debated and their use in the case of captured Islamic State supporters is less well known, at the very least they represent a substantial investment in efforts to prevent and counter violent extremism.[57] These individually focused efforts have been supplemented by larger initiatives to fight terrorist ideology such as the Global Center for Combating Extremist Ideology and the Ideological War Center, both based in Saudi Arabia and which engage in the broader "war of ideas" by creating counter-messaging as well as flagging terrorist content for removal from online spaces, among other efforts.[58] The fight against the Islamic State's ideology has also been the focus of a targeted effort by government and religious leaders to denounce the group.[59] Taken together with the government's approach to identifying and arresting the affiliate's supporters, the overall effort seems to have been effective at repressing the operational activities of the group.

Other Considerations

While Saudi Arabian efforts to counter the Islamic State's local affiliate appear to play a primary role, there may also be a unique dynamic at play that explains the lack of support for the Islamic State's local affiliate. The idea of a lack of support may seem surprising at first, especially given that an estimated 3,200 Saudi citizens traveled to Iraq and Syria to fight with the Islamic State.[60] This is one of the larger country contingents to have traveled, suggesting no shortage of support for the Islamic State. However, scholars have noted that Saudi Arabian support for jihad is unique in that it is most prominently manifested in distant fighting, not actions on the homefront.[61]

Islamic State in India

Brief Summary

Al Naba featured the first claim of an operation attributed to an India province of the Islamic State in May 2019.[62] Any persistent existence of the group, however, has been denied by the Indian government in repeated statements, noting that while there may be some sympathy toward the group, it does not have deep roots.[63] While there may be reason to view such denials cautiously, the fact remains that, at least through the group's own reporting, the India affiliate carried out only 17 attacks from May 2019 to July 2022. The last public communication from the group itself came in December 7, 2022, in which members of the India province of the group pledged allegiance to the Islamic State's new leader, Abu al-Husayn al-Husayni al-Qurashi.[64] Overall, the lack of directly connected activity could be an indication that the Indian affiliate of the Islamic State is struggling, but it might also indicate that the activity simply has changed form, as is discussed a bit more below.

Reflections on Current Status

Relatively little has come out from official Islamic State channels regarding the current status of the Islamic State's affiliate in India. Given that it has been more than three years since a claimed attack, it might be tempting to write the group off as having collapsed or having never existed. However, in March 2024, the Indian government announced the arrest of Haris Farooqi, claiming that he was the head of the Islamic State in India.[65] Still, outside of specific activity officially claimed by the Islamic State or an affiliate, there does appear to be a sizable amount of activity by, at the very least, supporters or sympathizers of the Islamic State. There have been approximately 44 arrests of individuals suspected to be connected in some form with the Islamic State generally, but nothing in either Indian government or Islamic State channels has tied these individuals directly to the Indian affiliate.[66] Thus, though the affiliate itself appears dormant, the underlying support for the ideology is not. As has been the case in other affiliates above, this lack of official communication from the Islamic State about the affiliate, combined with continued arrest and other activity, makes it hard to determine the status of the affiliate itself.

Counterterrorism Activities

Perhaps a more compelling reason is a very proactive effort by the Indian government to monitor and arrest those who express support for the group. According to the U.S. State Department, in 2020, India reported investigating 34 cases and arresting 160 suspects related to the Islamic State.[67] In 2021, India reported investigating 37 cases and conducting 168 arrests.[68] Finally, in 2023, the government reported investigating 21 cases and making 65 arrests.[69] Although formal reporting by the U.S. State Department has not been released since 2023, very recent indications suggest that such operations are ongoing. In September 2025, the Indian government reported arresting a cell of five Islamic State supporters in various cities who had been planning to carry out attacks, having gone so far to obtain suicide vests and other weapons.[70] Another arrest occurred in October 2025, in which an IED plot by two individuals suspected of having links to the Islamic State was said to be in "advanced stages."[71] As noted above, these arrests are part of about 44 arrests that have taken place since the last claimed operation of the India affiliate in the summer of 2022.

While potentially undercutting the narrative of no foothold for the group in India, the tempo of law enforcement activity suggests two things. First, the Indian government is making a vigorous effort to identify and intervene in cases where the Islamic State may be attracting adherents. Law enforcement action still seems to be the primary pillar of the government's response, supported by a vigorous effort to collect intelligence on individuals and cells operating in India. This is not to say that the government does not engage in counter violence extremism and deradicalization efforts. Indeed, legislative action to address financing of terrorism as well as increased efforts to engage in content moderation are also part of its approach.[72] Second, the fact that arrests are still occurring suggests that the Islamic State's ideology, if not its affiliate in the region, is still successfully attracting adherents who, whether alone or as part of an organized group, are trying to take actions in the name of the group. While some of the arrests that have taken place since the summer of 2022 are for lone individuals, about half of them are for two or more individuals, suggesting there are still small collectives willing sympathetic to the Islamic State. It is worth mentioning, however, that there did not appear to be any connection to a larger Islamic State in India organization in the open-source information related to these arrests.

Other Considerations

As discussed above, there has been a number of arrests of individuals for support of and participation in cells affiliated with the Islamic State since the last Al Naba claims of operations. The fact that these

recent arrests have not been formally tied to the group's main local affiliate, Islamic State in India, is perplexing. At least according to one scholar, Indian Muslims have generally found a place within the political process, lessening the need to participate in violent jihadi groups.[73] The general proposition that democracy might serve as an antidote to terrorism by providing alternate avenues for expressing dissent has found much less support in academic research.[74] Moreover, the pace of arrests and plots do not seem to indicate a lack of support for the Islamic State or for violence. A lack of support for this latter fact is also demonstrated by threats from numerous militant organizations other than the Islamic State that India faces, which indicates that there is some willingness on the part of individuals to carry out acts of violence in favor of political ideologies in the country.[f]

If the Islamic State in India's seeming disappearance cannot be attributed to a lack of willingness to engage in violence, perhaps another explanation is the group's activities have simply been redirected under the banner of a different affiliate. As was discussed above in the case of the Caucasus affiliate, the ISK affiliate has increased in prominence over the past few years. It is also proximate to India and could feasibly have taken over operations from the defunct or ineffective India affiliate. There is limited evidence to support this. Of the arrests the Indian government has carried out since the India affiliate's claims stopped, a small number specifically mentioned an ISK nexus to the suspects. In some cases, it was merely that the individual supported ISK and wanted to travel to its territory. In one case in western India in 2023, an individual was accused of leading an ISK cell in the region with the goal of facilitating transit to Afghanistan.[75] In 2025 in the same region, Indian security services arrested a man who was allegedly manufacturing ricin in order to poison local water supplies at the behest of an ISK handler based outside of India.[76] While these few actions do suggest that ISK plays a role in some of the cases in India, the open-source evidence since the summer of 2022 is not conclusive in showing that ISK has taken over the group's India portfolio. If anything, it raises the possibility that India's law enforcement pressure may have resulted in a more decentralized approach on the part of the group's supporters, with some sporadic connection to handlers abroad. It also suggests that there may be different Islamic State affiliate networks, with different levels or channels of support, active in the country. Though these networks may not operate under the official label of the group, it seems clear that support for the group's ideology has not been repressed, even if the affiliate itself appears to have been.

Islamic State in Libya

Brief Summary

The power vacuum present in Libya following the ouster of longtime dictator Muammar Gaddafi has been a boon to the Islamic State, which emerged in separate provinces in the country beginning in 2014.[77] In August 2015, Islamic State fighters in Libya established enough control over the city of Sirte that they were able to quell a subsequent rebellion and continue to implement their brutal form of governance.[78] This control lasted for approximately a year, until a coalition of local forces supported by Western airpower was able to eject the group from control of the city. Unfortunately, the group remained resilient, carrying out operations within Libya at an increased pace for the next couple of years, before ultimately slowing down in the summer of 2019.[79] The Islamic State Libyan affiliate carried out a handful of attacks over the next few years, until April 2022, when the last attack recorded in Al Naba took place. The last formal mention of the affiliate by an official channel of the Islamic State appears to have come in December 2022, when an officially branded photo of a small number of the affiliate's fighters appeared in support of the Islamic State's new caliph.[80]

Reflections on Current Status

Relatively little is known about the current status of this Libyan affiliate. Although the group has not carried out claimed attacks over the past several years, there are indications that it still exists as an organization. For example, in January 2024, Libyan security forces announced that they had arrested an individual they claimed was the leader of the Islamic State in Libya.[81] More recently, news reports in August 2025 indicated that Libyan security services had broken up three cells responsible for assisting in fundraising, smuggling, and recruiting for the Islamic State.[g] In September 2025, an editorial titled "Libya the Glorious" appeared in Al Naba and called on the group's fighters and supporters in Libya to rise up and return to the fight, whether as a group or individually.[82] Whether this call was a reference to an actual planned resurgence or a plea for future relevance is unclear, although in the months since it was issued, there does not appear to have been any additional activity.

Counterterrorism Activities

Libya presents an interesting case for counterterrorism efforts, in large measure because its governance structure has been fractured or in disarray during almost the entirety of the time that the Islamic State has been operating in the country. Today, control of the country remains split between the Government of National Stability (GNS), located in the eastern part of the country, and the Government of National Unity (GNU), located more to the west in Tripoli. This fractured governmental structure has led a number of analysts to suggest that the group will be able to recover from its setbacks.[83] However, despite this division, recent assessments have suggested that the Islamic State has been unable to regain much control or momentum, as noted in the 2021, 2022, and 2023 reports on terrorism in Libya by the U.S. State Department.[84] However, as noted above, the July 2025 U.N. report on the Islamic State more generally noted that Libyan intelligence services had managed to identify and disrupt three facilitation cells in Libya that were helping funnel people and resources in and out of Libya.[85] This

f Data from the South Asia Terrorism Portal indicates that the number of terrorism incidents, though down from its peak of 4,483 events in 2003, is still relatively high with 1,921 events as of November 3, 2025. See https://www.satp.org/datasheet-terrorist-attack/incidents-data/india. India also ranks number 14th in the world in the 2024 annual report of the risk of terrorism produced by the Institute for Economics & Peace. See https://www.visionofhumanity.org/maps/global-terrorism-index.

g It seems likely that these media reports refer to the same activities that appeared in the July 2025 U.N. report on Islamic State activities, indicating that these arrests likely took place well before August 2025. "Thirty-sixth report of the Analytical Support and Sanctions Monitoring Team submitted pursuant to resolutions 1267 (1999), 1989 (2011), and 2253 (2015) concerning Islamic State in Iraq and the Levant (Da'esh), Al-Qaida and associated individuals and entities," United Nations Security Council, July 24, 2025, p. 11; Dario Cristiani, "Weakened Islamic State Eyes Resurgence in Libya," Jamestown Foundation, October 22, 2025.

suggests that the threat, even though diminished, has certainly not disappeared completely.

As far as identifying potential sources to attribute the overall success against Islamic State elements in Libya, one would need to attribute some credit to the GNS and GNU forces, which have shown themselves to be willing in some cases to go after Islamic State members. However, there has also been a consistent involvement from the international coalition, led mainly by the United States, in initial and subsequent efforts to push back the gains made by the Libyan affiliate, especially in Sirte, during which as many as 500 airstrikes were carried out during the 2025-2016 effort to push back and dislodge the group from the city.[86] And, when the group began to resurge in 2018 after seemingly being on the decline for a few years, U.S. airstrikes carried out in 2019 allegedly killed a third of the affiliate's personnel.[87] U.S. security cooperation efforts have continued through to the present day, including in a demonstrative visit of a U.S. warship to key Libyan ports, during which the U.S. embassy noted that it had "increased engagement with Libyan partners across all regions of the country."[88]

Other Considerations

When explaining the repressed nature of the Libyan affiliate beyond just counterterrorism, one analyst has pointed to the group's own missteps, including the brutal way it governed and then lost Sirte, which created a stigma that made it hard for other militant groups in Libya to ally with it.[89] The stories of brutality from during the Libyan affiliate's control over Sirte do present a poor case for jihadis. A 2016 report by a human rights organization documented executions, shortages of medical supplies and food, and restrictions on public life.[90] While these stories may have played a role in weakening demand for the group, the 2019 resurgence showed that deeper issues and fractures within Libyan society could potentially give the group room to reemerge.[91]

Thus, in terms of longer-term challenges that may have inhibited counterterrorism and could do so in the future, it is critical to recall the fractured nature of the Libyan government. As noted, there was some belief that the divided nature of the Libyan government would provide an opportunity for the Islamic State to regroup and reengage in violence. At least at this point, although the group has not been totally eliminated, a reemergence has not happened. While a revival of the affiliate in terms of its operational activity may still come to pass, it also seems possible that the counterterrorism efforts of the divided parties in Libya have been enough to prevent the Islamic State from reengaging.[h] It also appears that the United States has been supporting the efforts of both parties, even while encouraging a political reconciliation, as evidenced by the decision to hold an annual special operations military exercise in Libya in 2026 in an effort to further "Libyan efforts to unify their military institutions."[92] Of course, the United States is not the only foreign power involved in Libya, as recent years have seen a buildup of Russian forces there.[93] Thus, the delicate balance between divided Libya parties has more than just counterterrorism implications. However, efforts by external actors to influence that balance may have counterterrorism consequences for better or for worse and is an issue that should be monitored moving forward.

Islamic State in Sinai

Brief Summary

Among all of the affiliates of the Islamic State, there are few that have achieved the notoriety and managed to maintain a high operational tempo like its affiliate in the Sinai Peninsula. Perhaps that is, in part, because it came into being as an already functioning group, Jama'at Ansar Bayt al-Maqdis (JABM). The head of JABM responded to the Islamic State's global call for allegiance, pledging it on November 10, 2014, and having their pledge accepted just a few days later.[94] Within a year, the Islamic State in Sinai claimed responsibility for downing a Russian airliner, killing the 224 passengers onboard.[95] While the attack against the airplane was certainly one of the group's higher profile attacks, it was able to carry out numerous other operations, with the U.S. intelligence community crediting the group with 500 attacks in the eight-year period between 2014-2022, including assaults that left anywhere from dozens to hundreds dead.[96] Despite this high operational tempo, by the end of 2022, the number of operations being reported on the part of the Sinai affiliate in Al Naba was experiencing a slowdown, with the last operation being recorded in early 2023.

Reflections on Current Status

The 2023 State Department report on the status of terrorism in Egypt noted that the Islamic State's affiliate was "significantly degraded."[97] In its most recent report in July 2025, the United Nations noted that the group was "not active" but had very little else to say about its size or future prospects.[98] Interestingly, the Israeli military carried out an airstrike in Gaza in August 2025 that allegedly killed a member of the Islamic State in Gaza who was responsible for operations in several locations, including the Sinai Peninsula.[99] The Egyptian government denied that the individual killed was part of any formal Islamic State organization, but if it were true, the fact that an individual in the Gaza Strip had been responsible for operations in the Sinai Peninsula might suggest some level of reduced capability in theater.[100] These scattered sources aside, reporting on the group's activities, if any, is difficult to obtain given that the government seems to be restricting press access to and reporting from the area.[101] Recognizing this caveat regarding the lack of media reporting from the region, there is, at least at the current time, very little public indication of this affiliate's ability to reemerge or even of what its current activities may be.

Counterterrorism Activities

There can be a tendency to credit a military intervention with success against Islamic State – Sinai, but this would appear to be an inaccurate reading of the facts. According to one expert, despite deploying over 40,000 troops and employing something akin to a scorched earth policy through most of 2018, little headway was being made against the group and its operational tempo continued mostly unabated.[102] But, around 2017-2018, Egypt shifted from relying mainly own its own armed forces to cooperating more with local tribes and militias, who were also bearing the brunt of the group's militant activity.[103] These efforts did not yield immediate success, with some analysts pointing out that the government's

h This is not to suggest that there are not legitimate concerns or that a political process should not move forward. It does seem likely that, if there is continued political uncertainty into the future and the underlying challenges of corruption are not addressed, there will be more fertile ground for militant groups, whether affiliated with the Islamic State or something entirely different. Vibhu Mishra, "UN envoy warns Libya's transition at risk amid stalled political roadmap," UN News, October 14, 2025.

approach had, at best, resulted in containment of the group and, at worst, furthered the conditions that would lead to more conflict in the future.[104] Despite these concerns, by early 2023 the Egyptian government declared victory against terrorism in the region, with President Abdel-Fattah Al-Sisi stating that "if the terrorists had been able to overcome us, they would have slaughtered us, but we were able to vanquish them."[105] In short, it appears that the effort to involve local tribes in the process of defeating Islamic State - Sinai was in part responsible for the success in the end, at least in reducing the levels of violence perpetrated by the group.[106]

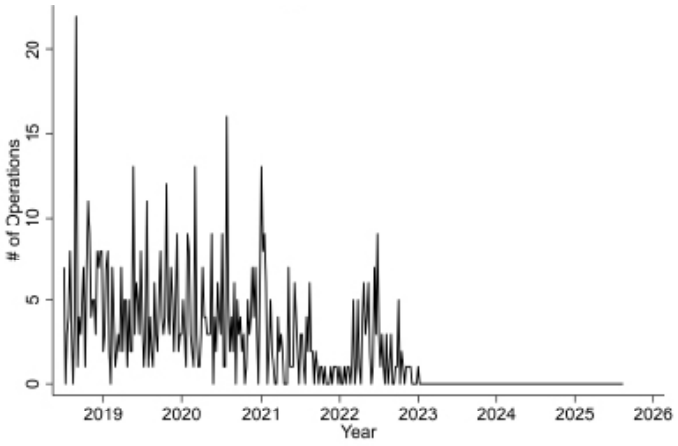

Figure 1: Attacks Claimed by Islamic State - Sinai Province

While the military efforts were the predominant focus, there were also reports of other aspects to the counterinsurgency campaign. For example, in its 2022 report on Egyptian counterterrorism efforts, the U.S. State Department noted that the government had implemented CVE initiatives, including efforts to counter Islamic State propaganda, as well as spending $224 million dollars to compensate residents for damage caused by counterterrorism efforts.[107] In addition to this, there have also been reports that one of the strategies used to lure fighters away from the Islamic State were offers of amnesty, although there is a lack of clarity on the terms of these agreements.[108] As with most non-kinetic counterterrorism efforts, however, there appears to be little analysis of the effectiveness of these policies.

Other Considerations

Even though the above discussion suggests that the use of the military instrument in tandem with local partners has brought some success, the effort to deal with Islamic State – Sinai is not without complications that may ultimately have implications for the future of the Islamic State and other militant actors in Egypt. More specifically, the campaign against the Islamic State's Sinai affiliate has brought serious allegations of human rights abuses by the Egyptian military, suggesting the campaign may have hidden costs not fully acknowledged or appreciated yet.[109] While there are no indications that such tactics have brought about a backlash or created additional support for the Islamic State at this point, Egypt's own history with jihadism suggests that it is important to be deliberate in ensuring that military power to counter extremists is employed in tandem with efforts that target both the ideas of jihadis and the motivating factors that draw individuals to their cause.[110]

Islamic State in Yemen

Brief Summary

Although the Islamic State in Yemen was part of the early group of affiliates recognized by Islamic State Central and started off with some fanfare in November 2014, one scholar noted that it "failed to gain significant traction" and began to decline by 2016.[111] Despite this, the group managed to rebound in 2018 and, according to its own reporting in Al Naba, carried out 174 operations between the summer of 2018 and its last recorded attack in the summer of 2022. Even though claimed attacks stopped after that point, this was not the final communication. As is the case with many other affiliates, the last official communications from the group came in the form of pledges of support for newly minted leaders of the Islamic State, one in December 2022 and another in August 2023.[112]

Reflections on Current Status

Despite the lack of attack activity, the recent July 2025 U.N. report noted that the group had about 100 fighters and focused mainly on "recruitment and facilitation efforts coordinated with ISIL affiliates."[113] Beyond this report, additional details about recent activities by or against the Islamic State's Yemeni affiliate were not easy to find, leaving the U.N. report as one of the only sources available. However, the fact that little information could be found, including any additional efforts by foreign governments to target Islamic State in Yemen, is suggestive of the fact that, while the group may not have failed, it is also not functioning in the way that it used to. Thus, it does seem repressed, even if it is not defeated.

Counterterrorism Activities

The Yemeni government, for many years before the civil war, relied heavily on the United States for counterterrorism support in the form of financial aid, military weapons, and kinetic strikes against groups such as al-Qa`ida in the Arabian Peninsula (AQAP).[114] Though most of the United States' effort was directed against AQAP, in some cases the United States also carried out airstrikes against Islamic State targets, as it did in 2017.[115] These efforts were very limited and were conducted as the Yemen government was collapsing due to the economic and political pressures it could not overcome.[116] Thus, although the United States was involved in Yemen, to give it or the Yemeni government most of the credit for reducing the operational pace of Islamic State Yemen in the country would be inaccurate.

The lack of strong governmental counterterrorism efforts shifts the focus to the role played by other actors in Islamic State - Yemen's decline. Indeed, another factor worth taking into account are the Islamic State's interactions with other militant groups in the area, notably AQAP and the Houthis. When it comes to AQAP's interactions with the Islamic State affiliate, after some period of time during which the two groups mostly ignored each other, the fighting turned vicious. For example, in 2019, facing increased fighting, part of al-Qa`ida's Yemeni network offered a $20,000 reward for the head of the leader of the Islamic State affiliate.[117] But, while the combat against AQAP likely weakened the Islamic State in Yemen, it seems probable that the Houthis dealt a significant blow to the group in a 2020 counterterrorism operation that resulted in an unknown number of dead Islamic State fighters.[118]

Other Considerations

Of course, the country of Yemen is in the midst of a civil war between

the Houthis and the internationally recognized government.[119] This conflict has also attracted considerable attention from third-party states seeking to impact the outcome. It seems entirely probable that this dynamic has impacted the ability of militant groups to organize and operate. As noted by one expert, Yemen has been the battleground for global powers, leading to the possibility that the Yemeni affiliate's fighters, if not its broader agenda and mission, have been co-opted or otherwise distracted by the challenges posed by the current environment.[120] What could happen to groups such as the Islamic State's Yemen affiliate when the civil war terminates is unclear, but depending on which entity is in charge, it could either find itself with breathing room and a new lease on life, or the target of a government seeking to assert its authority over the country.

A View of the Forest

The small snippets of each Islamic State affiliate above have attempted to present some of the factors that could potentially be credited for the decline in their operational activity. Any such exercise, in which a large number of examples are covered in a limited amount of space, will inevitably miss nuance and detail. Indeed, just as the familiar refrain in the radicalization literature is that each individual's case is unique, it is likely the case that the outcome of a specific Islamic State affiliate is the result of factors unique to its situation. While such nuance matters and should not be set aside casually, the author attempts to conclude this article by identifying common threads, as well as differences, running through each of these cases.[i]

The Decline of Islamic State Central. For many of the affiliates that struggled, it seems clear that the diminished capacity of the Islamic State's main body in Iraq and Syria furthered undermined their own groups. This appears to have been only in part due to decreases in tangible resources such as financial transfers, which in some cases still came to some of the affiliates through regional bureaucratic entities that the Islamic State created to manage its group of affiliates.[121] The mere fact that ISC had to create additional entities to help manage the affiliates also suggests a decreased ability to provide as much oversight and input into the affiliates as it had previously.[122] But, there also appears to have been something of a reputational hit to the group that may have also impacted the ability of affiliates to continue attracting people to the cause. The damage to the affiliate from the central group's military defeat likely compounded this issue.

This explanation for the struggles of some of the affiliates is, however, incomplete at best. All of the affiliates, those that were successful and those that failed, had to deal with a world in which their parent organization, ISC, no longer possessed the advantages that made it seem like such a powerful force in mid-2014. Yet, for reasons that are not entirely clear, it seems that the Islamic State's territorial defeats in Iraq and Syria constituted a stress test that some affiliates were able to weather while others folded under the pressure. One possibility to consider is that the stress test resulted in some affiliates being prioritized by ISC while others may have been left to their own devices.[j] In other words, ISC may have had to engage in prioritization that resulted in reduced resources and potentially even reduced communications with some of its affiliates. If ISC did have to engage in such prioritization, it may provide at least a partial explanation of uneven performance of the group's affiliates. While this possibility is intriguing, more detailed information than is available in this article would be necessary to make any sort of detailed assessment of how each affiliate responded to and was affected by the turning of the tides against ISC.

"For reasons that are not entirely clear, it seems that the Islamic State's territorial defeats in Iraq and Syria constituted a stress test that some affiliates were able to weather while others folded under the pressure. One possibility to consider is that the stress test resulted in some affiliates being prioritized by ISC while others may have been left to their own devices."

