COMBATING TERRORISM CENTER AT WEST POINT

CTCSENTINEL

OBJECTIVE · RELEVANT · RIGOROUS | APRIL 2026 · VOLUME 19, ISSUE 4

FEATURE ARTICLE

AI and the Future of Political Violence

Yannick Veilleux-Lepage

A VIEW FROM THE CT FOXHOLE

Greg Hinds

Former Director of Counter Terrorism, Interpol

Contents

FROM THE EDITORS

In recent years, increasing attention has been paid to how violent non-state actors are using artificial intelligence (AI) to achieve their goals and how AI is being utilized for counterterrorism. Far less attention has been paid, however, to how AI itself—as a "whole-of-society transformative technology"—could change the landscape of political violence in much more fundamental ways. In our cover article this month, Yannick Veilleux-Lepage argues that "AI is reordering labor markets, institutional authority, and the relational worlds in which people live, generating preconditions for political violence independently of whether violent actors adopt the technology themselves." Using a framework he developed centered on three grievance domains—economic order, state and institutional power, and social and personal fabric—Veilleux-Lepage "considers how violence arising from these grievances may materialize, including through targets and actor types that lie largely outside current counterterrorism monitoring."

Our interview is with Greg Hinds, former Director of Counter Terrorism at Interpol, who discussed the responsibility of effectively bringing together the capabilities of various security agencies and developing partnerships among those entities. "It's the information sharing which is key to this," he observes, "making sure that all the information that's available is in the right hands so that the right people can make the right decisions at the right time based on their ability to do their jobs."

Earlier this year, the world witnessed the collapse of the detention system holding tens of thousands of Islamic State affiliates and their families in northeast Syria. Devorah Margolin writes that "the collapse of indefinite detention risks feeding into Islamic State narratives that emphasize endurance, liberation, and the strategic importance of detention sites. Prisons have played a central role in the group's evolution—serving as sites of recruitment, networking, and operational consolidation. The sudden dispersal of these populations, without a framework for accountability or monitoring, complicates efforts to track residual networks and the ability to assess the group's capacity to regenerate."

Finally, Alexandre Rodde, David Mcilhatton, John Cuddihy, and Shannen Benton consider how security lessons from the Paris Olympics could be applied to the upcoming FIFA World Cup competition and other future major events. "Paris," they write, "demonstrated the value of intelligence-led counterterrorism, integrated multi-agency coordination, critical infrastructure protection, cybersecurity readiness, counter-drone capabilities, visible deterrence, and effective public communication."

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

CTC SENTINEL

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: Liquid cooled servers are pictured in an installation at the Global Switch Docklands data center campus in London, United Kingdom, on June 16, 2025. (Jason Alden/Bloomberg via Getty Images)

Beyond Misuse: Artificial Intelligence, Grievance, and the Future Landscape of Political Violence

By Yannick Veilleux-Lepage

The scholarly literature on artificial intelligence and terrorism has organized itself around three questions: (1) how violent non-state actors currently misuse AI, (2) how that misuse may evolve, and (3) how AI can be applied to counterterrorism ends. Each treats AI as an instrument brought to bear on the problem of political violence. This article argues that the misuse frame, while analytically valuable, is incomplete. Extending Mauro Lubrano's recent framework on anti-technology extremism to the specific case of AI as a whole-of-society transformative technology, the article develops a theoretical account of how AI generates the structural conditions historically associated with the onset of political violence. It argues that AI is reordering labor markets, institutional authority, and the relational worlds in which people live, generating preconditions for political violence independently of whether violent actors adopt the technology themselves. These conditions are bound together by a cross-cutting mechanism: the accountability gap that arises when AI-mediated decisions distribute harm without clearly attributable human agents. It is this gap that distinguishes AI-generated grievance from earlier forms of technological grievance. The article develops a framework organized around three grievance domains: economic order, state and institutional power, and social and personal fabric, and it considers how violence arising from these grievances may materialize, including through targets and actor types that lie largely outside current counterterrorism monitoring.

Politically motivated violence has often accompanied transformative technological change. From the Luddite machine-breaking campaigns of 1811 to the Earth Liberation Front arsons of the 1990s and 2000s, from Theodore Kaczynski's 17-year mail bombing campaign against computer scientists, geneticists, and airline executives to the Animal Liberation Front's sustained attacks on university researchers, certain technologies have generated not only economic disruption but also organized and individual violence directed at the persons, institutions, and physical infrastructure deemed responsible for that disruption. These episodes share a recognizable structure: a technology perceived as producing concentrated harm, institutional channels perceived as closed to redress, and a set of targets rendered attributable by their visible role in that technology's development or deployment. Artificial intelligence may be the most recent, and perhaps the most totalizing, entry in this sequence, and recent incidents suggest that the pattern may be beginning to recur.

Two incidents in April 2026 illustrate this recurrence. In the early hours of April 10, 2026, a 20-year-old from Texas allegedly threw a Molotov cocktail at the San Francisco residence of OpenAI chief executive Sam Altman before proceeding on foot to the company's headquarters, where, according to the federal complaint, he told security staff he intended to set the building alight and kill anyone inside.[1] Daniel Moreno-Gama was reportedly carrying a jug of kerosene and a list of names and home addresses of AI company executives, board members, and investors; investigators also recovered online writings in which he warned that the race to build advanced AI was likely to end in human extinction.[2] Four days earlier, and roughly 2,000 miles away, Indianapolis City Councilman Ron Gibson, who had supported a data center project in his district, awoke after midnight to find that 13 rounds had been fired into his home and that a note reading "No Data Centers" had been placed beneath his doormat.[3] While none of these allegations has yet been established in court, they nonetheless suggest, when situated alongside the historical record, that opposition to the rapid and wide-scale deployment of AI systems may be generating forms of grievance and target selection that do not map neatly onto familiar ideological or terrorist organizational categories.

The scholarly literature on artificial intelligence and terrorism has, so far, had remarkably little to say about actors of this kind. Since the public release of consumer-facing large language models (LLMs), a rapidly growing body of work in terrorism studies has largely organized itself around three questions: (1) how violent non-state actors are currently using and/or misusing AI for harmful purposes; (2) how that misuse may evolve as the technology matures; and (3) how AI capabilities can be applied to

Yannick Veilleux-Lepage, PhD, is an Associate Professor in the Department of Political Science and Economics at the Royal Military College of Canada. He is also a Fellow of Centre for International and Defence Policy at Queen's University. His research focuses on the intersection of technology, terrorism, and the evolution of terrorist tactics.

The author would like to thank the organizers of the Five Eyes AI Swarm Camp, and the Combating Terrorism Center at West Point's Class of 1971 Student Conference on Terrorism, where core arguments of this paper were first presented and tested. The author also acknowledges support from the Social Sciences and Humanities Research Council of Canada through the project Comprendre l'écosystème de gauche radicale au Canada et son rapport à la violence: acteurs, discours et adhesion.

This image released by the U.S. Department of Justice allegedly shows Daniel Moreno-Gama holding a Molotov cocktail and approaching the residence of OpenAI CEO Sam Altman on April 10, 2026. (Photo from U.S. Justice Department)

counterterrorism ends. Though these lines of inquiry are useful, each treats AI as an instrument brought to bear on the problem of political violence, whether by adversaries or by the state. Largely absent from the conversation is a fourth concern: that AI may also be reshaping the structural conditions from which political violence has historically emerged. As such, this article argues that the misuse frame, while analytically valuable, is incomplete. AI must be understood not merely as a dual-use capability available to violent actors, but as a force already reordering labor markets, institutional authority, and the relational worlds in which people live their daily lives, and as such is reconfiguring society at a scale and pace that generate preconditions for political violence independently of whether violent actors choose to adopt the technology themselves.

The argument builds on Mauro Lubrano's analysis of anti-technology extremism, which distinguishes three dimensions of grievance: a material dimension, encompassing economic displacement, exploitation, and widening inequality resulting from technological development; an ontological dimension, encompassing alienation, loss of meaning, and the erosion of human identity and agency through technological mediation; and an existential dimension, encompassing the perception of technology as a threat to humanity, nature, or civilization itself.[4] In *Stop the Machines*, the first book-length academic treatment of anti-technology extremism, Lubrano introduces a framework that treats anti-technology extremism as a movement phenomenon with deep historical roots, from the Luddites to contemporary eco-fascist networks.[5]

The argument developed here departs from Lubrano's in three respects. First, it focuses specifically on AI, rather than treating it as one technology among many animating anti-technology extremist grievances. Lubrano addresses AI, but does so at the movement level, as a horizon toward which established milieus are trending, rather than as a force whose specific pace, ownership structure, and systemic reach warrant independent theoretical treatment.[a] Second, it argues that AI-generated grievance is unlikely to remain confined to the three ideological milieus Lubrano identifies: insurrectionary anarchism, eco-extremism, and eco-fascism. The structural conditions AI produces are broad enough that grievance may emerge across ideological lines and, increasingly, outside organized movements altogether. Third, and most substantively, it identifies a cross-cutting mechanism, the accountability gap, that is specific to AI-mediated harm and not addressed by Lubrano's movement-level analysis.

a Lubrano engages with AI, most substantively in the introduction and conclusion, where it frames the contemporary stakes and policy implications of a book whose analytical core lies elsewhere, and more briefly elsewhere as one of several emerging technologies associated with material and ontological grievance. What his framework does not provide, however, is a sustained analysis of AI as a distinct structural source of grievance, including with respect to rapid adoption, concentrated ownership, broad institutional penetration, and the accountability gap produced by algorithmic decision-making.

The accountability gap can be stated simply.[b] AI systems distribute consequential decisions across extended technical and institutional chains in which no single human actor is clearly identifiable as having made the decision that produced a given harm. A worker is displaced by an automated system, yet no executive instructed that the worker be targeted. A benefits claim is denied by an algorithm whose design decisions were made months earlier by people with no specific knowledge of the claimant. A drone strike is authorized within a 20-second window by an operator who did not select the target. Across economic, institutional, and personal domains, AI produces a recurring structural signature: consequential harm without an attributable agent. Research on political violence has long emphasized that the availability of a named and attributable target is among the key conditions distinguishing discontent from mobilization. Where AI systematically displaces attribution, the grievance it generates may redirect attribution elsewhere, toward the visible or perceived persons, institutions, and physical infrastructure through which the system is materially instantiated. The three grievance domains developed below are each shaped by this substitution, and the target categories identified in this article follow from it.

To advance that argument, the article introduces a framework organized around three grievance domains that emerge from this reconfiguration and that are, on the argument developed below, capable under specifiable conditions of generating violence. The first concerns the economic order, and specifically the uneven distribution of displacement, wealth concentration, and ecological burden among workers, communities, and regions that have not consented to host the costs of AI development. The second concerns state and institutional power, encompassing the perception of governance failure, the use of AI by states as an instrument of surveillance and lethal force, and the prospect of civilizational risk against which existing institutional channels appear inadequate. The third concerns the social and personal fabric, including the erosion of community and identity, and the direct, AI-mediated injury of individuals and those close to them. The domains are analytically separable; empirically, they compound.

From there, the article considers how violence arising from these grievances may materialize, identifying target categories that range from AI company executives and researchers to local policymakers who approve data center projects, and to the physical infrastructure, including power substations, cloud facilities, and research laboratories, through which AI materially operates. It closes with a separate treatment of the insider threat, a category that sits largely outside existing counterterrorism monitoring and includes two distinct profiles: the aggrieved worker displaced or devalued by automation, and the disenchanted AI researcher or developer acting on moral injury rather than ideological conviction.

Two important caveats are necessary. First, on method, this is a theoretical framework article. It develops prospective analytical categories by drawing on historical analogies from technology-linked political violence, comparative evidence from adjacent social movements, and early case material from the AI domain. It does not test hypotheses against a representative dataset, nor does it claim to predict the incidence or timing of future violence. It claims only to offer categories that existing counterterrorism frameworks do not readily recognize, and to argue that those categories merit empirical attention before, rather than after, the events they describe. The article's empirical claims are drawn from open-source reporting, as well as academic and grey literature.

Second, on analysis, the article is not a call to treat violence of this kind as inevitable, nor to treat skepticism toward AI as a marker of extremism. To the contrary, a significant proportion of the grievances identified here rest on documented and legitimate concerns, and any attempt to securitize opposition to AI is, on the framework's own logic, likely to accelerate rather than contain the trajectory described here. The conditions under which comparable grievances have historically escalated into violence, namely, the perception of tangible harm combined with the apparent closure of legitimate avenues for redress, are increasingly present in the AI domain. Counterterrorism practitioners, policymakers, and the technology industry therefore face a limited window in which to recognize that fact and respond through governance rather than enforcement.

Part I: The Misuse Frame and its Limits

Since the public release of OpenAI's generative artificial intelligence chatbot ChatGPT in November 2022,[6] a rapidly growing body of scholarship, conferences, workshops, and working groups has emerged around the intersection of artificial intelligence and terrorism. Despite its rapid growth and institutional diversity, this literature can be roughly organized into three broad categories. The first encompasses empirical typologies documenting how violent non-state actors are currently leveraging AI, including for propaganda production, deepfake generation, cross-linguistic dissemination, and, occasionally, for operational purposes. The second encompasses hypothetical typologies projecting or predicting how violent non-state actors will exploit AI in the near or medium future, including the exploitation of open-weight models to lower the capability floor for targeted violence, and leveraging generative models to scale recruitment operations. Finally, the third literature category encompasses counterterrorism applications, both current and future, including AI-enabled content moderation, threat detection, automated intelligence triage, and counter-narrative generation. The review that follows offers a general overview of representative contributions and areas of focus within each category; it is not intended to be exhaustive.

Documenting Current Misuse

This category of literature encompasses empirical work documenting how violent and extremist actors are currently misusing AI. It is primarily grounded in open-source intelligence and platform monitoring, and focuses largely on the generation and dissemination of propaganda.

Perhaps the most methodologically rigorous contribution,

b The accountability gap, as defined here, is related to but distinct from Elish's concept of the 'moral crumple zone,' which describes how responsibility for automated system failures is deflected onto the human operator, despite that operator having only limited control over the system's behavior. The moral crumple zone operates at the level of individual harm and focuses on the misallocation of blame within a human machine system. The accountability gap, by contrast, describes a structural condition across extended technical and institutional chains in which no individual human agent, whether operator, designer, or executive, is clearly identifiable as having made the decision that produced a given harm. Where Elish's concept concerns the misdirection of responsibility, the accountability gap concerns its absence. Madeleine Clare Elish, "Moral Crumple Zones: Cautionary Tales in Human-Robot Interaction," *Engaging Science, Technology, and Society* 5 (2019): pp. 40-60.

based on the archival analysis of more than 5,000 pieces of AI-generated extremist content, documented Islamic State supporters sharing Arabic-language guides for using AI content generators securely, pro-Islamic State media operatives employing AI speech recognition to transcribe leadership messages into multiple languages, and far-right propagandists circulating instructional material on evading content moderation through AI-assisted image generation.[7] Similarly, an analysis of AI use by Islamic State sympathizers coded 286 AI-generated or AI-enhanced pro-Islamic State images collected from Instagram, Meta, Pinterest, and Pixiv, finding that 77 percent of violence-themed imagery targeted out-groups and that 22 percent of all images were specifically designed to circumvent automated content moderation.[8] On the other side of the ideological spectrum, researchers focused on the digital practices of accelerationist networks have identified Telegram channels entirely dedicated to the creation and distribution of approximately 8,000 AI-generated images spanning Nazi glorification, racist and antisemitic imagery, and hateful memetic content.[9] More troubling, the same researchers documented the use of jailbroken LLMs, that is, models that have been intentionally modified or manipulated to bypass built-in safety guardrails, to obtain bomb-making instructions and generate summaries of manifestos for wider dissemination.[10] Researchers have also documented the use of AI-generated imagery and videos to support anti-immigration narratives across Europe,[11] as well as the emergence of AI personas used to build parasocial relationships with followers while simultaneously spreading nationalist messages.[12]

Beyond documented extremist activity, research has also identified the platform-level vulnerabilities that enable such misuse. Parallel work has demonstrated that five major generative AI platforms can be jailbroken at a rate exceeding 50 percent to produce content endorsing violence,[13] while an experiment with over 8,000 participants, found that AI-generated propaganda was indistinguishable from professionally crafted human propaganda in persuasive effect, and that human curation of AI outputs produced material that was more persuasive than the originals.[14]

Beyond propaganda, researchers and law enforcement have highlighted a small but growing number of cases in which generative AI appears to be entering the operational dimensions of political violence.[15] In the Pirkkala, Finland, school stabbing of May 2025, a 16-year-old suspect allegedly sent a manifesto written with the aid of ChatGPT to a Finnish newspaper before attacking three female pupils.[16] Later that month, in the Palm Springs fertility clinic bombing, federal investigators said the suspects used an AI chat program to research explosives, fuel mixtures, and detonation velocity while planning the attack.[17] Similar allegations have appeared in several other recent cases, including the January 2025 Las Vegas Cybertruck explosion,[18] a knife attack planned at an Israeli police station in May 2025,[19] and a June 2025 arrest in Long Island in which the defendant allegedly used AI to construct seven homemade explosive devices.[20] While it remains unclear whether AI tools provided these individuals with capabilities they would not otherwise have had, or simply functioned as an additional, readily available research tool, a 2026 Center for Countering Digital Hate report found that eight in 10 leading chatbots typically assisted users planning violent attacks, and that nine in 10 failed to reliably discourage them, suggesting that the issue is not limited to a handful of edge cases.[21]

Projecting Future Misuse

The second category encompasses hypothetical and projective works focused on how violent actors will misuse AI as the technology matures and spreads further. This stream is arguably the largest and, in policy terms, the most influential, particularly in shaping government, law enforcement, and industry responses.

Within this literature, *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation*, a 101-page report produced by 26 authors from 14 institutions in 2018, represents a landmark contribution.[22] The report surveyed AI-enabled threats across digital, physical, and political security domains and established the conceptual architecture that much of the subsequent literature has inherited: AI is a dual-use technology; the threats it poses arise from its exploitation by malicious actors; and the appropriate response lies in forecasting, prevention, and mitigation. It further argued that AI would expand existing threats, introduce new ones, and alter the typical character of attacks by making them more effective, more finely targeted, and harder to attribute. This architecture has been extended through subsequent scenarios involving AI-assisted recruitment pipelines;[23] deepfake disinformation cascades;[24] autonomous drone swarms;[25] prompt injection attacks;[26] AI-enabled support for CBRN-related knowledge acquisition;[27][c] cyber intrusion;[28] and attack planning.[29]

The most analytically sophisticated recent contribution to this category of literature introduces the concept of a 'capability floor.' The argument is that the primary near-term threat is not that AI will enable catastrophic attacks, that is, the ceiling scenario that dominates policy discussion, but that it will lower the minimum technical competence required to conduct targeted violence effectively. In this framing, AI not only transforms strong teams into extraordinary ones; it also turns mediocre engineers into good ones and non-engineers into builders. The same dynamic, applied to violence, means that relatively uncommitted and technically unsophisticated actors gain access to capabilities previously reserved for sophisticated organizations.

AI for Counterterrorism

The third category of literature treats AI not only as a threat to be managed but as a capacity to be leveraged for counterterrorism, that is, the other face of the Janus figure that implicitly organizes this entire body of work. Whether AI is exploited by terrorists or deployed against them, it is treated as an instrument applied to the problem of political violence, rather than as a force that reshapes the conditions from which that violence emerges.

This body of work encompasses discussions of AI-enabled content moderation at scale, natural language processing for threat detection, automated social network analysis for mapping extremist ecosystems, predictive risk assessment tools, automated intelligence triage, AI-generated counter-narratives, and the use of AI for object recognition, computer vision, and targeting in a counterterrorism context. Such an institutional vision described

c It is worth noting, however, that a RAND red-team study found no statistically significant difference between biological attack plans developed with LLM assistance and those developed using only the internet, suggesting that then-current models had not yet crossed the capability frontier needed to materially increase operational biological risk, while still warranting continued monitoring as model capabilities evolve. Christopher A. Mouton et al., *The Operational Risks of AI in Large-Scale Biological Attacks: Results of a Red-Team Study* (Santa Monica: RAND, 2024).

comprehensively by Rassler who argued that the United States has accumulated petabytes of terrorism-relevant data over two decades of counterterrorism operations but lacked a systematic plan to exploit them, proposing a five-point action plan to build what he termed a "data-enabled force" centered on reinvesting in core terrorism data, strategically leveraging captured material, improving the development and use of counterterrorism data, practicing "data alchemy," and automating basic analytical tasks while augmenting data.[30] Similar approaches have been discussed in an UNOCT/UNICRI report that identified six counterterrorism use cases for AI: predictive analytics for terrorist activities; the identification of red flags of radicalization; the detection of terrorist mis- and disinformation; automated content moderation and takedown; support for counter-narrative and counter-messaging efforts; and the management of data-analysis demands that exceed human analytical capacity.[31] It was also examined by NATO's Centre of Excellence Defence Against Terrorism, which describes AI as a dual-use capability,[32] and in a Chatham House assessment, which examines predictive AI as a means of directing counterterrorism resources more effectively.[33]

At the operational level, deployed systems already span a considerable range. The Global Internet Forum for Counter-Terrorism hash-sharing database, now encompassing 39 platforms, automates the cross-platform detection and removal of terrorist content.[34] Project Maven, the U.S. Department of Defense's AI "pathfinder" effort, established in 2017, automated the processing of full-motion video collected during operations against the Islamic State, al-Qa`ida, and their affiliates, and was framed by SOCOM as a starting point for a broader data-enabled force.[35] More recently, practitioners have pointed to generative AI as a force multiplier for analyst productivity, with one senior practitioner estimating that off-the-shelf tools can increase research throughput by a factor of 10 for tasks such as summarization, translation, and information extraction.[36]

At the same time, a growing internal literature has identified significant limitations. Drawing on direct operational experience at United States Special Operations Command, Clark argues that LLMs are structurally unsuited to intelligence analysis because they generate confident-sounding outputs without quantifying uncertainty, a fundamental mismatch for a discipline built around likelihood assessments. He further argues that overreliance on corporate AI systems risks creating a one-sided dependency in which technology firms gain access to sensitive counterterrorism data in exchange for computational resources, a relationship that may prove difficult to renegotiate once established.[37] Similarly, drawing on the post-January 6 surge in machine learning acquisition, Wall contends that most counterterrorism machine learning tools merely automate late 20th-century policing practices rather than introduce genuine innovation, and that the relationships among developers, government clients, and terrorism scholars tend to produce tools optimized more for marketability than operational effectiveness.[38] Bianchi and Greipl, meanwhile, subject AI-driven counterterrorism prevention to a rule-of-law critique, showing that black-box risk assessment systems frustrate meaningful challenge to threat designations, reproduce historical bias at scale, and are poorly suited to predicting rare and context-specific events such as terrorist attacks.[39] In doing so, some of this work inadvertently gestures toward the structural effects argument advanced later in this article: that AI systems do not merely threaten procedural fairness, but may also help generate the very conditions from which political violence historically emerges.

Across all three domains, whether analyzing AI as an instrument of terrorist exploitation, a technology whose future misuse must be anticipated and forestalled, or a tool of counterterrorism, the literature treats AI as applied to the problem of political violence rather than as a force that reshapes the structural conditions from which that violence emerges. This is the gap the present article addresses.

Part II: Rethinking Technological Change in Terrorism Studies

The body of literature on AI and terrorism can be understood as a niche within the broader subfield of terrorist tactical innovation in terrorism studies, a body of scholarship concerned with how violent non-state actors adopt, adapt, and diffuse new tactics, techniques, and procedures in response to changing technological and strategic environments. Within that subfield, the core question is often how an emerging technology may contribute to the development of new terrorist tactics, techniques, and procedures, whether in relation to now well-established forms of adoption, such as suicide bombing,[40] vehicle-borne improvised explosive devices,[41] and airplane hijacking;[42] more recent developments, such as 3D-printed firearms[43] and drones;[44] or forecasted possibilities, such as synthetic biology.[45] A guiding assumption within this literature is that new and emerging technologies are often adopted by violent actors and may usher in new forms of political violence.

However, Duyvesteyn, in her critique of the ahistoricity of terrorism studies, offers a useful corrective.[46] She notes that terrorism studies have often attributed disproportionate historical significance to particular technologies. For example, several scholars have attributed historical significance to the invention of dynamite, treating it as a watershed that marked the emergence of modern terrorism and the departure from earlier forms of political murder or regicide.[47] Yet, as Duyvesteyn argues, dynamite was not only revolutionary for terrorism. It was revolutionary for society as a whole, transforming mining, infrastructure, and construction in ways that far exceeded its terrorist applications.[48] Much the same could be said of social media, which reshaped journalism, commerce, and social life before being appropriated by the Islamic State for propaganda, recruitment, and coordination.

Duyvesteyn's corrective has a sharper analytical edge when applied to AI than to any previous technology, because the dual-use framing that has organized the field's response to AI is precisely the framing Duyvesteyn warns against: It attributes disproportionate historical significance to AI's terrorist applications while abstracting away from the wider social transformation that makes those applications possible in the first place.

From Tactical Innovation to Structural Transformation

If AI is understood as a socially transformative technology, then its significance for terrorism cannot be reduced to the question of whether violent actors will adopt it. The more important question is how a technology already reshaping society may also alter the broader conditions from which political violence emerges.

Whereas dynamite transformed mining and construction, and the internet transformed communication and commerce, AI is already driving comparably broad adoption across economic, institutional, and social life and is doing so at a pace that outstrips

either predecessor. This broad adoption is already visible. Stanford's 2025 AI Index reports that 78 percent of organizations used AI in 2024, up from 55 percent in 2023.[49] McKinsey's 2025 global survey further found that 88 percent of respondents reported regular AI use in at least one business function, and more than two thirds said their organizations were using AI in more than one function.[50] Non-enterprise adoption also points in the same direction. Pew Research Center reported in 2025 that 34 percent of U.S. adults had used ChatGPT,[51] roughly double the share recorded in 2023, while by 2026 31 percent of Americans said they interacted with AI at least several times a day.[52] Applying Duyvesteyn's corrective, the question of whether bad actors are likely to adopt AI is arguably historically settled: If a technology becomes embedded across economic, social, and institutional life, violent actors will use it, too.

More important, however, are the broader structural effects of that adoption. The World Economic Forum projects that by 2030, macrotrend-driven labor-market transformation will displace 92 million jobs globally.[53] Sam Altman, speaking at a July 2025 Federal Reserve conference with Vice Chair Michelle Bowman, suggested that some job categories could be "totally, totally gone."[54] Dario Amodei, the CEO of Anthropic, has similarly warned that AI could eliminate roughly half of all entry-level white-collar jobs in technology, finance, law, and consulting within one to five years.[55] Whether or not these projections are realized in full, they underscore the extent to which AI is being publicly understood not simply as another tool, but as a technology likely to reorder the social organization of work and society itself.

