COMBATING TERRORISM CENTER AT WEST POINT

CTC SENTINEL

OBJECTIVE · RELEVANT · RIGOROUS | JULY 2025 · VOLUME 18, ISSUE 7

FEATURE ARTICLE

The War in Ukraine and Drone Terrorism

David Hambling

A VIEW FROM THE CT FOXHOLE

Adam Hadley

Executive Director,
Tech Against Terrorism

Contents

FROM THE EDITORS

What are the impacts of the war in Ukraine on the threat of drone terrorism? That is the question David Hambling addresses in our feature article this month. Specifically, he examines three of the most relevant drone types to counterterrorism—DJI Mavics, FPV racing drones, and Shahed-type long-range attack drones—whose "affordability, accessibility, and adaptability enable precision strikes, bypass traditional defenses, and democratize air power for state and non-state actors alike." In outlining possible defenses against drones, Hambling warns that while "there is currently no good single solution to the drone threat on the battlefield … defense is even more challenging outside of a war situation where readiness is lower, and rules may not allow defenders to engage drones."

Our interview this month is with Adam Hadley, executive director of Tech Against Terrorism, which works to disrupt terrorist activity online. He explains that despite the growth of AI, most terrorist activity online today is still "quite rudimentary. It's sharing content, it's having conversation, it's looking for bomb-making materials, it's doing basic ISR work." Nevertheless, he cautions that "unless we vastly accelerate the pace of our own understanding" of AI tools, "hostile nation-states will overtake us, and the more sophisticated terrorist organizations will as well. It is a race against time."

Nicolas Stockhammer, in analyzing six (foiled or executed) lone actor jihadi attacks in Europe since October 7, 2023, finds "a recurring radicalization pattern involving emotionally vulnerable, digitally native individuals exposed to algorithm-driven Islamist content in social media, but predominantly on TikTok." He writes that a convergence of radical content and the normalization of extremist narratives online, particularly targeted toward susceptible youth, "has transformed contemporary jihadism into a fluid, networked, and increasingly aestheticized movement—one capable of inspiring violence not through clandestine training camps, but through swipeable videos, viral slogans, and online 'tribalism.'"

The pace of U.S. airstrikes against jihadi groups in Somalia has increased significantly in 2025. David Sterman examines "the rationales that have been cited to explain the increase, and what existing evidence reveals about the potential threat to the U.S. homeland."

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: A serviceman of a special unit of a special forces police battalion carries a Domakha reconnaissance drone in the Donetsk region of Ukraine, on May 2, 2025. (Dmytro Smolienko/Ukrinform/NurPhoto via Getty Images)

Moving Targets: Implications of the Russo-Ukrainian War for Drone Terrorism

By David Hambling

Small and commercially available drones in the hands of violent extremists pose a rapidly growing terrorist threat. This article examines that threat in the light of the invasion of Ukraine. Consumer drones such as DJI Mavics, FPV racing drones, and Shahed-style one-way attack drones have become potent weapons. Their affordability, accessibility, and adaptability enable precision strikes, bypass traditional defenses, and democratize air power for state and non-state actors alike. This article details how these drones have been used in Ukraine—from grenade-dropping quadcopters to long-range strategic attacks—and highlights their potential adoption by violent extremist organizations (VEOs). The second part of the article assesses the implications for global counterterrorism, emphasizing the psychological impact, scalability, and low operational risk of drone attacks. It concludes by outlining countermeasures, including electronic jamming, physical barriers, kinetic interception, and the growing role of drone-on-drone defense, urging a comprehensive and adaptive response to this multifaceted and accelerating threat.

A trailer towed by a truck pops off a false roof, releasing dozens of miniature kamikaze drones that wreak havoc on a nearby military airbase. Dozens of aircraft are severely damaged or destroyed, amounting to billions of dollars in losses. This scenario used to be the stuff of Hollywood action movies but has now played out in real life, specifically in Ukraine's Operation Spiderweb against Russia at the beginning of June 2025.[1] More importantly, the underlying capability is based on commercial, commodity hardware and software that is available to everyone. Any actor can acquire and fly drones, carry out precision strikes from a significant range, and bypass legacy defensive measures. This reality has significant implications for terrorism.