The Rise of Powerful Affiliates. At the same time, while ISC has declined over the past several years, a few of its affiliates appear to have taken on new roles in ways that impact other affiliates. For example, ISK has become one of the more prolific and seemingly well-resourced of the group's affiliates.[123] Given that it operates in proximity to the base of operations for both Islamic State – Caucasus and Islamic State – India, the possibility exists that it may have taken over operations in those areas. At the very least, it does seem that ISK has overshadowed those other entities. In the open source, it is difficult to determine whether the affiliates in this region ceased and then ISK moved in or whether ISK moved in and took over these affiliates, or whether it has simply buttressed their seemingly fledgling operational capability. Nonetheless, there does appear to be evidence in the case of ISK that it has seen its own area of responsibility grow in ways that may have implications for some of the affiliates that formerly existed in those areas.

A Potential Deemphasis of Formal Affiliates. One possibility that is raised by the above analysis is that, either due to counterterrorism pressure or other strategic decisions made by the group, the formal affiliates themselves are simply not as important in the operational or propaganda strategy of the Islamic State in today's environment. For example, the case of the Islamic State in India, in which sizable number of arrests of individuals associated with the Islamic State have occurred, despite no official statements from the affiliate, might suggest that the Islamic State's overall approach to the Indian theater of operations has changed. If that is the case, whether that was an intentional decision by ISC for strategic or practical reasons (or some mix of both) is unclear. It may be the case that the Islamic State, in some theaters, has

i These commonalities are just that and should not be viewed as causal arguments regarding what leads to the decline of affiliates. To make a stronger argument about what actually leads to affiliate decline would require a comparison between the affiliates whose operations appear to have ended and the affiliates that remain operationally active. Instead, these factors should be viewed as potential explanations worthy of future research and study.

j The author wishes to thank Don Rassler for making this observation and suggesting a way to incorporate it here.

seen the deemphasis of affiliates as a smart move to mitigate counterterrorism pressure while continuing operations. It could also be the case that the affiliate structure no longer exists and the group has simply adjusted to that reality. The question of how the Islamic State is adapting in these spaces where "repressed" affiliates exist is an important question for both practitioners and researchers moving forward.

A Diverse Approach to Counterterrorism Partnerships. When considering the different ways in which hard power was brought to bear on some of the Islamic State's affiliates in these cases, one thing that seems clear is that there was much diversity in the actors applying that power and how they related to others. An array of counterterrorism partnerships appears to have factored into the decline of the Islamic State affiliates covered in this article. In some cases, it is an international coalition; in others, a single nation. In some cases, it is local government forces or tribal elements; in others, competing militant organizations. While it does appear that hard power, either from above in the form of airstrikes or from across the field of battle in the form of guns, is an important part of the story in the decline of some of these affiliates. However, though "hard power" has forms of value, it would be a mistake to argue that this pressure bears much similarity across these cases. In many of these cases, the nature of counterterrorism military cooperation had to be, of necessity, flexible to the realities on the ground. This led to a diverse set of partnerships, which might not have been chosen as ideal arrangements by military planners beforehand. Yet, the ability to adapt to the context-specific requirements and constraints allows military power to still be applied in an effort to weaken the affiliates.

The Value of Holistic Counterterrorism Strategies. Although some declines may be attributed, either in whole or in part, to concerted military or policing actions, in other cases it seems that the decline itself, or at least the durability of the decline, may also be related to the implementation of strategies that sought in other ways to undermine the Islamic State's appeal to the local populations. These include programs designed to encourage amnesty in order to provide fighters with a pathway to exit, economic development in high-risk areas, efforts to undermine and identify weaknesses in Islamic State propaganda, and so forth.[124] Moreover, even as it applies to the use of hard power, there was considerable variation in how nations facing the threat of Islamic State affiliates deployed their security services in pursuit of these groups. In the case of the Egyptian government's fight against the Islamic State's affiliate in Sinai, there was a considerable amount of effort dedicated toward partnering with local tribes and security forces. In fact, one interpretation of what ultimately led to success was this more comprehensive security effort as opposed to a unilateral approach by the national military alone.

The Hidden Costs of Repressed Affiliates. One of the things that stands out from some of the above discussion is that the use of hard power and limitations on some liberties may be a factor to consider in the repression of the operational activity of some affiliates. For example, in one case from 2017, a human rights organization expressed concern that pursuit of the Islamic State's Yemen affiliate by counterterrorism forces may have involved the use of torture.[125] In another case spanning the length of Egypt's campaign in the Sinai, allegations of extrajudicial killings and mass graves have emerged.[126] Whether in the case of Egypt, Libya, Russia, or Saudi Arabia, these measures might create second- or third-order effects that could serve to increase demand for terrorism. To put it another way, steps taken in the pursuit of security against these affiliates may result in grievances and frustrations that could serve to increase future security threats, whether on the part of reenergized affiliates or some other militant organization.

'Defeat' Remains an Elusive Goal. As noted in numerous places above, despite their claimed attack activity having diminished to essentially nil (at least according to the Islamic State's own reporting), very few, if any, of these Islamic State affiliates appear to have been destroyed to the point that they have no members and no longer pose a threat. As is the case in most open-source work, there is often a lack of granular detail regarding the true capabilities and threat posed by clandestine terrorist groups. As noted above, this is made even more complicated by the fact that terrorist groups have demonstrated the ability to "evolve and adjust their approaches in response to pressure."[127]

Indeed, there is evidence that some of the affiliates, though not carrying out claimed attacks, have sought to contribute to the overall Islamic State mission through other logistical or supportive activities, such as helping move people and weapons across borders and fundraising, as was noted above in the case of the Libya affiliate. If this is accurate, then another important consideration for counterterrorism forces comes in how to shift focus in the 'mopping-up phase' to dealing with group activities that are less visible on the battlefield and potentially require more intelligence and law enforcement support to address. In countries with at least some capabilities to do those types of operations, such as India and Egypt, there may be a good chance that the remnants of affiliates can be contained if not captured or otherwise disabled. However, for countries such as Libya and Yemen, such fine-grained counterterrorism efforts may be beyond their reach.

As a result, it is important not to consider the mission of defeating these repressed affiliates as having been accomplished. Additionally, it is possible (and potentially even likely) that the factors that would ultimately eliminate the threat posed by the group are different from those that lead to a reduction or pause in its attacks. For example, military power may eliminate the group's capacity to carry out operations, while de- and counter-radicalization efforts may be necessary to remove the motivational factors that remain on the part of whatever small number of group members remain. As discussed above, some countries appear to have implemented these types of policies, while others have not either due to lack of willingness or capability.

Conclusion

This article has sought to provide brief insight into the cases of "repressed" affiliates of the Islamic State, that is those affiliates which have seen a marked decline in their claimed operations. In doing so, the goal was to identify some of the commonalities and differences in each of these contexts. This analysis should not be seen as an exhaustive treatment of each affiliate, but rather as an attempt to obtain a strategic perspective on the potential lessons that might be drawn from looking at the decline of several affiliates at once. As some of the Islamic State's affiliates in Africa, notably in West Africa and Mozambique, and the group's capable affiliate in Afghanistan continue to operate with comparatively more levels of success than those covered in this article, the lessons from this article may provide insight into opportunities and constraints that governments are likely to face in countering them. CTC

Citations

1 Ahmed S. Hashim, "The Islamic State: From al-Qaeda Affiliate to Caliphate," *Middle East Policy* 21:4 (2014): pp. 69-83.
2 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.
3 Aaron Y. Zelin, "The Islamic State's Fourth Bayat Campaign," Jihadology, August 6, 2023.
4 Ayodele Oluwafemi, "Report: Over 170 killed during Boko Haram attack of Yobe community," Cable, September 10, 2024.
5 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; Daniel Milton, "Go Big or Stay Home? A Framework for Understanding Terrorist Group Expansion," *CTC Sentinel* 17:10 (2024): pp. 43-52; Aaron Zelin, "The Islamic State's External Operations Are More Than Just ISKP," Washington Institute for Near East Policy, July 26, 2024.
6 Andrew Engel, "The Islamic State's Expansion in Libya," Washington Institute for Near East Policy, February 11, 2015.
7 Jason Warner and Charlotte Hulme, "The Islamic State in Africa: Estimating Fighter Numbers in Cells Across the Continent," *CTC Sentinel* 11:7 (2018): pp. 21-28; Lachlan Wilson and Jason Pack, "The Islamic State's Revitalization in Libya and its Post-2016 War of Attrition," *CTC Sentinel* 12:3 (2019): pp. 22-31.
8 Aaron Y. Zelin, "Pledge of Allegiance of the Soldiers of the Caliphate in Libya to Abu-Husayn al-Husayni al-Qurashi," Islamic State Select Worldwide Activity Interactive Map, Washington Institute for Near East Policy, December 19, 2022.
9 Gregory Waters and Charlie Winter, "Islamic State Under-Reporting in Central Syria: Misdirection, Misinformation, or Miscommunication?" Middle East Institute, September 2, 2021; Aymenn Jawad Al-Tamimi and Charlie Winter, "The Islamic State in Dera'a: History and Present Situation," Current Trends in Islamist Ideology, April 24, 2023; Haid Haid, "Why ISIS doesn't always publicize its attacks," *Asia Times*, July 25, 2023; Aaron Y. Zelin and Devorah Margolin, "The Islamic State's Shadow Governance in Eastern Syria Since the Fall of Baghuz," *CTC Sentinel* 16:9 (2023): pp. 22-29.
10 Petter Nesser, "Introducing the Jihadi Plots in Europe Dataset (JPED)," *Journal of Peace Research* 61:2 (2023): pp. 317-329.
11 "Algeria's al-Qaeda defectors join IS group," Al Jazeera, September 14, 2014.
12 Chris Johnston and Kim Willsher, "French tourist beheaded in Algeria by jihadis linked to Islamic State," *Guardian*, September 25, 2014.
13 Aaron Y. Zelin, "Various Activity Reports," Islamic State Select Worldwide Activity Interactive Map, Washington Institute for Near East Policy, accessed November 10, 2025; Thomas Joscelyn, "Islamic State claims rare attack in Algeria," FDD's Long War Journal, November 21, 2019.
14 "Country Reports on Terrorism 2023 – Algeria," U.S. Department of State, December 12, 2024.
15 "Thirty-sixth report of the Analytical Support and Sanctions Monitoring Team submitted pursuant to resolutions 1267 (1999), 1989 (2011), and 2253 (2015) concerning Islamic State in Iraq and the Levant (Da'esh), Al-Qaida and associated individuals and entities," United Nations Security Council, July 24, 2025, p. 10.
16 Latifa Ferial Naili, "Algeria : Six Terrorists Eliminated, Nine Support Elements Arrested in One Week," Al24 News, October 1, 2025; Latifa Ferial Naili, "Algeria: Terrorist Surrenders, Seven Terrorist Supporters Arrested in One Week," Al24 News, October 15, 2025.
17 Warner and Hulme, "The Islamic State in Africa;" Geoff D. Porter, "AQIM Pleads for Relevance in Algeria," *CTC Sentinel* 12:3 (2019): pp. 32-36.
18 "Algerian army 'kills jihadist behind Herve Gourdel beheading,'" BBC, December 23, 2014.
19 "Country Reports on Terrorism 2015 – Algeria," U.S. Department of State, June 19, 2015.
20 "Country Reports on Terrorism 2020 – Algeria," U.S. Department of State, December 16, 2021.
21 Porter.
22 Hakim Gherieb, "US-Algeria Cooperation in Transnational Counterterrorism," Washington Institute for Near East Policy, March 27, 2017.
23 Kal Ben Khalid, "Evolving Approaches in Algerian Security Cooperation," *CTC Sentinel* 8:6 (2015): pp. 15-20; Nisan Ahmado, "Algeria Eyes Cross-Border Missions as Fear of Militant Spillover Grows," Voice of America, November 7, 2020.
24 Michael Greco, "Algeria's Strategy to Overcome Regional Terrorism," *National Interest*, February 27, 2019.
25 Abdelillah Bendaoudi, "How Lessons from Algeria Can Shape Iraq," Washington Institute for Near East Policy, August 8, 2018; Lotfi Sour, "From GIA to the Islamic State (IS): De-radicalization as countering violent extremism strategy in Algeria," *Journal of Central and Eastern European African Studies* 4:3-4 (2024): pp. 169-195.
26 *How the Islamic State Rose, Fell and Could Rise Again in the Maghreb* (Brussels: International Crisis Group, 2017), pp. 27-29.
27 David B. Ottaway, "Algeria: Bloody Past and Fractious Factions," Wilson Center, August 27, 2015.
28 Eleanor Beardsley, "Algeria's 'Black Decade' Still Weighs Heavily," NPR, April 25, 2011; Djamila Ould Khettab, "The 'Black Decade' still weighs heavily on Algeria," Al Jazeera, November 3, 2015.
29 Porter.
30 *How the Islamic State Rose*, p. 3.
31 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).
32 Olga Oliker, "Myths, Facts, and Mysteries About Foreign Fighters Out of Russia," CSIS, December 21, 2017.
33 Elena Pokalova, "The Islamic State Comes to Russia?" War on the Rocks, July 20, 2015.
34 Nick Sturdee and Mairbek Vatchagaev, "ISIS in the North Caucasus," New Lines Institute, October 26, 2020.
35 Ibid.
36 "Country Reports on Terrorism 2023 – Russia," U.S. Department of State, December 12, 2024.
37 "Thirty-sixth report of the Analytical Support and Sanctions Monitoring Team," pp. 16-17.
38 "The FSB of Russia Prevented A Series of Terrorist Crimes in the Republic of Ingushetia," Federal Security Service of the Russian Federation, August 28, 2024; Elizaveta Chukharova, "Three Ingushetian teenagers suspected of 'preparing a terrorist act,'" OC Media, March 17, 2025.
39 Elena Teslova, "Russia says over 120 terrorist crimes, including 64 attacks, thwarted in 2022," Anadolu Ajansi, December 13, 2022; "Russia Saw 40% Surge in Terrorism Cases in 2024, Top Investigative Body Says," *Moscow Times*, February 17, 2025.
40 Giuliano Bifolchi, "Counter-Terrorism Operations in Ingushetia and Adygea: Recent Developments," SpecialEurasia, September 2, 2024; Aaron Y. Zelin, "Various Activity Reports," Islamic State Select Worldwide Activity Interactive Map, Washington Institute for Near East Policy, accessed November 13, 2025.
41 "Russia Seeks to Quash the North Caucasus Terrorist Threat," CEPA, June 22, 2022.
42 "Country Reports on Terrorism 2020 – Russia," U.S.Department of State, December 16, 2021.
43 Sturdee and Vatchagaev; "IntelBrief: Radicalization and Extremism in Russia's North Caucasus Region," Soufan Center, April 12, 2024.
44 "Russia says it thwarted planned attack on synagogue," DW, March 7, 2024; Kathleen Magramo and Jerome Taylor, "Russia has seen two major terror attacks in just three months. Here's what we know," CNN, June 24, 2024.
45 "Thirty-sixth report of the Analytical Support and Sanctions Monitoring Team," pp. 16-17.
46 Giuliano Bifolchi, "Intelligence Report: The Ingush Jamaat and the Islamic State Wilayat Kavkaz," SpecialEurasia, April 19, 2024.
47 Thomas Hegghammer, "Islamist violence and regime stability in Saudi Arabia," *International Affairs* 84:4 (2008): pp. 701-715; Dodwell, Milton, and Rassler.
48 Aaron Zelin, "The Islamic State's Archipelago of Provinces," Washington Institute for Near East Policy, November 14, 2014; Scott Neuman, "ISIS Affiliate Claims Responsibility For Suicide Attack In Saudi Arabia," NPR, May 22, 2015.
49 Avaneesh Pandey, "Saudi Arabia Mosque Attack: New ISIS Affiliate 'Hijaz Province' Claims Responsibility," International Business Times, August 7, 2015.
50 "ISIS Says Saudi Bomb Attack Targeted France Over Cartoons," Agence France-Presse, November 13, 2020.
51 "Country Reports on Terrorism 2023 – Saudi Arabia," U.S. Department of State, December 12, 2024.
52 "Thirty-sixth report of the Analytical Support and Sanctions Monitoring Team."
53 Ralph Ellis, "Saudi Arabia arrests 431 with alleged ISIS ties," CNN, July 18, 2015.
54 "Country Reports on Terrorism 2016 – Saudi Arabia," U.S. Department of State, July 2017.

55 "Saudi arrests 13 linked to thwarted ISIL attack: State media," Al Jazeera, April 22, 2019.
56 Sumanto Al Qurtuby and Shafi Aldamer, "Terrorism and Counterterrorism in Saudi Arabia," *Contemporary Review of the Middle East* 8:1 (2020): pp. 56-76.
57 Deborah Amos, "Treating Saudi Arabian Jihadists With Art Therapy," NPR, April 5, 2015.
58 "Saudi Ideological War Center launches initiatives to fight terrorism," Arab News, May 2, 2017; Lori Plotkin Boghardt, "Is Saudi Arabia's Counterterrorism Approach Shifting?" Washington Institute for Near East Policy, January 9, 2018.
59 Cole Bunzel, "The Kingdom and the Caliphate: Duel of the Islamic States," Carnegie Endowment for International Peace, February 18, 2016.
60 Lila Hassan, "Repatriating ISIS Foreign Fighters Is Key to Stemming Radicalization, Experts Say, but Many Countries Don't Want Their Citizens Back," Frontline, April 6, 2021.
61 Thomas Hegghammer, "Jihad, Yes, But Not Revolution: Explaining the Extraversion of Islamist Violence in Saudi Arabia," *British Journal of Middle Easter Studies* 36:3 (2009): pp. 395-416; Bunzel.
62 Fayaz Bukhari and Alasdair Pal, "Islamic State claims 'province' in India for first time after clash in Kashmir," Reuters, May 12, 2019.
63 "ISIL 'has failed' to penetrate India," Al Jazeera, June 3, 2017; "ISIL claims 'province' in India, officials call it 'propaganda,'" Al Jazeera, May 12, 2019.
64 Aaron Y. Zelin, "Pledge of Allegiance of the Soldiers of the Caliphate in India to Abu-Husayn al-Husayni al-Qurashi," Islamic State Select Worldwide Activity Interactive Map, Washington Institute for Near East Policy, December 7, 2022.
65 "Who are ISIS India's two top leaders arrested by Assam Police?" Hindustan Times, March 21, 2024.
66 Author compiled data from Zelin's database. Aaron Y. Zelin, "Various Activity Reports," Islamic State Select Worldwide Activity Interactive Map, Washington Institute for Near East Policy, accessed November 13, 2025.
67 "Country Reports on Terrorism 2020 – India," U.S. Department of State, December 16, 2021.
68 "Country Reports on Terrorism 2021 – India," U.S. Department of State, February 27, 2023.
69 "Country Reports on Terrorism 2023 – India," U.S. Department of State, December 12, 2024.
70 Mukesh Singh Sengar, "ISIS Terrorists Planned On Targeting Right Wing Leaders, Reveal Chats: Sources," NDTV, September 12, 2025.
71 Raj Shekhar Jha, "ISIS module busted in Delhi: 2 operatives arrested; were planning IED blast," Times of India, October 24, 2025.
72 Mule Rohit Ashok, "The Evolution of India's `Counter-Terrorism (CT)' Policy in the 21st Century," *Journal of Terrorism Studies* 7:1 (2025): pp. 1-25.
73 Lauren Frayer, "'God, Please Help Her': Indian Parents Agonize Over Radicalization Of Their Children," NPR, May 26, 2019.
74 Erica Chenoweth, "Terrorism and Democracy," *Annual Review of Political Science* 16 (2013): pp. 355-378.
75 Aaron Y. Zelin, "Zubair Ahmed Munshi Arrested for Leading IS Cell," Islamic State Select Worldwide Activity Interactive Map, Washington Institute for Near East Policy, June 13, 2023.
76 "Ricin poison terror plot: Hyderabad doctor earned degree from China; ran shawarma stall after FMGE failure, say cops," Times of India, November 13, 2025.
77 Bardia Rahmani and Andrea Tanco, "ISIS's Growing Caliphate: Profiles of Affiliates," Wilson Center, February 19, 2016.
78 Jared Malsin, "ISIS Re-Establish Their Hold On Qaddafi's Home Town After Crushing a Rebellion," *Time*, August 19, 2015; "`We Feel We Are Cursed: Life Under ISIS in Sirte, Libya," Human Rights Watch, May 18, 2016.
79 Wilson and Pack.
80 Zelin, "Pledge of Allegiance of the Soldiers of the Caliphate in Libya."
81 Libya Mohammed, "Libyan Deterrence Apparatus arrests ISIS member in Libya," Libya Observer, January 5, 2024.
82 Aaron Y. Zelin, "Al Naba #512: 'Libya the Glorious,'" Islamic State Select Worldwide Activity Interactive Map, Washington Institute for Near East Policy, September 11, 2025; Cristiani.
83 Ibid.; Emily Milliken, "Is ISIS Making a Comeback in Libya?" *Newsweek*, September 8, 2021.
84 "Country Reports on Terrorism 2023 – Libya," U.S. Department of State, December 12, 2024; "Country Reports on Terrorism 2022 – Libya," U.S. Department of State, November 30, 2023; "Country Reports on Terrorism 2021 – Libya," U.S. Department of State, February 27, 2023.
85 "Thirty-sixth report of the Analytical Support and Sanctions Monitoring Team," p. 11.
86 "Libya forces make final push to clear ISIL from Sirte," Al Jazeera, October 12, 2016; Terri Moon Cronk, "U.S. Airstrikes Kill 80 ISIL Fighters in Libya, Carter Says," DOD News, January 19, 2017; Christopher Livesay, "ISIS regroups to attack a fragmented Libya," PBS News, September 29, 2018.
87 Kyle Rempfer, "US strikes culled ISIS-Libya encampments, unlikely to return to pre-2016 levels, defense official says," Army Times, October 14, 2019.
88 "USS Mount Whitney conducts Tripoli and Benghazi port visits to promote regional stability, national unity and Libyan sovereignty," U.S. Embassy Libya, April 21, 2025.
89 Wolfram Lacher, *Where Have All the Jihadists Gone? The Rise and Mysterious Fall of Militant Islamist Movements in Libya* (Berlin: German Institute for International and Security Affairs, 2024).
90 "'We Feel We Are Cursed': Life under ISIS in Sirte, Libya," Human Rights Watch, May 18, 2016.
91 Inga Kristina Trauthig, *Islamic State In Libya: From Force to Farce?* (London: ICSR, 2020).
92 John Vandiver, "US military's Libya outreach adds rung as rival sides to join special operations exercise," Stars and Stripes, October 16, 2025.
93 "Libya Emerges as an Arena for U.S.-Russia Competition," Soufan Center, March 31, 2025.
94 Nelly Lahoud, "The Province of Sinai: Why Bother with Palestine if You Can Be Part of the 'Islamic State'?" *CTC Sentinel* 8:3 (2015): pp. 12-14.
95 Barbara Starr and Catherine E. Shoichet, "Russian plane crash: U.S. intel suggests ISIS bomb brought down jet," CNN, November 4, 2015.
96 "Counterterrorism Guide: ISIS-Sinai," National Counterterrorism Center, May 2025.
97 "Country Reports on Terrorism 2023 – Egypt," U.S. Department of State, December 12, 2024.
98 "Thirty-sixth report of the Analytical Support and Sanctions Monitoring Team," p. 11.
99 Stav Levaton, "IDF says strike killed highest-ranking ISIS official in Gaza," Times of Israel, August 30, 2025.
100 Mohammad Zahran, "ISIS in Gaza: Israel's Propaganda Weapon Against Hamas," Al Mashhad, August 31, 2025.
101 "Explainer: Shift in reporting on Egypt's Sinai," BBC, June 15, 2022.
102 Ido Levy, "Egypt's Counterinsurgency Success in Sinai," Washington Institute for Near East Policy, December 9, 2021.
103 "TIMEP Brief: Sinai Tribes in Egypt's War on Terror," Tahrir Institute for Middle East Policy, November 28, 2018; David E. Thaler and Yousuf Abdelfatah, "Making Headway Against the Sinai Insurgency," RAND Corporation, August 12, 2019; Levy.
104 Allison McMaus, "The Egyptian Military's Terrorism Containment Campaign in North Sinai," Sada, June 30, 2020; Khalil Al-Anani, "Egypt's Counterterrorism Strategy in Sinai: Challenges and Failures," Arab Center Washington DC, August 28, 2020.
105 Gamal Essam El-Din, "The cost of terrorism," Ahram Online, February 9, 2023.
106 Mohamed Saad, "Localization of the counterinsurgency in Sinai: A case study on integrating local population into counterinsurgency combat operations in Sinai," *Digest of Middle East Studies* 33:2 (2024): pp. 108-124.
107 "Country Reports on Terrorism 2022 – Egypt," U.S. Department of State, November 30, 2023.
108 "Egypt: Questionable Amnesty Deals for ISIS Members," Human Rights Watch, March 13, 2024.
109 Kaamil Ahmed, "Mass grave reveals scale of unlawful killings by Egyptian army in Sinai, say campaigners," *Guardian*, September 22, 2025.
110 Lisa Blaydes and Lawrence Rubin, "Ideological Reorientation and Counterterrorism: Confronting Militant Islam in Egypt," *Terrorism and Political Violence* 20:4 (2009): pp. 461–479; Dina Al Raffie, "Extremism in moderation: Understanding state responses to terrorism in Egypt," in Michael J. Boyle ed., *Non-Western responses to terrorism* (Manchester: Manchester University Press, 2018), pp. 294-322.
111 Elisabeth Kendall, "The Failing Islamic State Within The Failed State of Yemen," *Perspectives on Terrorism* 13:1 (2019): pp. 77-86.
112 Aaron Y. Zelin, "Pledge of Allegiance of the Soldiers of the Caliphate in Yemen to Abu-Husayn al-Husayni al-Qurashi," Islamic State Select Worldwide Activity Interactive Map, Washington Institute for Near East Policy, December 3, 2022; Aaron Y. Zelin, "Pledge of Allegiance of the Soldiers of the Caliphate in Yemen to Abu-Hafs al-Hashimi al-Qurashi," Islamic State Select Worldwide Activity Interactive Map, Washington Institute for Near East Policy, August 6, 2023.
113 "Thirty-sixth report of the Analytical Support and Sanctions Monitoring Team," p. 15.
114 Christina Hellmich, "Fighting Al Qaeda in Yemen? Rethinking the Nature of the Islamist Threat and the Effectiveness of U.S. Counterterrorism Strategy," *Studies in Conflict & Terrorism* 35:9 (2012): pp. 618-633; Luke Hartig, "U.S. counterterrorism policy in Yemen from 2010–2020," in Michael A.