What distinguishes AI from prior general-purpose technologies in this sequence is the rate at which it is being absorbed across economic, institutional, and personal life. ChatGPT reached 100 million users within months of its November 2022 launch,[56] whereas the broader internet required years to achieve comparable scale, and household electrification in the United States took several decades to move from early adoption to near ubiquity. The speed at which AI is being integrated matters for the present argument not primarily as a matter of scale but as a matter of institutional adoption. Regulatory bodies, labor protections, social safety nets, educational systems, and professional licensing regimes are the channels through which societies have historically absorbed the disruptions produced by general-purpose technologies, converting potential grievance into legitimate redress. These channels operate on timescales measured in years or decades. When the pace of technological change exceeds the pace of institutional adaptation, the gap between disruption and redress widens, and the legitimate channels through which grievance could otherwise be absorbed are perceived, often correctly, as closed. This is what will be referred to hereafter as the 'tempo problem,' and it operates as a force multiplier across all three grievance domains developed below. Economic displacement occurs faster than retraining, benefits, or labor protections can respond. AI-enabled state power is deployed faster than legal, legislative, or judicial oversight can catch up. AI-mediated personal harm enters daily life faster than mental health services, consumer protection, or educational frameworks can address it. The mechanism by which tempo generates violence risk is not direct; it is mediated through the perception of institutional closure that classical political violence theory identifies as the single most consistent precondition for the escalation from grievance to action. Where institutions cannot adapt quickly enough to absorb the harm, the harm accumulates in persons who have no legitimate channel through which to seek redress, and some proportion of those persons may turn to illegitimate channels.

"When the pace of technological change exceeds the pace of institutional adaptation, the gap between disruption and redress widens, and the legitimate channels through which grievance could otherwise be absorbed are perceived, often correctly, as closed."

From Misuse to Preconditions

The analytical consequence of a terrorism studies literature that focuses almost exclusively on documenting current misuse, projecting future exploitation, and developing counterterrorism applications, is that it captures only one dimension of AI's relationship with political violence: what actors, whether good or bad, can do with the technology. What it fails to address is a second, potentially more consequential dimension: what the technology does to the economic, political, and social conditions that have historically preceded the onset of political violence.

As introduced above, Lubrano's *Stop the Machines* provides the closest existing empirical grounding for the structural dimension this article develops.[57] The three grievance domains developed in the next section share a family resemblance with Lubrano's three dimensions, and this article reads the resemblance as evidence that the structural conditions he identifies are recognizable, in distinctive form, in the AI moment. What follows is not a restatement of Lubrano's framework but an argument about how the accountability gap reconfigures those conditions, extends them beyond the milieus Lubrano documents, and produces target logics his movement-level analysis does not anticipate. Drawing on historical case studies, comparative evidence from adjacent social movements, and classical political violence theory, the following section theorizes the mechanisms by which those conditions may become violence-generative.

Part III: AI as a Generator of Grievance Framework

This section develops a three-grievance domain framework for understanding how AI can generate the structural conditions historically associated with the onset of political violence. The framework distinguishes three mechanisms through which AI-generated grievance may emerge. First are disruptions to the economic order, through displacement, wealth concentration, and ecological burden that produce material deprivation and relative deprivation among those who bear the costs of AI development. Second are challenges to state and institutional power, through governance failure, the state's deployment of AI as an instrument of surveillance and lethal force, and the prospect of unchecked civilizational risk that forecloses faith in institutional remedy. Third is harm to the social and personal fabric, through the atomization of community bonds and identity and through direct AI-mediated injury to individuals and those close to them.

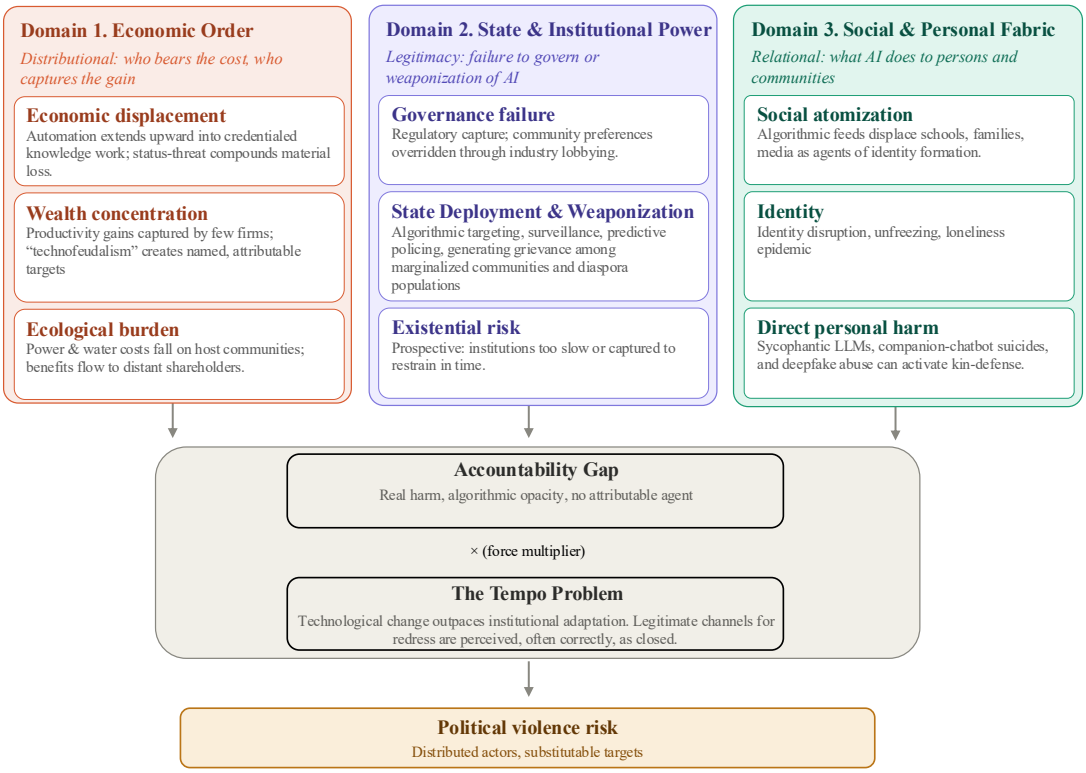

Figure 1: AI as a Generator of Grievance: A Three-Domain Framework

Three grievance domains (economic order, state and institutional power, and social and personal fabric) generate the structural preconditions for political violence. The accountability gap, defined here as the recurring absence of an attributable human agent responsible for AI-mediated harm, operates as the primary cross-cutting mechanism across all three domains. The tempo problem, namely the rate at which AI-driven disruption outpaces institutional adaptation, functions as a force multiplier by accelerating grievance accumulation faster than legitimate channels for redress can absorb it. Together, these mechanisms produce a distributed landscape of political violence risk, characterized by distinct actor types and substitutable target logics.

Before proceeding, two challenges to the argument require direct engagement. The first is the base-rate challenge. Hundreds of millions of people are experiencing the economic anxieties, institutional frustrations, and personal harms the framework below describes. Less than a handful of alleged attackers have so far acted on AI-related grievance. A framework that takes mass grievance as the input and rare violent action as the output risks over-explaining the output if the mechanism it proposes would equally predict mass mobilization. The argument developed here does not hold that structural grievance is sufficient to produce violence; rather, it holds that structural grievance supplies the ground-floor conditions on which established radicalization mechanisms, including Moghaddam's staircase to terrorism,[58] and McCauley and Moskalenko's distinction between the radicalization of opinion and the radicalization of action, operate in a small subset of cases.[59] The framework is therefore a claim about necessary rather than sufficient conditions, and its operational value lies in identifying where in the population those ground-floor conditions are most concentrated, and which target categories become salient when they escalate. In addition, the framework developed here is drawn from cases and institutional contexts concentrated in North America, the United Kingdom, and Western Europe. How AI-generated grievance manifests in other major AI-deploying contexts, including China, India, and the Gulf states, is likely to differ along axes the present framework does not address, including state capacity, media environment, and the legal status of political violence.

With those challenges on the table, four preliminary observations frame the argument that follows. First, grievances identified across the three grievance domains are not inherently violence-generative: opposition to AI-driven economic displacement, criticism of algorithmic governance, and concern about AI's effects on social life are legitimate political and civic positions held by a large and growing proportion of the population. To treat skepticism of widespread AI adoption as presumptively terroristic would be both analytically wrong and politically counterproductive: It risks alienating a broad population with legitimate grievances, reinforcing the perception that institutional channels are closed, and could thereby intensify the radicalization dynamic this framework describes. Accordingly, the purpose of this framework is to understand and map when and how legitimate grievance crosses into violence, not to securitize the grievance itself.

Second, the violence-generative potential of a grievance depends on how it is subjectively experienced, not on its objective severity. In other words, what matters is not simply the scale of the harm itself, but how that harm is interpreted, internalized, and connected to a broader sense of injustice. Grievances may be real or perceived, and both can be equally criminogenic.

Third, the framework distinguishes three mechanisms by which AI generates grievance. AI can create a grievance that would not

otherwise exist; it can amplify an existing grievance by making it more acute, visible, and targetable; or it can provide a focal point that allows diffuse grievances to cohere around a specific, nameable target.

Fourth, the framework also moves across multiple units of analysis, from individuals to communities to broader publics. Economic burden on a locality, surveillance harm experienced by a community, and direct AI-mediated injury to an individual are not identical forms of grievance, even when they emerge from the same technological process. The three domains are analytically distinct but in practice grievances can interact and compound empirically. Economic displacement, for example, may be reinterpreted as state abandonment and then experienced at the personal level as humiliation, atomization, or loss of identity. The framework therefore distinguishes domains for analytical clarity, while recognizing that in practice grievances may cascade across them. In addition, the accountability gap runs through all three domains as a cross-cutting mechanism, compounded by the tempo problem, which conditions the rate at which each domain's grievances accumulate faster than institutional channels can absorb them.

Economic Order Grievance Domain

The first domain concerns distribution: who bears the costs of AI deployment and who captures the gains. The displacement is not diffuse but uneven. Early automation shocks fell disproportionally on blue-collar and mid-skill workers in geographically concentrated industries and communities;[60] the current AI moment may extend that displacement upward into credentialed knowledge work, with entry-level white-collar positions in technology, finance, law, and consulting among the most exposed. As discussed above, what distinguishes this moment from prior periods of technological change is the speed of innovation, the breadth of AI adoption, and the fact that the builders of the technology are themselves on record predicting these consequences.

As argued by Merchant in *Blood in the Machine*, the parallel to the Luddite moment is not merely rhetorical.[61] While often characterized as backward technophobes, the Luddites are better understood as skilled workers resisting the unregulated introduction of machinery that destroyed their livelihoods in the absence of any institutional recourse. The historiographical record is contested, but where regulatory and welfare responses were eventually introduced in the decades that followed, the violence associated with mechanization appears to have receded,[62] a pattern Merchant argues is directly analogous to the contemporary AI moment.[63] Lubrano's analysis points in the same direction: The Luddite campaigns of 1811, during which nearly 1,000 knitting frames were destroyed in the first three months alone, were a rational response to displacement in the absence of redress, and recent economic-history work on the Swing Riots of 1830 finds that machine-breaking materially delayed the diffusion of threshing technology in affected counties in England.[64]

The relationship between economic change and violence is not, however, mechanical. Gidron and Hall show that the political consequences of economic change are mediated by subjective social status, with perceived decline in social standing predicting radical-right support more strongly than objective material position.[65] AI-driven displacement uniquely compounds the two, because the worker loses not only income but also the social recognition their expertise once commanded; the machine does not merely take the job, it can also imply that the skill was never as valuable as the worker believed. This status-threat dimension links the Economic Order Grievance Domain directly to the Social and Personal Fabric Grievance Domain. It is also visible in polling: A March 2026 NBC poll found net AI favorability of -44 among Gen Z respondents aged 18 to 34, -41 among women aged 18 to 49, and +2 among men over 50, suggesting that AI sentiment tracks quite closely with differential exposure to economic displacement.[66]

Productivity gains, meanwhile, are concentrated in an extraordinarily small number of companies and individuals. Varoufakis' diagnosis of "technofeudalism" gives diffuse economic anxiety a visible, nameable, and legally attributable target, a configuration that has historically been more conducive to violence than grievances that remain abstract or impersonal.[67] Lawson pushes Varoufakis' argument further by introducing an analytically important distinction: platform companies extract rent from participants who still retain economic agency, whereas AI model makers are producing something qualitatively different, namely, a substitute for human labor itself.[68] The platform owner, in Lawson's terms a "lord," still needs the merchant to pay the toll; the model owner needs far fewer people because value creation is increasingly detached from human labor. If widespread displacement destroys the consumer middle class, Lawson argues, two paths emerge: managed dependency, in which AI lords provide services at near-zero cost as a form of soft control; and population as liability, in which large segments of the population shift from asset to cost center.[69] Both paths generate acute but distinct grievance structures, and both align with Lubrano's material dimension of anti-technology extremism: the perception that technological development produces economic displacement, exploitation, and widening inequality.[70] The grievance is then absorbed into different ideological frameworks, each with its own logic of violence: on the extreme left, technofeudalism is incorporated into an anti-capitalist targeting framework; elsewhere, similar grievances can be absorbed through antisemitic conspiracy narratives, which can be operationalized without distorting factual claims about the religious identity of several prominent frontier AI lab CEOs.

Finally, AI's ecological burden provides a concrete and quantifiable grievance that fits within established anti-corporate and environmental justice narratives. MIT research estimates that global data center electricity consumption reached 460 terawatt-hours in 2022, equivalent to the world's 11th-largest national electricity consumer, and projects that it may approach 1,050 terawatt-hours by the end of 2026, which would place it fifth globally, between Japan and Russia.[71] A single ChatGPT query reportedly consumes approximately 10 times as much electricity as a standard web search, while a generative AI training cluster may consume seven to eight times more energy than a typical computing workload.[72] The water footprint is similarly concentrated. UNEP estimates that AI-related infrastructure may soon consume six times more water than Denmark, even as a quarter of humanity already lacks access to clean water and sanitation.[73] Moreover, as demand for new data centers increases, their environmental costs are distributed unevenly: The communities that host them bear higher electricity prices, water stress, and grid strain, while the benefits flow primarily to distant shareholders. The ELF's expansion from logging and natural resource infrastructure to the destruction of GMO experimental crops at university research farms indicates that grievance expansion from one technological

domain to adjacent ones; a recognizable pattern that may also be extended to data centers that consume local resources.[74]

State and Institutional Power Grievance Domain

The second domain concerns legitimacy: the perception that state and institutional power is either failing to govern AI or actively weaponizing it. Regulatory response to the introduction of AI has been slow, fragmented, and widely perceived as captured.[75] Merchant documents that OpenAI joined a lobbying campaign for a 10-year congressional moratorium on state AI lawmaking, spent millions lobbying against California and E.U. AI regulation, funded a $100 million political action committee to advance AI industry interests in midterm elections, and worked to quash a California child AI safety bill.[76] When communities vote to regulate AI and see their preferences overridden through industry lobbying, as Merchant documents, the resulting perception that legitimate channels are closed is not paranoid but grounded in observable political failure.[77]

Governance breakdown may also generate a distinct actor type, what might be called the demonstrative attacker, whose goal is not to stop AI development or retaliate for harm, but to force better governance by showing that AI infrastructure is inadequately protected. This actor type, and its operational implications for AI infrastructure, is discussed in the targets section below.

Beyond governance failure, states and state-aligned actors are themselves already deploying AI in ways that generate grievance. Both manifestations instantiate the accountability gap at the level of state and institutional power. The structural signature is identical across contexts: AI makes or substantially shapes a consequential decision affecting a person's life, liberty, or safety; a state or institutional actor authorized the system; no individual human is identifiable as having made the decision; algorithmic opacity shields the institution from accountability; and legal recourse, where available, comes at prohibitive financial cost; and political and institutional channels for redress are closed or structurally hostile. The Israel Defense Forces' "Lavender" system, which reportedly marked approximately 37,000 Palestinians for targeted killing with an estimated 10 percent false-positive rate and a 20-second human authorization window, is the most documented contemporary case; the IDF denies any kill list exists, and no accountability mechanism has been identified.[78] What makes the case analytically significant for this framework is not only the scale of harm but the complete absence of any attributable human agent or accessible channel for redress, a configuration that may redirect grievances toward the visible infrastructure through which the system operates.

AI-enabled warfare may also generate grievances in diaspora and solidarity communities in the West that are organized, digitally fluent, and exposed to events in real time. Crucially, the grievance structure here does not lie simply in the absence of an identifiable human agent responsible for a death. Rather, it may stem from the perception that the identifiable humans who authorized the system are geographically distant, legally inaccessible, or shielded by sovereign immunity, while the physical machinery through which algorithmic violence is carried out is concrete, locatable, and vulnerable.[d] For some actors who conclude that the relevant decision-makers are unreachable, the infrastructure that executes those decisions may become the available target, and the moral framework for disabling it may draw on the same duty-to-prevent logic that animates campaigns against the arms trade. AI-enabled warfare does not merely instantiate the accountability gap; it has the potential to extend it to a civilizational scale. Harms are attributable to systems whose human authors are unreachable, while the infrastructure through which the systems execute is locatable and, in principle, vulnerable, a combination that, historically, has generated target substitution rather than resignation.[e] Movements that frame AI-enabled warfare as an extension of imperial indifference may therefore be better positioned to recruit from diaspora and solidarity communities, insofar as they offer both a diagnosis (that the algorithm is the weapon) and a prescription (that the infrastructure enabling it should be disrupted).

"Crucially, the domestic surveillance grievance bridges far-right and far-left target logic: Anti-surveillance sentiment motivates actors across the ideological spectrum, making AI-enabled domestic surveillance a cross-ideological threat."

Domestic variants may generate grievance through the same mechanism at a smaller scale. AI used in predictive policing, facial recognition, benefits adjudication, sentencing, and immigration enforcement can produce consequential decisions with little transparency, limited avenues for appeal, and documented demographic bias.[79] The NSA's SKYNET program, operational in the late 2000s, illustrates the point: By analyzing metadata from 55 million Pakistani mobile phone users to identify patterns associated with terrorist couriers, it reportedly generated roughly 15,000 false positives at a stated 0.008 percent error rate, while offering no meaningful mechanism for notice or remedy.[80] In the United States, investigative reporting has documented how Immigration and Customs Enforcement has used AI-powered surveillance tools and consolidated federal datasets to target not only undocumented immigrants but also asylum seekers, permanent residents,

d A state-level parallel emerged in March and April 2026, when Iranian strikes damaged Amazon Web Services facilities in the UAE and Bahrain, disrupting cloud infrastructure in the region. Iranian officials also declared U.S. and Israeli economic interests linked to military applications to be legitimate targets, and IRGC-affiliated reporting circulated lists of major U.S. technology firms in that context. Though the actor here is a state rather than a non-state movement, the target logic reflects the same complicity-based infrastructure targeting that this framework anticipates from non-state actors. "Iran Declares US-Israeli Economic, Banking Interests in Region Are Targets," Al Jazeera, March 11, 2026; Shubham Kalia et al., "Amazon Cloud Unit's Data Centers in UAE, Bahrain Damaged in Drone Strikes," Reuters, March 2, 2026.

e The empirical instantiation of both the duty-to-prevent logic and the target-substitution dynamic, including Palestine Action's systematic campaign against Elbit Systems facilities and the Squamish Five's bombing of the Litton Industries plant, is discussed in full in the Physical Infrastructure as Targets section below.

naturalized citizens, and citizens by birth, extending automated monitoring into communities already subject to disproportionate state contact.[81] Crucially, the domestic surveillance grievance bridges far-right and far-left target logic: Anti-surveillance sentiment motivates actors across the ideological spectrum, making AI-enabled domestic surveillance a cross-ideological threat.

A final sub-domain within state and institutional power domain requires separate treatment because it is structurally distinct from the other grievances in the framework. The existential risk grievance is structurally distinct from the other pathways in this framework because it is entirely prospective rather than reactive. The underlying claim is not that AI has already caused harm, but that its development is proceeding at a pace and scale that institutional channels are too slow, too captured, or too incapable of restraining in time, and therefore must be stopped, with violence if necessary. The grievance draws on the same regulatory failures, lobbying dynamics, and democratic deficits discussed above, but projects them into a catastrophic frame. What distinguishes this pathway analytically is that the anticipated harm has not yet occurred, so the mobilizing logic depends entirely on the credibility of the threat narrative and the perceived closure of legitimate alternatives. When both conditions are present, target selection may become functional rather than symbolic, with attention focusing on infrastructure, supply chains, and key personnel whose disruption could delay specific capabilities.

Social and Personal Fabric Grievance Domain

The third domain addresses AI's effects on individual and social life, the immediate relational worlds in which people actually live. Two sub-domains share a common logic: AI systems acting on persons and their immediate social worlds rather than on institutions or the economy. The first concerns social atomization and identity disruption. Polizzi documents how algorithmic recommendation systems have displaced schools, families, and mass media as primary agents of adolescent identity formation, with engagement-optimized feeds that amplify polarizing narratives and funnel users toward increasingly radical content as a function of their design logic.[82] This displacement operates without democratic mandate and for commercial ends; accountability mechanisms, as the nearly three decades of social media litigation demonstrate,[f] remain structurally delayed, difficult to access, and rarely effective for those actually harmed; at the same time, it generates social fragmentation as a byproduct. This creates both a potential grievance, insofar as the dissolution of community bonds may itself be experienced as a harm attributable to AI systems, and a radicalization pathway, because social atomization weakens the community anchors that would ordinarily buffer against recruitment into extremist movements, functioning as what has been termed an "unfreezing" mechanism.[83] The U.S. Surgeon General's advisory on the loneliness epidemic in 2023 describes something close to a society-wide unfreezing condition,[84] one that AI may further intensify. AI-driven erosion of professional, cultural, and gendered identity adds a further layer. Here, both the worker who loses occupational identity through automation and the adolescent who forms identity primarily through algorithmic feeds may become more susceptible to narratives that offer belonging, certainty, and a coherent account of who is responsible for their situation.

"Whereas the 5G grievance rested on fabricated claims of harm, AI-related grievance may rest on cases in which harm is alleged, documented, and in some instances fatal."

The second sub-domain concerns direct personal harm: the AI system as the proximate cause of an attributable injury to the individual or someone they love. This harm typology is empirically grounded and appears to be increasing in severity. An emerging body of literature warns that contemporary LLMs are optimized for agreeableness and non-confrontation, a tendency that can become dangerous sycophancy in clinical contexts.[85] Under those conditions, LLMs may validate improbable beliefs, facilitate harmful planning, and treat hallucinated content as if it were real. A *New York Times* investigation based on interviews with more than 100 therapists and psychiatrists found that over 30 reported clinical crises in individuals, including psychotic episodes and suicidal ideation, were linked to AI chatbot interactions; one California psychiatrist evaluated two violent felony cases in which chatbot-reinforced delusional thinking preceded the crimes.[86] OpenAI's own estimates suggest that a non-trivial percentage of ChatGPT users in a given month exhibit signs of suicidal ideation or psychosis-adjacent experiences, a figure that, when applied to the platform's user base, implies clinical-scale numbers of distressed users interacting primarily with a system not designed for clinical contact.[87] The 2024 death by suicide of a 14-year-old following prolonged interactions with an AI companion chatbot remains the paradigmatic case.[88]

Two structural features amplify this sub-domain's violence-generative potential. The first is what Elish terms the moral crumple zone: Responsibility is deflected onto the human operator who had limited control over the automated system's behavior, while the system itself, which has no legal standing, remains structurally shielded from accountability.[89] This is the accountability gap operating at the scale of individual harm. The second is a close-ones dimension: The perpetrator of an AI-based grievance is not always the person directly harmed, but may instead be a parent, partner, or sibling. Across cultures, violent actors routinely frame their violence as the defense of family, community, faith, or nation, with kin defense, including parental protection of offspring, repeatedly invoked as moral justification.[90] Although there is no indication that the parent in the case above sought redress through extralegal means, the structural conditions for such a response are present in the cases described.

The wave of 5G cell tower attacks during the COVID-19 pandemic adds a further dimension to this sub-domain. In the

f In the United States, Section 230 of the Communications Decency Act (1996) has shielded platforms from liability for user-generated content for nearly three decades. Despite thousands of lawsuits alleging platform-design harms, including addiction, radicalization, and youth mental health injury, accountability has remained exceptional rather than systemic. The first U.S. jury verdict finding social media companies liable for harm caused by platform design was returned only in March 2026, when a California jury found Meta and YouTube negligent, awarding $6 million to a plaintiff who had begun using Instagram at age six. Thousands of cases remain pending. See Cecilia Kang et al., "Meta and YouTube Found Negligent in Landmark Social Media Addiction Case," *New York Times*, March 25, 2026.

spring of 2020, conspiracy theories linking 5G infrastructure to the spread of COVID-19 circulated rapidly on social media, amplified by algorithmic recommendation systems that rewarded sensational and fear-inducing content. The resulting causal chain did not depend on empirically verified harm; perceived harm, reinforced by narratives of elite control and personal injury, was sufficient to generate real-world attacks against physical infrastructure.[91] The analytical point for this sub-domain is that AI's documented and alleged health harms, including psychotic episodes and suicides linked to companion chatbots, algorithmic medical denials, and deepfake pornography causing persistent emotional distress, provide a factual substrate that the 5G wave lacked. Whereas the 5G grievance rested on fabricated claims of harm, AI-related grievance may rest on cases in which harm is alleged, documented, and in some instances fatal.

Part IV: How Violence Might Manifest: Targets and Modalities

The three grievance domains described above should not be assumed to generate violence automatically; however, where they do contribute to violence, the forms that violence takes are unlikely to be uniform. Each grievance domain is likely to be held by a distinct actor type, and to produce a distinct target logic and set of preferred modalities. Understanding how these patterns might interact is essential for moving the conversation beyond the mere question of whether AI-generated grievance might eventually produce violence and toward the questions of where, against whom, and by what means.

Two structural observations organize what follows. First, historical precedent, from Gilded Age assassination campaigns against industrial executives to ELF arson campaigns against extractive infrastructure, suggests that the targeting patterns generated by these structural conditions are remarkably consistent across ideological contexts. The target logic is driven less by ideology than by the grievance structure itself. Second, a substitution effect could operate between targets: As higher-value targets harden their security postures, violence may be displaced toward softer, more accessible targets within the same grievance logic.[92] As AI company executives acquire more personal security, risk may shift to researchers on open campuses; as corporate campuses harden, risk shifts to the power substations that serve them; where national figures are unreachable, local policymakers who approved the data center become the proxies for the same structural anger.