Small drones first entered the terrorism discussion in 2014.[2] In Iraq, the Islamic State utilized a number of different drone types, including consumer quadcopters[3] and Skywalker X-8 hobbyist fixed wing drones carrying explosives.[4] These caused alarm and delayed operations, but inflicted little serious damage and were largely countered by U.S. jamming.

But since then, the threat has evolved. A combination of technology and expertise has transformed small drones into the deadliest threat on the battlefield. According to a recent report by RUSI, small drones now "currently account for 60-70% of damaged and destroyed Russian systems" in the conflict with Ukraine.[5] To put it another way, small drones are inflicting twice as much damage as everything else—artillery, rockets, tanks, missiles, mortars, aircraft—put together. And these are drones that, unlike advanced military hardware, are available to, and affordable by, everyone.

At the same time, larger, low-cost drones assembled from commercial components[6] have become the most common weapon for long-range strikes, with aircraft, ballistic, and cruise missiles featuring less on the battlefield.[7] Many one-way attack drones are assembled in dispersed garage workshops,[8] and the technology is within the reach of well-supported violent extremist organizations (VEOs).

A complete account of drone use in the Ukraine conflict would be prohibitively lengthy. This article instead examines three major types of drones that are most relevant in a counterterrorism context: modified consumer drones, FPV kamikaze drones, and Shahed-type long-range attack drones. This first part of the article describes each of these types and their use and production. The second part examines how these drones contribute toward the terror threat and how the risks from terrorist drone attacks might be mitigated. The article closes with an outline of proposed countermeasures to combat the threat.

Part 1: Three Types of Threat Drone

"Mavics": Combat Quadcopters

Dai Jing Innovations, universally known by its initials DJI, is the biggest drone maker in the world, commanding approximately 70 percent of the global market.[9] Based in Shenzhen, China, DJI was not the first company to make a consumer quadcopter, but it was the first to realize its full potential as an aerial camera in 2013 with the Phantom (now Phantom 1).

The Phantom 1 quadcopter[10] was an immediate success. Flight time was just 15 minutes and top speed 22 mph, but the stabilized video camera and simple user interface gave operators an unprecedented ability to start flying immediately and capture footage previously only possible with a helicopter. The drone autopilot did most of the work, and the Phantom could automatically hover in place even in windy conditions. The control range was a modest 300 meters, and it was priced at $629 ($867 today).

DJI plowed early profits into R&D and developed a high level of vertical integration as well as economies of scale and quickly

David Hambling is an author, journalist, and consultant specializing in military technology, especially drones, and is based in South London. He writes for The Economist, Forbes, New Scientist, Aviation Week, *and other publications. His 2015 book,* Swarm Troopers: How small drones will conquer the world, *anticipated the rising to dominance of small UAS.*

A fiber optic-controlled drone is designed for the Ukrainian Armed Forces in the Kyiv region, Ukraine, on January 29, 2025. (Maxym Marusenko/NurPhoto via Getty Images)

overhauled the competition. They brought out new, more capable drones on an annual basis, much like the smartphone industry of the same era.

In 2016, DJI brought out the first of its Mavic series, which has become the company's flagship product. These fold up small enough to fit into a cargo pocket for easy transport but boast impressively capable cameras and other features. The latest version, the 2025 Mavic 4 Pro,[11] has a flight time of 51 minutes, a top speed of 54 mph, and three cameras including a specially engineered 100 MP Haselbad and can shoot 6K video. The Mavic 4 can be operated at a range of more than 20 miles. All this capability costs under $2,500, although it is not available in the United States due to a variety of issues including tariffs.[12]

In Ukraine, Mavics have become the de facto standard for small unit reconnaissance[13] and artillery spotting, and 'Mavik'/Mavic is used generically as a term for consumer quadcopters on the battlefield. These are modified on an industrial scale with 'hacks' to prevent the drone broadcasting its identity and location.[14]