Sheehan, Erich Marquardt, Liam Collins eds., *Routledge Handbook of U.S. Counterterrorism and Irregular Warfare Operations* (London: Routledge, 2021).
115 "Dozens of ISIS fighters killed after US strikes Yemen camps," ABC News, October 16, 2017.
116 Hartig.
117 Sudarsan Raghavan, "With the ISIS caliphate defeated in Syria, an Islamist militant rivalry takes root in Yemen: The Islamic State and al-Qaeda branches in Yemen are in a deadly contest for influence," *Washington Post*, April 13, 2019.
118 Elisabeth Kendall, "Twenty Years After 9/11: The Jihadi Threat in the Arabian Peninsula," *CTC Sentinel* 14:7 (2021): pp. 63-75.
119 "Conflict in Yemen and the Red Sea," Council on Foreign Relations, March 26, 2025.
120 Elisabeth Kendall, "ISIS in Yemen: Caught in a Regional Power Game," New Lines Institute, July 21, 2020.
121 "Fact Sheet on ISIS Financing," U.S. Department of the Treasury, August 8, 2024.
122 Tore Hamming, "The General Directorate of Provinces: Managing the Islamic State's Global Network," *CTC Sentinel* 16:7 (2023): 20-27.
123 Janatan Sayeh, "Analysis: From Afghanistan to America: the rising reach of the Islamic State Khorasan Province," FDD's Long War Journal, February 17, 2025.
124 Djallil Lounnas, "The Impact of ISIS on Algeria's Security Doctrine," *Middle East Policy* 24:4 (2017): pp. 128-129; "Egypt: Questionable Amnesty Deals for ISIS Members;" Froilan Gallardo, "Marawi endures slow, painful rebuilding," Inquirer.Net, June 15, 2025.
125 "Amnesty urges probe into report of UAE torture in Yemen," Al Jazeera, June 22, 2017.
126 K*illed In Cold Blood: Untold Stories of Extrajudicial Killings and a Mass Grave in Sinai* (London: Sinai Foundation for Human Rights, 2025).
127 Don Rassler, "Smart Pressure: Conceptualizing Counterterrorism for a New Era," *CTC Sentinel* 17:10 (2024): pp. 1-14.

Burden-Sharing with Non-Traditional Counterterrorism Partners

By Iselin Brady and Daniel Byman

The United States works with an array of counterterrorism partners in efforts to fight global jihadi groups such as al-Qa`ida and the Islamic State. Counterterrorism partners give the United States additional reach, reduce the cost of counterterrorism, and often bring strong intelligence and military capabilities to the table. Although many U.S. partners are state governments, some are substate groups, including several that have questionable pasts, troubling associations, poor human rights records, and come with diplomatic complications. These are flawed, but often necessary, counterterrorism partners. In navigating these relationships, the United States must consider the costs and burdens these partners bring and recognize that the United States at times risks undermining U.S. values even as it promotes its interests.

The United States does not fight every battle or bear every burden in its struggle against foreign terrorist organizations. Encompassed in the military doctrine 'by, with, and through,' the United States has numerous allies and partners that fight terrorism on their own soil, share intelligence, and at times contribute military force to fight groups such as al-Qa`ida and the Islamic State. In most countries, government security services, police, and military forces are the key partners, but at times non-state actors are the only power on the ground to fight terrorists. In still other cases, such as Afghanistan and Syria today, the government itself may be a current or former terrorist group—but still a potential counterterrorism partner.

Many terrorist groups are active in places where the government is weak or non-existent, making traditional counterterrorism partners more difficult to find. Some groups seek to carve out de facto mini-states in areas where government writ is limited, such as Hezbollah in Lebanon. In recent decades, Sunni jihadi groups in Afghanistan, Iraq, Mali, Nigeria, Somalia, Syria, Yemen, and elsewhere have seized control of local areas and joined civil wars, helping defend Muslims and seeking to transform conflicts to spread their jihadi worldview.[1]

Non-traditional partners can save U.S. lives and cost little money, especially when compared with deployments of U.S. military forces, which can amount to hundreds of millions or even billions of dollars for small operations. Local forces typically have superior knowledge of their own populations, making them better suited to gather intelligence on terrorist operations or personnel. The United States can minimize a hostile backlash from the local population by relying on forces drawn from local communities and avoiding or minimizing the deployment of its own forces.[2]

The price of cooperation, however, is high. Many of these forces, while demonstrating a degree of military proficiency, require considerable support and training. These forces also are not guaranteed to be loyal to the United States, and may have political goals, internal or external, that cause diplomatic complications. Another challenge is that some partners or specific units commit human rights violations and maintain ties to various dangerous actors, including terror networks hostile to the United States.

To mitigate these problems, the United States must carefully choose which partners it is comfortable working with, and which can deliver the most advantageous results with limited U.S. resources. The United States should also collect intelligence on its partners, to both ensure the credibility of their intelligence and to monitor for human rights abuses or other nefarious actions of partners. Washington should also not be fully reliant on non-traditional partners. If these actors know that the United States has no other alternatives, the bargaining power of the United States decreases significantly. Where possible, the United States should train alternative forces or increase its unilateral capabilities.

The remainder of this article unfolds in four parts. It first presents three recent instances of counterterrorism cooperation with complicated partners: the Sons of Iraq, Kurdish forces in Syria, and Hay'at Tahrir al-Sham, both before and after it came to lead the government in Syria in 2025. The second section assesses the benefit of such partnerships, while section three outlines their costs as well as their limits. The article concludes by proposing several steps for burden-sharing with troubling partners.

Three Cases Involving Troubled Partners

In the post-9/11 era, the United States regularly worked with a wide range of allies, partners, and non-state proxies. Several of the most effective involved considerable tradeoffs, with many having links to other terrorist groups and poor human rights records. This section looks at three different U.S. relationships: the Sons of Iraq (2006-2009); Kurdish fighters in Syria (2015-present); and Hay'at Tahrir al-Sham, its predecessors, and the new Syrian government (2011-present).

Iselin Brady is a student in the Security Studies Program at Georgetown University.

Daniel Byman is a professor in the School of Foreign Service at Georgetown University and the Director of the Warfare, Irregular Threats, and Terrorism Program at the Center for Strategic and International Studies.

Sons of Iraq

The Sons of Iraq (SoI) emerged in 2006 following the U.S. invasion of Iraq in 2003. After large-scale combat operations concluded in April 2003, the "war after the war" began with insurgent and terrorist activity increasing throughout the country.[3] By the start of 2004, insurgent attacks rose to 200 weekly and in April reached 600, largely perpetrated by al-Qa`ida in Iraq (AQI). These trends continued upward throughout 2005, in some cases reaching over 800 incidents a week throughout the country.[4]

Many Sunni tribes, alienated by the new Shi`a-dominated Iraqi government and bitter toward the United States for its removal of the Sunni-dominated old regime, passively or directly supported the insurgency early on. However, they eventually began to feel alienated by AQI, which not only failed to protect them against Iraqi government attacks, but also used widespread violence against the Iraqi population—conducting attacks against tribal leaders, enacting extreme regulations, and punishing those who did not fully comply.[5]

In late 2005, many Sunni tribal militias turned away from the insurgents and began attempting to expel them from their territory, a turnaround known as the Anbar Awakening.[6] The Sons of Iraq formed from this Awakening as a U.S.-sanctioned counterinsurgency program.[7] The United States funded the SoI program, paying fighters $300 a month.[8] Perhaps more importantly, the United States provided them with backup and firepower: If AQI or other groups threatened them, the United States would surge forces in the area and provide air support. In addition, the Iraqi government worked with, rather than targeted, SoI leaders. The Iraqi government promised SoI fighters permanent employment after the conflict, with 20 percent of these fighters to be integrated into its security forces and alternative government employment for the remaining 80 percent. In 2007, the surge saw an increase in both U.S. troops in Iraq and the relationship between SoI and coalition forces, and by 2008, SoI had over 100,000 fighters operating in about two-thirds of the country.[9]

The Sons of Iraq were a critical partner for the United States in decreasing violence from al-Qa`ida in Iraq. While not authorized to engage in offensive operations, SoI fighters operated in their home provinces, acting as local law enforcement, manning checkpoints, and gathering intelligence on the identities of suspected insurgents and locations of weapons caches or IEDs.[10] They were particularly important for obtaining local intelligence: They knew their own communities and had legitimacy, making it easy for them to identify foreign fighters and other AQI members who were not from the area. The SoI were not intended as a permanent solution, but a "temporary measure meant to help the Coalition and Iraqi Security Forces move forward in delivering security."[11] By April 2009, coalition forces had transferred all SoI fighters and responsibilities to the Iraqi government.[12]

The Awakening and subsequent Sons of Iraq program, combined with the U.S. surge, led to several successes against al-Qa`ida in Iraq. Within the first year of the program, U.S. Marines reported that "without the Awakening, the surge would not have stabilized Iraq by the summer of 2008."[13] The SoI "were responsible for finding, collecting, or reporting locations of literally hundreds of munitions caches which CF and ISF were able to recover or reduce."[14] In addition to seizing weapons, they disrupted insurgent propaganda and training information. SoI intelligence led to the capture of five high-value targets and 100 suspected insurgents. There was also a notable decrease in AQI attacks: "attacks against CF, ISF, and local nationals dwindled from nearly 35 in July 2007 to less than 10 in January and March of 2008."[15] An AQI leader from al-Anbar province confirmed that "the turnaround of the Sunnis against us had made us lose a lot and suffer very painfully."[16] There was a reported 70 percent decrease in AQI members within six months, going from an estimated 12,000 to 3,500.[17]

Although coalition forces praised the short-term successes of the Sons of Iraq, the Iraqi government's reservations about their integration led to long-term failures of the program. SoI members' former support of the insurgency, Sunni religion, and ties to the Baath Party in the Saddam era led to mistrust between them and the Shi`a-dominated Iraqi government.[18] This, along with bureaucratic and resource constraints, led to a failure from the Iraqi government to provide promised employment to SoI fighters. In July 2010, less than half of the former SoI had been given jobs.[19] The Islamic State in Iraq (ISI), which formed in 2006 from AQI, directed recruitment efforts toward former SoI members who had not received permanent employment in the Iraqi government as promised. Security and political officials reported that hundreds of former fighters had either defected to ISI or become double agents.[20] Former local Awakening leader Nathum al-Jubouri stated that "members have two options: Stay with the government, which would be a threat to their lives, or help al-Qaeda by being a double agent."[21] The situation further escalated after security forces began arresting former SoI fighters on terrorism charges. In Diyala province, 90 members were arrested between January and October 2010, half of whom were later released for lack of evidence.[22]

The Sons of Iraq represented a critical component of U.S. counterinsurgency strategy in Iraq, and there are lessons the United States can draw from this partnership. Being able to provide military backup for proxies made them more willing to oppose insurgents. Offering employment and monthly payments were key components to establishing the Sons of Iraq program and were successful in using people who had defected from AQI. Although it was necessary to transfer management of the program to the Iraqi government, failing to establish a mechanism that would guarantee SoI members were properly integrated into the new government allowed the Iraqi state to abandon these promises, causing widespread dissatisfaction among former militia members. ISI was able to exploit these tensions and recruit the very fighters that were essential to the U.S. strategy in Iraq.

The Kurds in Syria

The Kurdish people—through the Syrian Democratic Forces (SDF)—have been critical in U.S. efforts to defeat the Islamic State in Syria. The Kurdish community in Syria is small compared to that of Iran, Iraq, or Turkey: Only around 2.5 million Kurds live in Syria, mostly in the northeast.[23] Following the outbreak of the Syrian civil war in 2011 and the rise of the Islamic State in 2014—and the failure of a U.S. program to train Syrian rebels to fight the Islamic State—the United States supported the creation of the SDF in October 2015.[24] The SDF is a multi-ethnic military coalition of former U.S.-aligned Kurdish, Arab, Turkmen, Assyrian, and Armenian groups operating in the Democratic Autonomous Administration in North and East Syria (DAANES).[25]

The Kurdish People's Protection Unit (YPG) dominates the SDF.[26] The YPG is the military wing of the Democratic Union Party, the leading Kurdish political party in northern Syria.[27] Kurdish

Yekineyen Anti-Terror (YAT) soldiers prepare to engage targets during close-quarter battle training in northeast Syria on January 10, 2025. The exercise is part of ongoing coalition operations with the YAT, the Syrian Democratic Forces' Counter-Terrorism Force, aimed at enhancing squad-level tactics and improving overall combat proficiency. (Sgt. Keyona P. Smith/ U.S. Army)

fighters make up approximately 40 percent of the SDF's estimated 50,000 fighters.[28]

The SDF established itself as the West's main—and often only reliable—local partner in its fight against the Islamic State in Syria.[29] Its partnership with U.S. Special Operations Joint Task Force - Operation Inherent Resolve (SOJTF-OIR) was instrumental in defeating the Islamic State's territorial caliphate in March 2019. Since then, Washington has continued supporting—through advise and assist missions, equipment, training, intelligence, and logistics support—SDF counterterrorism operations.[30]

The overall effectiveness of the U.S.-Kurdish partnership was evident in the operations following the Islamic State's announcement of its caliphate in 2014 and the official establishment of the SDF. The SDF began clearing villages and towns in northwest Syria with coalition support in 2015.[31] The SDF conducted operations in, and successfully liberated, key sites, including the Tishrin Dam in 2015, Raqqa in 2017, and Deir ez-Zor in 2019.[32] In most of these operations, the United States provided intelligence, standoff strikes via air and other platforms, and other critical support, while the SDF did much of the heavy fighting on the ground, with losses estimated at 11,000 SDF soldiers during this time.[33]

The SDF role continued following the defeat of the physical Islamic State caliphate in 2019. Washington continued to focus on advising the SDF on "partnered patrols" and "combined exercises."[34] Advisors conducted training on counter-IED tactics and "noted improved capability in that area."[35] As one example of operations, in a June 2020 mission, the SDF detained 69 Islamic State members and seized multiple weapons and ammunition caches.[36] From December 2024 to February 2025, the SDF reported that it had carried out 75 operations against the Islamic State.[37]

During operations against the Islamic State from 2014 to 2019, the SDF established prisons and detention camps to hold Islamic State fighters and their affiliates. The SDF maintains control of these prisons today, with an estimated 50,000 Islamic State-affiliated individuals detained, including women and children linked to fighters.[38]

The prisons and camps were a short-term solution that has become a difficult longer-term issue. These prisons and camps have caused numerous concerns regarding the effectiveness of such camps, human rights abuses by SDF forces, and the radicalization risk it carries for those imprisoned.[39] The United States will likely continue to support these prisons, even indirectly, due to a lack of realistic alternatives for what to do with the Islamic State-affiliated individuals. Several E.U. countries do not wish to repatriate their citizens who traveled to Syria to fight alongside the Islamic State.[40]

While the Islamic State's physical caliphate fell in 2019, there are still an estimated 2,500 Islamic State fighters operating in Syria and Iraq today.[41] In addition to the continuation of Islamic State attacks,

there are key complications and policy failures that have hindered the U.S.-SDF partnership. The SDF's affiliation with the Kurdistan Workers' Party (PKK) complicates the U.S.-Turkey relationship. The PKK is a Kurdish separatist group originally formed to create an independent Kurdish state in Turkey, and the United States has designated it as a foreign terrorist organization (FTO) since 1997.[42] The YPG was formed by former PKK members and maintains links to the PKK.[43] Turkey views the two groups as directly linked, making the SDF complicit in all PKK activity. Following a pause in fighting, violence between the PKK and Ankara resumed in 2015, subsequently increasing Turkish attacks against Kurdish-controlled territory. Turkey, along with its Syrian allies, seized territory in northeast Syria in 2018 and 2019, forcing the SDF to shift troops and resources away from their counterterrorism goals and putting two important U.S. allies in conflict.[44]

Further, when SDF troops redeployed to respond to Turkish-backed forces, as was done in October 2019, it decreased the number of troops guarding detention camps.[45] The Ain Issa camp went from 700 guards to 60 or 70. After Turkish bombs struck near the camp, an estimated 850 detainees escaped, 100 of whom were reportedly not recaptured.[46]

The United States has established a counterterrorism partnership with the SDF that avoids other regional dynamics, including ethnic tensions, governance, or security concerns from other states. The limited nature of the partnership has both benefits and consequences, however. Ankara's continued attacks against the SDF will hinder its ability to protect the territory it controls, guard Islamic State prisons, and conduct counterterrorism operations.

Hay'at Tahrir al-Sham, the New Syrian Government, and Counterterrorism in Syria

Hay'at Tahrir al-Sham (HTS, or the Organization for the Liberation of the Levant) emerged from the Syrian civil war that began in 2011. After over a decade of hard fighting, in December 2024 HTS led the overthrow of the regime of Bashar al-Assad and assumed power in Syria, officially establishing a new government in March 2025.

After the civil war began, a host of jihadis, both local and foreign, joined the fray.[47] HTS grew out of the jihadi civil war that began in Syria in 2013 between the Islamic State in Iraq and Syria, which later became the Islamic State, and various other jihadis, including those linked to al-Qa`ida, particularly Jabhat al-Nusra. During this time period, the United States regularly bombed al-Nusra and tried to kill its leaders. U.S. officials believed that al-Nusra members planned external operations that would target the United States and its allies and that al-Nusra's growth in Syria would enable a long-term al-Qa`ida presence there that would increase the risk of international terrorism.[48]

After having fallen out with the Islamic State, Jabhat al-Nusra then publicly split from al-Qa`ida in 2016 and formed a new organization that, over time, became HTS, with over 10,000 fighters under arms.[49] Since 2017, HTS has controlled parts of Idlib Province. The leader of Jabhat al-Nusra, Abu Mohammad al-Julani, retained control of HTS and is now the leader of Syria, going by the name of Ahmed al-Sharaa. In 2018, the U.S. Department of State designated HTS as a terrorist organization because of its Jabhat al-Nusra legacy, and this lasted until July 2025. The United Nations continues to designate HTS.[50]

Despite these ties, HTS and after December 2024 the new Syrian government, has repeatedly attacked and suppressed al-Qa`ida-linked individuals, Islamic State forces, and the Lebanese Hezbollah in areas under its control. The enmity between HTS and Hezbollah runs deep. The Lebanese Hezbollah closely backed the former Syrian government of Bashar al-Assad, and when it controlled the Idlib area, HTS cracked down on Hezbollah and Iran. Even before that, in the days when it was Jabhat al-Nusra, the group conducted cross-border attacks and suicide bombings against Hezbollah targets in Lebanon and arrested Hezbollah fighters in Syria.[51]

"Because the United States is reluctant to deploy large numbers of its own forces to fight terrorists everywhere around the globe, it will continue to rely on local actors, and this will often lead to strange bedfellows."

Bad blood between HTS and the Islamic State has persisted for over a decade. During its time in control of Idlib, Islamic State fighters refused to recognize HTS' authority, and the Islamic State kidnapped, assassinated, beheaded, and otherwise attacked HTS officials and fighters and tried to coerce the population under HTS' control. In response, HTS security services arrested (and at times killed) Islamic State fighters—over 62 operations in total.[52] By 2018, HTS had successfully suppressed Islamic State attacks in areas it controlled.[53]

The United States, however, was slow to recognize the genuine break between HTS and other jihadi groups, in part because of continuing contact, rhetoric support, and other linkages and uncertainties.[54] In 2013, as the break between Jabhat al-Nusra and the Islamic State was beginning, the two groups continued to conduct joint operations, and al-Julani even praised the head of the Islamic State.[55] Islamic State leaders, including two of its self-proclaimed caliphs, also tried to hide out in HTS territory. Leading HTS scholar Aaron Zelin assesses that HTS probably was not aware of their presence there and that the leaders were simply taking advantage of the relative anonymity they enjoyed in this area, but even the possibility of cooperation was troubling.[56] Even as these possible ties continued, HTS may have also been a U.S. counterterrorism partner: Syria expert Wassim Nasr contends it is possible that by 2017, HTS was providing information on al-Qa`ida and other groups to enable U.S. targeting.[57]

Since taking power in Syria, the government (led by former HTS members) has continued to act against the Islamic State and Hezbollah, and it is not known to have provided support to any externally oriented terrorist groups. Before taking power, HTS tried to disrupt the flow of arms to Hezbollah in Lebanon from Iran, which for years has used Syria as a transit route. HTS has also disrupted Hezbollah cells in parts of Syria. With the Syrian government's tacit support, the United States had continued airstrikes against the Islamic State in Syria, working with the Syrian Democratic Forces, which operate uneasily under the new government and control several governorates in Syria where the Islamic State remains active. The Syrian government, acting on information provided by U.S. intelligence, has also stopped an

Islamic State bombing attempt in Damascus. The new government also shared information it gleaned from arrests to help target Islamic State operatives in Iraq.[58]

HTS was valuable as a counterterrorism partner before it led the overthrow of the Assad government, and the regime it leads today remains valuable as a counterterrorism partner for several reasons. The Syrian regime exercises control of much of Syria and, as such, controls the legal system; commands a large number of police, intelligence, military, and paramilitary figures; and otherwise is able to monitor and disrupt Islamic State and Hezbollah cells and operations. Sharing information from arrests and raids also allows Iraq and other countries to disrupt terrorist cells on their soil. In addition, HTS leaders' jihadi background gives it familiarity with jihadi networks, key individuals, and other vital components of groups such as al-Qa`ida. The Syrian regime's disruption of Hezbollah's presence in Syria removes a longstanding pillar the Lebanese group relied on and also makes it harder for Iran to support Hezbollah. According to Sebastian Gorka, the president's senior counterterrorism advisor, "We are working to try and make Damascus better at doing counterterrorism."[59]

Despite these advantages, the new Syrian government poses several difficulties, some severe, as a counterterrorism partner. Although the group is not known to have active ties to al-Qa`ida, individuals in what was HTS maintain ties to terrorists of various stripes from their days as Jabhat al-Nusra.[60] It is difficult to separate out how much contact, if any, is operational, especially with regard to external operations. HTS also had ties to Central Asian groups that have their own links to al-Qa`ida and the Islamic State.[61] Making this unclear picture even murkier, it is difficult to know HTS-linked individuals' genuine beliefs and true intentions. HTS in 2021 praised Hamas operations against Israel, and its ideologues in the past praised attacks in the West, including a beheading in France in 2020.[62] These associations and possible sympathies raise the risk of being wrong about whether HTS has truly changed and, in so doing, the United States would be providing assistance to a regime led by secret terrorists sympathizers and supporters.