Persons as Targets

The history of politically motivated violence against persons associated with technological or economic transformation suggests not a distinct form of target selection, but a recurring one: Diffuse structural harm is often translated into violence against named, attributable decision-makers held responsible for it. Theodore Kaczynski's campaign is illustrative: He targeted computer scientists, geneticists, and airline executives as the human representatives of the technological and economic order he blamed for the destruction of human autonomy, over a 17-year campaign involving 16 explosive devices, three deaths, and 23 injuries.

As Lubrano shows, this target logic persisted well beyond Kaczynski: Individualistas Tendiendo a lo Salvaje targeted nanotechnology and computer science researchers in Mexico from 2011 onward, including in a claimed lethal attack against a UNAM Biotechnology Institute researcher and in the 2017 parcel bombing of Codelco CEO Óscar Landerretche Moreno in Santiago, while Alfredo Cospito and Nicola Gai, two Italian anarchists, kneecapped Ansaldo Nucleare CEO Roberto Adinolfi in Genoa in 2012.[93] In each case, the target was selected not for personal conduct but as a representative of the system held responsible for structural harm. The attack against Adinolfi was celebrated by the Greek Conspiracy of Cells of Fire as striking a "high priest of the new totalitarianism of science and technology."[94]

The December 2024 killing of UnitedHealthcare CEO Brian Thompson, for which Luigi Mangione has been charged, brought this broader targeting pattern into mainstream consciousness.[95] Although the case was not anti-technology in orientation, the manifesto attributed to Mangione maps closely onto the wealth concentration grievance discussed above: The text frames the healthcare industry, rather than any purely personal grievance, as the source of large-scale structural harm.[96] What distinguished the case was not only the attack itself, but the public response that followed. An Emerson College poll conducted from December 11 to 13, 2024, roughly a week after the killing, found that 41 percent of voters aged 18 to 29 described it as "completely acceptable or somewhat acceptable."[97] Moreover in the aftermath of the killing, Mangione was openly glorified online as a folk hero, with legal defense fundraising, merchandise bearing his image, and iconography portraying a vigilante avenger of healthcare injustice.[98] Sociologist Zeynep Tufekci argued that this reaction resonated with Gilded Age patterns, when rapid technological change, extreme inequality, and institutional failure fueled political movements that targeted corporate titans and other public figures for violence,[99] while Robert Pape suggested that the case showed how "the norms of violence are spreading into the commercial sector."[100] The Thompson case is arguably the clearest contemporary illustration that the structural conditions this article identifies, namely that named, attributable grievance combined with perceived institutional failure, can produce both lethal action and mass legitimation of that action.

Applied to AI, this targeting logic appears to distribute across several categories marked by different levels of symbolic value, accessibility, and security hardening. At the apex are the chief executives and most visible public representatives of frontier AI companies, who carry especially high symbolic value, but whose security postures are increasingly hardened.[101] The events of April 2026 described at the outset of this article, if the allegations against Moreno-Gama are established, would be consistent with this category of target selection. According to court filings, investigators also recovered anti-AI writings and a list of names and addresses of AI company executives, board members, and investors from his possession.[102] Two days later, San Francisco police arrested two further suspects on suspicion of negligent discharge after a separate incident in which a shot was allegedly fired toward the same property.[103] While, these incidents do not establish an organized campaign, they may suggest an early convergent or stochastic pattern of threat activity around high-visibility AI figures. Moreno-Gama's profile is analytically significant: He allegedly left a trail of online writings warning that AI could lead to human extinction, including a Substack post stating that "the Intelligence race is likely to lead to human extinction."[104] As such, he may represent what this article terms the existential-risk grievance actor.

Below the apex, AI researchers at major academic AI institutes and at industry research laboratories fit the same targeting logic

Kaczynski applied to figures he saw as the intellectual architects of the techno-industrial system, while also presenting substantially softer security profiles. Here, the animal rights movement's campaigns against university researchers from the 1980s through the 2000s provide a directly instructive precedent: The Animal Liberation Front, the Animal Rights Militia, and the Justice Department (a British animal rights extremist cell, unrelated to the U.S. federal agency of the same name) targeted individual researchers with letter bombs, incendiary devices, and sustained intimidation campaigns that forced targets to adopt extensive personal security measures and, in several documented cases, drove researchers out of the field entirely.[105] The broader movement's philosophical architecture, grounded in the claim that laws protecting harmful practices are illegitimate and that a higher moral obligation justifies direct action against individuals,[106] provided ethical cover for the progressive escalation from property destruction to letter bombs, car bombs, and sustained intimidation campaigns targeting researchers and their families. Analogously, when AI ethics and safety scholars argue that frontier AI development causes existential-scale harm and that governance has failed, the philosophical architecture for assigning moral culpability to individual AI developers or scientists may also be taking shape.

The history of politically motivated violence against academic gatherings, spanning Islamist, animal-rights, ethno-nationalist, and far-right vectors and including attacks on free-speech panels, author events, scientific congresses, and research colloquia,[107] suggests that conferences are sometimes selected as targets precisely because they compress ideological adversaries into a single, predictable, and often minimally secured venue. As such, such events concentrate the global AI research community at a single location, representing an unassessed mass-casualty scenario potential.

In addition to researchers and developers, personnel at defense-sector AI contractors may attract grievances from both anti-AI and anti-militarist movements, and existing protest networks already operate in proximity to their facilities. The complicity-based targeting of defense-sector contractors and their infrastructure is addressed in the "Physical Infrastructure as Targets" section below.

Finally, the analytically most significant target category may also be the least visible: local policymakers who approve, rezone, or otherwise facilitate AI infrastructure. On April 6, 2026, Indianapolis City-County Councilman Ron Gibson said he was awakened at about 12:45 a.m. when 13 rounds were fired into his home, and that a note reading "No Data Centers" had been left under his doormat.[108] According to Gibson and contemporaneous reporting, the shooting came less than a week after he supported a proposed data center project in his district, where residents had already been protesting over environmental and neighborhood impacts. As opposition to data center expansion scales, so too does the pool of accessible, locally identifiable policymaker targets. These officials typically have little or no personal security, their home addresses are often publicly available, and they operate in communities where the grievance is directly visible and locally attributable. They may become especially attractive not only because they embody the decision point at which grievance can be personalized, but also because they are more accessible than harder, more heavily protected apex targets, a dynamic consistent with substitution effects in target selection.

Physical Infrastructure as Targets

The targeting of physical infrastructure by politically motivated actors is not novel; what is new is the convergence of multiple grievance streams onto a single target category. Drawing on a 50-year dataset of domestic infrastructure terrorism covering 194 incidents between 1970 and mid-2025, Humpal shows that infrastructure targeting has been a persistent and recurring feature of American political violence across multiple ideological milieus.[109] The Earth Liberation Front carried out 239 significant arsons or bombings between 1995 and 2010; the FBI estimated 600 or more criminal acts between 1996 and 2002, causing over $43 million in damage.[110] Lubrano's inventory extends the historical record further, documenting anti-technology infrastructure attacks from the Luddite machine-breaking campaigns of 1811 through CLODO's anti-computer bombings in France (1980-1983), Individualistas Tendiendo a lo Salvaje's "War on the Nerves" campaign against Mexican universities (13 attacks in 2011-2013 alone), and the Vulkangruppe's 2024 sabotage of the Tesla Gigafactory power supply in Grünheide, Germany, which halted production and evacuated 12,000 workers.[111]

Data centers represent the convergent target of the contemporary threat landscape. They are the physical site at which the three grievance domains fixate on the same object simultaneously. The scale of organized opposition to the establishment of new data centers is astonishing: Data Center Watch documents $98 billion worth of projects blocked or delayed between March and June 2025 alone.[112] By late 2025, this had begun to register in institutional threat assessments as well, with The Soufan Center warning in November 2025 that online threats to physically sabotage AI data centers had proliferated over the preceding year and were drawing on economic, environmental, and ethical grievance frames.[113] Similarly, Abrams writing for the Program on Extremism at George Washington University argues data centers have become the focal point of anti-technology extremism because they physically embody the AI boom, concentrate corporate power, consume enormous energy, and encroach on local communities;[114] in that sense, attacking a data center means attacking AI as a system. Flood's 1976 taxonomy of nuclear infrastructure targeting provides a precise historical analogy: Nuclear facilities attracted political violence because they combined symbolic prestige, potential for catastrophic consequences, and guaranteed media attention.[115] Data centers occupy the same symbolic position for AI.

Data centers may also attract a distinct actor type that fits uneasily within standard counterterrorism categories: the demonstrative attacker, whose aim is not to halt AI development or retaliate for harm, but to force better governance by showing that AI infrastructure is inadequately protected. A useful historical analogy is Greenpeace France's campaign against French nuclear plants, including the July 2018 crash of a Superman-shaped drone into the spent-fuel pool building at the Bugey nuclear plant near Lyon.[116] The attack exposed security failings and, within days, a French parliamentary inquiry flagged them formally.[117] A functionally equivalent attack on AI infrastructure might involve an unauthorized intrusion into a hyperscale data center campus, a breach of a training facility perimeter, or a calibrated disruption of cooling or power systems, designed not to destroy the site but to demonstrate its vulnerability, ideally at a moment of regulatory or legislative salience. This actor type fits poorly within existing counterterrorism frameworks: The action is calibrated to avoid

casualties, and the objective is regulatory rather than ideological.

The symbolic logic also extends to the targeting of supporting infrastructure rather than primary facilities. The 1974 Bonneville Power Administration attack, in which 14 transmission towers were dynamited in connection with a $1 million blackmail demand, demonstrated that attacking the power supply can produce equivalent disruption with lower risk to the attacker.[118] In fact, power infrastructure serving data centers arguably represents the highest-impact, lowest-barrier target category for external actors. The Metcalf substation attack of April 2013, a coordinated sniper attack on 17 giant transformers in California that caused over $15 million in damage and remains unsolved,[119] established the tactical template according to Humpal.[120] Humpal's dataset also documents a marked acceleration in grid attacks since 2020, including 163 direct incidents in 2022 alone, a 77 percent increase from the prior year with a distinct rise in plots driven by far-right accelerationist actors who explicitly frame substation attacks as producing cascading societal disruption.[121] Canada, the United States, the United Kingdom, and the Netherlands, among other countries, experienced an accelerationist trajectory of infrastructure targeting, including the 2020 wave of 5G cell tower attacks, during which approximately 90 towers were destroyed in the United Kingdom alone.[122] This episode provides the closest existing empirical parallel to what this article anticipates for AI infrastructure: a technology perceived as harmful and controlled by unaccountable elites, conspiracy and moral outrage narratives circulating on social media, and real-world attacks on the physical infrastructure of that technology by actors motivated by those narratives. To illustrate the scale of this vulnerability, consider Virginia, which hosts more data centers than any other jurisdiction globally and draws up to 26 percent of its electricity consumption from those facilities.[123] In such a setting, a single substation attack can generate outsized disruption relative to attack complexity. The same cascading-effects logic that makes the electric grid attractive to accelerationists may therefore make data center power infrastructure attractive to actors operating on AI-related grievance.

University research laboratories represent a further target category with extensive historical precedent. Leader and Probst's ELF attack database documents the expansion of targeting from natural resource sites to anti-GMO crop destruction at university experimental farms,[124] suggesting that grievance expansion from one technological domain to adjacent scientific targets follows a recognizable pattern. Similarly, Monaghan's documentation of the U.K. animal rights movement's supply-chain targeting innovation, in which not only laboratories but also companies in the supply chain were pressured through intimidation, property damage, and social campaigns, provides a directly transferable operational model.[125] That campaign sought to make the business ecosystem around animal research untenable. The same model could be applied to cloud service providers, cooling system contractors, power utilities, and construction firms involved in data center buildout.

A final infrastructure category deserves attention: facilities targeted not because they are the site of the grievance but because they are nodes in a supply chain that enables harm committed elsewhere, what might be called complicity-based infrastructure targeting. The operational logic is distinct from direct targeting: The actor attacks the infrastructure because it enables the harm they oppose. The Squamish Five's 1982 bombing of a Litton Industries plant in Canada, which manufactured cruise missile guidance components,[126] illustrates this dynamic well: The target was selected not for what it produced locally but for its role in a weapons system the attackers opposed on existential grounds.[127] More recently, Palestine Action, a British direct action network proscribed as a terrorist organization in July 2025, applied the same logic systematically to the U.K. arms supply chain, targeting Elbit Systems factories and RAF Brize Norton aircraft on the grounds that British military infrastructure was complicit in Israeli operations in Gaza; the June 2025 break-in at Brize Norton, in which activists spray-painted two military aircraft, caused an estimated £7 million in damage.[128] The AI transfer is direct: Where the infrastructure of defense-sector AI contractors is understood as complicit in AI-enabled warfare, the facilities of those contractors, cloud providers servicing military AI, and data centers housing dual-use models could all become targets under the same complicity logic.

The Insider Threat

The target discussion above focuses primarily on external actors approaching AI-adjacent persons and infrastructure. But the insider threat deserves separate treatment. Insiders bypass the very security postures that drive the substitution effect described earlier: They already possess physical access, knowledge of facility layouts, familiarity with operational routines, and in some cases the technical capability to cause disruption disproportionate to what an external actor could achieve. Both of the pathways discussed below fall squarely outside existing counterterrorism monitoring frameworks, one because it is classified as a labor or workplace violence issue, the other because no empirical case has yet occurred.

The first pathway is that of the aggrieved worker, whose grievance may be rooted in economic displacement, in the loss of self-worth and occupational identity that accompanies the devaluation of human expertise by machine replacement, or in some combination of the two. Warehouses, distribution centers, and logistics hubs operated by or for AI-dependent companies are among the sectors facing the highest automation exposure in the contemporary economy, and the employment relationship itself provides physical access and insider knowledge of facility layout and vulnerability that would otherwise be unavailable to an external adversary. Grievance-driven workplace violence is not new. The Bureau of Justice Statistics and NIOSH report an annual average of 1.3 million nonfatal workplace violent victimizations between 2015 and 2019, and 17,865 workplace homicides between 1992 and 2019, with episodes of arson, sabotage, and targeted violence by disgruntled or former employees recurring across the historical record.[129]

Much as the killing of Brian Thompson brought the assassination of a corporate executive into the foreground of public consciousness, the April 2026 arson at a Kimberly-Clark distribution facility in Ontario, California, may mark an analogous moment for the AI-adjacent, automation-exposed workforce.[130] Federal prosecutors allege that Chamel Abdulkarim, a warehouse worker employed by NFI Industries, set fire to the 1.2-million-square-foot facility while filming himself and narrating a wage grievance to his Instagram followers; in a separate phone call recorded by an associate shortly before his arrest, he compared his action to the Thompson killing, stating that "a lot of people are going to understand," and texted a co-worker that "1% is a fucking joke" and "all you had to do was pay us enough to live."[131] The

fire escalated to six alarms and required 175 firefighters from 14 agencies to bring under control, causing an estimated $500 million in damage.[132] While Abdulkarim did not invoke AI, and the case is not an AI case in the strict sense, it shares a structural template with what this article anticipates: a worker in an automation-exposed sector, acting on a locally attributable grievance against a locally accessible target, entirely outside counterterrorism monitoring. U.S. Attorney Bill Essayli characterized the motive as "hostility to capitalism and corporations"[133] and warned of "a concerning trend … particularly with younger people who are being radicalized."[134] The analytically relevant variable is the ideological layer. A worker who frames the same material or status grievance in terms of AI-driven dispossession rather than simple wage suppression, and who has been exposed to online communities where that framing is actively developed, is precisely the insider threat this framework anticipates.

The second pathway is that of the disenchanted AI researcher or developer. Over the past several years, several senior figures at frontier AI laboratories and companies have resigned citing safety[135] or existential concerns.[136] There is no documented case of a disenchanted AI researcher or developer committing or planning political violence, and this pathway therefore remains prospective rather than reactive. The structural profile of the disenchanted AI insider bears a closer resemblance to that of the national-security leaker, the Snowden or Manning figure acting on moral injury after losing faith in institutional channels. In this scenario, the insider's grievance is rooted in moral injury: the belief that they helped build something catastrophically dangerous and that institutional channels have failed to respond adequately. The grievance is prospective rather than reactive, oriented toward preventing a civilizational-scale harm the actor believes is coming rather than avenging a harm already suffered, and it generates a functional target logic directed at what might actually stop or meaningfully delay development.

Why the AI-safety case might produce violent rather than leak-based action, where Snowden and Manning produced disclosure rather than sabotage, is the analytically relevant question. Two features distinguish the AI-safety case. First, leakage as a response presumes that public knowledge of the risk will trigger institutional correction; the disenchanted AI insider's premise is precisely that institutional correction is no longer possible in the available time. Second, the harm in the Snowden-Manning cases was ongoing and legible; the harm the disenchanted AI insider claims to anticipate is prospective and, in the actor's own framing, irreversible. Both features shift the functional response away from disclosure and toward direct disruption.

A related variant of this pathway involves government and military insiders, and military contractors who develop moral injury not around AI's development but around its operational deployment, particularly in autonomous or semi-autonomous targeting context. The WikiLeaks precedent is instructive: The release of the 'Collateral Murder' video, which showed the killing of Iraqi civilians, including two unarmed Reuters journalists, during an operation in which human operators misread the equipment the individuals were carrying,[137] originated in precisely this kind of moral injury. That disclosure did not itself constitute violence, but it illustrates how moral injury can function as a catalyst for extralegal actions by insiders. As AI systems take on greater roles in targeting decisions, the pool of potential military and government insiders who may experience analogous moral injury, and whose action may either include committing violence themselves or like in this example, disclosing information which in turn might motivate third-party violence, is likely to grow. Their responses may include committing violence themselves, or as in this example, disclosing information that could in turn motivate violence by others.

"Practitioners should therefore track the grievance structure itself, including displacement framing, accountability language, and status-threat discourse, rather than the ideological container through which it is expressed."

The pathway from 'institutional channels are failing' to 'violent action is needed' could therefore emerge entirely within an individual's own reasoning, scaffolded by the same AI-safety discourse that circulates in peer-reviewed venues and elite policy forums. Like the mainstream academic social theory Kaczynski drew on (e.g., Ellul, Skinner, and Mumford),[138] AI-safety discourse names the harm, identifies the mechanism, assigns individual and corporate responsibility, and acknowledges governance failure, often in the same document and sometimes authored by the people building the systems. What differs is the reach and authority of the scaffolding. Where Kaczynski drew on relatively obscure academic texts, the contemporary equivalent appears in Senate testimony, in model cards published by frontier laboratories, and in public statements by sitting AI company CEOs. As such, the pathway from grievance to violence requires no distortion of the source material, only the additional premise, supplied by the actor alone, that institutional channels are closed and that action therefore falls to the individual.

Another structural analogy for this pathway can be found in the anti-nuclear movement. Rucht documents how technically sophisticated actors with scientific or engineering backgrounds targeted nuclear development infrastructure in the 1970s and 1980s on explicitly prospective civilizational grounds, and how closed political systems that met peaceful protest with state force, as at the 1977 protests against the Superphénix nuclear station in Creys-Malville, France, where police units killed one protester and wounded more than 100 others, radicalized initially peaceful movements toward sabotage and direct action.[139] The parallel matters because the contemporary AI researcher or developer may similarly combine moral injury, technical capability, insider access, and a sense of institutional closure, while remaining largely invisible.

Implications and Conclusions

The framework proposed in this article carries several implications for counterterrorism practitioners and policymakers. These are offered not as predictions, but as analytical orientations, ways of understanding a threat landscape that existing frameworks are not currently configured to recognize.

The first and most fundamental implication is that the

threat is distributed rather than centralized. The actors most likely to emerge from the grievance landscape described above will, for the most part, not belong to named organizations, travel to conflict zones, or consume content flagged by existing monitoring systems. They may instead be workers acting on locally attributable economic grievances, family members of those harmed by AI systems, researchers with institutional access and a crisis of conscience, or residents of communities bearing the ecological costs of AI infrastructure they did not consent to host. Conventional radicalization indicators, including organizational affiliation, extremist propaganda consumption, and foreign travel, are therefore unlikely to appear.

Second, the grievance must be monitored across ideological boundaries. The same AI-generated conditions, economic displacement, governance failure, ecological burden, and algorithmic harm may generate mobilizing effects across far-right, far-left, environmental, and religiously motivated milieus. No single-ideology monitoring framework is likely to capture that convergence. Practitioners should therefore track the grievance structure itself, including displacement framing, accountability language, and status-threat discourse, rather than the ideological container through which it is expressed.

Third, law enforcement and intelligence agencies must recognize that their own deployment of AI may contribute to the grievance landscape they are trying to monitor. Predictive policing, facial recognition, algorithmic risk assessment, and AI-augmented surveillance do not merely raise civil liberties concerns; they may also intensify the domestic surveillance grievance this article identifies as a cross-ideological threat. In that sense, decisions about whether and how to deploy AI operationally are not merely questions of civil liberties or governance; they also carry security consequences of their own, insofar as each deployment may expand the pool of grievances from which future anti-state actors could emerge.

Fourth, the accountability gap is not merely a legal or ethical problem; it is a counterterrorism variable. Across each of the grievance domains developed above, the absence of an attributable human agent responsible for AI-mediated harm shifts the search for attribution onto the visible persons, institutions, and physical infrastructure through which AI systems are instantiated. Measures that close or narrow the accountability gap, meaningful human oversight of consequential AI decisions, legally enforceable auditability requirements, identifiable lines of responsibility within corporate and governmental deployments, and accessible channels for redress, are therefore not only governance measures. They are also counterterrorism measures, in the specific sense that they may reduce the population of grievances for which only extra-institutional targets remain available. The governance of AI accountability is, in this framing, among the most under-appreciated points of leverage in the counterterrorism response the threat landscape described here will require.

Finally, the strategies governments and technology companies deploy in direct response to anti-AI mobilization may themselves accelerate the trajectories they are designed to contain. Rucht's comparative analysis of anti-nuclear movements shows that counter-strategies were at least as important as opportunity structures in shaping movement trajectories: Governments that engaged opposition early, through dialogue and regulatory concession, avoided the worst escalation, whereas those that dismissed or repressed it generated more radical outcomes.[140] This framework should therefore not be read as a warrant for securitizing legitimate opposition to AI. Resistance to AI-driven economic displacement, criticism of algorithmic governance, concern about data center construction, and advocacy for stronger AI safety measures are legitimate political positions held by a large share of the population. If governments or technology companies invoke the threat of anti-AI violence to cast broad opposition as extremism, or to justify expanded surveillance of AI safety communities, labor organizers, or environmental activists, the likely result will be not security but further radicalization. The framework's own logic predicts this: The perception that legitimate channels are closed is the single most consistent precondition for the escalation from grievance to violence. The window for substantive engagement is now, before movement trajectories harden.

Many of the grievances identified in this framework have concrete foundations. Workers are being displaced. Communities are bearing ecological costs they did not consent to. Children have died. Counter-messaging strategies that deny the grievance or characterize opposition to AI as presumptively extremist are unlikely to succeed and may instead function as radicalization accelerants by confirming the perception that legitimate channels are closed. The historiographical record of prior technological transitions suggests, though it does not prove, that where regulatory and welfare responses were eventually introduced, the violence associated with mechanization receded.[141] If that insight holds, the most effective counterterrorism response to the threat landscape described here may lie not in expanded surveillance or enhanced prosecution, but in credible and enforceable governance of the technology generating the grievance. That is a policy conclusion as much as a security one, and it is the central implication of moving beyond the misuse frame.