In addition to providing eyes in the sky, Mavics are also light bombers or 'drop drones.' While they are not designed to carry a payload, they have abundant spare power for the task. There was some small-scale use of quadcopters as bombers in the Donbas region before 2022,[15] but both sides now used them extensively. The typical drop drone is an unmodified Mavic with a 3D-printed harness strapped to it. The drone has an external LED light controlled by the operator; a sensor on the harness uses this light to trigger bomb release. Similar kits are sold to consumers for dropping fishing bait.[16] Mavics were initially armed with modified 30mm grenades[17] or hand grenades, but increasingly, both sides are fielding custom-made munitions. The Russians produce factory-made drone bombs,[18] while the Ukrainian effort is more artisanal.[19]

The most commonly seen drone bomb is a modified antipersonnel Vog-17 grenade weighing 350 grams (less than one pound). This has tail fins added for stability, and the usual setback fuse (armed by firing from a launcher) is replaced with a simple impact fuse. The warhead is high explosive/fragmentation. Although the effective radius is claimed at six meters, it frequently fails to incapacitate the target and multiple drops are needed. Mavics typically carry two Vog-17 type munitions or one larger grenade. This is typically a fragmentation hand grenade like the F1, but drones have also been observed with thermobaric grenades,[20] thermite,[a] shaped charges such as modified US 40mm M433 'Golden Egg' grenades,[21] and tear gas.[22]

There have also been examples of drop drones armed with

a Thermite is a mix of powdered metal and powdered metal oxide that burns at very high temperature. It is used for industrial welding and military demolition as it can melt/burn through metal. See David Hambling, "Why Thermite Is Drone Bombers' New Favorite Weapon," *Forbes*, July 12, 2024.

Molotov cocktails[23] or other incendiary mixtures.[24] A civilian version of this incendiary drone technology is used for controlled burns in the United States.[25] The drones can also act as minelayers, with one Mavic carrying up to eight PFM-1 "butterfly" antipersonnel mines.[26]

A skilled operator can drop grenades with great accuracy, thanks in part to the rock-steady hover function that allows the drone to be precisely positioned above a target. Abandoned vehicles are routinely destroyed by drone-dropped grenades through open hatches.[27] Uncovered foxholes and trenches, which provide protection from other weapons, become deathtraps when there are drop drones around. There are also videos of Mavics pursuing and bombing foot soldiers running away at speed. More recently, Mavics have been equipped with improvised shotgun attachments.[28] These fire a standard 12-gauge cartridge and are used to shoot down other quadcopters,[29] though they could also be employed against ground targets. One Mavic can carry two shotgun tubes.

Fast First Person View Drones

While the Mavic is affordable compared to military hardware—comparable military drones cost 10 times as much—the Ukraine conflict saw a demand for something even less costly for one-way attack missions: the first person view (FPV) drone. In the civilian world, FPV drones are racing quadcopters. They lack the complex sensors, control, and software of the Mavic in favor of more powerful engines. The operator wears viewing goggles, which gives them a drone's eye view essential for rapid maneuvering, which is the essence of FPV racing. Contestants negotiate a small track and fly through hoops at speeds of over 100 mph.

In Ukraine, soldiers who had been FPV enthusiasts in civilian life modified the racing drones into guided missiles by adding warheads,[30] typically RPG-7 or RKG-3 anti-tank grenades. These are much larger than the munitions carried by Mavic, thanks to the drones' more powerful engines. A typical FPV carries two kilograms, but there are larger versions such as the Queen Hornet[31] with a payload capacity of over seven kilograms depending on requirements. Such drones typically cost less than $500 to assemble.[32] The FPVs proved extremely effective and were produced first by the dozen, then by the thousand, and now in massive quantities. Ukraine aims to purchase 4.5 million FPV drones in 2025.[33]

FPVs have become the main anti-tank weapon in the Russo-Ukrainian war and also account for a large proportion of other targeted armored vehicles. With a range of 20 km and high precision, they are used for counter-battery fire against artillery.[34] To destroy an artillery piece, the FPV has to hover a few inches away from the barrel before detonating a shaped charge. The ability to hit fast-moving targets makes them effective against light vehicles—from trucks delivering supplies to Russian assault troops on motorbikes and ATVs. Their low cost and abundance mean FPVs are used freely to target individual Russian foot soldiers.