In addition to these troubling associations, the Syrian government, run by al-Sharaa and other members of what was HTS, as a whole is weak: It does not control all of Syrian territory, and Syria's economy suffers from many problems as a result of over a decade of civil war and decades more of economic mismanagement. As a result, the government's resources are stretched thin and groups such as the Islamic State remain active in parts of Syria. This will limit the value of the Syrian regime as a counterterrorism partner, even though it still offers many benefits. Beyond its counterterrorism performance, al-Sharaa appears to have authoritarian leanings, reflected both in HTS' policies when, as a rebel group, it governed the Idlib area and when government-linked Bedouins and others have attacked groups such as the Druze and other perceived opponents they often paint as apostates.[63] To be clear, the regime so far is less brutal than the Assad regime and makes gestures to include various Syrian communities, but its commitment to an open system remains unclear, and the apparent toleration of violence against the Druze raises troubling questions.[64] Bolstering the Syrian regime in the name of counterterrorism thus may strengthen an authoritarian government.

A Necessary Evil?

As with other counterterrorism partners, working with groups like the Sons of Iraq, SDF, and (indirectly) HTS both as a rebel group and as the government of Syria reduces the burden on the United States. These groups have provided, or provide, much of the fighting power against key terrorist groups active in the Levant, which has reduced the cost to the United States and the risk to U.S. personnel. By providing training, intelligence, resources, and military support to these three entities, U.S. counterterrorism efforts have been more effective and far cheaper than they would have been with a more unilateral approach.

"The United States will need to approach burden-sharing with a clearer understanding that such cooperation is inherently transactional, fragile, and shaped by shifting local power balances."

In all three instances examined above, the United States had few alternatives to the partners in question. Because terrorist groups are likely to operate in areas where the government is weak, the United States will often have to work with substate groups or other non-traditional partners, some of whom will have troubling histories or unsavory ties, as part of its CT efforts. In Syria, for example, the Obama administration saw the Assad regime as an enemy and repeatedly tried to work with various Syrian factions, spending hundreds of millions of dollars to little avail—only the SDF proved a competent and politically acceptable partner for the United States. The new Syrian government led by former HTS members is now the most powerful force in the country, and its cooperation is vital when seeking to suppress Islamic State remnants there. Similarly, support for the Sons of Iraq became necessary because existing Kurdish and government allies in Iraq had little support in Sunni areas where AQI was strong—indeed, they were often seen as an enemy force. The need for effective counterterrorism cooperation has often trumped concerns over the histories, associations, or other actions of these partners. Common counterterrorism goals between the United States and the three partners described has guided such cooperation and allowed each party to overcome concerns.

In addition to fighting power, partners on the ground offer intelligence and legitimacy. By working with fighting forces drawn from local communities as with the SoI and SDF, the United States was able to develop a granular intelligence picture. This helped identify al-Qa`ida and Islamic State fighters and their supporters and, just as importantly, reduce the likelihood of arresting or killing individuals not affiliated with the group and thus reducing the risk of blowback from the local community.

The Costs and Risks of Troubling Partners

Non-traditional partners come with their own problems and risks. Although all of these partners demonstrated a degree of military proficiency, they have many limits. Both the SoI and the SDF required considerable U.S. airpower and other military support to conduct effective operations. There was also a noticeable shift in the SDF's capabilities—both in military strength and local intelligence capability—once operations began moving south to the Deir ez-Zor

governorate, where there were no Kurdish communities. The battle in Deir ez-Zor lasted twice as long as Mosul, for example.[65] Further, forces that Assad supported were able to lift the siege in the town of Deir ez-Zor in two months, while the SDF's military campaign to the east lasted over a year.[66]

Many partners are involved in human rights abuses. HTS, for example, governed territory it controlled in an authoritarian manner, subordinating minority groups, and that record today, as it has pivoted to leading Syria, raises many questions.[67] SDF forces have been accused of forcefully entering into cities the Assad regime pulled out of, detaining or killing civilians, torturing prisoners in its detention camps, and recruiting child soldiers.[68] One observer described some SoI forces as "hunt[ing] al-Qaeda down with vengeance. They dragged al-Qaeda guys through streets behind cars… It was pretty much just a ruthless slaughter."[69] Such partners are also not confined to U.S. rules of engagement and can operate without accountability to the international community. This risks U.S. resources or weapons being used in unintended ways, with the United States potentially being implicated for its assistance. Nor are these partners necessarily aligned with the United States, especially after the immediate shared enemy is defeated. They have come together due to shared interests, but they seek to maximize the power of their community or faction, even if it conflicts with broader U.S. goals.

These partners often have troubling associations. The SoI grew out of AQI, and HTS grew out of the jihadi movement in Syria. In both cases, this background gave them superior knowledge of their eventual terrorist enemies, but it also risks lingering ideological sympathy and, as happened with the SoI, some members could later join a terrorist group if conditions change.[70] It also increases the risk that weapons, intelligence, and funding might be diverted to terrorist groups.

These partners also cause diplomatic complications, including with host or neighboring governments. Turkey, an important NATO ally, saw the Kurdish-dominated SDF as a potential threat to its own stability and firmly opposed U.S. support for the group. The SoI's independence angered the government of Iraq, which saw it as a rival as well as a counterterrorism partner. The new Syrian government, which is led by many former HTS members, will be important for containing the Islamic State and Hezbollah, but Israel sees the government as a potential threat and has launched military strikes on its forces, putting the United States at odds with an important ally.

Future Considerations on Burden-Sharing

Because the United States is reluctant to deploy large numbers of its own forces to fight terrorists everywhere around the globe, it will continue to rely on local actors, and this will often lead to strange bedfellows. Gorka, the president's senior counterterrorism advisor, noted that he considers the Taliban a cooperative counterterrorism power.[71] In addition to Afghanistan, the United States is expanding ties to the new Syrian government, and, in the future, Washington might consider increasing efforts to combat jihadi groups in Africa, which could involve an array of unsavory partners. In such cases, the partners' poor human rights records, ties to terrorists, and diplomatic complications will make them troubling counterterrorism allies.

The United States will need to approach burden-sharing with a clearer understanding that such cooperation is inherently transactional, fragile, and shaped by shifting local power balances. Taliban cooperation with the United States against the Islamic State Khorasan (ISK) branch is based on the threat ISK poses to the Taliban's rule and is further complicated by the Taliban's relationships with different power brokers within Afghanistan itself. Providing the Taliban with intelligence on ISK is sensible, but the long-term U.S.-Taliban relationship is likely to remain fraught.[72]

Furthermore, reliance on these partners complicates long-term strategy and demands sustained U.S. engagement beyond immediate battlefield objectives—for which the United States must prepare. Partners such as the Sons of Iraq show that tactical gains can collapse if the United States fails to support governance, economic inclusion, and political reintegration after fighting ends. When U.S. commitment is uncertain or when host governments later sideline or punish these partners, groups may splinter, re-arm, or even defect to terrorist organizations—as occurred when many former Sons of Iraq members were recruited by the Islamic State. Therefore, burden-sharing must be paired with long-term political planning and monitoring to avoid undermining initial security gains.

Future burden-sharing will require the United States to accept a persistent tension between *effectiveness* and *values*. Working with actors tied to prior insurgencies or human rights abuses risks moral compromise, diplomatic friction with allies, and reputational damage. The Taliban, for example, have a poor human rights record, and Israel is hostile to the new Syrian government.[73] Yet, refusing cooperation because of these or similar concerns may leave the United States without partners in key theaters. The implication is that burden-sharing going forward will not simply involve distributing military responsibilities. It will require continuous risk management: vetting partners, collecting intelligence on their behavior, maintaining fallback options, and being prepared to withdraw or shift support when partners diverge from U.S. interests. Burden-sharing will remain essential, but it will continue to be a strategic balancing act rather than a stable or low-cost solution. CTC

Citations

1 Thomas Hegghammer, "The Rise of Muslim Foreign Fighters: Islam and the Globalization of Jihad," *International Security* 35:3 (2010): pp. 53-94; Daniel Byman, *Road Warriors: Foreign Fighters in the Armies of Jihad* (Oxford: Oxford University Press, 2019).
2 Many of these points are developed in the literature on proxy wars. See, inter alia, Andrew Mumford, *Proxy Warfare: War and Conflict in the Modern World* (Cambridge: Polity Press, 2013); Tyrone L. Groh, *Proxy War: The Least Bad Option* (Stanford: Stanford University Press, 2019); Vladimir Rauta, "Proxy Warfare and the Future of Conflict: Take Two," *RUSI Journal* 165:2 (2020): pp. 1-10; and Daniel Byman, "Outside Support for Insurgent Movements," *Studies in Conflict & Terrorism* 36:12 (2013): pp. 981-1004.
3 Richard Shultz, "'The Irreducible Minimum': An Evaluation of Counterterrorism Operations in Iraq," *PRISM* 7:3 (2018): pp. 102-117.
4 Ibid.
5 Najim Abed al-Jabouri and Sterling Jensen, "The Iraqi and AQI Roles in the Sunni Awakening," *PRISM* 2:1 (2010): pp. 3-18.
6 "Iraqi Government Assumes Responsibility for All 'Sons of Iraq,'" DVIDS, April 1, 2009.
7 Nizar Mohamad, "A Coalition of Negatives: The Case of the Sons of Iraq and the US in their Counterinsurgency Alliance," *Journal of Military Strategic Studies* 18:4 (2018): pp. 149-176.
8 Farook Ahmed, "Backgrounder #23: Sons of Iraq and Awakening Forces," Institute for the Study of War, February 21, 2008.
9 Govinda Clayton and Andrew Thomson, "The Enemy of My Enemy is My Friend … The Dynamics of Self-Defense Forces in Irregular War: The Case of the Sons of Iraq," *Studies in Conflict & Terrorism* 37:11 (2014): pp. 920-935.
10 Ahmed.
11 Ibid.
12 "Iraqi Government Assumes Responsibility for All 'Sons of Iraq.'"
13 Shultz.
14 Andrew W. Koloski, "Thickening the Lines: Sons of Iraq, A Combat Multiplier," *Military Review* (January-February 2009): pp. 41-53.
15 Ibid.
16 Ahmed.
17 Ibid.
18 Ibid.
19 Adam Weinstein, "U.S. troops transitioning 'Sons of Iraq' to local control," U.S. Army, December 9, 2008.
20 Timothy Williams and Duraid Adnan, "Sunnis in Iraq Allied With U.S. Rejoin Rebels," *New York Times*, October 16, 2010.
21 Shultz.
22 Williams and Adnan.
23 "Kurds in Syria," Minority Rights Group, March 2018.
24 Hassan Hassan, "The Battle for Raqqa and the Challenges after Liberation," *CTC Sentinel* 10:6 (2017).
25 Eric C. Bullard, "Syrian Democratic Forces," EBSCO, 2025.
26 Hassan, "The Battle for Raqqa and the Challenges after Liberation."
27 Genevieve Casagrande, "The Road to Ar-Raqqah: Background on the Syrian Democratic Forces," Institute for the Study of War, November 22, 2016.
28 Mohammed Hassan, "Building Syria's new army: Future plans and the challenges ahead," Middle East Institute, June 12, 2025.
29 Wladimir van Wilgenburg, "Syrian Democratic Forces (Syria)," European Council on Foreign Relations, n.d.
30 Ibid.; "SDF Begins Raqqa Offensive, Progress Continues in Mosul," U.S. Department of War, June 6, 2017.
31 Terri Moon Cronk, "US-led coalition's support to continue after Raqqa's liberation, Army major general says," U.S. Army, November 2, 2017.
32 Ibid.; Seth Frantzman, "The strategic Tishrin Dam has become a flashpoint in post-Assad Syria," FDD's Long War Journal, January 26, 2025.
33 "Squaring the Circles in Syria's North East," Middle East Report N°204, International Crisis Group, July 31, 2019.
34 "Home: Who We Are," Operation Inherent Resolve, n.d.
35 Ibid.
36 Brandon Ames, "Syrian Democratic Forces Display Strength, Capabilities through Successful Operations," U.S. Army Central, July 20, 2020.
37 Samer Yassin, "SDF carries out 75 anti-ISIS operations since December – Spokesman," North Press Agency, February 17, 2025.
38 Ido Levy, "Supporting the SDF in Post-Assad Syria," Washington Institute for Near East Policy, December 13, 2024.
39 "Report to Congress on An Interagency Strategy with Respect to ISIS-affiliated Individuals and ISIS-related Detainee and Other Displaced Persons Camps in Syria," U.S. Department of State, 2025.
40 Van Wilgenburg. For further research on how to deal with foreign fighters detained by the SDF, see Brian Michael Jenkins, "Options for Dealing with Islamic State Foreign Fighters Currently Detained in Syria," *CTC Sentinel* 12:5 (2019).
41 Caroline Rose and Colin P. Clarke, "The Return of ISIS," *Foreign Affairs*, September 18, 2025.
42 "Kurdistan Worker's Party (PKK)," National Counterterrorism Center, April 2025.
43 Van Wilgenburg; "Counter-terrorism Pitfalls: What the U.S. Fight against ISIS and al-Qaeda Should Avoid," Special Report N°3, International Crisis Group, March 22, 2017.
44 Mohammed A. Salih, "US Policy in Northeast Syria: Toward a Strategic Reconfiguration," Foreign Policy Research Institute, May 6, 2024.
45 Martijn Vugteveen and Joshua Farrell-Molloy, "Turkish Military Offensive in Syria: Consequences for Counter-Terrorism Operations," International Centre for Counter-Terrorism, June 28, 2022.
46 Ibid.; Aron Lund, "What is the 'Khorasan Group' and Why Is the United States Bombing It in Syria," Carnegie Endowment, September 13, 2014.
47 Byman, *Road Warriors*, pp. 164-203.
48 Martin Chulov, "Al-Nusra Front cuts ties with al-Qaida and renames itself," *Guardian*, July 28, 2016.
49 "Hay'at Tahrir al-Sham (HTS): TNT Terrorism Backgrounder," Center for Strategic and International Studies, October 4, 2018; Daniel L. Byman and Jennifer R. Williams, "ISIS vs. Al Qaeda: Jihadism's global civil war," Brookings Institute, February 24, 2015.
50 Marco Rubio, "Revoking the Foreign Terrorist Organization Designation of Hay'at Tahrir al-Sham," U.S. Department of State, July 7, 2025; Jason M. Blazakis, "Understanding the Trump Administration's Delisting of Hay'at Tahrir al-Sham," Just Security, July 18, 2025.
51 "HTS Condemns U.S. Terror Designation, Demands Evidence of AQ Link," SITE Intelligence Group, June 1, 2018; Aaron Y. Zelin, "Jihadi 'Counterterrorism:' Hayat Tahrir al-Sham Versus the Islamic State," *CTC Sentinel* 16:2 (2023); Aaron Y. Zelin, "The New Syrian Government's Fight Against the Islamic State, Hezbollah, and Captagon," *CTC Sentinel* 18:3 (2025).
52 Zelin, "The New Syrian Government's Fight Against the Islamic State, Hezbollah, and Captagon."
53 Zelin, "Jihadi 'Counterterrorism.'"
54 "Amendments to the Terrorist Designations of al-Nusrah Front," U.S. Department of State, May 31, 2018.
55 Zelin, "Jihadi 'Counterterrorism.'"
56 Ibid.
57 Wassim Nasr, "The Syrian Civil War Part 1," "Conflicted" podcast, February 12, 2025, see minutes 27 and 31.
58 Zelin, "The New Syrian Government's Fight Against the Islamic State, Hezbollah, and Captagon;" Warren P. Strobel, Ellen Nakashima, and Missy Ryan, "U.S. shared secret intelligence with Syria's new leaders," *Washington Post*, January 24, 2025.
59 "Sebastian Gorka on the Trump Administration's Approach to Counterterrorism," C-Span, August 21, 2025.
60 Michelle Nichols, "Exclusive: UN report sees no active Syrian state links to Al Qaeda," Reuters, July 11, 2025; "Twenty-second report of the Analytical Support and Sanctions Monitoring Team submitted pursuant to resolution 2368 (2017) concerning ISIL (Da'esh), Al-Qaida and associated individuals and entities," United Nations Security Council, July 27, 2018.
61 Kathleen Collins, "Uzbek Foreign Fighter Groups in the Syrian Jihad: The Evolution of KIB and KTJ from 2011 through 2025," *CTC Sentinel* 18:9 (2025).
62 Zelin, "Jihadi 'Counterterrorism.'"
63 Ibid.; Beatrice Farhat, "Syria: Nearly 100 killed in fighting between Druze, Sunni tribes," Al-Monitor, July 14, 2025.
64 Christopher Blanchard, "Syria: Transition and U.S. Policy," Congressional Research Service, September 5, 2025.
65 Hassan Hassan, "A Hollow Victory over the Islamic State in Syria? The High Risk of Jihadi Revival in Deir ez-Zor's Euphrates River Valley," *CTC Sentinel* 12:2 (2019).
66 Ibid.
67 Nury Turkel et al., "Factsheet: Religious Freedom in Syria," United States Commission on International Religious Freedom, November 2022.
68 "2023 Country Reports on Human Rights Practices: Syria," Bureau of Democracy, Human Rights, and Labor, U.S. Department of State, 2023; "Syria 2024," Amnesty International, n.d.

69 Jon Moran, "State Crime, Irregulars and Counter-Insurgency," *State Crime Journal* 4:2 (2015): pp. 154-174.
70 Williams and Adnan.
71 "Sebastian Gorka on the Trump Administration's Approach to Counterterrorism."
72 "Senior Study Group on Counterterrorism in Afghanistan and Pakistan: Final Report," United States Institute of Peace, May 14, 2024; Dan De Luce, Mushtaq Yusufzai, and Tom Winter, "The Enemy of my Enemy: Biden Admin Weighs Working with the Taliban to Combat ISIS-K," NBC News, July 3, 2024.
73 "Afghanistan: Events of 2024," Human Rights Watch, n.d.

Foreign Terrorist Fighters: A Threat in Stasis

By R. Kim Cragin

This article examines the historical trajectory of "foreign terrorist fighters" associated with the Islamic State and its antecedents, al-Qa`ida and the Arab Afghans. The article argues that the threat of foreign fighters today is best understood as being in stasis. Foreign fighters continue to pursue external operations against the West. They also transfer new tactics, techniques, and procedures between conflict zones. These patterns are not new. Beyond these historical patterns, foreign terrorist fighters have become increasingly adept at reaching out to new sympathizers and serving as interlocutors between Islamic State affiliates in conflict zones and their sympathizers. FTFs also have utilized end-to-end encryption technologies, generative artificial intelligence, and cryptocurrencies to magnify their impact. Nevertheless, it is not yet time for alarm. Countries have strengthened their laws, intelligence-sharing, and law enforcement coordination over the past decade. If governments continue to build on this collective effort and devote resources toward mitigating foreign fighter flows, the threat should remain in stasis.

On February 27, 2025, Abdisatar Ahmed Hassan was arrested in Minneapolis, Minnesota, and charged with providing material support to the Somalia branch of the Islamic State.[1] According to the U.S. government, Hassan aspired to become a foreign terrorist fighter (FTF).[a] He attempted to travel from Minneapolis to Garowe, Somalia, on two occasions—December 13 and December 29, 2024—to join Islamic State-Somalia.[2] Yet, Hassan failed both times. These failures apparently prompted Hassan to shift his efforts to attacking the United States. He failed again. Hassan was arrested after he reposted Islamic State videos encouraging followers to "kill them where you find them"[b] as well as his own video clips depicting hands holding a knife and an Islamic State flag.[3]

The story of Abdisatar Ahmed Hassan illustrates the dilemma countries face when responding to FTF travel. Hassan was 22 years old at the time of his arrest. He was born in Kenya but became a naturalized U.S. citizen.[4] Upon learning of Hassan's intention to join Islamic State-Somalia, U.S. authorities had several options: allow him to depart for Somalia, prevent Hassan's departure and monitor him, or arrest him on somewhat minor terrorism charges. Each option has inherent risks. Historically, until late 2015, most countries opted to allow FTFs to depart for conflict zones abroad in the hopes that they would not return.[5] Yet, this approach had unforeseen consequences: It caused the tactics, techniques, and ideologies of terrorist groups to metastasize globally.[6]

The November 2015 attacks by the Islamic State against the Bataclan concert hall, restaurants in Paris' 11th District, as well as the Stade de France prompted a new global response to FTF travel. Western governments, in particular, reinterpreted FTFs as a threat not only to conflict zones, but also to countries of origin and transit.[7] Seven of the nine individuals responsible for executing the Paris attacks were FTF returnees. They had traveled from Belgium and France to fight in the Middle East. Led by Abdelhamid Abaaoud, they subsequently returned home to recruit others and build a network of approximately 30 individuals to support terrorist attacks in Paris and Brussels.[8] The Global Coalition to Defeat ISIS responded to this new understanding of the FTF threat with a collective effort to eliminate their recruitment, financing, and travel.[9] These efforts, combined with the territorial defeat of the Islamic State in Syria and Iraq, reduced FTF flows into those countries meaningfully: from 2,000 per month in 2014 to 500 per month in 2016 and to less than a dozen by 2020.[10]

Despite these successes, this article argues that the threat posed by foreign terrorist fighters has not disappeared, but is best described as being in stasis. Governments have passed new laws, improved coordination, and devoted resources toward minimizing FTF travel. The Islamic State no longer retains territorial control

a The United Nations Security Council defines foreign terrorist fighters as individuals "who travel or attempt to travel to a State other than their States of residence or nationality … for the purpose of the perpetration, planning, or preparation of, or participation in, terrorist acts, or the providing or receiving of terrorist training." This definition can be found in "United Nations Security Council Resolution 2178," United Nations, September 24, 2014.

b In January 2016, the Islamic State released a video that featured its November 2015 attacks in Paris, France, and encouraged its followers to "kill them where you find them." This directive was presented as an alternative to attempting to become foreign terrorist fighters. Subsequent Islamic State releases have echoed this call. Most recently, beginning in January 2024, the group announced a "kill them where you find them" campaign in solidarity with Palestinian residents of the Gaza Strip. For more information, see Aymenn Jawad Al-Tamimi, "Results of the Islamic State's 'And Kill Them Wherever You Find Them' Expedition," Middle East Forum, January 12, 2024.

Kim Cragin, PhD, is director of the Center for Strategy and Military Power within the National Defense University's Institute for National Strategic Studies. She is a widely published expert on counterterrorism, foreign fighters, and terrorist group adaptation. The opinions expressed here are her own and not those of the National Defense University, the Department of War, or the U.S. government.

Islamic State foreign fighters are pictured in this screen capture from a video titled "It Is He Who Has Named You Muslims," posted by Al-Furqan Foundation for Media Production in April 2014.

over large swathes of Syria and Iraq. Nevertheless, the Islamic State, al-Qa`ida, and likeminded terrorist groups still have access to safe havens in the Middle East, South Asia, and Africa. They continue their global outreach to sympathizers. FTF facilitators also have adjusted their tactics, techniques, and procedures (TTPs) and adopted new technologies. Security authorities, therefore, must likewise continue to adapt if they hope to prevent a flare-up in the future.

The following paragraphs address the evolution and impact of foreign terrorist fighters associated with Arab Afghans, al-Qa`ida, and the Islamic State. To do so, the paragraphs trace the past, examine the present, and project into the future. The article builds on prior research, including studies conducted by the author at the RAND Corporation, the National Defense University (NDU), as well as other studies by authors resident at West Point's Combating Terrorism Center.