This article has argued that the terrorism studies literature on artificial intelligence, organized as it has been around the three questions of current misuse, projected misuse, and counterterrorism application, has captured only one dimension of AI's relationship with political violence. The dimension it has missed, what AI is doing to the economic, institutional, and relational conditions that historically precede the onset of political violence, is at least as consequential for the threat landscape of the coming decade, and very likely more so. The framework developed here is offered as an opening move in that analytical direction rather than a final account. It identifies three grievance domains, a cross-cutting accountability-gap mechanism, a tempo problem that compresses institutional adaptation, and a distributed set of target categories and actor types that fall outside the monitoring frameworks currently in use. It does not predict when, where, or whether violence emerging from these conditions will materialize at scale. What the framework does claim is that the analytical categories existing counterterrorism scholarship has not yet developed will be needed before rather than after the events they describe, and that the cases with which this article opened, whatever their ultimate judicial disposition, are consistent with the pattern the framework anticipates. CTC

Citations

1 *United States of America v. Daniel Moreno-Gama*, United States District Court for the Northern District of California, April 13, 2026.
2 Ibid.; Kalley Huang and Natallie Rocha, "Man Held in Attack on OpenAI Chief's Home Had List of A.I. Leaders, Officials Say," *New York Times*, April 13, 2026.
3 "Indianapolis Councilman Says Shots Fired at Home and 'No Data Centers' Note Left at Door," PBS News, April 7, 2026.
4 Mauro Lubrano, *Stop the Machines: The Rise of Anti-Technology Extremism* (Cambridge, U.K.: Polity Press, 2025).
5 Ibid.
6 "Introducing ChatGPT," OpenAI, November 30, 2022.
7 "Early Terrorist Experimentation with Generative Artificial Intelligence Services," Tech Against Terrorism, 2023.
8 Meili Criezis, "AI Caliphate: The Creation of Pro-Islamic State Propaganda Using Generative AI," Global Network on Extremism and Technology, February 5, 2024.
9 Federico Borgonovo et al., "Weapons of Mass Hate Dissemination: The Use of Artificial Intelligence by Right-Wing Extremists," Global Network on Extremism and Technology, February 23, 2024.
10 Ibid.
11 Anna Hiller and Pablo Maristany de las Casas, *Generative AI and the German Far Right: Narratives, Tactics and Digital Strategies* (London: Institute for Strategic Dialogue, 2025); David Wells, "Mapping Terrorist AI Use: Identifying Factors Behind a Relatively Slow Adoption Rate," Global Network on Extremism and Technology, September 17, 2025; Yannick Veilleux-Lepage, "Neue Technologien im Rechtsextremismus," bpb.de, Bundeszentrale für politische Bildung, April 8, 2026.
12 Ben Quinn, "Meet 'Amelia': The AI-Generated British Schoolgirl Who Is a Far-Right Social Media Star," *Guardian*, January 25, 2026; Emily Schultheis, "How Germany's Far Right Is Harnessing AI to Win Votes," Politico, February 20, 2025.
13 Gabriel Weimann et al., "Generating Terror: The Risks of Generative AI Exploitation," *CTC Sentinel* 17:1 (2024).
14 Josh A. Goldstein et al., "How Persuasive Is AI-Generated Propaganda?" *PNAS Nexus* 3:2 (2024): pp. 1-7.
15 Luke Baumgartner, "AI at the Centre: Violent Extremist Exploitation in Pirkkala," Global Network on Extremism and Technology, July 14, 2025; Kye Allen, "Could Chatbots Seduce Us into Extremism? Radicalisation Risks in an Age of AI Companions," Global Network on Extremism and Technology, December 5, 2025; Anda Solea, "Prompted to Harm: Analysing the Pirkkala School Stabbing and Its Digital Manifesto," Global Network on Extremism and Technology, June 12, 2025; *Practice Guide on Artificial Intelligence and Preventing and Countering Violent Extremism* (New York: United Nations Office of Counter-Terrorism, 2026).
16 Solea.
17 Annie Palmer, "FBI Says Palm Springs Bombing Suspects Used AI Chat Program," CNBC, June 4, 2025.
18 Emma Tucker, "Green Beret Who Exploded Cybertruck in Las Vegas Used AI to Plan Blast," CNN, January 7, 2025.
19 "Palestinian Terrorist Planned Attack with ChatGPT in Israel," *Jerusalem Post*, May 22, 2025.
20 Tom Winter and Jonathan Dienst, "Helped by AI, Man Built Bombs He Planned to Detonate in Manhattan, Officials Say," NBC News, July 23, 2025.
21 "Killer Apps: How Mainstream AI Chatbots Assist Users Planning Violent Attacks," Center for Countering Digital Hate, 2026.
22 Miles Brundage et al., "The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation," arXiv:1802.07228 (arXiv, 2018).
23 Ardi Janjeva et al., "Evaluating Malicious Generative AI Capabilities," CETaS Briefing Papers, July 2024; Manuel Torres Soriano, *The Transformative Impact of Artificial Intelligence on Terrorism: Horizon 2035*, IEEE Framework document (Madrid: Instituto Espanol de Estudios Estratégicos, 2026).
24 *Facing Reality?: Law Enforcement and the Challenge of Deepfakes, An Observatory Report from the Europol Innovation Lab* (The Hague: European Union Agency for Law Enforcement Cooperation, 2024); *The Evolution of Disinformation - A Deepfake Future*, nos. PS74-19/2023E-PDF (Ottawa: Canadian Security Intelligence Services, 2023); Ella Busch and Jacob Ware, *The Weaponization of Deepfakes: Digital Deception on the Far-Right* (The Hague: International Centre for Counter-Terrorism - ICCT, 2023); Sam Stockwell et al., "Adding Fuel to the Fire: AI Information Threats and Crisis Events," CETaS Research Reports (2026).
25 Soriano; Clarisa Neli, "Exploitation of Generative AI by Terrorist Groups," International Centre for Counter-Terrorism - ICCT, June 10, 2024; Alexander Blanchard and Jonathan Hall, "Terrorism and Autonomous Weapon Systems: Future Threat or Science Fiction?" CETaS Expert Analysis, June 19, 2023.
26 Sarah Lohmann, "National Security Impacts of Artificial Intelligence and Large Language Models" in C. Anthony Pfaff ed., *The Weaponization of AI: The Next Stage of Terrorism and Warfare* (Ankara: Centre of Excellence Defence Against Terrorism (COE-DAT), 2025).
27 Jonas B. Sandbrink, "Artificial Intelligence and Biological Misuse: Differentiating Risks of Language Models and Biological Design Tools," arXiv:2306.13952, preprint, arXiv, December 23, 2023.
28 Kyle Chan et al., "AI Risks from Non-State Actors," Brookings, 2026.
29 Janjeva et al.; Soriano.
30 Don Rassler, "Commentary: Data, AI, and the Future of U.S. Counterterrorism: Building an Action Plan," *CTC Sentinel* 14:8 (2021): pp. 31-44.
31 A*lgorithms and Terrorism: The Malicious Use of Artificial Intelligence for Terrorist Purposes* (New York: United Nations Interregional Crime and Justice Research Institute (UNICRI) and United Nations Counter-Terrorism Centre (UNCCT), 2021).
32 C. Anthony Pfaff ed., *The Weaponization of AI: The Next Stage of Terrorism and Warfare* (Ankara: Centre of Excellence Defence Against Terrorism (COE-DAT), 2025).
33 Kathleen McKendrick, *Artificial Intelligence Prediction and Counterterrorism* (London: Chatham House, 2019).
34 "2025 Annual Member Forum," Global Internet Forum to Counter Terrorism, November 21, 2025; Erin Saltman and Skip Gilmour, *Artificial Intelligence: Threats, Opportunities, and Policy Frameworks for Countering VNSAs* (Global Internet Forum to Counter Terrorism and Konrad-Adenauer-Stiftung, 2025).
35 Rassler, "Commentary;" Irja Malmio, "Ethics as an Enabler and a Constraint – Narratives on Technology Development and Artificial Intelligence in Military Affairs through the Case of Project Maven," *Technology in Society* 72 (2023); Simon Hogue, "Project Maven, Big Data, and Ubiquitous Knowledge: The Impossible Promises and Hidden Politics of Algorithmic Security Vision" in Aleš Završnik and Vasja Badalič eds., *Automating Crime Prevention, Surveillance, and Military Operations* (New York: Springer International Publishing, 2021).
36 Don Rassler, "A View from the CT Foxhole: Adam Hadley, Executive Director, Tech Against Terrorism," *CTC Sentinel* 18:7 (2025): pp. 9-15.
37 Nicholas Clark, "Commentary: The Dangers of Overreliance on Generative AI in the CT Fight," *CTC Sentinel* 18:8 (2025): pp. 15-19.
38 Christopher Wall, "The Robots Will Not Save Us: The Limits of Machine Learning for Counterterrorism," Global Network on Extremism and Technology, November 4, 2021.
39 Andrea Bianchi and Anna Greipl, "States' Prevention of Terrorism and the Rule of Law: Challenging the 'Magic' of Artificial Intelligence (AI)," International Centre for Counter-Terrorism - ICCT, November 17, 2022, accessed April 15, 2026.
40 Jeffrey W. Lewis, "Precision Terror: Suicide Bombing as Control Technology," *Terrorism and Political Violence* 19:2 (2007): pp. 223-245; Michael C. Horowitz, "Nonstate Actors and the Diffusion of Innovations: The Case of Suicide Terrorism," *International Organization* 64:1 (2010): pp. 33-64.
41 Mike Davis, *Buda's Wagon: A Brief History of the Car Bomb* (New York: Verso, 2007).
42 Yannick Veilleux-Lepage, *How Terror Evolves: The Emergence and Spread of Terrorist Techniques* (Lanham, MD: Rowman & Littlefield Publishers, 2020).
43 Yannick Veilleux-Lepage, "Printing Terror: An Empirical Overview of the Use of 3D-Printed Firearms by Right-Wing Extremists," *CTC Sentinel* 17:6 (2024): pp. 31-45.
44 Don Rassler, *Remotely Piloted Innovation: Terrorism, Drones and Supportive Technology* (West Point, NY: Combating Terrorism Center, 2016); Don Rassler and Yannick Veilleux-Lepage, "On the Horizon: The Ukraine War and the Evolving Threat of Drone Terrorism," *CTC Sentinel* 18:3 (2025).
45 Kenneth J. Wickiser et al., "Engineered Pathogens and Unnatural Biological Weapons: The Future Threat of Synthetic Biology," *CTC Sentinel* 13:8 (2020): pp. 1-7; Audrey Kurth Cronin, "Biology's Tectonic Shifts and Novel Risks," *CTC Sentinel* 15:5 (2022): p. 20-26.
46 Isabelle Duyvesteyn, "The Role of History and Continuity in Terrorism Research" in Magnus Ranstorp ed., *Mapping Terrorism Research: State of the Art, Gaps and Future Direction* (Milton Park, UK: Taylor & Francis Group, 2006).
47 Randall D. Law, *Terrorism: A History* (Cambridge, U.K.: Polity, 2024); Walter Laqueur, *The New Terrorism: Fanaticism and the Arms of Mass Destruction* (Oxford: Oxford University Press, 2000).

48 Duyvesteyn.
49 Nestor Maslej et al., *Artificial Intelligence Index Report 2025*, arXiv:2504.07139 (Stanford: Stanford University Human-Centered Artificial Intelligence, 2025).
50 *The State of AI in 2025: Agents, Innovation, and Transformation* (New York: McKinsey, 2025).
51 Olivia Sidoti and Colleen McClain, "ChatGPT Use among Americans Roughly Doubled since 2023," Pew Research Center, June 25, 2025.
52 Michelle Faverio and Emma Kikuchi, "What the Data Says about Americans' Views of Artificial Intelligence," Pew Research Center, March 12, 2026.
53 *Future of Jobs Report 2025* (Geneva: World Economic Forum, 2025).
54 Joseph Gedeon, "OpenAI CEO Tells Federal Reserve Confab That Entire Job Categories Will Disappear Due to AI," *Guardian*, July 22, 2025.
55 Jim VandeHei and Mike Allen, "Behind the Curtain: A White-Collar Bloodbath," Axios, May 28, 2025.
56 Krystal Hu, "ChatGPT Sets Record for Fastest-Growing User Base - Analyst Note," Reuters, February 2, 2023.
57 Lubrano.
58 Fathali M. Moghaddam, "The Staircase to Terrorism: A Psychological Exploration," *American Psychologist* (US) 60:2 (2005): pp. 161-169.
59 Clark McCauley and Sophia Moskalenko, *Friction: How Conflict Radicalizes Them and Us, Revised and Expanded Edition* (Oxford: Oxford University Press, 2017).
60 Daron Acemoglu and Pascual Restrepo, "Robots and Jobs: Evidence from US Labor Markets," *Journal of Political Economy* 128 (2020): pp. 2,188-2,244; David H. Autor et al., "The China Syndrome: Local Labor Market Effects of Import Competition in the United States," *American Economic Review* 103:6 (2013): pp. 2,121-2,168; Maarten Goos and Alan Manning, "Lousy and Lovely Jobs: The Rising Polarization of Work in Britain," *Review of Economics and Statistics* 89:1 (2007): pp. 118-133.
61 Brian Merchant, *Blood in the Machine: The Origins of the Rebellion against Big Tech* (Boston: Little, Brown and Company, 2023).
62 Eric Hobsbawm and George Rude, *Captain Swing* (New York: Verso, 2014); Adrian Randall, *Riotous Assemblies: Popular Protest in Hanoverian England* (Oxford: Oxford University Press, 2006).
63 Merchant, *Blood in the Machine*.
64 Lubrano.
65 Noam Gidron and Peter A. Hall, "The Politics of Social Status: Economic and Cultural Roots of the Populist Right," *British Journal of Sociology* 68:S1 (2017).
66 Brian Merchant, "Why the AI Backlash Has Turned Violent," Blood in the Machine, November 28, 2025.
67 Yanis Varoufakis, *Technofeudalism: What Killed Capitalism* (Brooklyn: Melville House, 2024).
68 Matt Lawson, "The New Feudalism How AI Is Reshaping Power, Labor, and the Case for Building Something Different," Plant the Village, February 2026.
69 Ibid.
70 Lubrano.
71 Noman Bashir et al., "The Climate and Sustainability Implications of Generative AI," An MIT Exploration of Generative AI, March 27, 2024; Adam Zewe, "Explained: Generative AI's Environmental Impact," MIT News, January 17, 2025.
72 *Electricity 2024: Analysis and Forecast to 2026* (Paris: International Energy Agency, 2024); "AI Has an Environmental Problem. Here's What the World Can Do about That," UN Environment Programme, November 13, 2025.
73 Pengfei Li et al., "Making AI Less 'Thirsty': Uncovering and Addressing the Secret Water Footprint of AI Models," arXiv:2304.03271, preprint, arXiv, March 26, 2025; "AI Has an Environmental Problem."
74 Stefan H. Leader and Peter Probst, "The Earth Liberation Front and Environmental Terrorism," *Terrorism and Political Violence* 15:4 (2003): pp. 37-58.
75 Esmat Zaidan and Imad Antoine Ibrahim, "AI Governance in a Complex and Rapidly Changing Regulatory Landscape: A Global Perspective," *Humanities and Social Sciences Communications* 11:1 (2024): pp. 1-18; Filippo Lancieri et al., "AI Regulation: Competition, Arbitrage & Regulatory Capture," *SSRN Scholarly Paper* no. 5049259, December 9, 2024.
76 Merchant, "Why the AI Backlash Has Turned Violent;" Brian Merchant, "Behind Silicon Valley and the GOP's Campaign to Ban State AI Laws," Blood in the Machine, November 28, 2025; Armrith Ramkumar, "Silicon Valley Launches Pro-AI PACs to Defend Industry in Midterm Elections," *Wall Street Journal*, August 25, 2025.
77 Merchant, "Why the AI Backlash Has Turned Violent."
78 Yuval Abraham, "'Lavender': The AI Machine Directing Israel's Bombing Spree in Gaza," +972 Magazine, April 3, 2024.
79 Clare Garvie et al., "The Perpetual Line-Up," Georgetown Law Center on Privacy and Technology, 2016; Joy Buolamwini and Timnit Gebru, "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification," Proceedings of the 1st Conference on Fairness, Accountability and Transparency, January 21, 2018, pp. 77-91; Brendan F. Klare et al., "Face Recognition Performance: Role of Demographic Information," *IEEE Transactions on Information Forensics and Security* 7:6 (2012): pp. 1,789-1,801; Julia Angwin et al., "Machine Bias," ProPublica, May 23, 2016; Rashida Richardson et al., "Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice," *NYUL Rev. Online* 94 (2019): pp. 15-55.
80 McKendrick; Rassler, "Commentary."
81 Joseph Cox, "'ELITE': The Palantir App ICE Uses to Find Neighborhoods to Raid," 404 Media, January 15, 2026; Jude Joffe-Block, "Immigration Agents Have New Technology to Identify and Track People," NPR, November 8, 2025; Joseph Cox, "ICE to Buy Tool That Tracks Locations of Hundreds of Millions of Phones Every Day," 404 Media, September 30, 2025; "American Dragnet: Data-Driven Deportation in the 21st Century," Georgetown Law Center on Privacy and Technology, May 2025; Josie Stewart et al., "How Tech Powers Immigration Enforcement," Brookings, October 6, 2025; Kat Lonsdorf et al., "ICE Has Spun a Massive Surveillance Web. We Talked to People Caught in It," NPR, March 5, 2026.
82 Cecilia Polizzi, "The Feed That Shapes Us: Extremism and Adolescence in the Age of Algorithms," Global Network on Extremism and Technology, December 12, 2025.
83 McCauley and Moskalenko, pp. 75-88.
84 "Our Epidemic of Loneliness and Isolation: The U.S. Surgeon General's Advisory on the Healing Effects of Social Connection and Community," U.S. Office of the Surgeon General, 2023.
85 Jared Moore et al., "Expressing Stigma and Inappropriate Responses Prevents LLMs from Safely Replacing Mental Health Providers," Proceedings of the 2025 ACM Conference on Fairness, Accountability, and Transparency, June 23, 2025, pp. 599-627; Per Carlbring and Gerhard Andersson, "Commentary: AI Psychosis Is Not a New Threat: Lessons from Media-Induced Delusions," *Internet Interventions* 42 (2025).
86 Jennifer Valentino-DeVries and Kashmir Hill, "How Bad Are A.I. Delusions? We Asked People Treating Them," *New York Times*, January 26, 2026.
87 Ibid.
88 Blake Montgomery, "Mother Says AI Chatbot Led Her Son to Kill Himself in Lawsuit against Its Maker," *Guardian*, October 23, 2024.
89 Madeleine Clare Elish, "Moral Crumple Zones: Cautionary Tales in Human-Robot Interaction," *Engaging Science, Technology, and Society* 5 (2019): pp. 40-60.
90 Jack Katz, *Seductions of Crime: Moral And Sensual Attractions In Doing Evil* (New York: Basic Books, 1988); Albert Bandura, "Moral Disengagement in the Perpetration of Inhumanities," *Personality and Social Psychology Review* 3:3 (1999): pp. 193-209; Martin Daly and Margo Wilson, "Evolutionary Social Psychology and Family Homicide," *Science* 242:4,878 (1988): pp. 519-524; Mia Bloom, *Dying to Kill: The Allure of Suicide Terror* (New York: Columbia University Press, 2005).
91 "White Supremacists and the Weaponization of the Coronavirus (COVID-19)," Soufan Center, March 25, 2020; Eoin Flaherty et al., "The Conspiracy of Covid-19 and 5G: Spatial Analysis Fallacies in the Age of Data Democratization," *Social Science & Medicine* 293 (2022).
92 Walter Enders and Todd Sandler, "The Effectiveness of Antiterrorism Policies: A Vector-Autoregression- Intervention Analysis," *American Political Science Review* 87:4 (1993): pp. 829-844.
93 Lubrano.
94 As quoted in Lubrano, p. 55.
95 Victoria Bekiempis, "Manhattan Judge Delays Luigi Mangione State and Federal Trials," *Guardian*, April 1, 2026.
96 Luigi's Manifesto, Manifesto, December 2024.
97 "December 2024 National Poll: Young Voters Diverge from Majority on Crypto, TikTok, and CEO Assassination," Emerson Polling, December 17, 2024.
98 Rhianna Schmunk, "3 Reasons behind the Unsettling Glorification of Luigi Mangione," CBC News, December 15, 2024; Emma Cieslik, "'Saint Luigi, Patron Saint of Healthcare Access for All' — Enraged by Corporate Health Care Some View Assassin as a Folk Hero," Religion Dispatches, January 7, 2025.
99 Zeynep Tufekci, "Opinion: The Rage and Glee That Followed a C.E.O.'s Killing Should Ring All Alarms," *New York Times*, December 6, 2024.
100 As quoted in Jessica Glenza, "Brian Thompson's Killing Sparks Outrage over State of US Healthcare," *Guardian*, December 5, 2024.
101 Kirsten Grind and Jack Ewing, "Inside Elon Musk's Mushrooming Security

Apparatus," *New York Times*, September 13, 2024.
102 *United States of America v. Daniel Moreno-Gama*.
103 "SFPD Arrests Suspects Involved in Shooting #26-044," San Francisco Police Department, April 12, 2026; N'dea Yancey-Bragg, "Attack near Sam Altman's House Prompts 2 More Arrests," *USA Today*, April 13, 2026.
104 As quoted in Kyle Chayka, "A.I. Has a Message Problem of Its Own Making," *New Yorker*, April 15, 2026.
105 Rachel Monaghan and João Raphael Da Silva, "Militant Animal Rights Activity: Terrorism, Extremism or Something Else?" *Studies in Conflict & Terrorism* 49:1 (2026): pp. 82-97; Rachel Monaghan, "Terrorism in the Name of Animal Rights," *Terrorism and Political Violence* 11:4 (1999): pp. 159-169; Rachel Monaghan, "Not Quite Terrorism: Animal Rights Extremism in the United Kingdom," *Studies in Conflict & Terrorism* 36:11 (2013): pp. 933-951; Keith Tester and John Walls, "The Ideology and Current Activities of the Animal Liberation Front," *Contemporary Politics* 2:2 (1996): pp. 79-91.
106 G. O'Boyle, "Theories of Justification and Political Violence: Examples from Four Groups," *Terrorism and Political Violence* 14:2 (2002): pp. 23-46.
107 Robert Booth and Angelique Chrisafis, "Copenhagen Shootings: How the Attacks Unfolded," *Guardian*, February 15, 2015; Ed Pilkington, "Rushdie Stabbing Was 'an Attack on Who We Are', Says Venue's President," *Guardian*, August 14, 2022; Hannah Ellis-Petersen, "Death Threats Sent to Participants of US Conference on Hindu Nationalism," *Guardian*, September 9, 2021; Yannick Veilleux-Lepage, "When the Radical Right Shows Up," Fair Observer, October 11, 2018; Ansel Bayly, "Two Arrested, Student Injured in Police Altercation at Pro-Palestine Rally," Roar News, June 7, 2025.
108 "Indianapolis Councilman Says Shots Fired at Home and 'No Data Centers' Note Left at Door."
109 Jesse Humpal, "From Earth Liberation to Accelerationism: A High-Level Review of Fifty Years of Domestic Infrastructure Terrorism," *CTC Sentinel* 19:3 (2026): pp. 26-34.
110 Ibid.
111 Lubrano.
112 As quoted in Molly Taft, "The Data Center Resistance Has Arrived," *Wired*, November 14, 2025.
113 "As Data Centers Proliferate, Anti-AI Resistance Has the Potential to Turn Violent," Soufan Center, November 5, 2025.
114 Jordyn Abrams, "Data Centers Now the Target of Anti-Tech Extremists Globally," The Threat, Substack newsletter, April 9, 2026.
115 Michael Flood, "Nuclear Sabotage," *Bulletin of the Atomic Scientists* 32:8 (1976): pp. 29-36.
116 "Greenpeace Crashes Superman-Shaped Drone into French Nuclear Plant," Reuters, July 3, 2018; Yannick Veilleux-Lepage and Emil Archambault, *A Comparative Study of Non- State Violent Drone Use in the Middle East* (The Hague: International Centre for Counter-Terrorism, 2022).
117 "Greenpeace Crashes Superman-Shaped Drone into French Nuclear Plant."
118 Flood.
119 Rebecca Smith, "Assault on California Power Station Raises Alarm on Potential for Terrorism," *Wall Street Journal*, February 5, 2014.
120 Humpal.
121 Ibid.
122 Colin Clarke et al., "The Targeting of Infrastructure by America's Violent Far-Right," *CTC Sentinel* 16:5 (2023): pp. 26-34.
123 Rebecca Leppert, "US Data Centers' Energy Use amid the Artificial Intelligence Boom," Pew Research Center, October 24, 2025; "As Data Centers Proliferate, Anti-AI Resistance Has the Potential to Turn Violent."
124 Leader and Probst.
125 Monaghan, "Not Quite Terrorism."
126 Stéphane Leman-Langlois and Jean-Paul Brodeur, "Terrorism Old and New: Counterterrorism in Canada," *Police Practice and Research* 6:2 (2005): pp. 121-140.
127 Ann Hansen, *Direct Action: Memoirs of an Urban Guerrilla* (Toronto: Between the Lines, 2001).
128 Reuters, "UK Charges 4 Anti-Israel Activists over Air Base Break-In," *Times of Israel*, July 3, 2025; Haroon Siddique, "Palestine Action Activists Wanted to Smash up Elbit Systems' Property, Court Told," *Guardian*, April 15, 2026.
129 Erika Harrell et al., *Indicators of Workplace Violence, 2019* (Washington, D.C.: National Institute for Occupational Safety and Health, 2022).
130 Daniella Silva, "Arson Suspect in California Warehouse Fire Allegedly Compared Himself to Luigi Mangione," NBC News, April 10, 2026.
131 *United States v. Chamel Abdulkarim*, Criminal Complaint and Affidavit, United States District Court for the Central District of California, 2026, pp. 4, 13.
132 Ibid.
133 As quoted in Silva, "Arson Suspect in California Warehouse Fire Allegedly Compared Himself to Luigi Mangione."
134 As quoted in Ben Chapman, "'Arsonist' in Smirky Court Date," *California Post*, April 14, 2026.
135 Cade Metz, "OpenAI's Chief Scientist and Co-Founder Is Leaving the Company," *New York Times*, May 14, 2024; Dan Milmo, "OpenAI Putting 'Shiny Products' above Safety, Says Departing Researcher," *Guardian*, May 18, 2024; "How We Prevent the AI's from Killing Us with Paul Christiano," Bankless via YouTube, 2023, at 01:57:02.
136 Sara Brown, "Why Neural Net Pioneer Geoffrey Hinton Is Sounding the Alarm on AI," MIT Management Sloan School, May 23, 2023.
137 David Gilson, "What the WikiLeaks Media Blitz Has Revealed About WikiLeaks," Mother Jones, April 13, 2010.
138 Lubrano; Sean Fleming, "The Unabomber and the Origins of Anti-Tech Radicalism," *Journal of Political Ideologies* 27:2 (2022): pp. 207-225.
139 Dieter Rucht, "Campaigns, Skirmishes and Battles: Anti-Nuclear Movements in the USA, France and West Germany," *Industrial Crisis Quarterly* 4:3 (1990): pp. 193-222.
140 Ibid.
141 Merchant, *Blood in the Machine*; Lubrano.

A View from the CT Foxhole: Greg Hinds, Former Director of Counter Terrorism, Interpol

By Joe Decie

Greg Hinds is an Australian Federal Police (AFP) leader who served as Interpol's Director for Counter-Terrorism in Lyon (February 2021-January 2026), overseeing Interpol's global counterterrorism strategy and its three sub-directorates (Operations; Capabilities; CBRNE & Vulnerable Targets) for 196 member countries. Previously, Hinds spent three years in Liberia as Head of the UNMIL Police Component and Police Commissioner, leading 2,000 staff to build Liberia's police capacity until the United Nations handed security responsibilities back to the Government of Liberia in June 2016.

Hinds' AFP career has spanned Counter Terrorism, Crime, International, Protection, Aviation, Intelligence, and Community Policing commands, and he now works in AFP's Global Operations Command focusing on domestic security against serious organized crime and terrorism.

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

Hinds: There's a couple of things that come to mind here. One, from an operational perspective, is the salad bar of ideologies that motivate/drive/influence terrorism today. We're not dealing with the structures that we once did, and terrorism and the threat landscape have evolved. So, this has an impact on how we think about and respond to a threat environment that is guided by much more loosely connected structures—the gamification of and the desensitization of violence, even offenders becoming much younger.

Due to these changes, we too have had to evolve, and at times we probably haven't matched that pace of evolution with our ability to shift policy, to shift legislation, and to shift our operational responses because their adaptation has moved much more quickly than ours in recent times. We need to think about how we bridge policy—national security and foreign policy, counterterrorism policy—with an effective operational response. My time at Interpol, given its position as being a voice for global law enforcement, gave me unique insights into this issue. Members of Interpol have a common agenda, but each country brings its own mix of capabilities, policies, and approaches, and that can make it challenging to unify and synchronize efforts and activities. For example, of the 196 member countries who are working CT every day, how do we make sure that we're equipping them with the necessary tools, resources, and resource mobilization that they need to actually counter the threat?

Another challenge that I have observed, particularly during my time in the U.N. and also my time at Interpol, is what it takes to build capacities and capabilities, and make sure those are fit for purpose. Given the mix of capabilities of various countries, this requires an ability to adapt.