FPV payloads range from RPG warheads and other shaped charge munitions to fragmentation and thermobaric rounds capable of leveling buildings.[35] "Dragon drones,"[36] FPVs using thermite dripping red-hot material, can set alight hundreds of meters of tree line in a single mission. There are also Claymore-type antipersonnel fragmentation munitions,[37] which are carried on a drone and triggered by an operator at a distance to cover a wide area. In the last year, there has been growth in FPV interceptor drones[38] used to bring down fixed-wing scouts, and there have been a number of reports of FPV drone attacks on helicopters.[39]

"Battlefield FPV drones were used in the well-known Operation Spiderweb against Russian airbases in June 2025 ... While a similar operation would be highly ambitious for VEOs, all of the elements required are easily available. A smaller-scale effort using pre-positioned drones against a soft target such as an airport could be executed with much less effort than Spiderweb."

Basic FPVs can be assembled in a few hours from commercial components, mainly Chinese. Ukraine's Victory Drones effort teaches civilian volunteers how to assemble drones[40] from scratch using nothing more than a screwdriver and soldering iron, with a list of parts that can be purchased online. One volunteer might, for example, make 10 drones a month, which are sent for quality control checking before being shipped to the front.[41] Additional features, such as thermal imagers, significantly add to the cost, with even a low-grade imager costing $250 or more.[42]

In the last year, makers have introduced FPVs controlled via a fiber-optic cable rather than radio. This also adds $200 or more to the cost,[43] and the weight of the fiber spool reduces the FPVs payload capacity. But these fiber drones are immune to radio-frequency countermeasures and detection. Early fiber drones had limited range, but 10-20 km is now standard and the Ukrainians claim to have to destroyed targets from 42 km away with fiber drones.[44]

In another development, increasing numbers of FPVs are fitted with machine vision and lock-on-target lock.[45] Again, these add a few hundred dollars to the price but allow the operator to lock on to an objective so that even if communication is lost, the drone will still hit the designated target. More advanced versions of this capability will automatically select the most vulnerable point of the target.[46] Some makers, such as Ukraine's Saker, produce systems that are able to spot, identify, select, and engage targets without human intervention.[47]

Battlefield FPVs are still evolving quickly in Ukraine, and there is no sign of an end stage. Battlefield FPV drones were used in the well-known Operation Spiderweb against Russian airbases in June 2025.[48] In this case, the drones were piloted remotely by a 4G LTE connection over the Russian cellphone system. They also had backup AI targeting, which in some cases completed the task of guiding the drone to a target aircraft. Even a few kilos of explosive were enough to set four-engined aircraft ablaze. Israel carried out a similar attack with drones smuggled into Iran[49] at the outset of Operation Rising Lion, also in June 2025. While a similar operation would be highly ambitious for VEOs, all of the elements required are easily available. A smaller-scale effort using pre-positioned drones against a soft target such as an airport could be executed with much less effort than Spiderweb.

Shahed-Style One Way Attack Drones

The Iranian-designed Shahed-136, known in Russia as Geran-2,[50] is a low-cost, long-range, one-way attack drone with a wingspan of seven feet. Driven by a propeller, it flies at a modest 120 mph and typically carries a 45-kilogram warhead. Russia has built these drones by the thousands, and Ukraine experiences nightly barrages of Shaheds targeting civilian buildings and energy infrastructure.

The Shaheds have evolved rapidly throughout the campaign. Although there have been no major changes, modifications include improved, increasingly jam-resistant satellite navigation[51] and a variety of different warheads.[52] Later versions are credited with 'stealth' properties[53] with a black exterior that makes them harder to see at night and is claimed to reduce their radar signature.