A Recent History of Foreign Fighters

The modern history of foreign terrorist fighters[c] begins with the Soviet invasion of Afghanistan in December 1979.[11] Approximately 20,000 so-called "Arab Afghans" traveled abroad to support the *mujahideen* in their fight against Soviet forces.[12] Proponents argued that it was an individual religious duty (*fard ayn*) for Muslims to assist the Afghan *mujahideen* as they fought against Soviet occupation.[13] They spread their message with underground pamphlets. They also regularly spoke at private gatherings in homes and mosques throughout the Muslim world.[14] Maktab al-Khidamat (MAK), the "Office of Services," facilitated much but not all of the Arab Afghans' recruitment, fundraising, and travel.[15] Usama bin Ladin, the founder of al-Qa`ida, helped finance MAK soon after its inception.[16]

Significantly, not all of the Arab Afghans traveled to Afghanistan willingly or enthusiastically. Some were fleeing arrest, prosecution, and/or detention at home. Many of the Egyptians, for example, were forced to leave their country after Gama'a al-Islamiyya assassinated President Anwar Sadat in October 1981.[17] Other Arab Afghans traveled abroad with the implicit support of their governments.[d] Many brought their families. They took up residence in approximately 100 safe houses or training camps along the border between Afghanistan and Pakistan. This yielded a mix of expectations on the part of the Arab Afghans: Some hoped to remain, others planned to return home to their families, while still others expected to take their battlefield experiences home (or elsewhere) and continue the fight.[18] In the end, once Soviet forces withdrew from Afghanistan, an estimated 80 percent of the Arab Afghans returned home, 10 percent remained in the region, and the final 10 percent scattered, relocating to Bosnia, Sudan, Yemen, Tajikistan, Chechnya, the Philippines, and other locations.[19]

The Arab Afghans' dispersal led policymakers and experts to conclude that their impact would be localized.[20] In many ways, this assessment was correct. Arab Afghans from Saudi Arabia and Yemen, for example, were perceived as heroes and initially

c This article only examined foreign terrorist fighters associated with the Arab *mujahideen* in Afghanistan, al-Qa`ida, the Islamic State, and likeminded terrorist or insurgent groups.

d In his book, *Jihad in Saudi Arabia*, Thomas Hegghammer argues that the flow of volunteers from Saudi Arabia increased in 1987 after the Saudi mainstream media began to report on the activities of FTFs in Afghanistan and implicitly encourage their audiences to join them. See Thomas Hegghammer, *Jihad in Saudi Arabia: Violence and Pan-Islamism since 1979* (Cambridge: Cambridge University Press, 2010).

reintegrated peacefully.[21] In contrast, Algerian FTF returnees played an active role in that country's civil war between 1991 and 1998, even commanding the Armed Islamic Group (GIA).[22] The experiences of Arab Afghans in both Saudi Arabia and Algeria, therefore, reinforced experts' conclusion that FTF returnees' impact would be localized. They were mistaken. This first generation of foreign fighters retained their global relationships, newly learned skills, and well-established smuggling networks. These networks would eventually be turned against the West with attacks against military forces abroad, diplomatic facilities, and eventually homelands.

The most notable examples of Arab Afghans' global impact can be found in external operations against multiple U.S. and French targets. Ramzi Ahmed Yousef, for example, was responsible for an attack against New York City's World Trade Center in 1993.[23] Arab Afghans also played instrumental roles in the terrorist attacks against the Paris subway (July 1995) and Arc de Triomphe (August 1995).[24] They orchestrated the twin suicide attacks against U.S. embassies in Kenya and Tanzania in November 1998.[25] Likewise, Abd al-Rahim al-Nashiri was a member of al-Qa`ida in the Arabian Peninsula. He fought against Soviet forces in Afghanistan and initially relocated to Tajikistan in the early 1990s. Al-Nashiri was the lead planner for attacks against the USS Cole on October 12, 2000, as well as the French MV Limburg, on October 6, 2002.[26] Finally, perhaps most well-known, Khalid Sheikh Mohammad orchestrated al-Qa`ida's attacks against New York, Pennsylvania, and Virginia on September 11, 2001.[27] In hindsight, these attacks reflect the global and long-enduring impact of the Arab Afghans.

If the first generation of foreign fighters fought in Afghanistan during the 1980s, the United States' invasion of Iraq on March 20, 2003, referred to as Operation Iraqi Freedom, ushered in a second generation. These individuals traveled to Iraq to fight for the terrorist group that would eventually be known as al-Qa`ida in Iraq (AQI). AQI was led by Abu Musab al-Zarqawi, a Jordanian, who traveled to Afghanistan in the late 1980s but arrived too late to fight against Soviet forces. Instead, al-Zarqawi gathered testimony from the Arab Afghans and recorded the stories for *Al-Bunyan Al-Marsus*.[28] He eventually established his own training camp in Herat, Afghanistan, and built a terrorist network that complemented al-Qa`ida. Al-Zarqawi fled Afghanistan after the U.S. invasion and relocated to Iraq in September 2002.[29] Al-Zarqawi's network drew over 5,000 foreign terrorist fighters between March 2003 and December 2009.[30] Interestingly, approximately 60 percent of AQI's foreign fighters reportedly came from Saudi Arabia or Libya.[31] These and other FTFs conducted a vast majority—at one point, over 90 percent—of the suicide bombings against U.S. military and civilian targets during Operation Iraqi Freedom.[32]

More recently, on June 29, 2014, Abu Muhammad al-Adnani announced the creation of an Islamic caliphate in Syria and Iraq with Abu Bakr al-Baghdadi as its leader.[33] This sparked a third generation of foreign terrorist fighters and the largest influx in modern history. According to the U.S. government, an estimated 35,000-40,000 FTFs traveled to Syria and Iraq, with approximately 2,000 entering per month at its peak: twice the number of Arab Afghans and four times al-Qa`ida in Iraq.[34] FTFs played a prominent role in the Islamic State's outreach to global audiences[35] and, as part of this outreach, were responsible for many of its well-known atrocities. For example, the Islamic State cell sometimes referred to as "The Beatles" was responsible for the public execution of James Foley, as well as Steven Sotloff, David Haines, Alan Henning, and others.[36] Its members were called The Beatles because they had British accents. Mohammed Emwazi (aka "Jihadi John") became the most widely recognized. He was born in Kuwait and grew up in west London. Emwazi attempted to travel to Somalia and join al-Shabaab in 2009, but he was arrested in Tanzania and sent home. Three years later, Emwazi made it to Syria: Several Islamic State videos featured Jihadi John beheading his victims.[37]

Amniyat al-Kharji—the team responsible for the Islamic State's external operations—often sent foreign terrorist fighters home to execute attacks.[38] The most notable was the aforementioned November 2015 attacks in Paris. FTFs functioned as "virtual planners" for Amniyat al-Kharji, providing guidance and resources to sympathizers back home as they planned attacks in the name of the Islamic State.[39] Led by Abu Muhammad al-Adnani until August 2015, when he was killed by U.S. security forces, Amniyat al-Kharji conducted 132 external operations in its first two years. Fifty-two percent of these involved foreign terrorist fighters.[40] While some of Amniyat al-Khariji's early external operations were successful, others were not. In March 2017, for example, an Islamic State cell in Italy planned an attack against the famous Rialto Bridge in Venice. At least three individuals were part of this plot—Fisnik Bekaj, Dake Haziraj, Arjan Babaj—and one was a FTF returnee, having traveled previously to Syria. But this external operation was unsuccessful. Italian authorities discovered and disrupted the plot.[41]

The United Nations Security Council and the Global Coalition to Defeat ISIS galvanized a concerted, global effort to disrupt FTF recruitment, financing, and travel. These efforts were combined with the U.S.-led Operation Inherent Resolve, which eventually wrested territorial control away from the Islamic State. While 2019 saw the territorial defeat of the group, the Global Coalition's efforts against FTF travel continue over a decade later. In June 2024, for example, security authorities in the Netherlands, Germany, Spain, and Iceland cooperated to dismantle the I'lam Foundation's communication infrastructure in Europe. The I'lam Foundation had taken over from al-Hayat Media Center in 2018 as the key hub for Islamic State global propaganda.[42] Authorities found ties between I'lam Foundation and foreign fighter travel as well as plots against sports teams, stadiums, and events.

The Current State of Foreign Fighters

The current state of foreign terrorist fighters parallels, most closely, the period between the Arab Afghans departure from Afghanistan and Pakistan (1993) and the advent of Operation Iraqi Freedom (2003). Like this in-between period, the threat can be understood as falling into two historical categories: (1) metastasis of capabilities between conflicts abroad and (2) execution of external operations. In this sense, the present FTF threat remains consistent with historical precedent. FTFs' impact has been reduced, however, due to continued intelligence activities, law enforcement, and international cooperation against their networks.

FTFs today plan, resource, and conduct external operations. They recruit new sympathizers back home. They also bring new tactics, techniques, and procedures into conflict zones. New technologies, such as end-to-end encryption, also make FTF facilitation easier. These technologies allow terrorist recruiters to reach new audiences and planners to improve the efficacy of their "kill them where you find them" campaigns. The following paragraphs address these

trends, emphasizing the need for consistent attention and action against FTF networks globally.

Conflicts Abroad

FTF recruits continue to travel abroad to join foreign terrorist groups, most notably in the Middle East, South Asia, and Africa.[43] Table 1 (below) estimates the number and ratio of foreign terrorist fighters for five Islamic State-affiliated terrorist groups as of September 2025.[e] The overall numbers of foreign terrorist fighters are more dispersed and fall well below what existed in Syria and Iraq during the height of the group's so-called caliphate. By spring 2017, the Islamic State claimed to have over 100,000 fighters in Syria and Iraq, 40,000 (or 40 percent) of which were foreign terrorist fighters.[44] Comparatively, at present, there are approximately 11,550 Islamic State-linked foreign terrorist fighters across five conflict zones.

Table 1: Number and Ratio of Islamic State Foreign Terrorist Fighters, Present

	Est. Combatants	Est. Foreign Fighters	Est. Ratio
Islamic State-Syria and Iraq	3,000	1,200	40%
Islamic State-Somalia	1,600	850	53%
Islamic State-Afghanistan	2,000	500	25%
Islamic State-West Africa	12,000	4,000	33%
Islamic State-Sahel	15,000	5,000	33%

That said, the expansion and ratio of foreign to local fighters in some conflict zones—namely Somalia—are worrisome. According to the U.S. Africa Command, for example, Islamic State-Somalia increased in size from 300 fighters in 2023 to 1,600 by early 2025 with a complementary influx of foreign terrorist fighters.[45] The United Nations Sanctions Monitoring Group further delineated FTFs in Islamic State-Somalia as arriving from Syria, Yemen, Ethiopia, Sudan, Morocco, and Tanzania.[46]

Islamic State-Somalia's largest population of foreign fighters reportedly comes from Ethiopia.[47] This makes sense given the relative proximity of these two countries. But FTFs from other neighboring countries also have played prominent roles in the group. Most notably, Bilal al-Sudani was Islamic State-Somalia's primary facilitator and financier until he was killed in a U.S. military raid in January 2023.[48] Al-Sudani originally joined al-Shabaab, a competitor terrorist group in Somalia, but defected to the Islamic State in 2015, bringing his networks with him. Until his death, al-Sudani orchestrated the transfer of funds to Islamic State affiliates regionally, including Islamic State-Mozambique, Islamic State-Central Africa, as well as Islamic State cells in South Africa.[49] Islamic State-Somalia also sent funds to Islamic State Khorasan (ISK) in Afghanistan. In February 2023, the U.N. Security Council issued a report on the Islamic State's global network. It stated that Islamic State-Somalia had sent $25,000 in cryptocurrency per month to ISK in the year prior.[50]

Beyond Somalia, other regional conflicts also continue to draw foreign terrorist fighters. These include ongoing fighting in Afghanistan, Nigeria, Mozambique, and Mali. The estimated ratios of foreign to local fighters for these conflicts is not as high as for Somalia (see Table 1), but the FTFs arguably have had an outsized impact on the nature of these conflicts. For example, in the summer of 2024, 13 Islamic State fighters reportedly traveled from the Middle East to the Chad River Basin to provide Islamic State-West Africa Province (ISWAP) with the capabilities to acquire, assemble, and deploy armed drones.[51] ISWAP used this newly acquired knowledge to successfully launch a drone attack against Nigerian military installations in December 2024. It was the first time that ISWAP had used armed drones in a guerrilla attack.[52]

In sum, the overall pattern of FTFs in conflicts abroad remains consistent today with historical trends from the period between 1993 and 1998. Small numbers of FTFs continue to travel abroad to join the Islamic State or likeminded groups. These FTFs predominantly come from neighboring countries with some limited numbers traveling far distances. FTFs bring new tactics, techniques, and capabilities with them, as well as ties to well-established global networks. As such, FTFs enable the spread of new TTPs, resources, and technologies, as well as cooperation across terrorist networks. The most worrisome new TTPs for conflict zones appear to be the rapid spread and use of commercial drone technologies and cryptocurrencies.

External Operations

Foreign fighters are somewhat less of an immediate threat to their countries of origin or transit than conflict zones. Figure 1 illustrates this observation.[f] It identifies both successful and disrupted Islamic State external operations over time. Figure 1 further delineates the extent to which foreign fighters were reported to have been directly involved in the external operation. It shows a decreasing number of external operations attributable to FTF operatives. A few limited cases exist. In May 2025, for example, authorities

e The numbers in this table on the Islamic State in Syria and Iraq only include those not in detention facilities or camps. The numbers are estimates, derived from multiple sources, including "United Nations Sanctions Monitoring Team Report, S/2025/482," United Nations, July 24, 2025; "United Nations Sanctions Monitoring Team Report, S/23/95," United Nations, February 13, 2023; "Foreign Terrorist Fighters in the Sahel-Sahara Region of Africa," African Center for the Study of Terrorism (African Union), Policy Paper, April 2022; and Daveed Gartenstein-Ross, "How Many Fighters Does the Islamic State Really Have?" War on the Rocks, February 9, 2015.

f The data presented here was derived from a database developed and maintained by the author at the National Defense University. It includes all successful external operations conducted by Islamic State operatives and sympathizers from its inception. The database also includes all publicly reported disrupted plots, defined as the arrest of perpetrators who have identified the target, purchased the weapons, and made plans (e.g., logistics) to conduct the attack. The disrupted plots incorporate those halted by the U.S. military and its allies through airstrikes or raids on Islamic State external operations planners. The data was derived from multiple sources, including media reports, reports released by the United Nations, Europol, and the African Union. The author also attempts to validate the data through interviews with academics, experts, and officials in countries with the highest level of external operations. Finally, U.S. Central Command also regularly provides updates on its strikes and often names the operative targeted. If basic research through media reports and/or Islamic State propaganda confirms that these individuals helped plan a previous external operation, then this strike is counted as "disrupting" a future plot.

arrested an individual in Guadalajara, Spain, on terrorist charges. He had previously fought for the Islamic State in Syria and Iraq.[53] Nevertheless, Figure 1 suggests that the current threat posed by FTF returnees to their countries of origin is fairly limited.

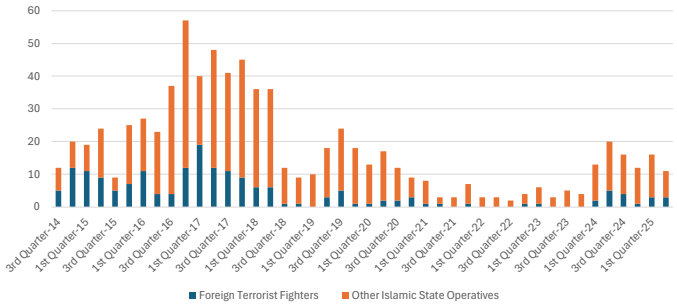

Figure 1: External Operations Execute by FTFs (July 1, 2014-June 30, 2025) N=780

Of course, as noted previously, Islamic State affiliates also have encouraged their sympathizers to "kill them where you find them" over the years. Experts tend to refer to these external operations as being *inspired* rather than planned and executed by known Islamic State members and returnees. Some inspired attacks, however, are instigated, planned, and financed by foreign fighters. Indeed, FTFs continue to play a role in facilitating recruitment of sympathizers, providing them with guidance, as well as resources for external operations. Figure 2 (below) illustrates this observation. It shows the proportion of external operations executed by foreign fighters as compared to those enabled remotely by FTFs planners and financiers and those fully inspired with no foreign fighter involvement.

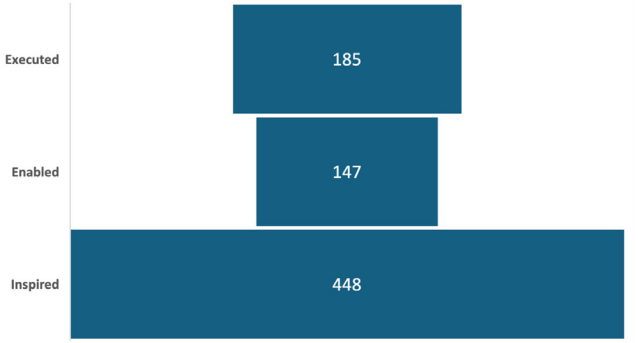

Figure 2: External Operations by Perpetrator (July 1, 2014-June 30, 2025) N=780

FTFs have taken advantage of new technologies in pursuit of external operations. I'lam Foundation, discussed above, utilized generative artificial intelligence (GenAI) to create and translate propaganda as part of its outreach to sympathizers.[54] FTF facilitators also have reportedly used a Monero wallet to send and receive cryptocurrency between Islamic State affiliates and their sympathizers. In May 2025, Turkish intelligence discovered that Özgr Altun, also known as Abu Yasser al-Turki, planned to travel from Afghanistan into Pakistan. Al-Turki was the senior-most foreign fighter in Afghanistan from Turkey. He functioned as a propagandist, fundraiser, and facilitator and, as such, contributed to travel into and out of Europe, including in support of Islamic State external operations.[55] Turkish intelligence notified their counterparts in Pakistan and al-Turki was arrested. Soon after his arrest, pro-Islamic State channels on Rocket.Chat noted al-Turki's absence, and a new Monero wallet address was distributed with the notation that the old address was compromised.[56]

Finally, some individuals have attempted both. That is, they aspire to fight for the Islamic State abroad, encourage others to do so, but also cannot overcome the hurdles to get into a conflict zone. These individuals often turn their attention inward. Abdisatar Ahmed Hassan, the individual from Minnesota who aspired to fight for Islamic State-Somalia, illustrates this growing trend in foreign terrorist fighters. Indeed, approximately 10 percent of all "inspired" attacks since July 1, 2014, have been conducted by individuals who tried to get to conflict zones, but were halted along the way and sent home or could otherwise not overcome the hurdles. It is not new per se. The number and percentage also arguably are indicative of "success" in global counterterrorism. However, it requires constant attention by local and international law enforcement to maintain these low numbers.

Conclusion

Foreign terrorist fighters remain a threat. They continue to travel abroad and, in doing so, transfer new tactics, techniques, and procedures between conflict zones. Foreign terrorist fighters also continue to be interested in executing external operations back home. These patterns are not new. Beyond these historical patterns, foreign terrorist fighters have become increasingly adept at reaching out to new sympathizers and serving as interlocutors between Islamic State affiliates in conflict zones and their sympathizers. FTFs also have utilized end-to-end encryption technologies, GenAI, and cryptocurrencies to magnify their impact.

Nevertheless, while foreign fighters remain a threat, current trends are worrisome but not alarming. They simply mean that security authorities cannot dismiss the threat of foreign terrorist fighters as something that may, potentially, rise in the future. It must be managed on an ongoing basis. It requires sustained resources devoted to intelligence collection on foreign fighter flows. Intelligence agencies also need to share this intelligence with their counterparts in other countries to effectively mitigate FTF travel. Law enforcement agencies must continue to investigate and arrest individuals who not only plan, finance, or execute attacks within their borders, but also those enabling attacks abroad. Immigration and border security officials, likewise, should share information on possible foreign fighter recruitment, facilitation, and travel.

Most importantly, as governments monitor and coordinate their efforts, special attention should be given to how foreign fighters adapt and change their tactics, techniques and procedures. Officials should expect FTFs to adapt under pressure, especially if they are attempting to mobilize support in response to a particularly resonate conflict. Intelligence, military, and law enforcement agencies will need to be equally adaptive. Further, rapid influxes of people, money, and weapons into and out of conflict zones should trigger warnings. These influxes could be an indicator of a potential increase in the threat of external operations. Finally, intelligence and law enforcement agencies should be wary of falling into the trap of believing that FTFs' departure makes their own country safe. Foreign fighters inevitably turn their attention back home. CTC

Citations

1 *United States of America vs Abdisatar Ahmed Hassan*, 25-mj-104 (DLM) United States District Court for the District of Minnesota, February 27, 2025.
2 Ibid.
3 Ibid.
4 Ibid.
5 R. Kim Cragin, "Preventing the Next Wave of Foreign Terrorist Fighters: Lessons Learned from the Experiences of Algeria and Tunisia," *Studies in Conflict & Terrorism* 44:7 (2019).
6 R. Kim Cragin and Susan Stipanovich, "Metastasis: Exploring the Impact of Foreign Fighters in Conflicts Abroad," *Journal of Strategic Studies* 42:1 (2017).
7 "United Nations Security Council Resolution 2396," United Nations, December 21, 2017.
8 R. Kim Cragin, "The November 2015 Paris Attacks: The Impact of Foreign Fighter Returnees," *Orbis* 61:2 (2017).
9 "United Nations Security Council Resolution 2396."
10 Cragin, "Preventing the Next Wave of Foreign Terrorist Fighters;" "U.S. military softens claims on drop in Islamic State's foreign fighters," Reuters, April 29, 2016.
11 Lawrence Wright, *The Looming Tower: Al-Qaeda and the Road to 9/11* (New York: Vintage Books, 2006); Abdel Bari Atwan, *The Secret History of al-Qa'ida* (London: Saqi Books, 2006).
12 Thomas Hegghammer, "The Rise of Muslim Foreign Fighters," *International Security* 235:3 (2010/2011): pp. 53-94.
13 Kim Cragin, "Early History of al-Qa'ida," *Historical Journal* 51:4 (2008): pp. 1,047-1,067.
14 Montasser al-Zayat, *The Road to al-Qaeda: The Story of Bin Laden's Right-Hand Man* (edited by Sara Nimis, translated by Ahmed Fekry) (London: Pluto Press, 2002).
15 Ibid.; Abdullah Anas, *To the Mountains: My Life in Jihad from Algeria to Afghanistan* (translated by Tam Hussein) (London: Hurst Publishers, 2019).
16 Cragin, "Early History of al-Qa'ida."
17 Al-Zayat.
18 S. Gharib, "Abu Hamzah on Life, Islam, Islamic Groups," al-Mujalla, March 21, 1999; R. Kim Cragin, "The Challenge of Foreign Fighter Returnees," *Journal of Contemporary Criminal Justice* 33:2 (2017).
19 Cragin, "The Challenge of Foreign Fighter Returnees."
20 Thomas Hegghammer, *Jihad in Saudi Arabia: Violence and Pan-Islamism since 1979* (Cambridge: Cambridge University Press, 2010); Abdel Bari Atwan, *After Bin Laden: Al Qaeda, The Next Generation* (London: The New Press, 2012); Kenneth Conboy, *The Second Front: Inside Asia's Most Dangerous Terrorist Network* (Jakarta: Equinox, 2006).
21 Atwan, *After Bin Laden*.
22 Cragin, "The Challenge of Foreign Fighter Returnees;" Omar Ashour, *The De-Radicalization of Jihadists: Transforming Armed Islamist Movements* (London: Routledge, 2009); Jean-Pierre Filiu, "The Local and the Global Jihad of al-Qa'ida in the Islamic Maghrib," *Middle East Journal* 63:2 (2008): pp. 213-226.
23 Steve Coll, *Ghost Wars: The Secret History of the CIA, Afghanistan, and Bin Laden, From the Soviet Invasion to September 10, 2001* (New York: Penguin Books, 2004).
24 "The 'A-Team' of Islamic Extremists," *Ottawa Citizen*, December 31, 1999; "Islamic extremists use Europe as support base," *Calgary Herald*, July 30, 1995.
25 "FactSheet: Steps Taken To Serve Justice in the Bombings of U.S. Embassies in Kenya and Tanzania," U.S. Department of State, August 4, 1999.
26 *United States vs Al Nashiri*, CMCR 23-005, United States Court of Military Commission Review, January 30, 2025; Carol Rosenberg, "Alleged al Qaida bomber emerges from CIA shadows, waves," *Miami Herald*, March 25, 2016.
27 Terry McDermott, Josh Meyer, and Patrick J. McDonnell, "The Plots and Designs of al-Qaeda's Engineer," *Los Angeles Times*, December 22, 2002.
28 Jean-Charles Brisard, *Zarqawi: The New Face of Al-Qaeda* (New York: Other Press, 2005), pp. 14-26.
29 Ibid., p. 87.
30 Cragin, "The Challenge of Foreign Fighter Returnees." See also Arie Perliger and Daniel Milton, *From Cradle to Grave: The Lifecycle of Foreign Fighters in Iraq and Syria* (West Point, NY: Combating Terrorism Center, 2016).
31 Brian Dodwell, Daniel Milton, and Don Rassler, *Then and Now: Comparing the Flow of Foreign Fighters to AQI and the Islamic State* (West Point, NY: Combating Terrorism Center, 2016).
32 "Most suicide bombers in Iraq are foreigners," Associated Press, June 30, 2005.
33 For further background on the Islamic State and its origins, see Michael Weiss and Hassan Hassan, *ISIS: Inside the Army of Terror* (New York: Regan Arts, 2015) and Abu Muhammad al-Adnani, "This is the Promise of Allah," statement released by al-Hayat Media Center, June 30, 2015.
34 Karen Parrish, "Stopping flow of foreign fighters to ISIS 'will take years,' Army official says," DoD News, April 6, 2017.
35 Jyette Klausen, "Tweeting the Jihad: Social Media Networks of Western Foreign Fighters in Syria and Iraq," *Studies in Conflict & Terrorism* 38 (2014): pp. 1-22; J.M. Berger and Jonathan Morgan, "The ISIS Twitter Census: Defining and Describing the Population of ISIS Supporters on Twitter," Brookings Institution Analysis Paper, No. 20, March 2015; Ali Fisher, "Swarmcast: how jihadist networks maintain a persistent online presence," *Perspectives on Terrorism* 9:3 (2015).
36 For more information, see James Harkin, *Hunting Season: James Foley, ISIS and the Kidnapping Campaign that Started a War* (New York: Hachette Books, 2015); Seth Loertscher and Daniel Milton, *Held Hostage: Analyses of Kidnapping Across Time and Among Jihadist Organizations* (West Point, NY: Combating Terrorism Center, 2015); and R. Kim Cragin and Phillip Padilla, "Old Becomes New Again: Kidnappings by Daesh and Other Salafi-Jihadists in the Twenty-First Century," *Studies in Conflict & Terrorism*, September 20, 2016.
37 Ibid. See also Tucker Reals, "How did 'Jihadi John' slip through the cracks?" CBS News, February 27, 2015.
38 Daveed Gartenstein-Ross and Nathaniel Barr, "Recent Attacks Illuminate the Islamic States' Europe Network," Hot Issues, Jamestown Foundation, April 27, 2016; Anne Speckhard and Ahmet S. Yayla, "The ISIS Emni: Origins and Inner Workings of ISIS's Intelligence Apparatus," *Perspectives on Terrorism* 11:1 (2017): pp. 2-16.
39 Ibid.
40 R. Kim Cragin and Ari Weil, "'Virtual Planners' in the Arsenal of Islamic State External Operations," *Orbis*, February 17, 2018.
41 "Italy foils IS-inspired plot to blow up Rialto Bridge in Venice," *Times of Israel*, March 30, 2017.
42 "Major Takedown of Critical Online Infrastructure to Disrupt Terrorist Communications and Propaganda," EUROPOL, June 14, 2024.
43 Benjamin R. Farley, "The Syrian Democratic Forces, Detained Foreign Fighters, and International Security Vulnerabilities," Articles of War, Lieber Institute, October 24, 2022.
44 Daveed Gartenstein-Ross, "How Many Fighters Does the Islamic State Really Have?" War on the Rocks, February 9, 2015; Parrish.
45 Carla Babb, "VOA Exclusive: AFRICOM Chief on threats, way forward for US military in Africa," VOA News, October 2, 2014; Jeff Seldin, "Key Islamic State planner killed in airstrike, US says," VOA News, February 11, 2025.
46 Jeff Seldin, "Foreign fighters flocking to Islamic State in Somalia," VOA News, November 20, 2024.
47 Caleb Weiss and Lucas Webber, "Islamic State-Somalia: A Growing Global Terror Concern," *CTC Sentinel* 17:8 (2024).
48 Cecilia Macaulay, "Bilal al-Sudani: US forces kill Islamic State Somalia leader in cave complex," BBC, January 27, 2023.
49 Weiss and Webber.
50 "United Nations Sanctions Monitoring Team Report, S/23/95," United Nations, February 13, 2023.
51 "United Nations Sanctions Monitoring Team Report, S/2025/482," United Nations, July 24, 2025.
52 Taiwo Adebayo, "Lake Chad Basin insurgents raise the stakes with weaponised drones," ISS Today, Institute for Security Studies, South Africa, March 17, 2025.
53 Juana Viúdez, "Detenido en Guadalajara un 'combatiente terrorista extranjero' del ISIS reclamado por Marruecos," *Pais*, May 16, 2025.
54 "Major Takedown of Critical Online Infrastructure." See also Tim O'Connor, "Generating Jihad: How ISIS Could Use AI to Plan Its Next Attack," *Newsweek*, September 19, 2025.
55 "A Prominent Leader Of ISIS, Holds Turkish Citizenship, Arrested In A Joint Turkish-Pakistani Security Operation," Iraq News Gazette, June 1, 2025.
56 Ibid. See also "Pro-ISIS Channel Releases New Monero Wallet Address Following Arrest of Alleged Propagandist," Counter Extremism Project, released by the Targeted News Service, June 10, 2025.