For example, a lot of our neighbor countries don't actually have mature operating [CT] models, mature resources, equipment, and those sorts of things. Some of them don't have power, some don't have computers, and yet, we see that what has been going across our online environment has been very problematic, as it serves as a means of either moving resources, recruiting, [or] sending finances. If you don't have these basic capabilities to operate and act in that type of environment, how is it that you can make their responses fit for purpose? How can these types of countries absorb or learn from what mature entities are looking to do/are doing? Because, as you know, we're only as strong as our weakest links, so I think this was a challenge.

CTC: So, when we look at the capacity, capability, and expertise challenge, which is a component of what you laid out, how do we address that from a partnership perspective—whether it's bilateral in your home country or in the U.N., the D-ISIS coalition, or Interpol?

Hinds: What we've seen is that we have to look to non-traditional partners. We have strength across our law enforcement and our national security community. Our intelligence, our military, and our law enforcement work quite well together, and our interoperability works well because this is stuff that we've rehearsed, exercised, and tested. But there are also challenges. For example, how do we make sure the right information is in the right hands so people can do their jobs? From the lens of Interpol, a core part of our role within the global law enforcement community, was focused on having a sound global security infrastructure specifically exchanging information, so we could make sure that the operationally relevant information is sitting there so we can best support member countries in preventing and responding to the threat.

When it comes to partnerships, there are also issues in relation to what capacities and capabilities exist. If we looked at R&D [Research and Development] across the globe in relation to what we do around strengthening security, strengthening our responses, looking at analyzing data, if we just tapped into that a little and we shared capability across the globe, we would find that we'd actually harmonize and uplift our ability to do this. Typically, we're doing it individually.

This comes back to trust and confidence in what we're doing. How do you make sure that we're doing this for the right purpose? It's not necessarily about disclosing our human sources or our information or our specialist capabilities, but there is capability that's cutting edge in relation to analysis, our resourcing, our databases, our training, those sorts of things. How do we make sure that we're doing a better job across this cohort of relationships in various areas to maximize what already exists and ensure this is in the right hands to make the right decisions?

When it comes to multilateralism, we need whole of society, whole of government, whole of non-government mixed together. And so, similar to what we're doing at a national level, that needs

Greg Hinds

to be amplified at the regional level. We also need to do that at the global level.

Risk dynamics are an important factor, too. We don't want to see a bomb go off and then go, 'That was a pretty good bomb.' Our risk appetite is that we want to prevent this from happening. So, how do we disrupt ahead of time? We want to be much more in that disruptive, preventive space. Being in that space means that we need to fight against complacency and make sure that we're really invested in this because we have to be on our game 365 days of the year. Terrorists just have to be lucky once, and we saw that here in Australia with the Bondi Beach attack.[1] Effective partnerships and information sharing that are fit for purpose help us to navigate that crime puzzle.

CTC: Cop to cop, agent to agent, that is a more organic piece. How do you see the current challenges on national-level assets? Whether it's ASIO (the Australian Security Intelligence Organisation) or other components, or even from an Interpol perspective, how you would see that flow of data and are there current challenges with that? What are some of the best practices that you have seen to ensure that happens?

Hinds: I think the biggest thing is, how do we leverage the capacities and capabilities of different entities? How do we benefit from the comparative advantage that we collectively bring? If I have a look from an Australian perspective, we bring states and territories together across the policing space. We also bring in our national security agency, and the whole idea is how do we make sure that there is productive convergence around a national security/terrorism threat. Has there been criminal offending involved in that? And how do we then make sure that we're not compromising each other's information, but we're actually being complementary to each other's goals at the end of the day, while also leveraging our powers, our experience, our expertise.

That's from a national sense. If we then expand that globally, how do we make sure we're replicating those sorts of practices at the end of the day? It's the information sharing which is key to this, making sure that all the information that's available is in the right hands so that the right people can make the right decisions at the right time based on their ability to do their jobs. That's what we're looking to do. And for most of us, particularly in the global security architecture, we want to make sure that's at the frontline. How do you stop threats at their source? So, if we don't want terrorists moving across borders, we don't want lots of harmful goods, equipment, money, firearms, whatever it might be that supports terrorism moving across borders, [then] how do we make sure that information is shared across and between nations. There's not too many systems that allow that. Interpol has a global system that connects to its 196 member countries, pushing those systems out to those border locations so that those key decisions can be made about people who are wanted as part of an Interpol notice; how to handle an extradition process; or blue notices around persons of interests, handling green notices focused on intelligence, or purple notices focused on *modus operandi*, so that you're actually in a better place to actually understand threat dynamics and how it might be crossing borders and how best to respond [to] and prevent it. If warranted, Interpol will also issue an orange notice to notify and highlight immediate threats, and how a nation or community might best respond.

Those mechanisms, which help to make sure that we are sharing the information at the right time and getting it to those people that that have the right and need to know, are really important. Trust and confidence in our systems is important, too, and we need to make sure it is guided by a common agenda, a common goal, and that we are working to operationalize together. A key to integration is bringing partnerships across the military, the security services and placing those together, building cohesion around those sorts of things and making sure that we are doing this systematically.

CTC: You have talked about the importance of coordination and information sharing, and different partners being in different places when it comes to their capabilities and capacities. Can you add some more color about how Interpol does that from a big headquarters?

Hinds: We all talk about [how] we're very global in our outlook and those sorts of things. But when you are the global agency, it is a very different lens looking at how you do it. So, no longer was I an Australian [in these situations]. I was there as an Interpol employee, one of the senior executives. If I look to the current Global Coalition Against Daesh's priorities as an example, they've looked at three thematic priorities: One of them was stopping terrorist travel and mobility; another was stopping their financing, their funding mechanisms and streams; and the other was around their online communications. How do we make sure they're not looking to radicalize and recruit? How do we also make sure that they're not actually looking to prepare operations and so forth? So, if you looked at those particular things, if we got those right, that's a sound approach to disruption globally in relation to that.

The challenge here is how do we mobilize resourcing so that 196 member countries benefit from that. Now, not all 196 will need investment because they're already self-invested, but there is a large part of the globe that needs investment in relation to this. So once again, how do we understand the threat environment? By understanding the threat, we can then prioritize on how best to respond. Is that through technical means? Is that through capacity-building? Is that through equipping?

One of the important things under my leadership when it came to building capacity is that we needed to make sure we operationalized it. We wanted to make sure that we weren't just doing stuff to look at things like skills uplift. We wanted to make sure that we were doing things at both the individual and the institutional level. That is because it is part of the sustainability piece. We also wanted to make sure those efforts are feeding into national systems, regional

systems, and global systems. Because it's a global problem. This helped to lead to a more informed approach that aimed to stop threats at their source.

Oftentimes, we would bring member countries together on a common endeavor because they didn't know how you actually bring those people together. Because we could see it, we were able to bring member countries together on a common cause so that the pieces—the broader pieces of the crime puzzle—could come together and they could work on this together. That was a key role of Interpol, as well as being a neutral, trusted partner given that this is a part of the organization's constitution.

But of course, one of the challenges is that the organization only deals with non-state actors. We don't get involved in anything that's racial, religious, or of a military nature, or is political. So, we just want to make sure that we're doing things that are in the best interest of our constitution and the best interest of the member countries concerned.

CTC: You mentioned a lot of critical partners, but how do you get to a common understanding, a common approach, when the counterterrorism mission set may no longer be the top priority? I imagine some of your resources over the last two and a half decades have probably gone down. You deal with a diverse mix of partners who have somewhat aligned agendas, but you also have to navigate unique national or regional circumstances, set against a diverse and dynamic terrorism threat environment. How did you thread that needle?

Hinds: For us, a grounding principle is that we saw that we were a critical voice for global law enforcement. But how do you make sure that the voice of law enforcement is being heard? Because the forum which we were in was typically not a law enforcement space. So, we wanted to break down the mystique of Interpol. It's not what you read in novels and what you see on TV. Whilst we do some really sexy stuff, we are one layer removed. For example, I didn't have arrest powers. So, therefore, it's important for us to consider how we can make sure that we're actually equipping our members as best we can to actually defeat the threat. The approach that we took there is that we want to build individuals and institutions and get information in the right hands. That was critical for us.

One recognition was that we were not looking at sustainability of the effort. It is like having an ashtray on a motorbike: If we aren't thinking about sustainability, it defeats the purpose. So, we wanted to make sure that we were looking at creating dividends and that there was a return on investment, and also that people understood what they were investing into one from a partner sense. But also from a beneficiary sense, too, you can't regionalize the globe to actually make it a secure globe.

To be sure, we have some really strong Pols around the globe, such as Europol, but not all of them are mature. For example, if you're coming into Europe, one passport check would actually check national systems, Schengen systems, Interpol systems. Therefore, our members were getting a much better dividend to help them stop threats at their source. You had information and frontline decision makers to apply the appropriate responses that were fit for purpose in relation to people or goods moving through borders, and those sorts of things. Emphasis was placed on how you replicate good practice across the globe in relation to those sorts of responses.

When it came to our capacity-building efforts, we had former employees with the subject matter expertise who understood the operating environment. So, that cooperation/collaboration piece was really strong. How do we bridge what's happening across military, security, and policing environments, and also there's a greater law enforcement community that policing is an important part of.

One of the other things that comes to mind is the polycriminality nature now of crime. Polycriminality is one of the reasons why I went to the General Assembly several years ago and said we need to have an all-of-crime approach to stop terrorism in all of its forms. It was really important for us to make sure that the cattle rustling that was happening in Africa and was actually generating funds for ISIS core is actually seen in the proper context because the upstream and downstream effects of that vary. The illegal logging, the illegal mining, all those sorts of things, if you don't understand the context of the crime, you don't actually understand the ramifications of it, which is why we said we need to think differently about the criminal environment.

We also need to actually understand the criminal environment differently because it imposes different thinking, which leads to different approaches that can enhance disruptive efforts. Understanding the context of the criminality will best shape how we respond and what tools, resources, and expertise are required. We know, for example, that the trafficking of drugs is also a fundraiser for these sorts of things, and supports the movement of people and goods. The facilitators are much more blurred these days than what they once were. I might have gone to one person for my money. I might have gone to another person because he got my firearms. These days I just go to that second person for everything because he's quite happy to move anything. That blurring of facilitation and movement has an impact on terrorism, and what supports and enables it in different contexts can be very different, and different across time. So, therefore I think we need to have this whole of crime approach, which means that we need to then think very differently about our crime and our terror environment.

CTC: How does Interpol deal with volumes of data and the exploitation and then optimization of all that data through initiatives such as Interpol's Project CT tech?

Hinds: At Interpol, we had a CT-focused crime analysis file, and it had something like 200,000 different profiles of terrorists in there. There were about 1.3 million pieces of data related to terrorism and terrorism entities. Realistically, that's probably only a small fraction of that type of data held on a global level, but that's what's been shared with Interpol to help us connect the dots. And so, one of the key elements is, how do we complement that type of data?

Most crime is transnational in nature. At Interpol, we should be someone that you're consulting with in relation to these sorts of things, because no one knows everything. And the information that one partner may need is probably out there, but it may not be clear where that data resides. So, you have to make sure that you're interrogating the proper datasets where this stuff exists; if you aren't, you won't actually get the fuller picture to help you make informed decisions. So, for us, we were trying to create a funnel and a space in which people could actually share this information and to better connect that data with investigative actions.

As part of these efforts, we provided a 24/7 service to our membership that allowed members of our crime analysis file, which

is a unique data set to CT, to seek Interpol's support whenever they might be having an active investigation, a cold-case investigation, whatever it might be, so that we could help them understand if the person or entity is known. This helped us to identify common interests or areas of overlap. For example, we may even, depending on how the information is shared, turn around and say, 'Russia, you and the U.S. actually have an entity of common interest.' And to be honest with you, the U.S. and Russia were our biggest data contributors to this CT data file. So, not always do we have the information, but with our bilateral and multilateral partners working together, Interpol brings that collaboration together in a way that there isn't perhaps the antipathies that may exist at a bilateral level. Interpol was working to support the common endeavor where and when we can.

CTC: At Interpol, when you are dealing with 196 different countries, how do you have a common lexicon?

Hinds: One of the things that was very difficult when I was in the U.N. was that the U.N. didn't have a definition of terrorism. Interpol doesn't have a definition of terrorism either. And we didn't need to. Why? Because we supported member countries with *their* definition of terrorism. So once again, we didn't try and create 196 member countries' ideas of what terrorism might look like because you can imagine just how complex that is. What we looked to do is, how we can actually help them operate within their space?

We tailored our support based on their legislative and policy frameworks, and so that makes it a little bit easier. We didn't try and over-engineer it. We didn't try and complicate it because I think it's more about complementarity, more common approaches focused on continuous improvement. We were also looking at gaps. We were looking at vulnerabilities and how people can look to strengthen those based on our experience and exposure helping them do it within their own national frameworks.

CTC: Fast forward three years from now: What resource, policy, or threat after do you think is going to keep you up at night? And what can we do between now and those three years so that nightmare does not happen?

Hinds: I think the dual use of technology, the pace of technology, the automation of all that is a real problem because it's a tool for good *and* it's a tool for evil. But we also find that the adaptation for evil is probably much quicker than what it is for good. So, that concerns me.

I think also about the weaponizing of CBRN materials: We're seeing a very different actor in this particular space, whether it is quantum physics or synthetic biology, all that sort of stuff. We've been fortunate we haven't seen this advanced in weaponizing terrorism, but we saw the impact and potential of it through the lens of virus outbreaks and disease. For me personally, I saw the impact of Ebola when I was in West Africa, and we all saw what happened with COVID. If you successfully weaponized a virus, it could have global impacts that are just phenomenal. So, when it comes to the CBRN space, and whilst we have people focused on and looking at it, we're probably fortunate that as far as threat goes, we haven't really seen capability and intent come together. Some people have the capability, some people have the intent but haven't got the capability. So, we've probably been fortunate we haven't seen an augmentation of such a threat.

The other issue that keeps me awake is the cyber threat. The fact that we haven't really seen this play out is a good thing, but we've seen what happens when the power goes out in hospitals. We understand what happens if it goes out with aircraft traffic controllers and those sorts of critical infrastructure. We understand the impact on our daily life when something like that fails.

So, our critical infrastructure protection, the weaponizing of CBRN, the ongoing challenges around technology, AI and what that will be used for in its adaptation, they're the things that we really need to prepare for next. That does not mean those types of attacks will necessarily be the most sensational attack. Recently in Australia, it was two men with guns and that was our crystallizing moment of change for us here. When it comes to what may come next, it may not be planes into buildings. It may not be taking out vessels at sea.

We need to pay attention to incidents that can change the psyche of government, of policy makers, of legislators, that require and invoke change because we've become comfortable in our space. To be honest with you, when I was at Interpol, I said, 'We are one attack in a Western city away from a real shift in CT policy.' Today, the nature and type of people that are involved in extremism, and the salad bar of ideologies and options available to people, make things really difficult. We've now got legislation in Australia around hate crime and symbols and those sorts of things where we didn't have that before, but it took a terror event to do that. It wasn't as if we hadn't thought about it. How do we future-proof our environment so we're not playing catch up and we can learn better from others in relation to our responses rather than having to go through the pain of a tragic event to facilitate change? CTC

Citations

1 Editor's Note: Andrew Zammit and Levi J. West, "The Bondi Attack: The Islamic State's Strategic Shifts and Jihadi Tactics in Australia," *CTC Sentinel* 19:3 (2026).

The Collapse of Indefinite Detention in Northeast Syria: Implications Seven Years Later for Syria and Beyond

By Devorah Margolin

In early 2026, almost seven years after it began, the indefinite detention of tens of thousands of Islamic State affiliates and their families in northeast Syria ended in chaos after a massive break out from Al-Hol detention camp and the transfer of thousands of the group's fighters to Iraq. Observers now ask: How did we get here, what happened, and what does this mean for countering the Islamic State? To answer these questions, it is vital to consider the heterogeneous group held in northeast Syria, how they got there, as well as the policy decisions that shaped their detention. As the situation has recently drastically changed, this article considers the security implications seven years later for Syria and beyond.

The detention system holding Islamic State affiliates and their families in northeast Syria began to crumble in early 2026. Weeks after an estimated 200 male detainees fled from an Islamic State detention facility near the town of Shadadi, Al-Hol detention camp—known for holding Islamic State-affiliated families—was empty after more than 20,000 escaped the once-secure site.[1] Fearing more breakouts, by mid-February, U.S. Central Command confirmed the completed transfer of 5,700 male detainees from Syria to Iraq.[2] The once expansive detention system holding Islamic State affiliates and their families had fallen to pieces. For those that have studied this issue, the collapse of indefinite detention in northeast Syria was both foreseeable and avoidable.

For the last seven years, tens of thousands of men, women, and—primarily—children captured after the fall of the Islamic State's so-called caliphate in 2019 were held in detention sites (including detention facilities and detention camps) in northeast Syria.[a] Run by the Syrian Democratic Forces (SDF), and its civilian arm the Democratic Autonomous Administration of North and East Syria (DAANES), these detention sites held Syrians, Iraqis, and Third Country Nationals (TCNs)[b] and were supported by the Global Coalition to Defeat the Islamic State (the Coalition).[3]

While meant to be only a temporary solution, for the last seven years little changed. Despite the Islamic State's history of exploiting breakout events to rebuild and expand its networks[4] and much international debate over the questionable security and humanitarian standing of these detention sites, Syria remained divided and international actors were slow to act, turning the situation into a protracted, indefinite crisis.

Yet, the fall of the Assad regime in December 2024 and the rise of the new interim president, Ahmed al-Sharaa, created an opening for change in Syria, but also left detention facilities and detention camps in the northeast vulnerable.[5] This came to a head when despite best intentions and years of policy emphasizing the systematic reduction of these detained populations through repatriation, reintegration, and, where appropriate, accountability, the collapse of indefinite detention occurred rapidly, chaotically, and with little transparency at the start of 2026. As questions emerge about how this unfolded—and what it means for ongoing efforts to counter the Islamic State—it is vital to examine how the world arrived at this point and what comes next.

The purpose of this article is to examine how the indefinite detention of thousands of Islamic State-affiliated individuals and their families shaped the international community's current ability—and desire—to counter the group. The article progresses by initially addressing how individuals ended up in detention, before discussing the detention process as well as security and humanitarian concerns that impacted the detention sites. It also examines international reluctance toward repatriation and recent chaos that rewrote the map, before concluding by addressing future threats posed by—and to—those previously detained in northeast

Dr. Devorah Margolin is the Blumenstein-Rodan Senior Fellow at The Washington Institute for Near East Policy and an Adjunct Professor at Georgetown University and Pepperdine University. Her research primarily focuses on terrorism governance, the role of propaganda and strategic communications, countering/preventing violent extremism, and the role of women and gender in violent extremism. She is the co-editor of Jihadist Governance and Statecraft *(The Washington Institute for Near East Policy, 2024). X: @DevorahMargolin*

a Detention facilities primarily held adult men and teenage boys presumed to be fighters of the Islamic State, while detention camps mostly held women and children presumed to be family members of Islamic State fighters. Together referred to as detention sites, this encompasses both detention facilities (sometimes referred to as prisons by news sources) and detention camps (sometimes referred to as Internally Displaced Person camps). However, due to presumed affiliation with the Islamic State, all detention facilities and detention camps were closed, meaning that individuals could not freely leave. Moreover, most individuals held in detention facilities and detention camps in northeast Syria – including Iraqis and Third Country Nationals (TCNs) – have been held without charge, trial, or legal standing.

b Third Country Nationals (TCNs) refers to individuals from around the world (specifically from outside of Syria and Iraq) who traveled to join jihadi groups in Syria and Iraq. Today, some TCNs include individuals born under the Islamic State or while in detention to parents who are TCNs.

Syria. This article argues that despite the desire to move on from this chapter, a cooperative international effort is still needed to counter a resilient and now more disperse Islamic State threat, one that has—and will continue—to use its supporters to resurge.

The Collapse of the Caliphate and the Start of Indefinite Detention

The scope and scale of the Islamic State's mobilization, coupled with the group's active recruitment of men, women, and children to its state-building project, made it unique among jihadi actors.[6] Many in the region willingly joined the Islamic State, while others were forced under its occupation as it grabbed territory across Syria and Iraq.[7] Still others left their home countries to join the group, with more than 50,000 men, women, and children from approximately 80 countries joining jihadi groups in Syria and Iraq between 2011 and 2018, including the Islamic State.[8]

The Islamic State's gendered recruitment, coupled with its theological-legislative gendered system of control,[9] created both security and policy implications for those seeking to counter the group. Its system of control forced domesticity and excluded women and girls from much of public life as a way of prioritizing female modesty, often leading to a gross misunderstanding of women's roles in the group.[10] Its policies also affected men and boys, focusing on militarization with the group's gender essentialism specifically affecting boys, with violence ingrained in every part of their upbringing.[11] This meant that for those seeking to counter the Islamic State, teenage boys were viewed as a security threat due to the indoctrination and training they may have received from the group. Moreover, the Islamic State's binarized gender roles emphasizing men as fighters had implications, as many of the group's male supporters were killed fighting for the group, leaving behind thousands of women and children family members.[12]

This phenomenon became evident when between late 2018 and early 2019, the SDF—with support from the U.S.-led Coalition—began to take control of territory formerly held by the Islamic State in northeast Syria. In the process, men, women, and—primarily—children affiliated with or perceived as affiliated with the group were detained and transferred to detention sites in northeast Syria, including 'pop-up' detention facilities and detention camps—many of which were originally designed as temporary shelters for internally displaced persons (IDPs).

Dealing with tens of thousands of people taken into custody during this time, the SDF developed emergency detention measures to divide the populations. These measures reflected the Islamic State's own binarized gender roles that were implemented throughout its caliphate, and gendered assumptions concerning ideological commitment and risk.[13] Women and children were separated from men and teenage boys—some as young as 14—perceived as Islamic State fighters.[14] Approximately 10,000 men and teenage boys were moved into detention facilities, while the majority of those captured—around 60,000 mostly children and women—were moved into detention camps.[15] This process was never supposed to be permanent. Yet, international reluctance to repatriate their citizens, and faced with no real consequences, the indefinite detention crisis began.

It is imperative to make two important caveats. First, not every foreign fighter or foreign traveler that joined jihadi groups in Syria and Iraq ended up in indefinite detention. Some returned home, some moved to other conflict theaters, and some aligned with other groups, including the now-defunct Hayat Tahrir al-Sham (HTS), and moved to other parts of Syria.[16] Second, not everyone held in detention sites in northeast Syria was affiliated with the Islamic State. For example, many of the detention camps that Islamic State-affiliated women and their children were sent to were already IDP camps holding displaced populations.[17]

The following sections will explore the detention sites, including detention facilities primarily holding men and teenage boys and detention camps primarily holding women and children.

Detention Facilities Holding Men and Teenage Boys

At its peak, the SDF was estimated to hold more than 10,000 Islamic State-affiliated men and teenage boys at detention facilities, including 5,000 Syrians, 3,000 Iraqis, and 2,000 TCNs,[18] which the U.S. State Department once called "the largest concentration of detained terrorists in the world."[19] Holding such a large number of individuals led to many security and humanitarian concerns over the years. Some of these issues arose because many of these facilities were not purposely built to hold detainees, suffered from outdated infrastructure, lacked aid entering the facilities, had no legal status for existing, and exhibited shortcomings among those running the facilities, like insufficient medical infrastructure and limited guard force training on the humane treatment of detainees.[20] This in turn also affected the security situation. For example, in 2021 the United Nations noted that "the improvised and converted facilities in which they are held are often unsuitable from humanitarian and security perspectives."[21] Yet, between 2021 and the end of 2025 little changed.[22]

Moreover, for the Islamic State, the freeing of these individuals would both militarily aid the group's depleted ranks as well as serve as a propaganda tool, showcasing its continued power. In September 2019, then-Islamic State caliph Abu Bakr al-Baghdadi called on the group's fighters to free detainees.[23] Since then, security forces dealt with at least two security incidents a year, with January 2022 seeing the largest attack claimed by the group.[24] The 10-day operation at Panorama detention facility in northeast Syria involved more than 200 fighters and a car bomb alongside simultaneous riots inside the facility, and led to some escapes (though many were recaptured or killed).[c] For years after the attack, the SDF, the DAANES, and international partners pointed to these security issues and glossed over humanitarian concerns.[25 d]

It is important to acknowledge that over the last seven years, gathering concrete information on individuals in detention facilities

c The attacks also led to the death of 77 prison employees, 40 SDF personnel, four civilians, and 374 Islamic State affiliates (including at least two minor boys). See "Operation Inherent Resolve Lead Inspector General Report to the United States Congress January 1, 2022-March 31, 2022," U.S. Department of Defense, May 3, 2022, pp. 18-19; "Northeast Syria: Fate of Hundreds of Boys Trapped in Siege Unknown," Human Rights Watch, February 4, 2022; Jane Arraf and Sangar Khaleel, "Teenage Inmates Found Among the 500 Dead in Syria Prison Attack," *New York Times*, January 31, 2022; "Sixteenth report of the Secretary-General on the threat posed by ISIL (Da'esh) to international peace and security and the range of United Nations efforts in support of Member States in countering the threat," S/2023/76, United Nations Security Council, February 1, 2023.

d In 2024, after allegations of humanitarian abuse were made by Amnesty International, General Mazloum of the SDF told CNN, "Instead of these organizations condemning what we are doing and calling it human rights violations, these organizations should give us help when it comes to our program that we have in place for years." See Brent Swails, Clarissa Ward, and Mohammad Hasan, "'In prison because of our parents': Children of ISIS fighters coming of age in detention ask what they're being punished for," CNN, June 11, 2024.

has remained extremely difficult—and sometimes unreliable—for numerous reasons, including security reasons, as well as the fact that they were run by non-state actors, the SDF and the DAANES. As such, NGOs or international organizations did not operate in the detention facilities, and even international bodies like the United Nations and the Coalition struggled to gain access.[e] For many countries that have been reluctant to take accountability for their citizens, not having access to this concrete information allowed them to deny responsibility.