The claimed range of the Shahed-126 is 2,500 km. Actual range is unknown but, in some cases, exceeds 1,200 km, and longer ranges are certainly possible.[b] The drones typically follow an indirect route to avoid air defenses and remain at high altitude—5,000 to 8,000 feet or more[c]—until they are over the target area.

Some Shaheds have been found fitted with 4G modems and Ukrainian SIM cards. Rather than enabling remote piloting, the purpose of these appears to be to determine which drones complete their mission or where they are downed[54] so that follow-up attacks can avoid air defenses. They may also allow drones to be rerouted in flight. Individually, Shaheds are easy to counter, but stopping hundreds of them is another matter. Shaheds cost perhaps $35,000 each[55] and can easily be mass produced. A surface-to-air missile like the Patriot PAC-3 costs millions and the United States can only make several hundred a year.[56] Even the shoulder-launched Stinger missile costs $480,000 per shot[57] and stocks are limited, while Russia is launching thousands of Shaheds per month.

Ukraine has countered the Shahed with a layered array of defensive systems. In addition to surface-to-air missiles, there are hundreds of mobile fire units equipped with anti-aircraft machineguns with thermal imagers and tablet computers. These teams are moved into position to intercept the slow-moving Shaheds. High-flying Shaheds may be intercepted by F-16s, others by helicopters using machineguns or automatic cannon. These are supplemented by large-scale electronic warfare systems and supported by networks of radar and acoustic sensors that track incoming drones. At one point, these were intercepting over 90 percent of the Shaheds,[58] though this had dropped as the barrages became heavier.

Ukraine has developed its own equivalent attack drones such as the AN-196 Lyutyi[59] and UJ-26 Bobr,[60] and has used them to set Russian oil refineries and storage facilities ablaze.[61] Ukrainian drones have also hit military factories, airbases, and other strategic targets. The warhead of such drones is much smaller than the 500-kilograms-plus of a typical cruise of ballistic missile. But it is more than sufficient to damage or destroy anything except the largest and most heavily hardened targets. As terror weapons, multiple small drones can create a much greater effect, and have a much greater chance of getting through, than a single missile. And a group that could never aspire to acquire a ballistic missile could acquire attack drones comparatively easily.

While such drones are significantly more challenging to acquire than Mavic or FPVs, they can still be assembled from basic components in a garage workshop. Ukraine's drone production is highly decentralized. One maker, Terminal Autonomy,[62] uses wooden airframes manufactured the same way as flat pack furniture.[63] And even the Russian state manufacturer uses commercial electronics, many of them smuggled in from the West,[64] rather than expensive custom electronics.

Part 2: The Terror Drone Threat, And Countering It

The three types of drones discussed above all present particular terrorist threats. Mavic-type quadcopters with drop drone kits are the most easily accessible and can be acquired by anyone with nefarious intent. In fact, there has already been at least one notable case of drone bombing in the United States, when Jason Muzzicato used a DJI drone to drop home-made bombs on his ex-girlfriend's house in 2019.[65] It is only surprising that such attacks have not been more common.

VEOs could use Mavics to scout a site in preparation for an attack, identifying and locating security measures. It is now easy enough to build a detailed 3D model of an area[66] by flying a drone over it and feeding the camera data into an app. But most concern will be over drones used for attacks. Mavics can bypass walls, fences, and other barriers against terrorist attack, fly (in many places) over security personnel with impunity, and reach into supposedly secure areas including sports stadia and airports.

Mavic-type drones, even without warheads, also present a significant terror risk to aircraft in flight. The most obvious danger is that drones would be deliberately flown in the approach to an airport, in the path of incoming airliners. Impact at 200+ mph is likely to cause severe or possibly catastrophic damage.[67] Bird strikes are relatively mild because birds are essentially soft, low-density organic material. Drones, however, which have higher density and include hard components like batteries, are a much greater hazard to both jet engines and cockpit glass.