Rise of the E-Militias: Designated Terrorist Groups Infest Iraq's Digital Economy

By Michael Knights

Iraq's digital economy is one of its fastest-growing sectors, driven by an expanding youth population, a transition to e-governance services, and the potential for Iraq to become a regional data transit hub. As with militia monetization of Iraq's oil sector, the telecommunications industry is attracting the attention of U.S.-designated terrorist groups. They have two motives: to generate threat finances and to control and monitor data to strengthen their grip on the population and on Western diplomatic, military, and commercial entities inside Iraq. In the year before Iraq's November 2025 elections, the outgoing government of Prime Minister Mohammed Shia al-Sudani revealed the extent of militia penetration of the sector by awarding sensitive telecoms contracts to a now-sanctioned militia economic conglomerate, while also offering U.S.-origin equipment to militias and channeling lucrative 5G mobile telephony licenses exclusively to militia businessmen.

This study is the eighth in a series of *CTC Sentinel* articles since 2019 that have detailed the ongoing rise of the self-styled, Tehran-backed resistance (*muqawama*) factions in Iraq, and of Iran's growing dominance within the Iraqi state. These studies[1] initially focused on how the *muqawama* had achieved one element of state capture by establishing, formalizing, and assuring Iraqi government funding for the Popular Mobilization Forces (PMF), Iraq's equivalent of the Iranian Islamic Revolutionary Guard Corps (IRGC).[2] More recently, the series has begun to drill-down into militia penetration of specific sectors of the Iraqi political, security and economic systems.[3] An article featured in the April 2025 issue of *CTC Sentinel* took a deep-dive into the unparalleled terrorist threat financing potential of the Iraqi oil sector.[4] That study explained in detail how Iraq had become a terrorist-run state with greater resources than any of Iran's other proxy networks, the world's fifth-largest oil producer[5] being run by U.S.-sanctioned groups behind the façade of a sovereign country.[6]

This study will take forward the chronology of the evolution of the Tehran-backed *muqawama* factions in Iraq by next exploring their penetration of telecommunications and data services in Iraq. The piece draws upon the same kind of detailed interview process with U.S. and Iraqi subjects that underpinned the prior *CTC Sentinel* studies referenced above.[a] This includes the author's networks of contacts and especially the citizen journalism that has made available numerous leaked contracts and Iraqi government documents shared with the author.[b] To assess and assure their veracity, the author has taken the original and translated versions of the documents to former and serving Iraqi government officials, who checked the documents against known samples of the same format, seals, stamps, and signatures found in genuine documents within their possession.[7]

The overarching theme of this analysis is that, second only to the oil sector, closely monitoring Iraq's telecommunications sector should be a priority for counterterrorism and sanctions analysts. Domination of this sector brings not only enormous and growing threat finance opportunities to the Iran Threat Network, but also a new capacity to suppress dissent inside Iraq, to shape societal views, and to eavesdrop on the communications of Iraqi officials and foreign diplomatic missions. This should be of strong interest to any U.S. agency charged with the implementation of the maximum pressure effort on Iran's regime, most recently re-energized by the United States via National Security Presidential Memorandum 2 (NSPM-2).[8]

To begin with, the study will lay out the formula set by Iran itself for the domination of national information networks, which has subsequently been adopted in part by Lebanese Hezbollah, Yemen's Ansar Allah (Houthi) movement, and now by Iraqi terrorist groups and militias close to Iran. The article will then echo April 2025's analysis of militia penetration of Iraq's energy sector by describing the comparatively simple takeover of the Iraqi telecommunications ministry, state companies, and the regulator since 2022 under the government of Prime Minister Mohammed Shia al-Sudani.

Thereafter, the following sections will examine fast-tracked contracting that has given unprecedented access to Iraqi fiber optic networks to the Muhandis General Company,[9] which has since been designated by the United States under counterterrorism

Dr. Michael Knights is the Chief Product Officer at energy advisory Horizon Engage. He is also an Adjunct Fellow with the Washington Institute for Near East Policy. X: @mikeknightsiraq

a Militia Spotlight's online blog and group profiles were established to track this process in detail and produce evidentiary building blocks, using legal standards of proof and certainty. The project collects militia statements in Arabic and other languages, archives evidence that risks being taken offline at a later point, and uses a data fusion process to synthesize information and analyze trends. The Militia Spotlight blog is at https://www.washingtoninstitute.org/policy-analysis/series/militia-spotlight and the Militia Spotlight profiles page is at https://www.washingtoninstitute.org/policy-analysis/series/militia-spotlight-profiles

b Five sets of Arabic-language soft copy documents were provided by contacts in the Iraqi telecommunications sector, Iraqi intelligence services, and the Iraqi Prime Minister's Office. These included three contracts that were also used as the basis of an investigative article by Robert Worth, "Iran's Last Ally in the Middle East," *Atlantic*, October 28, 2025. The contracts were also publicized by a range of Iraqi civil society activists and citizen journalists on social media.

authorities.[10] The article will also look at diversion of U.S. technologies to the PMF through abuses of end-user monitoring by the Iraqi Ministry of Communications. The penultimate section will identify new efforts by the PMF leadership to gain exclusive control of 5G mobile telephony in Iraq, and the concluding section will highlight emerging issues for intelligence analysts and telecommunications industry regulators to watch.

How Iran-Backed Terrorists Dominate Communications Sectors

There are two compelling reasons for Iranian and Iran-backed terrorist movements and their affiliates to seek control of digital telecommunications networks. First, these networks provide critical advantages for regime security forces in countries with non-democratic systems such as Iran, Houthi-controlled Yemen, and even within weak democracies dominated by Iran-backed terrorist groups such as Lebanon and Iraq. Control of telecommunications systems allows Iran and its partners to isolate their countries from piped data connections (inbound and outbound) in the rest of the world at moments of potential threat to the regime. The speed of internet connection can be selectively throttled in order to prevent domestic use of certain modes of communication (such as video-messaging and encrypted messaging services).[11]

With sophisticated equipment provided by vendors including Russia and China, or developed inside Iran, data can be analyzed to provide the location of users, their pattern of communication with others, their efforts at encryption or bypassing of censorship, and even the content of text and voice communications of Iraqis and foreigners, including foreign diplomatic and military missions.[12] Controlling national regulators allows Iranian and pro-Iran factions to gain the approvals to import such systems, while potentially denying them to rivals. Conversely, control of telecommunications systems also allows the Iranian regime and Iran-backed forces greater ability to secure their own messaging and device security by dominating public systems and by establishing new secure networks for their own exclusive use.[13]

An important secondary objective of controlling telecommunications are the economic benefits of monetizing data access within and through these countries. By seizing monopoly control of international internet connectivity, a government can set the price of internet services without competition and can control the speed and performance of providers.[14] Key infrastructure can be nationalized at will, for instance allowing terrorist and militia actors to "piggyback" on existing fiberoptic lines and microwave or cellular towers, significantly lowering the cost of entry to the market for Iran-linked factions.[15] Preferred access to superior service offerings—such as 5G coverage—can be channeled to Iran-linked entities in order that they profit first and foremost from such advances.[16] And finally, unutilized broadband throughput capacity can be sold to other users outside the country, an important potential source of U.S. dollars or other hard currency for U.S.-sanctioned persons and groups.[17]

Iran's Digital Control Playbook

To achieve these fruits, Iran's security agencies have developed a playbook—not a literal publication but rather a methodological blueprint—that is increasingly being adopted in many respects by other Axis of Resistance members in Lebanon, Yemen, and now Iraq. In Iran, the playbook was conceived in the early 2000s and accelerated after the regime suffered a serious scare in the 2009 "green movement" protests.[18] From 2013 to the present year, the planned National Information Network (NIN) was reportedly 60 percent completed at a cost of $6 billion,[19] during which time both Lebanese Hezbollah[c] and Yemen's Houthi movement[d] have sought to rapidly mimic the effort. The key elements of the playbook, which will be applied to the Iraq case study in subsequent sections, comprise the following.

"Control of telecommunications systems allows Iran and its partners to isolate their countries from piped data connections (inbound and outbound) in the rest of the world at moments of potential threat to the regime."

Utilize a single internet gateway. A single internet gateway is a system whereby all landline and subsea internet cables are only connected to a host government controller. To be connected to the global internet, local Internet Service Providers (ISPs) must be licensed by the government and work under their terms.[20] The only alternate way to access the global internet is a satellite-based internet provider, for instance Elon Musk's Starlink.[e]

Control key agencies. For optimal control of a nation's telecommunications sector, one must ideally control the national chief executive (Supreme Leader, president, prime minister),

c Lebanese Hezbollah has executed the playbook to a significant degree. The Ministry of Telecommunications, the regulator (Telecommunications Regulatory Authority), and the state-owned phone and fiber optic operator OGERO are all vulnerable to Hezbollah pressure, both via parliamentary committees and through physical intimidation. Commercial ISPs and providers with foreign joint venture partners have been squeezed out of the sector. Hezbollah has its own fiber optic network that the state cannot access, while the state is unable to prevent Hezbollah from accessing the national grid. Deep Packet Inspection technology has been detected in the Lebanese environment. See "Freedom in the World 2025: Lebanon," Freedom House, 2025; "Hezbollah's Telecom Network Reportedly Remains Fully Intact," This is Beirut, September 26, 2024; and Hanin Ghaddar, "Hezbollah Takes Aim at Lebanon's Central Bank and Telecom Sector," Washington Institute for Near East Policy, May 4, 2020.

d The Houthis hit the ground running after their takeover of Sanaa in September 2014, taking over the Ministry of Telecoms and Information Technology, as well as all the public and private telecoms providers and ISPs in Houthi-controlled Yemen, including the Public Telecommunications Corporation, the General Company for Regulating Telecommunications and Post, and TeleYemen. The Houthis banned Starlink, blocked numerous foreign news sites and encrypted messaging apps, installed Deep Packet Inspection technologies and IMEI tracking, and reportedly developed some localized secure fiber optic networks of their own. Houthi monetization of the telecoms sector is estimated to raise around $150 million per year. For a breakdown of the Houthi use and abuse of their control of the internet, see "Letter dated 21 February 2023 from the Panel of Experts on Yemen addressed to the President of the Security Council," U.N. Security Council, February 21, 2023, pp. 33-34 and "The Houthis' Use of Technology for Repression," Counter-Extremism Project, October 2023.

e Starlink gets around national censorship primarily by bypassing the physical, ground-based internet infrastructure that governments control and monitor, including single national internet gateways linked to terrestrial fiber-optic lines. For a how-to guide on using Starlink to bypass national systems, see Colby Baber, "Using Starlink In Unsupported Countries," Dishlink, November 8, 2023.

the communications ministry,[f] the national telecommunications regulator (if separate from the ministry),[g] and the state telecommunications operator[h] (which usually directly operates infrastructure or does so as the lead partner in a public-private partnership. Typically, the blueprint involves removal of commercial competition to state-run telecoms, which reduces foreign involvement, increases fees and government take, and often reduces accountability for poor service.[21] [i]

Access fiberoptic lines and microwave towers. Through the above dominance of institutions, the Iranian regime or Iran-backed elements have the ability to physically access submarine and land-based cable landing stations at the country's borders, plus fiberoptic junction rooms and data centers, even as localized as fiber-to-the-home connections to individual residences.[j] This provides the access needed for service denial, speed reduction, and intrusive monitoring of traffic data and even content.[k]

Import and use Deep Packet Inspection (DPI) technologies. Using this access, the Iranian state and its partners can gain access to IP addresses and unique IMEI numbers of individual devices, and then correlate those addresses or numbers with locations, other personal devices, and the use of privacy measures (virtual private networks, encryption, and SIM card-switching). When combined with throttled speed and other measures, users can be channeled toward insecure communications where data and voice content can also be accessed.[l]

Militia Capture of Telecommunications Institutions

In one form of another, Iran-backed factions in Iraq have rapidly accelerated their application of the above playbook under since the formation of Prime Minister Mohammed Shia al-Sudani's government in October 2022.[22] Prior to al-Sudani's term, the Iraqi *muqawama* had only tinkered at the margins of the telecommunications sector, usually for profit as opposed to establishing security control.[23] Lebanese Hezbollah-linked businessmen connected to the U.S.-sanctioned Iraqi terrorist Shibl al-Zaydi made the first tentative steps toward cashing in on telecoms in 2018-2020,[m] but their approaches using U.S.-sanctioned persons were too obvious and generally attracted the scrutiny of the U.S. government, leading to these efforts being blocked by the first Trump administration.[24] Under Prime Minister Mustafa al-Kadhimi in 2020-2022, the Kata'ib Hezbollah terrorist group was also blocked from setting up their own fiber-optic landline communications from the Iranian border to the Najaf and Karbala area.[25]

What changed under al-Sudani was the rapid accumulation of control by militias of the Prime Minister's Office, the Ministry of Communications and its subsidiary operators, plus the regulator, the Communications and Media Commission (CMC). The rot started at the very top, with the appointment of al-Sudani by the Coordination Framework (CF) bloc.[26] This bloc included U.S.-designated terrorist organizations Asaib Ahl al-Haq (AAH)[27] and Kata'ib Hezbollah,[28] as well as the U.S.-formed Badr Organization.[29] AAH leader Qais al-Khazali thereafter characterized al-Sudani diminutively in a November 2022 television interview as that of a "general manager."[n] The militias—not al-Sudani—appointed all the cabinet ministers[o] in what they called "the resistance government."[30]

In al-Sudani's cabinet, the Minister of Communications was Hiyam al-Yassiri,[p] a ministry advisor whose October 2022 candidacy was sponsored by U.S.-designated human rights abuser Falah al-Fayyadh.[31] As *CTC Sentinel* readers will recall, al-Fayyadh is the chairman of the Popular Mobilization Forces (PMF), the emergency reserve force raised in 2014 to fight the Islamic State but which quickly became a proto-IRGC parallel military in Iraq under the leadership of a cadre of U.S.-designated terrorists, the bulk of whom were seconded from Kata'ib Hezbollah.[32] Al-Fayyadh

f In Iran's case, the Ministry of Communications and Information Technology.

g In Iran, this is nominally the Communications Regulatory Authority, but increasingly, the Supreme Council for Cyberspace also plays a role.

h In Iran, this is the Telecommunications Company of Iran, which was sold in 2009 to a consortium called Etemad Mobin Development, which consisted of the IRGC and the Execution of the Imam Khomeini's Order (EIKO), a foundation controlled by Supreme Leader Ali Khamenei. See "The Revolutionary Guards bought eight billion dollars of telecommunications shares," BBC Persian, September 27, 2009.

i Ghasseminejad notes that "the IRGC's takeover of Iran's communications infrastructure gave it free rein over the industry. The forcing of high-cost, low-quality service on customers has been one price Iranians have had to pay for the concentration of the communications industry in IRGC hands."

j With physical access, one can insert optical splitters on cables in order to obtain a copy of the optical signal, which includes the entirety of voice, video, and other data carried by the line. The author consulted with a number of communications experts to write this article, including Iraqi officials with experience of Iraq's fiber optic system.

k Throttling bandwidth can be an effective tactic to push users off encrypted apps. While the encryption itself is not broken by the throttling, the resulting slow speeds can make the applications functionally unusable. See Wilson Wahome, "Behind the scenes: Weaponizing throttling," Democracy in Africa, November 2, 2022.

l As The Intercept revealed in 2022, Iran operates a system called SIAM. "SIAM is a computer system that works behind the scenes of Iranian cellular networks, providing its operators a broad menu of remote commands to alter, disrupt, and monitor how customers use their phones. The tools can slow their data connections to a crawl, break the encryption of phone calls, track the movements of individuals or large groups, and produce detailed metadata summaries of who spoke to whom, when, and where." Sam Biddle and Murtaza Hussain, "Hacked Documents: How Iran Can Track and Control Protesters' Phones," Intercept, October 28, 2022.

m The early period of militia interest in telecoms was principally protection racket activity: shaking down ISPs and telecoms companies with threats to their staff and their infrastructure. Other groups tapped into fiber optic lines to "smuggle internet" into the market at reduced rates. Author interviews, multiple Iraqi telecoms-focused and Iraqi intelligence community contacts, 2020-2025; exact dates, names, and places withheld at request of the interviewees.

n This appears to have been a calculated action to show al-Khazali's power, by disparaging Iraq's prime minister – the country's highest executive and the commander-in-chief of the military – by comparing him to a low-ranking bureaucrat. Hamdi Malik, "'Sudani Is a General Manager': How Militias View Iraq's New Prime Minister," Militia Spotlight, Washington Institute for Near East Policy, December 1, 2022.

o This is a well-established consensus view among Iraq-watchers. While other premiers had been able to pick certain ministers to serve alongside them in the cabinet, either due to the size of their win (and resultant surplus entitlement beyond just the PM's role) or by special dispensation due to the conditions of cabinet formation, al-Sudani picked no ministers in his cabinet. Author interviews, multiple U.S. and Iraqi intelligence community contacts, 2022-2023; exact dates, names, and places withheld at request of the interviewees.

p Minister of Communications Dr. Hiyam Aboud Kazem al-Yassiri is a planning and administration expert, an academic with the University of Technology in Baghdad, with a family background from Baghdad and Najaf. The minister is open in her biography about her family's involvement in the Daawa and later Fadhila movements, including persecution under the Saddam Hussein regime for Daawa links. The minister's bio can be found at https://www.moc.gov.iq/?article=1109

was designated by the United States after he used his authority as the PMF chair and (then) Iraq's National Security Advisor to orchestrate the killings and abductions of unarmed protesters in the 2019 "Tishreen" youth uprising.[q] Al-Yassiri's political and sectarian background is from the Fadhila (Virtue) Party, a smaller sub-block within the CF.[r] Within the post-2022 ministry, al-Yassiri has appointed a deputy minister for technical affairs, Buraq Abdal-Qader Abdal-Karim,[33] from the inner circle of another U.S.-sanctioned Iraqi politician, Khamis Khanjar, who was designated for his corrupt activities in favor of the Iran-backed militias.[34] She also appointed a ministry head of media relations, Omar Abdal-Razaq Muhsib, who was previously al-Fayyadh's personal photographer in the PMF leadership office.[35]

The regulator, the CMC, was likewise packed with CF appointees since 2022.[36] Originally set up by the U.S.-led occupation authorities in 2004 to manage communications and media licensing and regulation, the CMC has (in the assessment of this author) been recently twisted into a tool of repression that reinforces, not acts as a check upon, the Ministry of Communications.[37] Under the al-Sudani government, the CMC board fell under the domination of CF factions, with all six members drawn from Shi`a Islamist parties, including Mahmoud al-Rubaie, spokesman for the political office of the U.S.-designated terrorist group Asaib Ahl al-Haq (AAH).[38s] (The same happened to the state-run Iraq Media Network on February 28, 2024, when the Iraqi cabinet placed its board under the majority control of three U.S.-designated movements.[39 t]) CMC issued draconian new draft social media regulations in March 2023 and began keyword-based and informant-based blocking and banning of digital media in the same month.[40] Lacking a data protection standards agency or a specific cybersecurity regulator, CMC is Iraq's repository of personal data from all SIM card registrants and ISP users.[41]

In the assessment of this author, working together, the CF-appointed al-Sudani, al-Yassiri, and the CMC have worked rapidly to emulate the Iranian playbook within Iraq's telecommunications sector since 2022.[42] The following sections identify recent developments that have placed the centralized fiber optic backbone under the control of U.S.-designated entities.