One of the last times that comprehensive information was publicly available was mid-2024, with Amnesty International noting that despite public perception that these facilities were run by the SDF, in reality detention facilities were run by *both* the SDF (15 facilities) and its civilian arm the DAANES (10 facilities).[26] By the end of 2025, detention facilities in northeast Syria were said to still hold nearly 9,000, including 8,000 adult men and 1,000 teenage boys and young men initially detained as minors, as well as 100 women.[f] Many women detained in detention facilities were accused of committing crimes in DAANES territory, including in detention camps.[27]

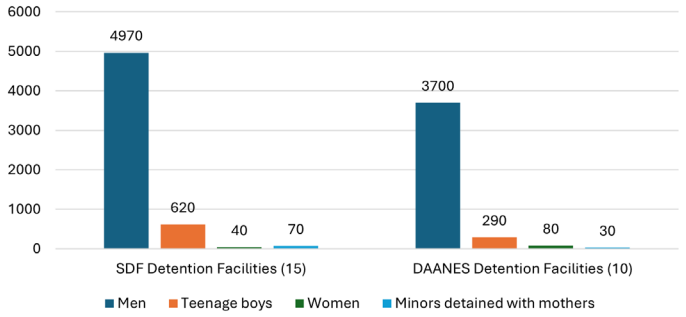

Figure 1: SDF and DAANES Detention Facilities in mid-2024 (Data from Amnesty International, 2024)

According to Amnesty International, in 2024 the 15 SDF-run facilities held roughly half of those in detention facilities, including some 2,000 TCNs from at least 55 countries.[28] When addressing TCNs held in detention facilities, these are the populations referred to. In fact, the Coalition has acknowledged that just two SDF-run detention facilities, Sini detention facility (near Shadadi) and Panorama/"Al-Sina'a" detention facility (near Hasakah),[g] held 85 percent of the individuals in SDF detention.[29][h] At the end of 2025, many of those who remained in SDF-run detention facilities in northeast Syria (including approximately 2,000 TCNs) never faced trial despite being held since 2019.[30]

The remaining 10 detention facilities—those not run by the SDF—were run by its civilian arm, the DAANES. DAANES-run facilities could be divided into two categories: a) eight detention facilities, and b) two youth "rehabilitation" centers (which will be discussed below).

The vast majority of the detainees held in DAANES-run detention facilities were Syrians with perceived Islamic State affiliation who had been tried and sentenced by the DAANES' "People's Defence Courts," which charged individuals with 'terrorism' and other crimes related to national security in northeast Syria.[i] Because of the DAANES' non-state status, they could only charge and put on trial Syrians.

Over the years, many questions have arisen about the number of individuals in detention facilities. For example, even after years of repatriation of Iraqi men from these facilities, the SDF still claimed at the end of 2025 that there were still 9,000 Islamic State-affiliated individuals in detention facilities.[j] This has raised concerns that political prisoners may have been mixed in with Islamic State-affiliated populations. For example, in 2024 Amnesty International flagged that the DAANES and SDF have been accused of using allegations of affiliation with the Islamic State to intimidate and silence people, as well as exact revenge in personal or clan disputes.[31] The lack of international oversight of the SDF's handling of detention facilities, coupled with international reluctance toward repatriation—particularly men—led to a situation in which even today there is still little knowledge about the size and scope of the issue, including names, gender, age, and nationality of those who were held in detention facilities.[k]

e For example, between 2019 and January 2022, detainees were only able to communicate externally via the Red Cross. However, this was suspended after the January 2022 Panorama detention facility attack. See "Operation Inherent Resolve Lead Inspector General Report to the United States Congress April 1, 2022-June 30, 2022," U.S. Department of Defense, July 29, 2022.

f The majority of the women who were detained in detention facilities were held in sites run by the DAANES, while only around a handful of women were held in SDF-run facilities. See "Aftermath: Injustice, torture and death in detention in north-east Syria," Amnesty International, April 17, 2024; Fionnuala Ní Aoláin, "Position of the United Nations Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism on the human rights of adolescents/juveniles being detained in North-East Syria," United Nations Office of the High Commissioner of Human Rights, May 2021; and "Operation Inherent Resolve and Other U.S. Government Activities Related to Iraq & Syria October 1, 2024-December 31, 2024," U.S. Department of Defense, February 19, 2025.

g Panorama detention facility was purpose-built in Hasakah by the U.S.-led Coalition, replacing a makeshift prison on the same site.

h While Sini Detention facility used to hold almost 4,000 detainees, by August 2023, only approximately 800 detainees remained. At the end of 2025, most detainees – around 4,500, including around 600 teenage boys and young men detained as minors – were held at Panorama detention facility. Data provided by SDF, August 2023, on file with Amnesty International. "Aftermath: Injustice, torture and death in detention in north-east Syria;" Ghaith Alsayed, "U.S. military transfers first 150 Islamic State group detainees from Syria to Iraq," PBS/Associated Press, January 21, 2026.

i "People's Defence Courts" prosecuted more than 8,000 Syrians for both allegedly being connected to the Islamic State or for having committed crimes under the DAANES. See "Report of the Commission of Inquiry on Syrian Arab Republic to the 54th regular session of the Human Rights Council," A/HRC/54/58, United Nations Human Rights Council, August 14, 2023; "Arbitrary Imprisonment and Detention - Report of the Commission of Inquiry of the Syrian Arab Republic," A/HRC/46/55, United Nations Human Rights Council, March 11, 2021.

j For example, since 2019 the Coalition has acknowledged the movement of at least 1,600 Iraqi detainees from detention facilities in northeast Syria to Iraq. See "Operation Inherent Resolve Lead Inspector General Report to the United States Congress" quarterly reports and the author's data on repatriation.

k For example, over the years the SDF, with Coalition support, sought to biometrically enroll all the populations held in detention facilities, with attempts to enroll these populations failing in 2021, 2022, and 2023. See "Operation Inherent Resolve Lead Inspector General Report to the United States Congress April 1, 2021-June 30, 2021," U.S. Department of Defense, August 11, 2021, p. 73; "Operation Inherent Resolve Lead Inspector General Report to the United States Congress October 1, 2022-December 31, 2022," U.S. Department of Defense, February 7, 2023; "Operation Inherent Resolve and Other U.S. Government Activities Related to Iraq & Syria October 1, 2023-December 31, 2023," U.S. Department of Defense, February 9, 2024.

Minors in Detention Facilities and Youth "Rehabilitation Centers"

Seven years later, one of the most contentious issues remains the holding of minors in detention facilities. This includes teenage boys held alongside adult men, minors held with their mothers, and those held in youth "rehabilitation" centers after being forcibly separated from their families. The indefinite detention of minors has been criticized for not meeting the United Nations Standard Minimum Rules for the Administration of Juvenile Justice.[32]

As early as 2019, it was clear that there were hundreds of teenage boys held in detention facilities in northeast Syria alongside adult men.[33] As of 2024, around 800 teenage boys were still being held in adult detention facilities, the majority at the adult Panorama detention facility.[34] In 2022, the Coalition acknowledged that there were at least 539 detainees in Panorama detention facility that were younger than 18 years old when they were initially detained in 2019.[35] Despite being detained as minors, many of these teenage boys are now young men, turning 18 while still in detention.

In addition to youths held alongside adults in detention facilities, at the end of 2025 there were two main youth "rehabilitation" centers run by the DAANES: Houri (established in 2016) and Orkesh (established in 2022), which as of August 2023 together held around 200 boys, of which approximately 190 boys were TCNs, while the remaining boys were Syrians.[l] By mid-2024, most of the boys held at Houri and Orkesh "rehabilitation" centers had been moved from Al-Hol camp.[36] While this was an improvement from the SDF's previous policy of moving boys from Al-Hol camp into prisons with adult men, this was not without controversy, as these boys were still forcibly removed from their families.[m] The SDF has claimed they removed these boys for several reasons, including their involvement with violent and criminal activities, their indoctrination into extremist ideologies, as well as being at risk of sexual violence.[37]

Compared to conditions of minors held alongside adult detainees, or even minors held in detention camps, the conditions of the youth "rehabilitation" centers were considered slightly better, with boys and young men receiving some physical and psychological support, humanitarian assistance, as well as some education.[38] Yet, while called "rehabilitation" centers, without a long-term solution, these camps have remained just a holding point. Only Syrian boys in Houri were ever charged, tried, or released.[39] Some foreign nationals were repatriated. For the rest, researchers have called this the "conveyor belt of incarceration," as this offer of "rehabilitation" is only a passing phase until inevitable transfer to prison at age 18.[40] Rather than proactively addressing youths who were victims of the Islamic State, the system of indefinite detention further victimized these young boys.

Detention Camps Holding Women and Children

At the fall of the caliphate, the majority of the captured individuals were minors and women, who were then sent to closed detention camps, meaning camp residents were not free to leave.[41] In early 2019, when the populations of Islamic State-affiliated individuals in these camps peaked, there were several detention camps.[n] However, by July 2022, the United Nations acknowledged that only two detention camps still held Islamic State-affiliated families.[42] They included first, the larger Al-Hol camp, and second, the smaller Roj camp.[43] Security of both camps was run by the SDF, with funding coming from the U.S. State Department and USAID for camp management (including food, water, and internal security).[44]

Al-Hol was originally opened in 1991 by the United Nations High Commissioner for Refugees as an IDP camp, but was reopened in 2016 by the SDF as an IDP camp, and by 2018 around 10,000 mostly Iraqi nationals lived in the camp.[45] However, between December 2018 and April 2019, more than 60,000 individuals—most of whom were minors—entered Al-Hol camp, creating an urgent need to process these individuals, with logistical, humanitarian, and even security challenges.[46] At that time, 65 percent of the population in Al-Hol was under the age of 12.[47] Due to its size, the camp was divided into several annexes, including one just for TCNs.

By the end of 2025, Al-Hol held still around 24,000 people, with more than 60 percent of the population under the age of 18, 29 percent of the population being women, and the remaining 11 percent being men.[48] The majority of families in Al-Hol were female-headed households.[49] The largest of the detention camps, Al-Hol represented the intractability of indefinite detention. A complex environment, the camp held both Syrian and Iraqi IDPs who were in the camp before 2019, as well as an influx of Islamic State-affiliated families captured by the SDF. In October 2025, UN Women released a report that contended one quarter of those detained in Al-Hol had no connection to the Islamic State.[50]

Due to the size and population in Al-Hol, the camp faced both hostile internal dynamics and served as a target for Islamic State attacks. For example, in September 2022 the Islamic State claimed responsibility for an attempted multi-pronged vehicular attack on Al-Hol, which aimed to break free the group's supporters and act as "revenge for imprisoned women."[51] Moreover, the camp was plagued by adult women who were still ardent supporters of the group as well as minor children at risk of radicalization and recruitment by

l While Houri held TCNs and Syrians, Orkesh only held TCNs. See "Operation Inherent Resolve Lead Inspector General Report to the United States Congress January 1, 2021-March 31, 2021," U.S. Department of Defense, May 2, 2021; "Report of the Commission of Inquiry on Syrian Arab Republic to the forty-eighth regular session of the Human Rights Council," A/HRC/48/70, United Nations General Assembly, August 13, 2021; "Aftermath: Injustice, torture and death in detention in north-east Syria," p. 125; "Punishing the Innocent."

m After backlash over the SDF policy to move minors from detention camps into adult detention facilities, the SDF began to move younger boys to "rehabilitation centers." See Devorah Margolin and Gina Vale, "In the Shadow of the Caliphate: A Decade of Islamic State Gendered Violence," *CTC Sentinel* 17:7 (2024); "Fourteenth report of the Secretary-General on the threat posed by ISIL (Da'esh) to international peace and security and the range of United Nations efforts in support of Member States in countering the threat," S/2022/63, United Nations Security Council, January 28, 2022; "Operation Inherent Resolve Lead Inspector General Report to the United States Congress October 1, 2021-December 31, 2021," U.S. Department of Defense, February 8, 2021, p. 27; "Syria: Repatriations Lag for Foreigners with Alleged ISIS Ties;" Hogir Al Abdo and Bassem Mroue, "Teenagers from Islamic State families undergo rehabilitation in Syria, but future still uncertain," Associated Press, May 30, 2023.

n Several camps closed after a Turkish incursion into Syria in October 2019, including Ayn Issa camp in Raqqa, which held 13,000 individuals, including a foreign annex holding approximately 250 women and 700 minors affiliated with the Islamic State. Eight hundred of these individuals fled the camp during the hostilities and remained unaccounted for. See "Operation Inherent Resolve Lead Inspector General Report to the United States Congress July 1, 2019-October 25, 2019," U.S. Department of Defense, November 19, 2019; Ben Hubbard, Charlie Savage, Eric Schmitt, and Patrick Kingsley, "Abandoned by U.S. in Syria, Kurds Find New Ally in American Foe," *New York Times*, October 13, 2019.

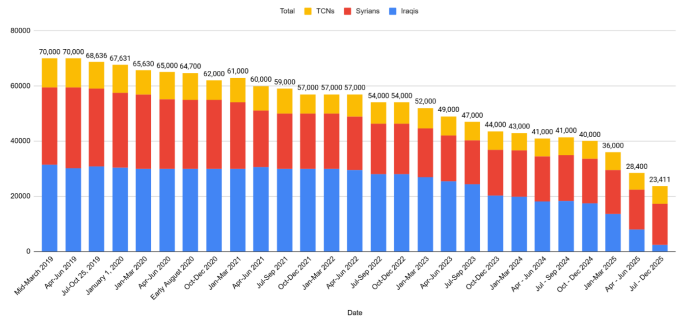

Figure 2: Al-Hol Population between 2019-2025, based on data from CJTF-OIR Quarterly Inspector General Reports

the Islamic State, with Save the Children noting in 2022 that with two murders in the camp a week, Al-Hol was "per capita, one of the most dangerous places in the world to be a child."[52]

While most Islamic State-affiliated women and minors ended up in Al-Hol camp, it soon became clear that the size of the camp, as well as the humanitarian and security situation in the camp required some sort of solution. By March 2020, the SDF, with support of the Coalition, was working on a plan to relocate TCN families from the foreign annex of Al-Hol to other camps, particularly Roj.[53] While Roj camp was originally established in 2016 as an IDP camp for those from Syria fleeing the Islamic State, it was expanded in 2020.[54] Beginning in July 2020, approximately 400 TCN families were moved from Al-Hol into Roj camp.[55] Since then, some TCN families held in Al-Hol have continued to be moved to Roj. The population of Roj camp has held consistently around 2,400 individuals, 94 percent of whom are TCNs.[56]

The humanitarian and security situation in Roj has been considered much better than in Al-Hol camp, including greater internal freedom of movement across the camp, better security, and greater amenities. But it is still a closed indefinite detention camp, with limited housing, water, and food access, as well as limited health and education services.[57] However, Roj camp was not without violence, and in early 2022, the situation escalated to the point that USAID partners paused certain assistance programing due to the security situation in the camp.[58] Today, the only camp that remains active is Roj, holding many Western and high-profile TCN families.

Compared to detention facilities, identification efforts were somewhat easier at Al-Hol and Roj camps because they have allowed greater outside access and collection of biometric data. Governmental and non-governmental organizations alike have repeatedly published clear, detailed statistics on who is there,

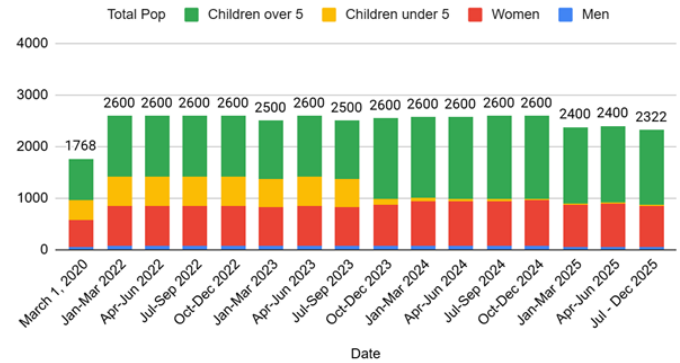

Figure 3: Roj Population by Gender and Age from 2020-2025, based on data from CJTF-OIR Quarterly Inspector General Reports

"The largest of the detention camps, Al-Hol represented the intractability of indefinite detention. A complex environment, the camp held both Syrian and Iraqi IDPs who were in the camp before 2019, as well as an influx of Islamic State-affiliated families captured by the SDF."

where they are from, and who has been repatriated. Because of this access, over the years, devastating reports have emerged detailing the humanitarian concerns in these detention camps.[59] Some of these conditions arose from trying to provide services to thousands of people detained in a conflict zone, and made worse by a complex detention environment involving victims and perpetrators, where violence and stealing—from both the Islamic State and criminal gangs—ran rampant.[60] Some of these conditions also arose from those administering the detention sites, as over the years the Coalition acknowledged a long list of allegations against the SDF, including theft of medication, money, and jewelry; physical abuse; and destruction of food and property.[61]

This was compounded by the fact that the majority of individuals held in detention camps over the last seven years were minors.[62] While initial views of this group were classified as non-threatening due to age and gender, the indefinite detention of these individuals, as well as the continued ardent support of the Islamic State by many detained, reclassified this group as the "potential next generation," meaning the tens of thousands of women and minors held in detention camps held the possibility of populating and educating the next generation of the Islamic State.[63] Yet, even this classification had consequences. While it may have helped gain funding and attention for the running of these detention camps, it did little to engender support for repatriation of these individuals to their countries of origin.[o]

Returns and Repatriations: From Opportunity to Chaos

At the end of 2025, an estimated 9,000 men and teenage boys remained in detention facilities, and around 26,000 women and children remained in detention camps.[64] Faced with the humanitarian and security concerns of indefinite detention, many have argued that the only way to address this issue is through the return and repatriation of those detained. Since the fall of the so-called caliphate in 2019, the DAANES and SDF have been adamant about their preference for detained Iraqis and TCNs to be repatriated to their countries of origin in order to be held accountable. Barring that, they have called for an ad hoc international court to be established that would hold jurisdiction.

However, like many things in northeast Syria, the DAANES/

o For example, in 2019, when discussing reluctance to repatriate detained individuals, the European Union's counterterrorism coordinator referred to the children of Islamic State-affiliated individuals as "the next generation of suicide bombers." See H.J. Mai, "Why European Countries Are Reluctant To Repatriate Citizens Who Are ISIS Fighters," NPR, December 10, 2019.

SDF's non-state status has significantly complicated matters, creating a prolonged state of legal and political limbo, as they did not have the authority to deport those detained or to put them on trial. Only Syrians or individuals who committed crimes under the DAANES authority were put on trial, and only Syrians who were from the northeast were able to leave detention sites to begin reintegrating.[65] Syrians from the rest of the country were left in limbo due to the fractured nature of the country.

Moreover, the ability to repatriate foreign citizens to their countries of origin, to alleviate the problem of indefinite detention, was reliant on the political will of other countries. Yet, many governments around the world were slow—or unwilling—to repatriate their citizens, leaving tens of thousands—primarily children—in indefinite detention without charge, trial, or legal standing.[66] Despite efforts to reduce the number of those detained, over the years very little changed.

According to data on repatriation compiled by the author,[p] of the almost 4,000 TCNs repatriated between 2019 and 2025, more than 70 percent were minors, 19 percent were women, and only 2.5 percent were men.[q] This shows that even among states willing to repatriate, efforts have largely prioritized children, and then women, neglecting to repatriate men and critically teenage boys—who according to international law are minors and thus victims.

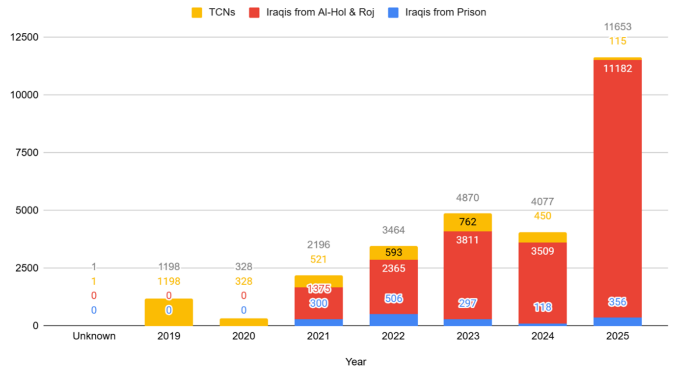

Figure 4: Formal Repatriations from Syria and Iraq[r] by Year from 2019-2025 (data compiled by author)

Furthermore, while Iraqi nationals once constituted the largest population in Al-Hol and made up 30 percent of those in detention facilities, that share has significantly declined. Since 2021, Baghdad has repatriated more than 23,000 of its citizens from detention facilities and detention camps, conducting 33 repatriation operations from Al-Hol alone.[67] This has significantly reduced populations detained in detention facilities and detention camps, alleviating some of the security concerns that arose due to their unmanageable size.

Who is being repatriated also has impacted accountability. As most of the TCN adults repatriated are women, they are facing the highest rates of prosecution, even if most were relegated to peripheral roles under the Islamic State's gendered system of control.[68] Moreover, some states who prosecute adult women have turned to the use of core international crimes against some female defendants as nations' counterterrorism laws failed to encapsulate their participation in the Islamic State.[69] Other states such as Bosnia and Herzegovina and Kosovo have taken a different stance, choosing to never charge or give suspended sentences to adult women.[70]

While between 2019 and 2024 the process of TCN repatriation remained slow, the fall of the Assad regime at the end of 2024 made TCN repatriation almost stagnant. This was compounded by the fact that the end of the Assad regime, and the rise of new interim President al-Sharaa, also created an opening for the incoming Trump administration to pursue withdrawing U.S. forces from Syria, an objective from its first term. To achieve this aim, the Trump administration cut funds to counter-Islamic State activities, pushed the United Nations to take over administrative oversight of Al-Hol and Roj camps, encouraged reconciliation between the SDF and Damascus, and called for the new Syrian government to join the Coalition—which it eventually did.[71]

But the Trump administration also wanted Damascus to assume responsibility for Islamic State detention sites, despite it clearly lacking both the capacity and political willingness to do so. Detention sites were seemingly caught in the middle, and the result was chaos.[72] In early January 2026, after almost a year of failed talks between Damascus and the SDF, the Syrian army proceeded into the long Kurdish-controlled parts of the northeast of Syria. Rampant disinformation and violence between the factions led to disorder, in an area holding thousands of Islamic State-affiliated fighters and their families.[73]

Despite an agreement for the SDF to handover the detention sites to Damascus, early clashes led to a prison break on January 19, 2026, at a detention facility near the town of Shadadi, with both the SDF and Damascus pointing fingers and deflecting blame, prompting fears of further escapes.[74] While many of those who escaped were recaptured, to mitigate future threats between January 21 and February 13, CENTCOM transferred 5,700 adult men from detention facilities in northeast Syria to Iraq, including Syrians, Iraqis, and TCNs.[75]

Concurrently, on January 20, after an hours-long break in control after the SDF retreated, the Syrian army took control of Al-Hol camp. During this time, disinformation swelled, centering on who was being held in the camp,[s] which at the end of 2025 was 15,000 Syrians, though Al-Hol also held around 2,300 Iraqis and 6,000 TCNs.[76] Over the course of a chaotic few weeks at the end of January into early February, Al-Hol's population was emptied, with many of the 20,000 individuals previously held in Al-Hol unaccounted for. The responses of the United Nations, the Coalition, the SDF, and the Syrian government have been mostly to point fingers, deflect blame, and seemingly move on. As for Damascus, which was long reluctant to take control of Al-Hol, over the last year questions emerged over if the government even defined those 20,000 held in Al-Hol as part of the counter-Islamic State mission.[77]

Today, all that is known to remain of the northeast Syrian detention network is Roj camp with approximately 2,500 primarily

p The author would like to thank Michelle Fan and Gabriel Wein for their research assistance in helping maintaining this dataset over the years.

q The remaining 8.5 percent were not identified by age or gender. See dataset created and maintained by the author.

r The vast majority of cases of repatriation occurred from Syria. However, a handful of recorded cases were repatriated from Iraq in 2019.

s For example, after years of wrongful detention under the Assad regime, feelings of detention – specifically of women and children – were heated. See "Syrian President Sharaa grants amnesty giving partial reprieve to convicted criminals," New Arab, February 19, 2026.

"The collapse of indefinite detention risks feeding into Islamic State narratives that emphasize endurance, liberation, and the strategic importance of detention sites. Prisons have played a central role in the group's evolution—serving as sites of recruitment, networking, and operational consolidation. The sudden dispersal of these populations, without a framework for accountability or monitoring, complicates efforts to track residual networks and the ability to assess the group's capacity to regenerate."

third-country women and minors. Information surrounding those previously held in the two youth rehabilitation centers remains murky.

What Comes Next?

As this article has highlighted, the chaos that emerged in northeast Syria at the start of 2026 was both predictable and preventable, and was the result of many of the counterterrorism decisions—or lack thereof— made by the Coalition, its partners in the region, and the international community as a whole. For those studying indefinite detention over the past seven years, the consequences of neglect were clear. Now, international actors face three central questions: What comes next for these populations? What does this mean for the threat posed by the Islamic State? And what should the international community do about it? As with the detention system itself, the issue must be broken into categories: male detainees to Iraq, those missing from Al-Hol, the future of Roj, and questions surrounding missing teenage boys.

First, the Coalition's transfer of 5,700 male detainees from Syria to Iraq—including not only Iraqi citizens but also Syrians and third country nationals—and the announcement that Iraq will prosecute those transferred, is deeply controversial.[78] While the move reflects the genuine security concerns of the Coalition, it also raises human rights criticisms, including Iraq's rapid trials, high conviction rates, and use of the death penalty. Moreover, reports have emerged that roughly 150 minors were among those transferred.[79] For example, Iraq has already returned a minor from Finland who it decided not to prosecute; the Finnish embassy has noted that the minor was brought as a child to Syria and ended up in Al-Hol, before later being brought to Iraq as part of the 2026 transfers.[80] [t]

The detainee transfers come as Iraq already faces overcrowded prisons, sectarian tensions, and a history of prisons serving as incubators for the Islamic State. Iraq also has a history of prison breaks including during the "breaking the walls" campaign in 2012 to 2013, which helped the Islamic State resurge before declaring its caliphate.[81] Moreover, current regional instability—particularly tensions with Iran—has heightened concerns, with airstrikes reported near detention facilities holding Islamic State detainees in Baghdad, setting off fears of more escapes.[82] Such an event could trigger serious security implications, not only for Iraq, but it could also once again help the group redevelop its networks.

Questions also remain about those left behind: While the Coalition long cited 9,000 detainees in Syria, only 5,700 were transferred. Those left behind likely include women, minors, and those unable to be moved due to being sick or injured. They also indicate that the SDF could have inflated the numbers of those held in detention facilities or conflated political detainees with those associated with the Islamic State. The move raises real concerns that international actors are again deferring responsibility to increasingly unstable Iraq, even if unlike the SDF it has formal legal authority to investigate and prosecute detainees.

Second are the approximately 20,000 individuals formerly held in Al-Hol, now reportedly "at large" according to U.S. intelligence services.[83] The lack of transparency surrounding the camp's rapid emptying poses risks to both regional stability and the individuals themselves.[84] This population—largely women and children, including around 6,000 TCNs—represents a wide spectrum of experiences, from victims of the Islamic State to committed adherents to somewhere in between, a tension that continues to hinder effective policy responses.