FPVs require more resources to acquire and greater skill to operate than Mavics. They can carry out a precision attack from many miles away, even reaching across national or other borders. Again, most security methods that keep attackers at a distance away are ineffective against attackers with drones. The high speed means there may be little warning of an FPV attack.

The larger payload of FPVs compared to Mavics means they can inflict significantly more damage. This applies with fragmentation weapons to cause mass casualties, with thermobaric warheads to damage structures, or with other payloads such as chemical agents. "Dragon drone" attacks might be spectacular rather than dangerous, though there is a risk with flammable targets and they could cause sudden massive wildfires under the right conditions. Fiber drones present the added threat of infiltrating buildings to seek targets inside. In Ukraine, this is mainly a matter of locating vehicles inside garages and hangars[68] but could equally be applied in an urban environment.

b "The range of the 136 version has been estimated by various analysts as anywhere between 1,000 and 2,000 km … If the fuel tanks are located in the fuselage, then its increase in length from 2.6 to 3.5 metres provides a 35% increase in fuel volume. Hence, it stands to reason that the Shahed 136 has a range somewhere between 1,350 and 1,500 km." See Uzi Rubin, "Russia's Iranian-Made UAVs: A Technical Profile," RUSI, January 13, 2023.

c "Starting from February-March 2025, the Russian occupation forces began using Shaheds not in the traditional lowpass format—flying at extremely low altitudes—but instead at average altitudes of 1,500 meters over mainland Ukraine and 2,000–2,500 meters from maritime directions." Alexander Kovalenko, "Alexander Kovalenko: Russia has changed its tactics of "kamikaze" drone strikes on Ukraine," Odessa Journal, April 14, 2025.

Increasing autonomy opens the possibility of an attack without a human operator on the spot. Drones could be pre-positioned for an attack, with the perpetrators leaving the country before it is carried out. It also means that multiple drones can be flown at once without the need for skilled pilots. In principle, a single terrorist could activate dozens of autonomous drones and send them to seek targets simultaneously.

Both Mavic and FPV drones can create a considerable psychological effect just by their presence. The buzzing of rotors carries well, and in Ukraine, the presence of drones is enough to keep troops lying low in their dugouts. They would likely have a similar effect on civilian targets and might be able to trigger panic behavior crowds. This psychological impact could be dangerous even if the drones are unarmed or deliver a dummy payload such as smoke bombs or harmless white powder.

Drones have a further appeal to VEOs in that attacks are self-documenting. Drones shoot video constantly in flight, so attacks are recorded in detail. FPVs only show attacks up to impact, but follow-up FPVs or accompanying Mavics can show the aftermath. The political impact of a terrorist incident is measured in part by the amounts of news coverage it receives. By filming their own attacks, VEOs can release their own version of an attack on social media or other platforms, and this is likely to gain attention. Again, in Operation Spiderweb, without Ukrainian video Russia could simply have denied the attacks did any damage. The dramatic footage went viral, though, and made front pages and TV opening headlines worldwide.

Shahed or Bobr type drones represent a different type of threat, one which is more likely to come from large organizations such as Hamas, Hezbollah, or the Houthis, all of whom have access to Iranian drone technology. Iran in particular has supplied clients with drone hardware. (Note that the Houthis used long-rang attack drones to successfully strike airports and oil facilities in Saudi Arabia in 2022,[69] and reportedly against targets in the UAE that same year.[70])

There is no specific limit to the range that such drones can reach. While the current generation seen in Ukraine are currently reaching around 2,000 km, a U.S.-made drone with a 36-foot wingspan with global reach developed for the U.S. military by a commercial company has been seen.[71] Ultra-long range strikes drones could carry warheads far enough to start fires at oil or gas storage or processing sites, destroy parked aircraft, or cause mass casualties in a crowded area. In the next few years, VEOs around the world may be able to threaten targets in the United States from their own countries.[72]

While some may focus on the larger systems and more elaborate possibilities suggested by Operation Spiderweb and Shaheds, the low end may be more important. In Ukraine, the small drones did not come from the aerospace industry but from the soldiers themselves.[73] Drone users appreciated the possibility of drones on the battlefield. Soldiers with FPV experience before the conflict put their FPV knowledge to use after hostilities erupted.