Fast-Tracking Militia Control of Iraq's Fiber-Optic Backbone

On April 23, 2024, the Iraqi Minister of Communications Hiyam al-Yassiri sent a letter to the General Secretariat of the Council of Ministers (the Iraqi cabinet) marked "extremely urgent" and requesting that two fiber optic contracts be exempted from contracting rules and regulations.[43] The two contracts included one to rehabilitate and maintain the existing fiber optic network, and the other to build Iraq's first new alternate fiber optic network in decades.[44] The letter justified the fast-tracked and non-competitive status with the claim that the ministry "desperately need[ed]" the accelerated contracting due to "the increase in digitalization and automation in state institutions" and to "address the need for the increase in demand of internet in state institutions, GSM providers and Iraqi citizens," and also to enable "data transit projects through Iraq."[45] At no point in the letter was any reason given for the sudden, specific urgency.[46] Until that time, it was unprecedented for the Ministry of Communications to single-source a major contract without a competitive bid.[47]

Despite the paucity of a specific justification for acceleration, both fiber optic contracts were then processed with extraordinary, unheard-of speed:[48 u] The contracts were both added, with zero notice and none of the usual preparation by the cabinet staff, to the same day's cabinet agenda.[49 v] According to a April 23, 2024, letter from the Ministry of Communications' Minister's Office, signed by Minister Hiyam al-Yassiri,[50] both were approved to be non-competed awards by the cabinet on the same day: April 23, 2024.[51] Again, most irregularly, the Ministry of Communications received notice back on the same day, April 23, 2024.[52] Unusually, cabinet consideration of the contracts was not included in the publicly released cabinet minutes.[53] The two contracts were then negotiated and signed in a mere two-month window in September to November 2024.[54] Taken in combination, these are very strong indicators of political favoritism, especially when the ministry's typical record of often slow and grudging approvals is considered.[w]

The awardee of both contracts was the Muhandis General

q The United States designated Falah al-Fayyadh for human rights abuses during the October 2019 crackdown. See "Treasury Sanctions Iran-Backed Militia Leaders Who Killed Innocent Demonstrators in Iraq," U.S. Department of the Treasury, December 6, 2019.

r The Fadhila Party (officially the Islamic Virtue Party; Hizb al-Fadhila al-Islamiyya al-Iraqi) is an Iraqi Shi`a Islamist political party that has a connection to both the Daawa Party and the Sadrist Trend formed by Mohammed Sadiq al-Sadr. For a recent update on Fadhila, see "Deep Dive: The stakes for Shiite parties in Iraq's elections," Amwaj, June 6, 2025.

s "Mahmoud al-Rubaie, who served as spokesman for the political office of the U.S.-designated terrorist group Asaib Ahl al-Haq before his appointment to the CMC board. Amtar Rahim al-Mayyahi, a former Badr Organization representative on the Basra provincial council. Her husband is high-ranking Badr member Abu Ahmed al-Rashed. Mohammad al-Hamad, a figure close to State of Law Alliance chief Nouri al-Maliki. Previously, Hamad served as general manager of Afaq TV. He is now deputy head of the Iraqi Radio and Television Union, an offshoot of Iran's Islamic Radio and Television Union (IRTVU). In October 2020, the U.S. Treasury Department's Office of Foreign Assets Control designated IRTVU and other Iranian entities for obtaining American voter registration data in order to influence U.S. elections and incite unrest. Moayyad al-Lami, head of the Iraqi Press Syndicate, affiliated with Prime Minister Sudani. The only CMC board member not drawn from CF factions is Abdaladhim Mohammad al-Saleh, affiliated with the Sadrist movement." Michael Knights, Hamdi Malik, and Crispin Smith, "Profile: Communications and Media Commission," Militia Spotlight, Washington Institute for Near East Policy, May 15, 2023, last updated February 19, 2025.

t "Awsam Majid Ghanem Hassan al-Mohammedawi, a media operator of the U.S.-designated terrorist group Kataib Hezbollah (KH) … Thaer Hattat Ibrahim al-Ghanemi, who is close to multiple militias, particularly the U.S.-designated terrorist groups KH, AAH, Kataib Sayyid al-Shuhada (KSS), and Harakat Hezbollah al-Nujaba (HaN) … Sanaa Saied Hadi Karumi, a representative of U.S.-sanctioned human rights abuser Rayan al-Kildani, a Christian member of the IMN board who works for Holy Quran Radio." Ameer al-Kaabi, Michael Knights, and Hamdi Malik, "Profile: Iraqi Media Network," Militia Spotlight, Washington Institute for Near East Policy, February 29, 2024.

u Same-day processing of major contracts from ministry to cabinet and back again, fully-signed, is unheard-of.

v The cabinet secretariat usually takes weeks (or at least a week) to process a new request, schedule it on the cabinet agenda, and prepare a legal opinion on the eligibility of the matter for cabinet approval.

w To give an example provided by the Ministry of Communications itself, the ministry has been very slow to activate fiber-optic distribution terminals constructed by its primary private sector partner, Earthlink. See "Internet providers prioritize profits: 3.5 million fiber optic lines ready in Iraq, but 700k are in use, says communications minister," 964 News, July 24, 2024.

Iraq's fiber optic infrastructure (map produced by Jules Duhamel)

Company for Construction, Engineering and Mechanical, Agricultural and Industrial Contracting (hereafter shortened to Muhandis General Company, or MGC).[55] Both contracts were signed by MGC's Dhia Johi Hussein[x] "as per the power of attorney issued by Muhandis General Company" on November 25, 2024, (maintenance of existing network) and December 18, 2024 (creation of new alternate network).[56]

Since its formation on November 28, 2022,[y] MGC had been identified as a construction arm of the PMF, named after Abu Mahdi al-Muhandis, the U.S.-designated terrorist and Kata'ib Hezbollah founder who was killed by a U.S. airstrike on January 3, 2020.[57] It was described as being modeled on the IRGC's Khatam al-Anbia construction arm in Iran—that is, a commercial vehicle with unique advantages in winning business, designed to be unlimited in terms of activities, sectors, and the types of government assets transferred to it.[58] Beginning in 2018, Iran-backed militias and politicians pressured successive prime ministers to facilitate the creation of such an economic conglomerate under the PMF's control.[z]

The MGC was later sanctioned by the United States[59] on October 9, 2025, "pursuant to E.O. 13224, as amended, for having materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services to or in support of, Kataib Hizballah and the IRGC Qods Force; and for being owned or controlled or directed by, or having acted or purported to act for or on behalf of, directly or indirectly, Kataib Hizballah."[60] The U.S. Treasury specifically noted that "the Muhandis General Company is controlled by Popular Mobilization Commission Chief of Staff and U.S.-designated Kataib Hizballah leader Abd al-Aziz Malluh Mirjirash al-Muhammadawi (Abu Fadak)."[61] The Treasury concluded: "Muhandis General Company, under the control of Kataib Hizballah, uses a sub-contracting method to divert funds from Iraqi government contracts."[62]

MGC Fully Accesses Iraq's Existing Fiber Optic Network

The first contract awarded by the Ministry of Communications to the Muhandis General Company was entitled "Rehabilitation and Development Contract – National Fiber Optic Network Routes," which was signed on behalf of the MGC General Manager Falah

x Iraqi commercial records show Dhia Johi Hussein to be a shareholder in Ishraqa al-Baraka Telecomm LLC, Al-Baraka Industrial Investments Ltd, and Al-Saqr Petroleum Services LLC. See author's own dataset and those of other Iraq-focused investigators, which include current Iraqi corporate databases.

y After replacing al-Kadhimi in 2022, Prime Minister Mohammed Shia al-Sudani announced the formation of the MGC in his sixth cabinet session (November 28, 2022). Michael Knights, Crispin Smith, and Hamdi Malik, "Profile: The Muhandis General Company," Militia Spotlight, Washington Institute for Near East Policy, May 17, 2023, updated November 5, 2024.

z The first two attempts in 2018 and 2020 – named Motassim and Al-Rashid – were blocked by international pressure and opposition from the government of former prime minister Mustafa al-Kadhimi. This is described in Michael Knights, Hamdi Malik, and Crispin Smith, "Iraq's New Regime Change: How Tehran-Backed Terrorist Organizations and Militias Captured the Iraqi State," *CTC Sentinel* 16:11 (2023).


المادة (٢٤) لغة العقد

حرر هذا العقد باللغة العربية ما عدا الملاحق الفنية المحررة باللغة الانكليزية وفي حالة حدوث أي خلاف حول العقد بخصوص الترجمة او التفسير فتعتمد الصيغة المكتوبة باللغة العربية.

حررهذا العقد بو اقع (٥) نسخ اصلية ووقع في بغداد بتاريخ / / ٢٠٢٥

الطرف الأول
وزارة الاتصالات- الشركة العامة للاتصالات والمعلومات تمثلها الدكتورة المهندسة هيـام الياسـري وزيرة الاتصالات
/ / ٢٠٢٥

الطرف الثاني
شركة المهندس العامة
يمثلها السيد ضياء جوحي حسين
وحسب كتاب التخويل الصادر من شركة المهندس
المرقم (ش/م/٩٣ في ٢٠٢٤/١٢/١٨)

السيد علي ياسين داود
رئيس مجلس الإدارة والمدير العام
/ / ٢٠٢٥

معاون المدير العام للشؤون الفنية
معاون المدير العام للشؤون الإدارية والمالية
مدير مديرية البنى التحتية
مدير القسم المالي
مدير قسم التدقيق والرقابة الداخلية
مدير قسم شبكة الالياف الضوئية
مدير قسم العقود

Signature page from the contract awarding the National Alternate Fiber Optic Network to the Muhandis General Company. The circular black stamp on the right is the MGC official stamp, overlapping by the Ministry of Communication's hollow circle stamp to the left.

al-Fayyadh by Dhia Johi Hussein on November 25, 2024.[63] The contract included "excavation and execution of new routes, development of the channels for the fiber optic cable routes, provision of maintenance services and warranty for the supplied materials for a period of three years."[64] The contract allows MGC unlimited access to fiber optic vaults that handrail major roads to install new cable and transmission equipment along the way.[65] The value of the contract is interesting: just 15.70 billion Iraqi dinars ($11.98 million), which Iraqi businesspersons and officials canvassed by the author viewed as a very low number for a 285-day project involving 25 routes in 10 governorates.[66] [aa] This approach to pricing is typically behavior intended to prepare the way for a no-bid award, with costs usually rising in implementation, a common formula used by politically connected contractors in Iraq.[67] The contract commits MGC to send ministry personnel for "on-the-job training" in Oman and Egypt.[68]

The second contract awarded by the Ministry of Communications to the Muhandis General Company was entitled "Contract for the Establishment of the National Alternate Fiber Optic Network (First Phase)."[69] Again, it was signed on behalf of the MGC General Manager Falah al-Fayyadh by Dhia Johi Hussein, this time on December 18, 2024.[70] The contract envisages the creation of a new network referred to in the contract only as "the eastern, northern and Baghdad routes"—an unknown length of fiber optic, though the parts list suggests 1,152km of new cable being procured.[71] The value of the contract is 31.75 billion Iraqi dinars ($24.23 million), a more normal amount for the 365-day project.[72] On May 30, 2024, another letter (this time from the al-Sudani cabinet secretariat) chivvied the Ministry of Communications with encouragement to account for any delay in executing the contract, roughly one month after its cabinet approval on April 23, 2024.[73]

This contract broke a long-standing precedent[74] that the Ministry of Communications' own state-owned Informatics and Telecommunications Public Company (ITPC) laid all new fiber optic cabling in Iraq.[ab] The de facto leaders of MGC—Kata'ib Hezbollah's Abu Fadak and Falah al-Fayyadh—had previously tried to break the monopoly on fiber optic-laying, in 2020-2021.[ac] The value of major new northern Baghdad and eastern fiber optic lines installed by MGC are assessed by the author as two-fold: They offer surveillance and internet-blocking capabilities in the cross-sectarian areas where the PMF garrisons Sunni communities, and they can become a source of future funding.[75] PMF units have, as recently as 2020, been discovered implanting illegal taps on fiber optic lines for the financial benefit of stealing and reselling the bandwidth to ISPs and small networks.[ad] These fiber optic lines can also serve as secure communications channels for the PMF and its constituent militias and U.S.-designated terrorist groups.[ae]

PMF Satellite Internet, Powered by U.S. Equipment

A third contract involving the PMF[76] casts a spotlight on another communications-related risk—that of the PMF gaining access to Western and specifically U.S. satellite internet technology. The PMF are not yet sanctioned by the United States, though their subsidiary, MGC, is, and (in this author's assessment) it may not be long before more elements of the force are sanctioned.[77] Nevertheless, even

aa At just under $12 million, the project lacks the margins typically associated with this kind of contracting and might even have been provided at cost or a slight loss. Author interviews, multiple Iraqi telecoms-focused contacts, 2025; exact dates, names, and places withheld at request of the interviewees.

ab ITPC is a subsidiary of the Ministry of Communications, with special responsibility for landline communications, including a historic monopoly on laying new fiber optics.

ac They sought to lay a new landline between the Iranian border and major Shi`a religious pilgrimage areas. Author interviews, multiple Iraqi intelligence contacts, 2023; exact dates, names, and places withheld at request of the interviewees.

ad In June 2020, a so-called "shock and awe" effort by law enforcement uncovered networks that were reselling bandwidth worth $10-20 million per month. Author interviews, multiple Iraqi telecoms-focused contacts, 2023-2024; exact dates, names, and places withheld at request of the interviewees.

ae Both Iran and Lebanese Hezbollah are reported to have created expansive dedicated fiber optic networks in parallel to national civilian systems. The issue of a secure landline grid for major Iraqi militias has been a recurring theme on anecdotal reporting among Iraqi militia networks, particularly as regards Asaib Ahl al-Haq. For Lebanese Hezbollah, see "Hezbollah's Communications Infrastructure – A Strategic Asset For Its Operational Activity," Alma Research, March 9, 2021. For Iraq, the author is describing recurring indicators that AAH and other Iraqi groups have sought to build landline communications that reduce their vulnerability to eavesdropping, geolocation, and targeting. Author interviews, multiple Iraqi intelligence contacts, 2018-2025; exact dates, names, and places withheld at request of the interviewees.

without formal sanctioning, the U.S. government has long sought to avoid allowing any of its security assistance to directly benefit the PMF.[af] When Kata'ib Hezbollah elements within the PMF seized and held seven U.S. M1 Abrams tanks, the U.S. effort to recover those vehicles was energetic, persistent, and (eventually) largely successful.[78]

On November 28, 2024, the U.S.-sanctioned Falah al-Fayyadh signed a contract with the Ministry of Communications for the provision of satellite communications systems to the PMF headquarters.[79] The contract, entitled "Contract for the Supply of Strategic Satellite Communications Systems for the Popular Mobilization Committee,"[80] was countersigned by Nabeel Abdal-Baqi,[ag] then the general manager of the Ministry of Communications' Al-Salam State Company (for telecommunications).[ah] Though relatively small in size (1.09bn Iraqi dinars or $832,000), the contract's Price Technical Annex contains a list of Kymeta U8 Very Small Aperture Terminal (VSAT) equipment made in the United States.[81] (Most of the Table of Quantities in the contract identify U.S. and European-origin equipment.[82]) In the author's assessment, these systems may have been sold in good faith to the Iraqi Ministry of Communications, in the belief that the ministry is the end-user, while actually the ministry is reexporting them to the PMF, which would probably not be viewed favorably by the U.S. government.[83]

Exclusive 5G Rights Being Fast-Tracked to Unknown Parties

The next step for militias and terrorist groups within Iraq's communications sector is the domination of long-awaited faster mobile telephony. While much of the world is experiencing 5G wireless broadband standard, most of Iraq is still stuck at 4G and some communities even at 3G.[84] In the assessment of the author, that means that a breakthrough moment and a huge commercial opportunity is awaiting whoever can unlock 5G in Iraq,[85] which will raise average internet speeds from around 30 megabits per second (mbps) to 1,000 mbps.[ai] Though Iraq has struggled for many years to create a formula to enable a public-private partnership to install 4G, let alone 5G, the period since November 2024 has witnessed what this author and Iraqi telecoms experts assess to be another improbable acceleration in deal flow as militia-linked firms have made their play to gain exclusive control of 5G service.[86]

The leading edge of the 5G effort became visible in November 2024 when a populist opposition party, the New Generation Movement, exposed concerns that 5G would be offered in a no-bid award.[87] The talk of the town amid Iraqi businessmen in late 2024 was then that a big name, a foreign investor with a strong brand, would be used as a respectable wrapper for a consortia largely composed of Iraqi investors linked to CF parties.[aj] In March 2025, the effort went into high-gear with the beginning of the formation of the National Mobile Telecommunications Company (NMTC)[ak] by the Ministry of Communications and its Informatics and Telecommunications Public Company (ITPC) subsidiary, with funding from the State Employees' Pension Fund, the Trade Bank of Iraq (TBI), and Al-Salam General Company of the Ministry of Communications.[88]

In the author's assessment, the deal was pockmarked by irregularities, fitting neither into the category of an advantaged state-owned enterprise working in the national interest, nor a private sector-led effort subject to competitive bidding rules.[89] To speed its progress and reduce the costs of the 5G license, the CMC instructed existing private sector players that the NMTC would be allowed to piggyback on telecoms towers constructed by the existing providers, none of whom were able to bid for the 5G contract.[90] The NMTC could not or would not answer the judiciary's standard inquiries about such a telecommunications project—such as the future location of computer servers—nor was a security committee formed from the relevant government agencies to review the sovereign and security risks posed by the project.[91] As a result, an Iraqi specialist security judge placed a hold on the 5G contract in October 2025, aiming to prevent the deal from being railroaded through before the end of the al-Sudani government (i.e., the November 11, 2025, general elections in Iraq).[92] The hold remained in place by the time of writing on November 13, 2025, by which time the al-Sudani government was relegated to caretaker status awaiting new government formation.

Looking Deeper at the 5G Consortia

The consortia put together to rush the 5G contract into existence was designed in an ingenious manner. It was brought into being in a set of meetings in Oman in 2024,[93] attended by Minister of Communications Hiyam al-Yassiri and two key political figures, Qais Saeed al-Ameri and Ahmed Mutawa al-Saeedi. Qais Saeed al-Ameri was then the Iraqi *charge d'affairs* in Oman (he is now full ambassador), and he is the brother-in-law of Falah al-Fayyadh.[94] [al] Ahmed Mutawa al-Saeedi, also known as Abu Yusuf al-Saeedi, is a business agent of various CF parties in Oman, and is a brother-in-law to Falah al-Fayyadh's son Raed.[95]

As Iraqi MPs and businessmen feared, the involvement of a reputable foreign operator, Vodafone, was minimal in nature, limited

af The United States has historically not provided any security assistance to the PMF. See the history laid out in Michael Knights, Hamdi Malik, and Aymenn Jawad Al-Tamimi, "Honored, Not Contained: The Future of Iraq's Popular Mobilization Forces," Washington Institute for Near East Policy, March 23, 2020.

ag Like Minister Hiyam al-Yassiri, Abdal-Baqi was a Fadhila Party member. Author interviews, multiple Iraqi political contacts, 2025; exact dates, names, and places withheld at request of the interviewees.

ah The Al-Salam company has responsibility for approving the licensing of all devices that potentially impact frequency management, including VSAT equipment and also jamming, navigation, CCTV, and sensing equipment.

ai Freedom House states that in 2024, "the median fixed-line broadband download and upload speeds [in Iraq] were 33.99 Mbps and 31.39 Mbps, respectively." "Freedom in the World 2025: Iraq," Freedom House, 2025.

aj The non-operatorship of Vodafone and its use largely as a big-name advisor is the consensus finding of multiple Iraqi telecoms-focused contacts. Author interviews, multiple Iraqi telecoms-focused contacts, 2025; exact dates, names, and places withheld at request of the interviewees. Some useful discussion can be found here, including alleged leaked documents cited by Iraqi journalist Qusay Shafiq that detailed a mere $62 million worth of financial commitments to Vodafone. These claims have not been independently verified. See "Judicial freeze: Iraq's new national 5G carrier on hold," Shafaq News, October 13, 2025.

ak The NMTC was authorized by the Iraqi Ministry of Trade Registrar of Companies on September 3, 2025. An electronic copy of the registration certificate is in the author's possession and has been evaluated as genuine by multiple experts in the Iraqi cabinet and ministry procedures.

al Qais al-Ameri was the last chief of staff to the militia-appointed Prime Minister Adel Abdal-Mahdi in 2019.

to consulting support and brand use,[am] but the use of a major logo guaranteed strong U.K. and U.S. government lobbying in favor of the deal, regardless of warnings about potential militia involvement in the deal.[an] In reality, neither Vodafone nor the main equipment provider Nokia has a major role in the project.[96] The NMTC instructed Vodafone to select Nokia as the technology provider,[ao] and Nokia was directed by the Ministry of Communications to select local firms Enkidu Information Technology and by Atlas for Information Technology and Security Solutions.[97] In the author's assessment, the whole 5G deal in 2024-2025 appears to have been structured around Enkidu and Atlas.[98]

These companies share a number of similarities. For instance, they both share the same accountant, a man called Hossein Abdal Zahra al-Azzawi, who is a recurring figure in CF-linked oil smuggling and Iran sanctions evasion networks.[ap] Enkidu has been linked by some contacts of the author to the operation of Deep Packet Inspection technology inside Iraq, in particular correlation of phone IMEI signatures and IP addresses to locations and proximity to other users.[99] A major shareholder in Atlas Information Systems (one of a chain of Atlas-named companies) is Ghazzi Faisal Fahad al-Fayyadh, the brother of U.S.-sanctioned PMF chairman Falah al-Fayyadh.[aq]

Next Steps for the Digital Terrorist Economy in Iraq

In the assessment of the author, the pace of digitalization in Iraq is likely to continue at breakneck speed, creating major opportunities for the Iranian regime, Iran-backed terrorists and militias in Iraq, and even foreign terrorist groups such as Lebanese Hezbollah and the Houthis. In the coming years, vast swathes of personal and societal data will become digital as the Iraqi economy moves away from paper records and cash transactions.[100] Iraq will keep pushing toward high-speed fiber optic coverage, a role in international communications corridors, broader e-government, and development of a digital economy.[101] In the author's view, voter registers, electronic payment systems, food rations, health insurance, student portals, and e-visa systems are all fertile ground for digital surveillance and taxation by Iran-backed actors in Iraq.[102]

"The pace of digitalization in Iraq is likely to continue at breakneck speed, creating major opportunities for the Iranian regime, Iran-backed terrorists and militias in Iraq, and even foreign terrorist groups such as Lebanese Hezbollah and the Houthis."

The spectrum of players in this space defies simple characterization. Already, it is apparent (in the assessment of the author) that Iran-backed groups within the CF are competing as much as collaborating in the domination of digital systems.[103] There are various competing camps, including but not limited to the Kata'ib-Hezbollah-led PMF leadership under Abu Fadak; the related but separate PMF network linked to Falah al-Fayyadh and his sponsored Minister of Communications Hiyam al-Yassiri; and a sprawling economic office within Asaib Ahl al-Haq led by U.S.-designated Laith al-Khazali, the brother of AAH leader Qais al-Khazali.[104] When telecommunications officials or private sector players find themselves under pressure from KH or the ministry, they often turn to AAH for "protection."[105] From a U.S. government perspective, this may be no better—swapping one designated group for another, jumping from the proverbial frying pan into the fire, in the author's view.[106]

Intelligence analysts can support future policymaker demand by paying close attention to the personnel installed in key leadership positions in Iraq's telecoms sector in the future. After the November 11, 2025, parliamentary elections, which resulted in no clear winner,[107] there probably will be months of jockeying for position in the next cabinet formation.[108] Analysts should pay close attention to the identity of the next Minister of Communications, which has arguably changed from being a second-tier role in the cabinet to a much sought-after position as the security and commercial value of data is recognized.[ar] Likewise, the appointment of non-technocrats to leadership of ministry subsidiaries is important to watch. Analysts should notate changes to leadership in the National

am A document in the author's possession lists the intended fees due to come to Vodafone and demonstrates the limit of their alleged role in the intended deal: €30 million for administration; €10 million and 3% of revenue (whichever larger) for brand use; €2.5 million every six months for travel and security for expatriate consultants; €13 million annually for app use; 3.5% of the value of all "purchase orders" immediately paid to Vodafone; and €75 million and 3.5% of all procurement, paid annually to Vodafone. This appears to be the same information partially cited by Iraqi journalist Qusay Shafiq in "Judicial freeze." Shafiq is paraphrased thus: "According to these materials, the contract would have required Iraq to pay €30.3 million annually in management fees, €2.5 million every six months for travel and protection expenses, €10 million per year (or 3 percent of revenues) for brand use, and €13 million in platform and service fees."

an The Iraqi judiciary allegedly received multiple direct entreaties by U.K. and U.S. diplomats, as well as by a business associate of Falah al-Fayyadh, to shortcut security reviews and process the 5G contract in October 2025, before the Sudani government expired on November 11, 2025. These entreaties were rebutted. Author interviews, multiple Iraqi telecoms-focused and government contacts, 2025; exact dates, names, and places withheld at request of the interviewees.

ao As more public scrutiny has focused on the deal, in the run-up to Iraqi elections, the enthusiasm of foreign investors in the deal has waned. Author interviews, multiple Iraqi telecoms-focused contacts, 2025; exact dates, names, and places withheld at request of the interviewees.

ap The author inquired after Hossein Abdal-Zahra al-Azzawi within his own dataset and those of other Iraq-focused investigators, which include current Iraqi corporate databases. Al-Azzawi is a very well-documented figure, an Iraqi national who serves as an accountant for several militia-linked firms in Iraq. These firms have done business directly and indirectly with Iran-backed front companies exposed by mass email leaks, notably Sahara Thunder and Sepehr Energy Jahan Nama Pars. For background on these sanctioned entities, see "Treasury Targets Networks Facilitating Illicit Trade and UAV Transfers on Behalf of Iranian Military," U.S. Department of the Treasury, April 25, 2024.

aq Ghazzi Faisal Fahad al-Fayyadh is shown in Iraqi corporate records to be the main shareholder in Atlas Information Systems. See author's own dataset and those of other Iraq-focused investigators, which include current Iraqi corporate databases.

ar In the author's view, which is shared by most of the experts canvassed for this article, the shift toward the Minister of Communications being a sought-after role has only manifested in the 2022-2025 term of government. The contracts being discussed in this article have demonstrated the potential commercial and security importance of the role to all the CF militias.