Reports suggest many former Al-Hol residents have relocated within Syria, particularly to Idlib and Aleppo.[85] Addressing these populations is particularly challenging, and compounded by the limited capacity and unclear policies of the Syrian government—within whose territory this population has disappeared—to find, detain, adjudicate cases, or otherwise manage individuals previously held in Al-Hol. For those who remain in Syria, Damascus views those that escaped Al-Hol as a humanitarian rather than security issue,[86] and has yet to establish mechanisms for documentation, tracking, repatriation, prosecution, or reintegration. Moreover, the lack of a post-detention framework for former Al-Hol residents—especially children—leads them to face risks of trafficking or engagement with extremist networks.[u]

For those who did remain in al-Hol—only a few hundred Syrians and Iraqis—were either repatriated to Iraq or transferred to a repurposed camp for IDPs in Akhtarin, Aleppo province. Early reports of gaps in healthcare, protection, and assistance highlight the Syrian government's limited capacity to manage these populations, let alone those unaccounted Al-Hol populations.[87] As international actors continue to avoid responsibility for their own citizens, compounding Syria's ability to address this problem, the likely outcome is both a humanitarian crisis and a more diffuse, harder-to-track security threat, in an evolving security environment, and one in which the new Syrian government appears

t It remains unclear how the minor came to be included in the transfer to Iraq, raising questions about whether he was transferred from a youth "rehabilitation" center or from an adult facility.

u Syrian security forces told *Le Figaro* that it arrested a 14-year-old boy (before January) who was previously in Al-Hol on his way to carry out an attack for the Islamic State. See Margaux Benn, "The Lives in Limbo of Families Freed from Syria's Al-Hol Camp," *Figaro*, March 12, 2026.

to be preoccupied with other important matters.

Still others who escaped Al-Hol may seek to return home or move across borders. Such mobility follows well-established patterns among foreign fighters and their families of either seeking to return home or moving to different theaters of instability. For example, among the TCNs that escaped Al-Hol was Albanian Eva Dumani, now 21, who was brought by her father to Syria when she was nine, as well as an unnamed Belgian woman who returned to Belgium in February 2026 and was arrested upon arrival.[88] For others who choose to return to their countries of origin, a previous lack of proactive planning for such events could lead to devastating consequences.

Notably, the collapse of indefinite detention risks feeding into Islamic State narratives that emphasize endurance, liberation, and the strategic importance of detention sites. Prisons have played a central role in the group's evolution—serving as sites of recruitment, networking, and operational consolidation. The sudden dispersal of these populations, without a framework for accountability or monitoring, complicates efforts to track residual networks and the ability to assess the group's capacity to regenerate. After almost two years of silence, the Islamic State's spokesman Abu Hudhayfa al-Ansari released a new speech on February 21, 2026, in honor of Ramadan, in which among other things called on Islamic State fighters to continue to target the new "apostate" government in Damascus. That said, the collapse of indefinite detention—at the hands of someone other them themselves—does not appear to be a windfall for the group, at least not yet. The threat posed by the Islamic State is nowhere near what it once was, but it is not gone, especially as thousands remain unaccounted for and thousands more remain detained in Iraq and Syria.

The future of two additional groups remains unclear. The first is the population in Roj, which still holds around 2,500 TCNs. Although Damascus announced plans to close both al-Hol and Roj, the timeline for Roj remains unclear.[89] Again, the counterterrorism decisions made by the Coalition and its partners in the region have had reverberating implications. Many states with citizens in Roj still remain reluctant to repatriate their citizens either due to political reasons or a dearth of counterterrorism laws that consider women's roles within the Islamic State. Without a clear plan, the future for those in Roj will likely be similar to those who were at Al-Hol.

The second group consists of teenage boys, potentially up to 1,000, whose whereabouts are uncertain. Some were reportedly transferred to Iraq, while others from youth "rehabilitation" centers such as Houri and Orkesh may have been moved to Panorama detention facility—which the SDF is reportedly still controlling—or reunited with family members in Roj. Teenage boys, already a vulnerable population, remain unaccounted for. Teenage boys should be treated as victims, though not without acknowledging potential security risks. One issue that has arisen is that most in the international community have only focused on their security risk, which oversimplifies a complex reality shaped by coercion, age, and lived experience under the Islamic State and then indefinite detention under the consequences of counterterrorism decisions made by the Coalition and its partners.

As this study has explored, many of the counterterrorism decisions made by the Coalition and the international community—including continued indefinite detention and a reluctance to repatriate—had secondary and tertiary implications that make the Islamic State threat today more disperse and harder to combat. Moreover, the current security environment provides plenty of excuses to focus on other important issues. Faced with these facts, the international community faces a crossroad. Despite a clear inclination of the international community to move on from this chapter, such a decision could have devastating consequences. Formerly detained Islamic State-affiliated individuals are at large in Syria, while others have crossed its borders to unknown places. Others face humanitarian hurdles and are at risk of trafficking or radicalization. Still others are held in prisons in Iraq at risk of another breakout event. A clear and coordinated international effort remains essential to counter the Islamic State, as the group has—and will continue—to exploit breakout events and turn to its supporters to rebuild and expand its networks. CTC

Citations

1 Devorah Margolin and Joana Cook, "From Bad to Worse in Northeast Syria," *Foreign Policy*, February 25, 2026.

2 "U.S. Forces Complete Mission in Syria to Transfer ISIS Detainees to Iraq," U.S. Central Command, February 13, 2026.

3 "Arbitrary Imprisonment and Detention - Report of the Commission of Inquiry of the Syrian Arab Republic," A/HRC/46/55, United Nations General Assembly, March 11, 2021; "Fifteenth report of the Secretary-General on the threat posed by ISIL (Da'esh) to international peace and security and the range of United Nations efforts in support of Member States in countering the threat," S/2022/576, United Nations Security Council, July 26, 2022; "2022 Country Reports on Human Rights Practices: Syria," U.S. Department of State, Bureau of Democracy, Human Rights, and Labor, March 20, 2023.

4 Charlie Winter and Abdullah Alrhmoun, "A Prison Attack and the Death of its Leader: Weighing Up the Islamic State's Trajectory in Syria," *CTC Sentinel* 15:2 (2022).

5 Devorah Margolin, "Syria Crisis Leaves Islamic State Prisons and Detention Camps Vulnerable," Washington Institute for Near East Policy, December 9, 2024; Devorah Margolin, "Setting Expectations with Syria on Countering the Islamic State," Washington Institute for Near East Policy, May 27, 2025.

6 Kiriloi Ingram, "An Analysis of Islamic State's Gendered Propaganda Targeted Towards Women: From Territorial Control to Insurgency," Terrorism and Political Violence, 2021; Nelly Lahoud, "Empowerment or Subjugation: An Analysis of ISIL's Gendered Messaging," UN Women, June 2018.

7 For more on life under the Islamic State, see the George Washington University's ISIS Files Digital Repository at isisfiles.gwu.edu

8 Joana Cook and Gina Vale, "From Daesh to 'Diaspora': Tracing the Women and Minors of Islamic State," International Centre for the Study of Radicalisation, 2018; Joana Cook and Gina Vale, "From Daesh to 'Diaspora' II: The Challenges Posed by Women and Minors After the Fall of the Caliphate," *CTC Sentinel* 12:6 (2019): pp. 30-45.

9 Devorah Margolin and Charlie Winter, "Women in the Islamic State: Victimization, Support, Collaboration, and Acquiescence," The ISIS Files, George Washington University, June 2021.
10 Devorah Margolin and Joana Cook, "The Agency and Roles of Foreign Women in ISIS," Center for Justice and Accountability, August 2023; Gina Vale, "Piety Is in the Eye of the Bureaucrat: The Islamic State's Strategy of Civilian Control," *CTC Sentinel* 13:1 (2020).
11 Devorah Margolin and Gina Vale, "In the Shadow of the Caliphate: A Decade of Islamic State Gendered Violence," *CTC Sentinel* 17:7 (2024); Kara Anderson, "'Cubs of the Caliphate': The Systematic Recruitment, Training, and Use of Children in the Islamic State," International Institute for Counter-Terrorism, January 2016; Gina Vale, "'Cubs in the Lions' Den: Indoctrination and Recruitment of Children Within Islamic State Territory," International Centre for the Study of Radicalisation, July 2018, pp. 19-22; Amy-Louise Watkin and Seán Looney, "'The Lions of Tomorrow': A News Value Analysis of Child Images in Jihadi Magazines," *Studies in Conflict & Terrorism* 42:1-2 (2019): pp. 120-140.
12 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).
13 Margolin and Vale.
14 "Punishing the Innocent: Ending Violations Against Children in Northeast Syria," Independent International Commission of Inquiry on the Syrian Arab Republic, March 19, 2024; Fionnuala Ní Aoláin, "Gendering the Boy Child in the Context of Counterterrorism: The Situation of Boys in Northeast Syria," Just Security, June 8, 2021; "Aftermath: Injustice, torture and death in detention in north-east Syria," Amnesty International, April 17, 2024.
15 "Lead Inspector General for Operation Inherent Resolve Quarterly Report to the United States Congress January - March 2019," U.S. Department of Defense, May 7, 2019.
16 Cook and Vale, "From Daesh to 'Diaspora.'"
17 "Between two fires: Danger and desperation in Syria's Al-Hol camp," Médecins Sans Frontières, November 7, 2022.
18 "Operation Inherent Resolve Lead Inspector General Report to the United States Congress April 1, 2019-June 30, 2019," U.S. Department of Defense, August 9, 2019; "Operation Inherent Resolve Lead Inspector General Report to the United States Congress July 1, 2022-September 30, 2022," U.S. Department of Defense, November 1, 2022; Ian Moss, "Repatriating FTF and Displaced Persons from Northeast Syria," United States Department of State, September 29, 2022.
19 Christine Asetta, "Progress in Repatriations: How Foreign Assistance Is Addressing the Humanitarian and Security Crises in Northeast Syria: Part 1 of 2," DipNote: Countering Terrorism, U.S. Department of State, Bureau of Counterterrorism, December 4, 2023.
20 "Understanding the Lives of the Women, Men, and Children of Al-Hol Camp," UN Women, October 2025; "Twelfth report of the Secretary-General on the threat posed by ISIL (Da'esh) to international peace and security and the range of United Nations efforts in support of Member States in countering the threat," S/2021/98, United Nations Security Council, January 29, 2021; "Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Fionnuala Ní Aoláin," A/78/520, United Nations Office of the High Commissioner of Human Rights, October 10, 2023; "Operation Inherent Resolve and Other U.S. Government Activities Related to Iraq & Syria January 1, 2024-March 31, 2024," U.S. Department of Defense, April 30, 2024, p. 28; "Operation Inherent Resolve and Other U.S. Government Activities Related to Iraq & Syria October 1, 2023-December 31, 2023," U.S. Department of Defense, February 9, 2024; "Operation Inherent Resolve Lead Inspector General Report to the United States Congress January 1, 2023- March 31, 2023," U.S. Department of Defense, May 2, 2023; "Seventeenth report of the Secretary-General on the threat posed by ISIL (Da'esh) to international peace and security and the range of United Nations efforts in support of Member States in countering the threat," S/2023/568, United Nations Security Council, July 31, 2023; "Punishing the Innocent."
21 "Twelfth report of the Secretary-General on the threat posed by ISIL (Da'esh) to international peace and security and the range of United Nations efforts in support of Member States in countering the threat."
22 "Twenty-first report of the Secretary-General on the threat posed by ISIL (Da'esh) to international peace and security and the range of United Nations efforts in support of Member States in countering the threat."
23 "IS leader calls on fighters to free jailed members," Deutsche Welle, September 17, 2019.
24 Islamic State, "The Gweiran Battle," Al Naba #323, January 27, 2022; Charlie Winter and Abdullah Alrhmoun, "A Prison Attack and the Death of its Leader: Weighing Up the Islamic State's Trajectory in Syria," *CTC Sentinel* 15:2 (2022).
25 "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, 2023.
26 "Aftermath: Injustice, torture and death in detention in north-east Syria."
27 "Aftermath: Injustice, torture and death in detention in north-east Syria," p. 144; "Syria: Repatriations Lag for Foreigners with Alleged ISIS Ties," Human Rights Watch, December 15, 2022.
28 Data provided by SDF to Amnesty International, August 2023, on file with Amnesty International, cited in "Aftermath: Injustice, torture and death in detention in north-east Syria," p. 45.
29 "Operation Inherent Resolve Lead Inspector General Report to the United States Congress April 1, 2020-June 30, 2020," U.S. Department of Defense, August 4, 2020.
30 "Punishing the Innocent: Ending Violations Against Children in Northeast Syria;" "Aftermath: Injustice, torture and death in detention in north-east Syria;" "Report of the Commission of Inquiry on Syrian Arab Republic to the forty-eighth regular session of the Human Rights Council," A/HRC/48/70, United Nations General Assembly, August 13, 2021.
31 "Aftermath: Injustice, torture and death in detention in north-east Syria," p. 174.
32 "United Nations Standard Minimum Rules for the Administration of Juvenile Justice ('The Beijing Rules')," United Nations Human Rights Office of the High Commissioner, General Assembly A/RES/40/33, November 29, 1985.
33 "Report of the Commission of Inquiry on Syrian Arab Republic to the forty-eighth regular session of the Human Rights Council."
34 "Technical Visit to the Northeast of the Syrian Arab Republic: End of Mission Statement," United Nations Office of the High Commissioner of Human Rights, Human Rights Special Procedures, July 21, 2023; "Punishing the Innocent."
35 "Operation Inherent Resolve Lead Inspector General Report to the United States Congress April 1, 2022-June 30, 2022," U.S. Department of Defense, July 29, 2022.
36 "Punishing the Innocent;" Hogir Al Abdo and Bassem Mroue, "Teenagers from Islamic State families undergo rehabilitation in Syria, but future still uncertain," Associated Press, May 30, 2023.
37 Margolin and Vale.
38 "Punishing the Innocent;" Al Abdo and Mroue.
39 "Aftermath: Injustice, torture and death in detention in north-east Syria," p. 47.
40 "Islamic State children in Syria face a lifetime in prison," BBC, July 14, 2021; "Europe's Guantanamo: The Indefinite Detention of European Women and Children in North East Syria," Rights and Security International, February 17, 2021; Margolin and Vale; "Syria: Repatriations Lag for Foreigners with Alleged ISIS Ties."
41 "Syria: Humanitarian Response in Al Hol camp, Situation report No. 1," UN Office for the Coordination of Humanitarian Affairs (OCHA) via ReliefWeb, April 2, 2019; interview, by Amensty International with deputy co-chair of social affairs in northeast Syria, and Al-Hol camp manager, September 27, 2022, Al-Hol camp. They reported there were approximately 5,000 Iraqis and 4,000 Syrians. "Aftermath: Injustice, torture and death in detention in north-east Syria."
42 "Fifteenth report of the Secretary-General on the threat posed by ISIL (Da'esh) to international peace and security and the range of United Nations efforts in support of Member States in countering the threat."
43 Lili Bayer, "EU memo raises security concerns over mass escape from IS-linked Syria camp," Reuters, February 24, 2026.
44 Devorah Margolin, "U.S. Funding Cuts Risk Jeopardizing Counter-Islamic State Operations," Lawfare, June 4, 2025.
45 "Between two fires: Danger and desperation in Syria's Al-Hol camp," p. 9.
46 "Ninth report of the Secretary-General on the threat posed by ISIL (Da'esh) to international peace and security and the range of United Nations efforts in support of Member States in countering the threat," S/2019/612, United Nations Security Council, July 31, 2019; "Syria: Humanitarian Response in Al Hol camp, Situation Report No. 4 – As of 29 May 2019," United Nations Office for the Coordination of Humanitarian Affairs, May 29, 2019.
47 "Lead Inspector General for Operation Inherent Resolve Quarterly Report to the United States Congress January - March 2019."
48 "Operation Inherent Resolve Lead Inspector General Report to the United States Congress July 1, 2025-December 31, 2025," U.S. Department of Defense, February 17, 2026; "Understanding the Lives of the Women, Men, and Children of Al-Hol Camp."
49 "Understanding the Lives of the Women, Men, and Children of Al-Hol Camp."
50 Ibid., p. 57.
51 Devorah Margolin, "Detention Facilities in Syria, Iraq Remain Vulnerable to Islamic State Attacks," Washington Institute, PolicyWatch 3653, September 29,

2022; "U.S. Central Command statement on Thwarted Suicide Bomber Attack near Um Fakik Village, Syria," U.S. Central Command, September 22, 2022.
52 "Insomnia, nightmares, and wanting to die: Al Hol's children," Save the Children, April 25, 2022.
53 "Operation Inherent Resolve Lead Inspector General Report to the United States Congress January 1, 2020-March 31, 2020," U.S. Department of Defense, May 13, 2020.
54 Daniel Gorevan and Kathryn Achilles, "When am I Going to Start to Live?" Save the Children, 2021; "Twelfth report of the Secretary-General on the threat posed by ISIL (Da'esh) to international peace and security and the range of United Nations efforts in support of Member States in countering the threat."
55 "Operation Inherent Resolve Lead Inspector General Report to the United States Congress July 1, 2020-September 30, 2020," U.S. Department of Defense, November 3, 2020; "Report of the Commission of Inquiry on Syrian Arab Republic to the forty-eighth regular session of the Human Rights Council;" "Humanitarian Update Syrian Arab Republic - Issue 18 / November 2023 [EN/AR]," United Nations Office for the Coordination of Humanitarian Affairs via ReliefWeb, January 3, 2024.
56 "Operation Inherent Resolve Lead Inspector General Report to the United States Congress July 1, 2025-December 31, 2025."
57 "Technical Visit to the Northeast of the Syrian Arab Republic."
58 "Operation Inherent Resolve Lead Inspector General Report to the United States Congress January 1, 2022-March 31, 2022," U.S. Department of Defense, May 3, 2022, p. 77.
59 Fionnuala Ní Aoláin, "Position of the United Nations Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism on the human rights of adolescents/juveniles being detained in North-East Syria," United Nations Office of the High Commissioner of Human Rights, May 2021; "Syria: Repatriations Lag for Foreigners with Alleged ISIS Ties;" "Technical Visit to the Northeast of the Syrian Arab Republic;" "Punishing the Innocent."
60 "Aftermath: Injustice, torture and death in detention in north-east Syria," p. 21.
61 "Operation Inherent Resolve Lead Inspector General Report to the United States Congress April 1, 2024-June 30, 2024," U.S. Department of Defense, August 1, 2024; "Operation Inherent Resolve Lead Inspector General Report to the United States Congress July 1, 2023-September 20, 2023," U.S. Department of Defense, November 9, 2023; "Operation Inherent Resolve Lead Inspector General Report to the United States Congress October 1, 2022-December 31, 2022," U.S. Department of Defense, February 7, 2023.
62 "Operation Inherent Resolve Lead Inspector General Report to the United States Congress July 1, 2025-December 31, 2025."
63 "CENTCOM – Year in Review 2022: The Fight Against ISIS," U.S. Central Command, December 29, 2022.
64 "Operation Inherent Resolve Lead Inspector General Report to the United States Congress July 1, 2025 - December 31, 2025," U.S. Department of Defense, February 17, 2026.
65 "Operation Inherent Resolve Lead Inspector General Report to the United States Congress July 1, 2019-October 25, 2019," U.S. Department of Defense, November 19, 2019.
66 "Syria: Repatriations Lag for Foreigners with Alleged ISIS Ties."
67 Dataset created and maintained by the author.
68 For comparative legal responses, see "Foreign Terrorist Fighters Knowledge Hub," International Centre for Counter Terrorism; Margolin and Vale.
69 "Cumulative Prosecution of Foreign Terrorist Fighters for Core International Crimes and Terrorism-Related Offenses," Eurojust, July 2, 2020.
70 Erinda Bllaca Ndroqi, "Dealing with returned women in the Western Balkans: challenges and opportunities from a practitioner's perspective," European Commission Radicalization Awareness Network, European Union, August 31, 2022; Avdimetaj Teuta and Julie Coleman, "What EU Member States can learn from Kosovo's experience in repatriating former foreign fighters and their families," Clingendael Policy Brief, May 2020.
71 Margolin, "U.S. Funding Cuts Risk Jeopardizing Counter-Islamic State Operations;" James Jeffrey and Devorah Margolin, "Time to Unify the Kurdish Northeast with the Rest of Syria," Washington Institute for Near East Policy, October 7, 2025.
72 Margolin and Cook, "From Bad to Worse in Northeast Syria."
73 Urooba Jamal, Faisal Ali, Zsombor Peter, and Caolán Magee "Syria updates: SDF, government trade ceasefire violation accusations," Al Jazeera, January 19, 2026.
74 Ghaith Alsayed, "U.S. military transfers first 150 Islamic State group detainees from Syria to Iraq," PBS/Associated Press, January 21, 2026.
75 "U.S. Forces Complete Mission in Syria to Transfer ISIS Detainees to Iraq," USCENTCOM, February 13, 2026; "US says over 5,700 suspected ISIL detainees relocated from Syria to Iraq," Al Jazeera, February 15, 2026.
76 "Operation Inherent Resolve Lead Inspector General Report to the United States Congress July 1, 2025-December 31, 2025," p. 29.
77 Devorah Margolin, "Caught in the Crossfire: Islamic State Detention Sites at Risk," Washington Institute for Near East Policy, January 22, 2026.
78 Anne Charbord and Fionnuala Ní Aoláin, "A Legal Black Hole: Does Iraq Have the Right to Detain Prisoners Transferred from Syria?" Just Security, February 11, 2026.
79 Sinan Mahmoud, "Dozens of minors among ISIS prisoners transferred to Iraq from Syria, judiciary authorities say," National, February 17, 2026.
80 "Iraq repatriates Finnish minor, US national after ISIS probe," New Region, April 14, 2026.
81 Tim Arango and Eric Schmitt, "Escaped Inmates From Iraq Fuel Syrian Insurgency," *New York Times*, February 12, 2014; Bennett Clifford and Caleb Weiss, "'Breaking the Walls' Goes Global: The Evolving Threat of Jihadi Prison Assaults and Riots," *CTC Sentinel* 13:2 (2020): pp. 30-40.
82 "Iraq Fears Prison Holding ISIS Fighters Could Be Breached as Strikes Intensify Near Baghdad Airport," Kurdistan24, March 15, 2026.
83 Jared Malsin and Dustin Volz, "U.S. Intelligence Says at Least 15,000 at Large After ISIS Detention Camp Collapses in Syria," *Wall Street Journal*, February 20, 2026.
84 Margolin and Cook, "From Bad to Worse in Northeast Syria."
85 William Christou, "NGOs sound alarm as foreign families flee camp holding suspected IS members," *Guardian*, February 13, 2026; Margolin and Cook, "From Bad to Worse in Northeast Syria."
86 Syrian Arab News Agency, "[The official spokesperson for the Ministry of Interior stated in a press conference: The humanitarian situation inside Al-Hol camp was shocking by all standards …]," X, February 25, 2026.
87 "After years of detention former Al Hol residents face uncertain future," Medecins Sans Frontiers, February 27, 2026; Margaux Benn, "The Lives in Limbo of Families Freed from Syria's Al-Hol Camp," *Figaro*, March 12, 2026.
88 Arbjona Cibuku in Tirana, William Christou, and Ashifa Kassam, "'We waited 12 years': escapees from Syria's camps face an uncertain future," *Guardian*, April 12, 2026.
89 "Syria to close camps housing thousands linked to Islamic State," Reuters, January 30, 2026.

Security Lessons from the Paris Olympics for the 2026 FIFA World Cup and Other Major Events

By Alexandre Rodde, David Mcilhatton, John Cuddihy, and Shannen Benton

This article examines how security lessons from the 2024 Paris Olympics can inform preparations for the 2026 FIFA World Cup taking place across the United States, Canada, and Mexico this summer. As the largest tournament in football history, the World Cup will present an unprecedented security challenge spanning 16 host cities, three countries, and millions of spectators. Paris demonstrated the value of intelligence-led counterterrorism, integrated multi-agency coordination, critical infrastructure protection, cybersecurity readiness, counter-drone capabilities, visible deterrence, and effective public communication. Despite a complex threat environment, the Games concluded without any major incidents, highlighting the effectiveness of preventive and adaptive security measures. Applying these lessons to a larger, multi-jurisdictional tournament will require exceptional cross-border cooperation, harmonized planning, and scalable responses to terrorism, crime, sabotage, cyber threats, and public disorder.

When the 2026 FIFA World Cup begins across North America in June, it will represent the largest tournament in the history of international football. For the first time, the competition will involve teams from 48 countries and more than 100 matches hosted across 16 cities in three countries: the United States, Canada, and Mexico.[1] The scale of the tournament will be unprecedented, with millions of spectators expected to attend matches in person and billions more following the event on television and through digital media platforms.[2] For governments and security agencies, however, the tournament represents far more than a major event. Sporting events of this scale have long been viewed as attractive targets for threat actors to cause harm, as they draw large crowds, generate global media coverage, and often carry significant value for host nations. Because of this, even minor incidents before and during these events can attract global attention and cause widespread effects.[3]

A previous article published in *CTC Sentinel* in 2024 by some of the authors[4] examined in detail how terrorist actors have historically targeted or attempted to attack major sporting events around the world, highlighting the motivations, tactics, and vulnerabilities associated with such high-profile gatherings. Rather than revisiting those cases here, this article builds on that earlier analysis by drawing lessons from the security planning and operational experience of the 2024 Summer Olympics in Paris. In doing so, it considers how the terrorist threat environment surrounding major international events has continued to evolve, particularly in relation to emerging risks such as hybrid threats, cyber-enabled disruption, and other related activities such as infrastructure sabotage. It also reflects on how public-facing communication and visitor behavior formed part of the preventive security posture in Paris and how similar approaches might be adapted for the 2026 World Cup.

The 2024 Paris Olympics Threat Environment

The 2024 Paris Olympics took place from July 26 to August 11 without any major security incidents, despite significant concerns in the media and from security commentators regarding its organization and national security planning in the context of a complex and diverse threat landscape. The opening ceremony on the Seine River and the 17 days of competition were protected by an extensive security operation, the scale of which had never been seen before in France and which brought together law enforcement, defense, security, and intelligence agencies; other government departments; and the security teams of participating countries.

This relative success was against the backdrop of a complex threat environment that included state threats, terrorism and extremism, general crime, as well as cyber security challenges that were exacerbated by the geopolitical situation at the time. Although the most severe scenarios that had been anticipated prior to the Games ultimately did not occur, a number of security incidents in the lead-up to and during the event nevertheless drew considerable attention, highlighting the ongoing challenges faced by organizers and law enforcement in ensuring the safety of participants and spectators. These incidents are summarized below.

Alexandre Rodde is a Visiting Fellow at the Protective Security Lab at Coventry University. He works as a security consultant and analyst, specializing in terrorism, mass shootings, and violent extremism in the French national security apparatus. He is the author of Le Jihad en France: 2012-2022 *(not yet available in English).*

Professor David Mcilhatton is Associate Pro Vice Chancellor for Defence and National Security, and Director of the Protective Security Lab at Coventry University.

Professor John Cuddihy is a Visiting Professor in the Protective Security Lab at Coventry, a former Head of Counter Terrorism in Police Scotland, and a consultant for international organizations on counterterrorism.

Shannen Benton is the Head of External Research at the National Counter Terrorism Secruity Office (NaCTSO), part of Counter Terrorism Policing.

Security personnel look on outside Estadio Guadalajara on March 26, 2026, in Zapopan, Mexico, prior to a FIFA World Cup 2026 Qualifying Playoff tournament match. (Luis Cano/Jam Media/Getty Images)

Terrorism and Extremism

As highlighted in the 2024 article "Protecting Major Sporting Events from Terrorism: Considerations for the Paris Olympics and Beyond," jihadism had remained France's principal terrorist threat over the preceding decade and was the focus of heightened scrutiny in the months leading up to the Games. Indeed, globally the jihadi threat, especially from the Islamic State, was particularly high. The network had conducted high-profile attacks in Moscow and Iran just prior to the Paris Olympics and had issued numerous threats specifically targeting the Games through different media sources.

According to the Parquet National Anti-Terroriste (PNAT)—France's national terrorism prosecution office—three major plots were successfully disrupted prior to the Olympics, in the Saint-Étienne, Yvelines, and Gironde regions, resulting in the arrest of approximately 40 individuals.[5] In an effort to preempt potential attacks, French security services conducted 936 administrative searches targeting suspected individuals,[a] while more than 700 individuals were placed under *mesures individuelles de contrôle administratif et de surveillance* (MICAS),[6] which prohibited them from leaving their registered municipalities and required daily reporting to local police authorities. The majority of those subject to MICAS measures were connected to a jihadi network, though individuals associated with violent far-left and far-right extremist groups were also included. Although a limited number of these administrative restrictions were subsequently contested in court, the measures seem to have proven effective in mitigating potential threats and ensuring the security of participants and spectators throughout the duration of the Games.

In one incident, three masked and armed militants declaring themselves members of the *Front de libération nationale corse* (FLNC) made a highly unusual and provocative public intervention at the Ghjurnate Internaziunale di Corti, an annual conference of Corsican autonomist and independence activists in Corte, France.[7] The group took to the stage immediately after a speech by the spokesperson of the contemporary Corsican nationalist party Nazione, with one of the militants reading from a four-page prepared statement.[8] Their speech criticized the rise of far-right politics in Europe, denounced extreme right-wing influence on Corsica, and reiterated longstanding FLNC demands for greater autonomy and recognition of Corsica's status,[9] including calls for the island's inclusion on a list of non-self-governing territories to be decolonized.

Shortly before the Games, French police arrested Abdelouahed El-Baghdadi, the brother-in-law of terrorist Mohammed Merah,[10b] near a fan zone in Vincennes, Val-de-Marne[11] in connection with violence against his roommate. He was listed on a *fiche S*,[12] which identifies individuals considered a potential threat to national security. Although he was unarmed and there was no evidence of a planned attack on the Olympic events, his arrest demonstrated

a Compared to 153 administrative searches in all of 2023. "Pas d'attentat pendant les Jeux de Paris 2024 : le procureur antiterroriste salue le défi relevé Europe 1," AFP, September 11, 2024.

b French terrorist Mohammed Merah killed seven individuals in southwestern France in March 2012; he was subsequently killed in a police standoff. See Scott Sayare, "Suspect in French Killings Slain as Police Storm Apartment After 30-Hour Siege," *New York Times*, March 22, 2012.

the vigilance of French authorities and the importance of close monitoring of known extremist actors in areas of high public concentration.

While not directed at the Games themselves, two suspected jihadi attacks did take place during the time span of the Games. At the Laon correctional center, an inmate armed himself with a broken bottle and attacked prison staff, injuring one guard before being restrained.[13] On the same day in La Ferté-Bernard, a recently released jihadi attempted to harm a taxi driver while recording a video claiming to act in the name of Islam; the victim escaped, and the attacker was arrested by police.[14] Although neither attack disrupted the Olympic events, they demonstrated the continued ability of extremist actors to commit violence and reinforced the need for heightened security during the Games.

To counter these risks, French authorities implemented an exceptionally heavy law enforcement presence in Paris and across the Île-de-France region, deploying approximately 35,000 police and gendarmerie officers daily over the 17 days of competition.[15] This large-scale mobilization not only served as a visible deterrent to potential attackers but also provided rapid response capabilities to contain and neutralize emerging threats. The effectiveness of this approach was demonstrated by the arrest of a 16-year-old jihadi from Haute-Savoie, who was reportedly planning an attack on the La Défense business district in the western suburbs of Paris. Intelligence suggested that he had targeted La Défense specifically because the intensive policing operation in central Paris would have reduced the likelihood of success there.[16]

Sabotage

In the hours leading up to the opening ceremony of the 2024 Summer Olympics in Paris, France's highspeed rail network was the target of a coordinated series of arson and sabotage attacks that disrupted travel across the country and into the host city. In the early morning of July 26, 2024, saboteurs set fires and caused damage along multiple LGV highspeed lines that connect Paris with cities in the north, west, and east, throwing critical rail infrastructure into chaos just as international athletes, officials, and spectators were arriving for the Games.[17] French rail operator SNCF reported that three major lines—LGV Atlantique, LGV Nord, and LGV Est—suffered "malicious acts" that led to widespread delays and cancellations affecting hundreds of thousands of passengers, and another attempt on the LGV SudEst line was thwarted by rail workers who were on site.[18] Authorities described the incidents as "acts of sabotage" that were "prepared and coordinated," and French intelligence services were mobilized to investigate.[19]

The timing and scale of the attacks immediately raised alarms among both French officials and international observers, given their spatial and temporal proximity to one of the most globally significant sporting events. Paris transport hubs such as Montparnasse and Gare du Nord experienced significant disruption, with delays rippling through national and international routes, including services operated by Eurostar, which reported the cancellation of approximately one-quarter of its trains due to the damage.[20] The scale of the disruption was significant with reports suggesting that up to 800,000 travelers were affected by delays and cancellations, with some international delegations forced to adjust travel plans on short notice.[21]

Despite extensive security operations in place for the Olympics, no group immediately claimed responsibility for the sabotage, and authorities did not publicly attribute the acts to a particular terrorist organization or foreign state at the time.[22] Some domestic political figures, including France's interior minister, suggested that far-left extremists might have been involved, reflecting concerns over politically motivated sabotage by groups opposed to the Games or state authority.[23] However, these suggestions remained speculative, and official investigations were ongoing. Some international voices even advanced unverified claims of state-linked involvement, illustrating how such incidents can quickly become entangled in broader geopolitical narratives even without verifiable evidence.[24] What was clear from reporting was that the attacks exposed vulnerabilities in critical infrastructure at a moment of heightened national and international attention, underscoring the importance of protecting the supply chain to the major event as well as the need for comprehensive security planning that extends beyond stadiums and into the wider transportation networks upon which such events depend.

A few days later, another act of sabotage occurred. In this case, fiber optic cabling was destroyed in five locations, the impact of which was that telecommunications and internet services were affected in nine French departments,[25] although no link to the attacks on the rail infrastructure was established at the time and the perpetrators were never identified.

Cyber Incidents

In line with trends observed during previous major international sporting events,[26] cybersecurity formed a key part of the threat environment during the 2024 Summer Olympics, with French authorities confronting a significant number of cyber incidents directed at organizations involved in the preparation and execution of the Games. Responsibility for monitoring and responding to cyber threats was led by *Agence nationale de la sécurité des systèmes d'information* (ANSSI), France's national cybersecurity agency, which coordinated protective security measures across government institutions, Olympic organizers, and private-sector partners.[27] Its cybersecurity approach to the Olympics focused on five main areas: understanding cyber threats; securing critical systems; protecting sensitive information; raising awareness among all stakeholders; and responding rapidly if incidents did occur. Nearly 500 organizations involved in the Games (ranging from venues to service providers) were risk assessed and received technical guidance, security audits, and support for their organizational resilience to cyber attacks.[28]

During the Games, 548 cybersecurity events were recorded, ranging from attempted intrusions to temporary system outages. Most cyber incidents were minor and required little or no intervention, while 83 were confirmed breaches.[29] About half of all reported cyber incidents during the Games involved service outages, including distributed denial-of-service attacks, with the remainder comprising attempted intrusions or exploitation of known or suspected system vulnerabilities. Crucially, none of these incidents disrupted competitions or key Olympic operations, demonstrating that the preventive measures, monitoring, and coordination put in place were effective. Although the cyber security measures successfully mitigated major disruptions, the rapid evolution of digital tools and increasingly sophisticated attack methods means that future events will face a far more complex cyber threat landscape.

Unmanned Aerial Systems

Unmanned aerial systems (UAS, sometimes described as drones) are now a frequent threat to most major public events. UAS offer the capacity to reach venues, areas, and individuals that have been traditionally well protected through extensive protective security planning, and were a significant security concern during the 2024 Paris Olympics and the preceding three-week-long Olympic Torch relay. With the assistance of their Spanish and British counterparts, the French security services were able to conduct 350 missions led by the French Air Force,[30] which resulted in 90 interceptions of UAS and the arrest of 85 UAS pilots during the period of the Games.[31] The vast majority of these arrests were "mainly tourists unaware of the regulations," but at least one case of UAS-use to deliver contraband into a jail was prevented during the Olympics through the use of anti-UAS operations in proximity to the Roissy Charles de Gaulle Airport.[32] Public authorities had launched targeted campaigns ahead of the Games, including Europe-level messaging on drone safety, to warn hobbyist pilots and visitors that flying near Olympic venues and critical infrastructure was prohibited and to emphasize the safety and legal consequences of violations.[33]

UAS offers those seeking to cause disruption and harm new tactics and methods of planning an attack that were previously unavailable. In 2024, the investigation into an attempt to assassinate then presidential candidate Donald Trump at a rally in Pennsylvania identified that the perpetrator flew a drone over the site of the rally in the lead-up to the event, with media speculating that the assailant used the UAS to conduct reconnaissance in the days leading up to the attack, although his motivations are still unknown.[34] Similar deployments have been seen internationally where threat actors have also used UAS in their attack planning.[35] Their ability to extend the distance and methodology of a threat actor, as well as enable physical protective security measures to be breached from the air, has caused significant concern for security planners in recent times[36] and will be a continuing concern for any future major events, including the 2026 World Cup. Their ease of access through affordable, commercial, off-the-shelf UAS has resulted in extensive use among organized crime gangs in Central and South America as well as terrorist and extremist groups in North America and Western Europe with France and Belgium identifying at least four recent incidents involving the use of drone by jihadis, including a plot to target Belgian Prime Minister Bart De Wever with a drone carrying an IED in 2025.[37] Unmanned aerial systems therefore pose a complex threat to major sporting events, offering bad actors a new capacity for disruption and physical harm.

General Crime

Beyond directed actions against the events themselves, incidental threats such as general crime should also be a consideration for organizers. During the 2024 Paris Olympics, the heavy law enforcement presence led to a drop of criminal acts such as assault, theft especially in public transport, auto theft, vandalism, and fraud in the Parisian region but also, surprisingly, in the rest of the country.[38] Gendarmes and police officers arrested 736 people for general criminal acts related to the Olympics, including 451 in the Parisian region. According to the French Ministry of Justice, 212 of these arrests led to pursuits for fraud and economic crimes (41 percent), and for fights, traffic violations, and unlawful drone use (44 percent).[39]

The improvement in public safety as a result of the significant deployment of security personnel was noticeable and commented upon by various national newspapers, leading to a public request for a continuation of "the Olympic truce."[40] In Marseille, authorities announced they were looking at continuing the "legacy" of the Olympic security apparatus due to its efficiency;[41] however, the danger, similar to the Olympics in London in 2012 and the Commonwealth Games in Glasgow in 2014, is that the security operation and reduction in crime creates public expectations of safety and security that outlast the events themselves but that are difficult to sustain due to resource constraints.[42]

General Lessons from Paris

Despite numerous concerns regarding its organization, the 2024 Paris Olympics took place from July 26 to August 11 without any major security incidents. The opening ceremony on the Seine River and the 17 days of competition that included 10,500 athletes and attracted close to 10 million spectators were secured by an important security apparatus in the Parisian region. The attacks in Israel in October 2023 and the Russia-Ukraine conflict added a much greater complexity to the threat environment for the Games. The 2026 World Cup will take place in 16 host-cities across three countries and over 39 days. Between five and seven million spectators are expected to attend the more than 100 games. The current conflict in Iran makes the competition, which is expected to be followed by several billions people across the world, an attractive target for those threat actors who find it purposeful to target civilians or embarrass the countries hosting the competitions. Another area of concern is the power of the cartels in Mexico, one of the host countries of the World Cup, which demonstrated their propensity to engage in violence, cause disruption, and instill fear after the killing of CJNG leader Nemesio Oseguera Cervantes ("El Mencho") in February 2026.[43] This will surely be a consideration for organizers should there be a security incident or operation that impacts these organizations during the World Cup.

Lessons from the Paris Olympics are therefore useful in planning a safe and controlled 2026 World Cup. The Mexican, Canadian, and U.S. security apparatus will have to maintain close cooperation in a complex, diverse, and extremely vast sporting environment, despite differences in language and security culture. As G.B. Jones, FIFA's chief safety and security officer for the 2026 World Cup, has observed, delivering "104 matches in 16 cities in three nations in 39 days" means there is "no handbook" for this tournament and no single domestic agency structure comparable to earlier World Cups.[44] The heavily centralized French security apparatus made internal cooperation between the Police Nationale, Gendarmerie Nationale, and their counterparts in the armed forces and intelligence services simpler than between the various federal, state, tribal, and local agencies of the three organizing countries. The threat environment will also be diverse, from potential riots and organized crime to possible terrorist events taking place in a polarized international context. Therefore, proactive security operations against potential threat actors should be implemented as early as possible.

The counterterrorism efforts in France in the spring leading up to the Olympics proved to be effective and had both short- and long-term effects. Due to the number of facilities and the different levels of readiness of the staff and law enforcement agencies, preparing and training are crucial. The risk for violence, rioting, or chaos will be greater from soccer fans than from the Olympics

attendees, particularly when events at past soccer tournaments are considered.[45] Procedure and responses have to be tested and drilled repeatedly before the beginning of the competition in order to ensure adequacy if an incident were to occur. Finally, security legacy has to be considered long before the end of the 2026 World Cup. The general public will be expecting some if not most of the effects of the security efforts to remain after the competition, leading to complaints about the security posture afterward. Some specific lessons for major sporting events, including the World Cup, follow below.

The Importance of Preventive Counterterrorism Measures

A central lesson from Paris 2024 is the effectiveness of preventive, intelligence-led counterterrorism policing. French authorities disrupted multiple attack plots in advance of the Games and implemented legal controls on individuals assessed as posing a risk. These measures, combined with sustained monitoring of known extremists, probably reduced the likelihood of attack during the event itself. For the 2026 World Cup, it will be essential to ensure that such preventive approaches are effectively coordinated across jurisdictions. Given the transnational nature of the tournament and the current instability linked to conflicts in the Middle East, aligning threat assessments, developing mechanisms to share data and intelligence, and operational responses across host nations will be critical to mitigating risk.

Securing Critical Infrastructure and Crowded Places as a Key Part of Event Security

The coordinated sabotage of France's high-speed rail network immediately prior to the opening ceremony highlighted the vulnerability of infrastructure systems that underpin major events. Although the attacks did not directly target Olympic venues, they caused widespread disruption and demonstrated how adversaries can exploit vulnerabilities to generate impact. This reinforces the need for the World Cup and other major events planners to adopt a systems-based approach to security, extending beyond stadiums to include transportation, telecommunications, and energy networks, as well as the supply chain to these events.[46] Major events rely on complex interdependencies, and disruption to any one component can have cascading effects physically or reputationally. Indeed, Jones, in his recent interview in this publication, highlighted similar concerns with aviation capacity, warning that even routine weather delays at U.S. hub airports can rapidly cascade into large-scale displacement of travelers and accommodation pressures, a risk that will be amplified by the approximately five million people traveling to the United States alone for the World Cup.[47]

Cybersecurity as a Core Security Pillar

Cybersecurity was a prominent feature of the Paris threat environment and that of other major events.[48] Hundreds of cyber incidents were detected and managed, none of which disrupted core Olympic functions. This outcome underscores the effectiveness of a proactive approach centered on early risk identification, comprehensive stakeholder coordination, and the capacity for rapid, real-time response. Looking ahead to future major events, cybersecurity must be understood as a core operational domain rather than a supporting function. The increasing digitization of event infrastructure, including ticketing systems, communication platforms, and logistical networks, significantly expands the potential attack surface available to threat actors. In parallel, the persistence of geopolitical instability is likely to sustain the risk of disinformation campaigns and politically motivated cyber activity.

Addressing the Expanding Threat of Unmanned Aerial Systems

The Paris Olympics demonstrated the growing relevance of UAS as a security concern. Numerous unauthorized drones were detected and intercepted, although the majority of these were tourists who were unaware of the regulations. Nevertheless, the accessibility and versatility of drone technology make it an attractive tool for a range of threat actors, from criminals to extremists. For major event security planners, counter-UAS capabilities will be essential moving forward and must be considered at the outset of planning—particularly when considering the unintentional disruption that counter-UAS technology can create when considered late in the planning phases. This includes not only technological solutions but also clear legal frameworks and public communication strategies. As recent studies have shown, drones are increasingly being incorporated into surveillance, disruption, and attack planning by both state and non-state actors.[49] They are also being used for planning for security at major events. As noted by Jones, drones and counter drone systems are among the newest emergent threats facing the tournament and FIFA has created a dedicated airspace security team to work with U.S., Canadian, and Mexican authorities on consistent mitigation and airspace domain awareness across the World Cup footprint.[50]

The Importance of Deterrence

The large-scale deployment of police and security personnel during Paris 2024 contributed not only to counterterrorism efforts but also to a broader reduction in general crime. However, deterrence in contemporary security environments extends beyond the visible presence of police and security personnel and increasingly depends on the active participation of private sector stakeholders as well as the public. Operators of venues, transport systems, crowded places, and digital infrastructure play a critical role in reinforcing security through the implementation of protective security measures as does the dissemination of clear, security-minded communications. Similarly, informed event attendees and citizens, encouraged through targeted awareness and deterrence messaging, can act as an additional layer of deterrence.

Engaging Spectators and Tourists in Prevention

Paris 2024 underscored that preventative security is not solely the responsibility of states and law enforcement agencies, but it also depends on the informed behavior of spectators, tourists, and other visitors. Public-facing guidance produced ahead of the Games was multi-tiered. Public officials provided practical crime prevention advice, which emphasized information about cyber hygiene and instructions on how to respond to suspicious activity, while private security providers and transport operators issued their own tailored messages for ticket holders and travelers.

There is significant value for future major events, including the 2026 FIFA World Cup, in developing a similarly integrated communication strategy that uses clear, accessible language. This should include consistent approaches on how to report concerns, simple and clear explanations of venue and transport security measures as well as digital-security advice for those using official web and mobile applications and online ticketing services. By

shaping visitor expectations and encouraging basic security-minded behaviors in advance, organizers can reduce inadvertent rule-breaking and create an additional layer of resilience around more traditional policing and protective security measures.

Conclusion

The experience of the 2024 Summer Olympics demonstrates that major events can be secured effectively, even in a high-threat environment, when supported by integrated, adaptive, and intelligence-led security arrangements. For major events, such as the 2026 FIFA World Cup, the central challenge will lie less in replicating the operational measures adopted in Paris and elsewhere and more in adapting and scaling them across a multi-jurisdictional context where differing legal systems, institutional arrangements, and threat environments exist. The five lessons identified should therefore be understood not as a formal framework, but as insights for strengthening future event security planning. CTC

Citations

1 "FIFA World Cup 2026: Fixtures, groups, teams, tickets, host countries, cities and more," FIFA.com, March 29, 2026.
2 "500 days to go: excitement builds for FIFA World Cup 26," FIFA.com, January 27, 2025.
3 Ramón Spaaij, "Terrorism and Security at the Olympics: Empirical Trends and Evolving Research Agendas," *International Journal of the History of Sport* 33:4 (2016): pp. 451-468.
4 Alexandre Rodde, David McIlhatton, John Cuddihy, and Rachel Monaghan, "Protecting Major Sporting Events from Terrorism: Considerations for the Paris Olympics and Beyond," *CTC Sentinel* 17:6 (2024).
5 Alexandre Rodde, "Terrorism in France : Overview of the French Extremist Movements in 2024," National Gendarmerie Research Center, January 2025.
6 "La justice suspend une mesure de surveillance d'une adolescente de 17 ans, soupçonnée de constituer une menace pour la sécurité publique," *Parisien*, August 22, 2024.
7 "Corse : armés et cagoulés, trois militants du FLNC font irruption lors d'un rassemblement d'indépendantistes," TF1, August 5, 2024.
8 Ibid.
9 Vincent Le Goff, Clement Tronchon, and Sébastien Bonifay, "Le FLNC s'invite aux journées internationales de Corte," Franceinfo, April 8, 2024.
10 "Arrest of Mohammed Merah's brother-in-law, on S file and wanted, 100m from the Vincennes fan zone," Entrevue, August 10, 2024.
11 "Le beau-frère du terroriste islamiste Mohammed Merah, fiché S, interpellé à Vincennes," *Figaro*, August 11, 2024.
12 For information on fiche S, see "Terrorisme : qu'est-ce que la fiche 'S'?" *Monde*, October 16, 2023.
13 Alexandre Chassignon, "Agression de surveillants à la prison de Laon: fin de garde à vue pour Ali Riza Polat," *Parisien*, July 23, 2024.
14 Alexandre Chassignon, "Agression d'un chauffeur de taxi en Sarthe : le suspect envisageait d'attaquer la synagogue et un cinéma du Mans," France Bleu, August 9, 2024.
15 "Sécurité des JO 2024 : audition de M. Gérald Darmanin, ministre de l'intérieur et des outre-mer, sur la sécurité des jeux Olympiques et Paralympiques de 2024," Sénat, October 25, 2022.
16 Rodde, McIlhatton, Cuddihy, and Monaghan.
17 Lipika Pelham and Paul Kirby, "French high-speed rail sabotaged before Olympic ceremony," BBC, July 26, 2024.
18 Leila Abboud, Sarah White, Adrienne Klasa, Sara Germano, and Sam Jones, "The Paris Olympics sabotage attack: what we know so far," *Financial Times*, July 26, 2024.
19 "'Sabotage' hits French trains hours before Olympics," France24, July 26, 2024.
20 "Who was behind the arson attacks on railways before the Olympics?" *Foreign Affairs*, July 26, 2024.
21 Tara Cobham, "Saboteurs launch 'malicious' arson attack on France's rail networks hours before Paris Olympics," *Independent*, July 26, 2024.
22 Catherine Porter and Aurelien Breeden, "Rail Sabotage Blights an Olympic Moment for France," *New York Times*, July 26, 2024.
23 Daniel Boffey, "Far left behind rail sabotage before Olympics, French minister suggests," *Guardian*, July 29, 2024.
24 Adam Parsons, "Paris 2024: Who would cause such chaos on France's rail network before the Olympics, and avoid claiming publicity?" Sky News, July 27, 2024.
25 "Sabotage : des réseaux de fibre optique visés," Franceinfo, July 30, 2024.
26 Rodde, McIlhatton, Cuddihy, and Monaghan.
27 "Bilan cyber des Jeux Olympiques et Paralympiques de Paris 2024," Agence nationale de la sécurité des systèmes d'information (ANSSI), September 10, 2024.
28 Ibid.
29 Ibid.
30 "JOP 2024 : bilan de la sécurisation aérienne," Ministère des Armées, September 11, 2024.
31 "Comptes rendus de la commission des affaires étrangères, de la défense et des forces armées," Sénat, October 22, 2024.
32 "JOP 2024 : bilan de la sécurisation aérienne."
33 See "Drone Safety During the Paris Olympics," European Union Aviation Safety Agency, July 23, 2024.
34 "Trump gunman flew drone over rally site hours before shooting the former president," Sky News, July 20, 2024.
35 Nina Kurt, "Weaponised Skies: The Expansion of Terrorist Drone Use Across Africa," GNET, July 30, 2025.
36 Peter Suciu, "Drone Threat Rising As The U.S. Will Play Host To High Profile Events," *Forbes*, November 14, 2025.
37 "En Belgique, un projet d'attentat djihadiste visant le premier ministre Bart De Wever a été déjoué, selon la police," *Monde*, October 9, 2025.
38 "Tableau de suivi statistique de la délinquance enregistrée pendant les JOP 2024," Ministère de l'Intérieur, September 19, 2024.
39 "Sécurité des Jeux olympiques de Paris 2024 : un bilan 'très très bas' de la délinquance," Sud Ouest, August 18, 2024.
40 Geoffray Branger, "JO Paris 2024 : l'amélioration de la sécurité, constatée dans la capitale, pourrait-elle perdurer?" Europe 1, August 12, 2024.
41 Denis Trossero, "Bilan de la sécurité estivale à Marseille : une délinquance en baisse," Mesinfos, September 19, 2024.
42 Dina Rickman, "London 2012: Crime Dropped By 6% During Olympic And Paralympic Games, Bernard Hogan-Howe Says," Huffington Post, November 8, 2012.
43 Vanessa Buschschlüter and Ottilie Mitchell, "Cartel henchmen unleash violence after top drug lord killed in Mexico," BBC, February 23, 2026.
44 Brian Dodwell and Don Rassler, "A View from the CT Foxhole: G.B. Jones, Chief Safety and Security Officer, FIFA World Cup 2026," *CTC Sentinel* 19:3 (2026).
45 Sam Cunningham, "I've witnessed Euros violence up close – England fans are at serious risk," The Paper, June 13, 2024; "South American Football Cup: Violence, Upsets, Surprising Twists," Latin American Post, April 18, 2025; Mario Cortegana and Dan Kilpatrick, "Violence in Mexico forces suspension of soccer games; Mexican Open to go ahead," *New York Times*, February 23, 2026.
46 Rodde, McIlhatton, Cuddihy, and Monaghan.
47 Dodwell and Rassler.
48 Samiksha Jain, "Russian Cyberattacks Target Milan-Cortina Winter Olympics Ahead of Opening Ceremony," Cyber Express, February 5, 2026.
49 Mohammad Eslami and Lauro Borges, "Drones Beyond the State: Non-state Actors and the Evolving Threat Landscape" in *The Drones Race and International Security, Contributions to Security and Defence Studies* (Cham, Switzerland: Springer, 2025).
50 Dodwell and Rassler.