Mobile Telecommunications Company, the Informatics and Telecommunications Public Company (ITPC), the Al-Salam State Company, the State Company for Internet Services (SCIS),[as] and any other new subsidiaries spun off by the ministry in restructuring.[109]

The leadership of the Communications and Media Commission should also be closely watched and profiled.[110] If and when Iraq develops a specialized digital regulator, that role should be scrutinized, especially to ensure that an Iran-style Supreme Committee on Cyberspace does not emerge without U.S. policymakers having an opportunity to signal concern and guide Iraq away from that outcome.[111] Likewise, U.S. policymakers need to be aware of pressures being brought on the checks and balances within Iraq's system—the judiciary, the Iraqi National Intelligence Service, parliamentary committees, and commercial ISPs like Earthlink and Scopesky.[112] Public-private partnerships with reputable non-militia companies are an important source of transparency within the sector, so attention should be focused on preventing enforced buy-outs of private telecoms operators and ISPs. Any non-competed contract awards in the Iraqi telecommunications sector need to be viewed with special care.

Most important, the rising role of the Muhandis General Company and other PMF spin-offs needs to be closely monitored.[113] MGC is now a U.S.-sanctioned entity, with one agricultural subsidiary (Baladna) also designated.[114] Other MGC subsidiaries and commercial partners need to be identified and sanctioned, perhaps beginning in the telecommunications sector. The Ministry of Communications bears close watching as a pass-through for Western technology being sent on to the PMF in violation to end-user monitoring commitments.

Outside of MGC, Falah al-Fayyadh's family networks—involving relatives and in-laws—should be a priority focus due to their apparent specialization in telecommunications and data projects. There is a dense web of shared connections between Atlas and Enkidu and a company called Supercell Internet Services LLC (Mahwar al-Kimma in Arabic).[115] These include common use of the accountant Hossein Abdal Zahra al-Azzawi and use across multiple companies in the group of a legal advisor called Ali Mohammed Abdal-Sada.[116] The group has been favored in digitalization contracts for a number of government agencies (trade, municipalities, and the Baghdad local government).[117] In the view of Iraqi businessmen, MPs, and intelligence professionals canvassed by the author, the Supercell, Enkidu, and Atlas companies are a group under the effective control and beneficial ownership of Ghazzi Faisal Fahad al-Fayyadh, the brother of Falah al-Fayyadh.[118] This hypothesis is worthy of further testing by government intelligence analysts. Also providing a nexus to sanctionable activities, Ghazzi Faisal Fahad al-Fayyadh's son Ali is a major shareholder in the now-sanctioned Baladna,[at] a subsidiary of MGC that was specifically designated by the U.S. Treasury.[119]

The ties between Iraqi networks (MGC and Falah al-Fayyadh) and Chinese companies such as Huawei should be the subject of closer scrutiny, with special regard to PMF and Iraqi Prime Minister's Office data centers and internal communications systems.[au] Likewise, focus should be directed toward understanding the commercial tie-ups between the very active Iranian embassy economic section and various Chinese and Russian equipment providers seeking inroads in the Iraqi telecoms sector.[av] It should be assumed that Iran-backed factions in Iraq—and numerous other actors—already have access to Deep Packet Inspection capabilities, which Freedom House reported in its 2024 country update, citing an anonymous source within an Iraqi telecommunications company.[aw] U.S. interactions and intelligence-sharing with the Iraqi government and security sector have arguably never been less technically secure than they are at present, but the situation can always get worse. CTC

as Freedom House notes: "The SCIS is responsible for internet subscribers and internet communications in Iraq. It provides broadband wireless internet access for government agencies, DSL and dial-up (VOIP) services, and Internet Protocol (IP) address registration." "Freedom in the World 2025: Iraq."

at Ali Ghazzi al-Fayyadh is shown in Iraqi corporate records to be the main shareholder in Baladna. See author's own dataset and those of other Iraq-focused investigators, which include current Iraqi corporate databases.

au The use of Huawei technology in the PMF and Prime Minister's Office is an open secret in Iraq's government circles. Author interviews, multiple Iraqi telecoms-focused and Iraqi intelligence contacts, 2025; exact dates, names, and places withheld at request of the interviewees.

av One area of recurring interest in conversations undertaken by the author is the Iranian embassy in Baghdad's role in teeing up business, with a cut of the proceeds, for Chinese firms in Iraq's oil, transport, and telecoms sectors. This is worth a separate study.

aw Freedom House noted in 2024: "During the coverage period it was reported that the [Iraqi] National Security Agency was working on implementing a deep packet inspection (DPI) system that would enable more thorough monitoring of online activities in Iraq. The agency has reportedly asked internet companies to install the relevant components of this system." The information was attributed to an "anonymous interview with employee at Al-Tameer Company, March 29, 2024, Baghdad." Freedom House, "Key Developments, June 1, 2023 – May 31, 2024," Freedom on the Net 2024.

Citations

1 Michael Knights, "Iran's Expanding Militia Army in Iraq: The New Special Groups," *CTC Sentinel* 12:7 (2019); Michael Knights, "Soleimani Is Dead: The Road Ahead for Iranian-Backed Militias in Iraq," *CTC Sentinel* 13:1 (2020); Michael Knights, "Back into the Shadows? The Future of Kata'ib Hezbollah and Iran's Other Proxies in Iraq," *CTC Sentinel* 13:10 (2020); Michael Knights, Crispin Smith, and Hamdi Malik, "Discordance in the Iran Threat Network in Iraq: Militia Competition and Rivalry," *CTC Sentinel* 14:8 (2021); and Michael Knights, Hamdi Malik, and Crispin Smith, "Iraq's New Regime Change: How Tehran-Backed Terrorist Organizations and Militias Captured the Iraqi State," *CTC Sentinel* 16:11 (2023).

2 The best deep-dive on the PMF is Michael Knights, Hamdi Malik, and Aymenn Jawad Al-Tamimi, "Honored, Not Contained: The Future of Iraq's Popular Mobilization Forces," Washington Institute for Near East Policy, March 23, 2020.

3 Unpacking this chronology in detail is the focus of Knights, Malik, and Smith, "Iraq's New Regime Change."

4 Michael Knights, "Iraqi Oil and the Iran Threat Network," *CTC Sentinel* 18:4 (2025).

5 "What countries are the top producers and consumers of oil?" Energy Information Administration, September 22, 2023.

6 Ibid.
7 The documents were assessed by four experts from the Iraqi telecommunications sector, Iraqi intelligence services and in the Iraqi Prime Minister's Office. The criteria used to judge them included format, presence, and location of official stamps, plus names and signatures.
8 "National Security Presidential Memorandum-2/NSPM-2," The White House, February 4, 2025.
9 Michael Knights, Hamdi Malik, and Crispin Smith, "The Muhandis Company: Iraq's Khatam al-Anbiya," Militia Spotlight, Washington Institute for Near East Policy, March 21, 2023. See also Michael Knights, "Translated Certificate of Incorporation of the Muhandis General Company," Militia Spotlight, Washington Institute for Near East Policy, June 3, 2023.
10 "Treasury Takes Aim at Iran-Backed Militia Groups Threatening the Safety of Americans," U.S. Department of the Treasury, October 9, 2025.
11 For a useful explanation of this phenomenon, see "How Does Encryption Affect Data Transfer Rate?" Friendly Statistician, April 29, 2025.
12 Calla O'Neil, "Iran's Digital Fortress: The Rise of the National Information Network," Iran Strategy Brief, American Foreign Policy Council, August 2025, pp. 3-4.
13 Ibid., pp. 3-4.
14 See Ahmed Al-Azizi, "Understanding Monopoly vs. Oligopoly in Telecommunications: Implications for Regulation," LinkedIn Essays, September 22, 2024.
15 O'Neil, pp. 2-3.
16 Sofia Wickberg, "Overview of corruption in the telecommunications sector," Anti-Corruption Resource Center, Transparency International, April 8, 2014.
17 Jorge Luis Alvarado, "The Data Economy: How to Turn Information into Revenue," Ai Tech & Business Insider, May 9, 2025.
18 Saeed Ghasseminejad, "The IRGC Took Over Iran's Telecoms Industry with a Disinformation Campaign. Then, It Used the Industry to Amplify Its Own Lies," Foundation for the Defense of Democracies, May 2, 2019.
19 O'Neil, pp. 3-4.
20 For an extreme example of a national internet gateway, see this description of the "Great Firewall of China": "When is the Internet Not the Internet?" National Internet Gateways, Internet Society, December 1, 2023.
21 Ghasseminejad.
22 This is the author's assessment based on all the available evidence and the author's analytic processes.
23 Author interviews, multiple Iraqi telecoms-focused contacts, 2020-2025; exact dates, names, and places withheld at request of the interviewees.
24 Author interviews, multiple U.S. and Iraqi intelligence community contacts, 2020-2023; exact dates, names, and places withheld at request of the interviewees.
25 Author interviews, multiple Iraqi telecoms-focused and Iraqi intelligence community contacts, 2024-2025; exact dates, names, and places withheld at request of the interviewees.
26 The best single chronology of the CF takeover of Iraqi politics is Knights, Malik, and Smith, "Iraq's New Regime Change."
27 Michael Knights, "Profile: Asaib Ahl al-Haq," Militia Spotlight, Washington Institute for Near East Policy, April 27, 2021.
28 Michael Knights, Crispin Smith, and Hamdi Malik, "Profile: Kataib Hezbollah," Militia Spotlight, Washington Institute for Near East Policy, April 1, 2021, updated October 2, 2023.
29 Michael Knights, Crispin Smith, and Hamdi Malik, "Profile: Badr Organization," Militia Spotlight, Washington Institute for Near East Policy, September 2, 2021.
30 Hamdi Malik and Crispin Smith, "Muqawama Lauds 'Resistance Government' in Iraq," Militia Spotlight, Washington Institute for Near East Policy, January 11, 2023.
31 Again, this is a well-established consensus view among Iraq-watchers. Author interviews, multiple U.S. and Iraqi intelligence community contacts, 2022-2023; exact dates, names, and places withheld at request of the interviewees.
32 This KH leadership domination is documented in great detail in Knights, Malik, and Al-Tamimi.
33 Author interviews, multiple Iraqi telecoms-focused and Iraqi intelligence community contacts, 2025; exact dates, names, and places withheld at request of the interviewees.
34 See "Treasury Sanctions Iran-Backed Militia Leaders Who Killed Innocent Demonstrators in Iraq," U.S. Department of the Treasury, December 6, 2019.
35 Author interviews, multiple Iraqi telecoms-focused and Iraqi intelligence community contacts, 2025; exact dates, names, and places withheld at request of the interviewees.
36 Michael Knights, Hamdi Malik, and Crispin Smith, "Profile: Communications and Media Commission," Militia Spotlight, Washington Institute for Near East Policy, May 15, 2023, last updated February 19, 2025.
37 This is the author's assessment based on all the available evidence and the author's analytic processes.
38 Knights, Malik, and Smith, "Profile: Communications and Media Commission."
39 Ameer al-Kaabi, Michael Knights, and Hamdi Malik, "Profile: Iraqi Media Network," Militia Spotlight, Washington Institute for Near East Policy, February 29, 2024.
40 Michael Knights, "Iraqi CMC Draft Regulation on Digital Content in Iraq," Militia Spotlight, Washington Institute for Near East Policy, May 15, 2023.
41 Ibid.
42 This is the author's assessment based on all the available evidence and the author's analytic processes.
43 An electronic copy of this leaked document is in the author's possession and has been evaluated as genuine by multiple experts in the Iraqi cabinet and ministry procedures.
44 An electronic copy of this leaked document is in the author's possession and has been evaluated as genuine by multiple experts in the Iraqi cabinet and ministry procedures.
45 An electronic copy of this leaked document is in the author's possession and has been evaluated as genuine by multiple experts in the Iraqi cabinet and ministry procedures.
46 An electronic copy of this leaked document is in the author's possession and has been evaluated as genuine by multiple experts in the Iraqi cabinet and ministry procedures.
47 This is a well-established consensus view among Iraq-watchers. Author interviews, multiple Iraqi telecoms-focused and Iraqi intelligence community contacts, 2020-2025; exact dates, names, and places withheld at request of the interviewees.
48 This is a well-established consensus view among Iraq-watchers. Author interviews, multiple Iraqi telecoms-focused and Iraqi intelligence community contacts, 2020-2025; exact dates, names, and places withheld at request of the interviewees.
49 An electronic copy of the letter, including its signature pages, is in the author's possession and has been evaluated as genuine by multiple experts in the Iraqi cabinet and ministry procedures.
50 An electronic copy of the letter, including its signature pages, is in the author's possession and has been evaluated as genuine by multiple experts in the Iraqi cabinet and ministry procedures.
51 An electronic copy of the letter, including its signature pages, is in the author's possession and has been evaluated as genuine by multiple experts in the Iraqi cabinet and ministry procedures.
52 An electronic copy of the letter, including its signature pages, is in the author's possession and has been evaluated as genuine by multiple experts in the Iraqi cabinet and ministry procedures.
53 The deals are not included in either "Cabinet Decisions of 16th Regular Session, held on April 22, 2025", or "Cabinet Decisions of 17th Regular Session, held on April 29, 2025" "Iraqi Cabinet Decisions, both archived in English at the website, https://www.cabinet.iq/en/category/KwWTdmx%25I_9@4Y2/KwWTdmx%25I_9@4Y2
54 Electronic copies of both leaked contracts are in the author's possession and have been evaluated as genuine by multiple experts in the Iraqi cabinet and ministry procedures. They are dated November 25, 2024 (maintenance of existing network) and December 18, 2024 (creation of new alternate network).
55 Michael Knights, Crispin Smith, and Hamdi Malik, "Profile: The Muhandis General Company," Militia Spotlight, Washington Institute for Near East Policy, May 17, 2023, updated November 5, 2024.
56 Electronic copies of both leaked contracts are in the author's possession and have been evaluated as genuine by multiple experts in the Iraqi cabinet and ministry procedures.
57 Knights, Smith, and Malik, "Profile: The Muhandis General Company."
58 Knights, Malik, and Smith, "The Muhandis Company."
59 "Treasury Takes Aim at Iran-Backed Militia Groups Threatening the Safety of Americans."
60 Ibid.
61 Ibid.
62 Ibid.
63 An electronic copy of this leaked contract, including its signature pages, is in the author's possession and has been evaluated as genuine by multiple experts in the Iraqi cabinet and ministry procedures.
64 An electronic copy of this leaked contract, including its signature pages, is in the author's possession and has been evaluated as genuine by multiple experts in the Iraqi cabinet and ministry procedures.
65 An electronic copy of this leaked contract, including its signature pages, is in

the author's possession and has been evaluated as genuine by multiple experts in the Iraqi cabinet and ministry procedures. Author interviews, multiple Iraqi telecoms-focused and Iraqi intelligence community contacts, 2025; exact dates, names, and places withheld at request of the interviewees.
66 This was the consensus finding of multiple Iraqi telecoms-focused contacts.
67 Author interviews, multiple Iraqi telecoms-focused contacts, 2025; exact dates, names, and places withheld at request of the interviewees.
68 An electronic copy of this leaked contract is in the author's possession and has been evaluated as genuine by multiple experts in the Iraqi cabinet and ministry procedures.
69 An electronic copy of this leaked contract, including its signature pages, is in the author's possession and has been evaluated as genuine by multiple experts in the Iraqi cabinet and ministry procedures.
70 An electronic copy of this leaked contract, including its signature pages, is in the author's possession and has been evaluated as genuine by multiple experts in the Iraqi cabinet and ministry procedures.
71 An electronic copy of this leaked contract, including its signature pages, is in the author's possession and has been evaluated as genuine by multiple experts in the Iraqi cabinet and ministry procedures.
72 Author interviews, multiple Iraqi telecoms-focused contacts, 2025; exact dates, names, and places withheld at request of the interviewees.
73 An electronic copy of this leaked May 30, 2024, letter, from the Council of Minister's Secretary General to the Ministry of Communications, Minister's Office, including its signature block, is in the author's possession and has been evaluated as genuine by multiple experts in the Iraqi cabinet and ministry procedures.
74 This was the consensus finding of multiple Iraqi telecoms-focused contacts. Author interviews, multiple Iraqi telecoms-focused contacts, 2025; exact dates, names, and places withheld at request of the interviewees.
75 This is the author's assessment based on all the available evidence and the author's analytic processes.
76 An electronic copy of this leaked letter, including its signature block, is in the author's possession and has been evaluated as genuine by multiple experts in the Iraqi cabinet and ministry procedures.
77 This is the author's assessment based on all the available evidence and the author's analytic processes.
78 For a recounting of the M1 Abrams saga, see Knights, Malik, and Al-Tamimi.
79 An electronic copy of this leaked letter, including its signature block, is in the author's possession and has been evaluated as genuine by multiple experts in the Iraqi cabinet and ministry procedures.
80 An electronic copy of this leaked letter, including its signature block, is in the author's possession and has been evaluated as genuine by multiple experts in the Iraqi cabinet and ministry procedures.
81 An electronic copy of this leaked letter, including its signature block, is in the author's possession and has been evaluated as genuine by multiple experts in the Iraqi cabinet and ministry procedures.
82 Ibid.
83 This is the author's assessment based on all the available evidence and the author's analytic processes.
84 Sam Fenwick, "Iraq: Mobile Network Experience Report," Open Signal, January 2025.
85 This is the author's assessment based on all the available evidence and the author's analytic processes.
86 This is the author's assessment based on all the available evidence and the author's analytic processes. The assessment is based, in part, on the consensus finding of multiple Iraqi telecoms-focused contacts. Author interviews, multiple Iraqi telecoms-focused contacts, 2025; exact dates, names, and places withheld at request of the interviewees.
87 For one example (in English), see Dana Taib Menmy, "Behind closed doors?: Iraq's Vodafone 5G deal raises concerns on transparency," New Arab, November 29, 2024. There are many other Arabic equivalents, including social media comments by Iraqi politicians.
88 "Judicial freeze: Iraq's new national 5G carrier on hold," Shafaq News, October 13, 2025.
89 This is the author's assessment based on all the available evidence and the author's analytic processes. The assessment is based, in part, on the consensus finding of multiple Iraqi telecoms-focused contacts. Author interviews, multiple Iraqi telecoms-focused contacts, 2025; exact dates, names, and places withheld at request of the interviewees.
90 Author interviews, multiple Iraqi telecoms-focused contacts, 2025; exact dates, names, and places withheld at request of the interviewees.
91 Author interviews, multiple Iraqi telecoms-focused contacts, 2025; exact dates, names, and places withheld at request of the interviewees.
92 "Judicial freeze."
93 Author interviews, multiple Iraqi telecoms-focused and Iraqi intelligence community contacts, 2025; exact dates, names, and places withheld at request of the interviewees.
94 Author interviews, multiple Iraqi telecoms-focused and Iraqi intelligence community contacts, 2025; exact dates, names, and places withheld at request of the interviewees.
95 Author interviews, multiple Iraqi telecoms-focused and Iraqi intelligence community contacts, 2025; exact dates, names, and places withheld at request of the interviewees.
96 Author interviews, multiple Iraqi telecoms-focused contacts, 2025; exact dates, names, and places withheld at request of the interviewees.
97 Author interviews, multiple Iraqi telecoms-focused and government contacts, 2025; exact dates, names, and places withheld at request of the interviewees.
98 This is the author's assessment based on all the available evidence and the author's analytic processes. The assessment is based, in part, on the consensus finding of multiple Iraqi telecoms-focused contacts. Author interviews, multiple Iraqi telecoms-focused contacts, 2025; exact dates, names, and places withheld at request of the interviewees.
99 Author interviews, multiple Iraqi telecoms-focused and Iraqi intelligence contacts, 2025; exact dates, names, and places withheld at request of the interviewees.
100 This is the author's assessment based on all the available evidence and the author's analytic processes. The assessment is based, in part, on the consensus finding of multiple Iraqi telecoms-focused contacts. Author interviews, multiple Iraqi telecoms-focused contacts, 2025; exact dates, names, and places withheld at request of the interviewees.
101 This is the author's assessment based on all the available evidence and the author's analytic processes. The assessment is based, in part, on the consensus finding of multiple Iraqi telecoms-focused contacts. Author interviews, multiple Iraqi telecoms-focused contacts, 2025; exact dates, names, and places withheld at request of the interviewees.
102 This is the author's assessment based on all the available evidence and the author's analytic processes. The assessment is based, in part, on the consensus finding of multiple Iraqi telecoms-focused contacts. Author interviews, multiple Iraqi telecoms-focused contacts, 2025; exact dates, names, and places withheld at request of the interviewees.
103 This is the author's assessment based on all the available evidence and the author's analytic processes. The assessment is based, in part, on a broad-based list of episodes when CF militias acted competitively, not collaboratively. Author interviews, multiple Iraqi telecoms-focused contacts, 2025; exact dates, names, and places withheld at request of the interviewees.
104 This is the author's assessment based on all the available evidence and the author's analytic processes. The assessment is based, in part, on the consensus finding of multiple Iraqi telecoms-focused contacts. Author interviews, multiple Iraqi telecoms-focused and Iraqi intelligence contacts, 2025; exact dates, names, and places withheld at request of the interviewees.
105 This is the author's assessment based on all the available evidence and the author's analytic processes. The assessment is based, in part, on the consensus finding of multiple Iraqi telecoms-focused contacts. Author interviews, multiple Iraqi telecoms-focused and Iraqi intelligence contacts, 2025; exact dates, names, and places withheld at request of the interviewees.
106 This is the author's assessment based on all the available evidence and the author's analytic processes.
107 Jared Malsin and Saleh al-Battati, "Iraq Election Results Set Stage for a Long Power Struggle," *Wall Street Journal*, November 13, 2025.
108 This is the author's assessment based on all the available evidence and the author's analytic processes, in particular his close experience of monitoring the prior six elections since 2005.
109 This is the author's assessment based on all the available evidence and the author's analytic processes.
110 This is the author's assessment based on all the available evidence and the author's analytic processes.
111 This is the author's assessment based on all the available evidence and the author's analytic processes.
112 This is the author's assessment based on all the available evidence and the author's analytic processes.
113 This is the author's assessment based on all the available evidence and the author's analytic processes.
114 Knights, Smith, and Malik, "Profile: The Muhandis General Company."
115 This is the author's assessment based on all the available evidence and the author's analytic processes. The assessment is based, in part, on the consensus finding of multiple Iraqi telecoms-focused contacts. Author

interviews, multiple Iraqi telecoms-focused and Iraqi intelligence contacts, 2025; exact dates, names, and places withheld at request of the interviewees.

116 Author interviews, multiple Iraqi telecoms-focused and Iraqi intelligence contacts, 2025; exact dates, names, and places withheld at request of the interviewees. The author used his own dataset and those of other Iraq-focused investigators, which include current Iraqi corporate databases.

117 Author interviews, multiple Iraqi telecoms-focused and Iraqi intelligence contacts, 2025; exact dates, names, and places withheld at request of the interviewees. The author used his own dataset and those of other Iraq-focused investigators, which include current Iraqi corporate databases.

118 This is the author's assessment based on all the available evidence and the author's analytic processes. The assessment is based, in part, on the consensus finding of multiple Iraqi telecoms-focused contacts. Author interviews, multiple Iraqi telecoms-focused contacts, 2025; exact dates, names, and places withheld at request of the interviewees.

119 "Treasury Takes Aim at Iran-Backed Militia Groups Threatening the Safety of Americans."