There has been a rise in opportunistic terror attacks with actors using the tools on hand, such as motor vehicles.[74] Munitions tend to be the most challenging aspect of an operation, and skilled bomb makers are usually in shorter supply. But there are millions of drone users, and drones enable attacks without explosives. Incendiaries, including thermite, are easier to acquire and deploy than bombs, as are shotguns and other firearm attachments. Even at the lowest level, the kinetic effect of an FPV armed with nothing more sophisticated than a two-kilogram metal spike should not be underestimated.

Drones also give the appearance of being able to carry out risk-free attacks. Unlike the suicide bomber, the shooter, or the perpetrator of a car-ramming VAW [vehicle as a weapon] attack, the drone operator may feel there is no immediate personal risk. Forensics may allow such drones to be traced to their source, but this may not deter a reckless or foolish drone terrorist.

Countering Terrorist Use of Drones

As the war in Ukraine shows, there is currently no good single solution to the drone threat on the battlefield. Defense is even more challenging outside of a war situation where readiness is lower, and rules may not allow defenders to engage drones. That said, there are three main methods of defense: electronic, physical and kinetic.

Electronic defense consists of radio-frequency jamming of the control signal or the drone's satellite navigation, or other techniques to interfere with or even take over control of the drone. In Ukraine, jammers are universal, from portable 'trench jammers'[75] to vehicle-mounted systems.[76] Reportedly something over 50 percent of FPV drones are downed by jamming, many by friendly fire.

In the United States, jamming is more difficult because of legal restrictions. The FCC only allows GPS signals to be jammed by a few specified authorities, and there are severe limits of other types of jamming.[d] Bad actors are likely to select frequencies that authorities will be reluctant to jam such as those used by cellphone or emergency services. In addition, according to FAA rules, it is illegal to interfere with an aircraft in flight, which includes uncrewed aircraft.[77] While four federal agencies have the power to down drones[78] under some circumstances, this is tightly restricted. Hence, there were hundreds of unauthorized drone flights over U.S. military installations in 2024 without being downed.[79]

In Ukraine, jamming is already being countered by a variety of methods. In addition to jam-resistant communication and navigation receivers, some are abandoning radio frequency completely. Optical navigation systems, which do not require a satellite signal,[80] are becoming more common. Fiber drones, which communicate via a cable, are now used at scale by both sides, leading to a landscape draped with glittering fibers.[81] And AI-enabled drones that are immune to jamming are also being fielded in larger numbers.[82]

Physical protection against small drones generally means netting.[83] In Ukraine, there have been all sorts of anti-drone nets from basic camouflage netting to repurposed fishing nets to chain-link fences and industrial steel mesh. These are intended to counter FPVs by catching them and preventing them from exploding or making bombs from Mavic-type drones explode prematurely. In some cases, miles of roadway are now enclosed by netting.[84] There have also been some far more ambitious examples of counter-drone protection with entire buildings fitted with steel cages[85] intended to stop larger long-range drones.

There are two problems with netting. One is that FPVs in

d According to current U.S. law, four federal departments—DHS, DOJ, DOD, and DOE—have "express statutory authority to conduct drone detection and counter-drone operations" in the United States. For background, see "Aviation Safety: Federal Efforts to Address Unauthorized Drone Flights Near Airports," U.S. Government Accountability Office, March 18, 2024.

particular have demonstrated an ability to go through any small gaps,[86] limiting the protection it provides. The other is that nets can be damaged by one drone, leaving a gap for others to go through.[87] On the battlefield, any possible protection from drones is seized upon eagerly. It is not clear how well this type of protection will work outside of a war zone. However, in high-security locations where, for example, exposed windows are already fitted with bulletproof glass or blast curtains, it is possible and advisable to add protective measures—netting or other coverings—to prevent drone ingress through any openings.

Kinetic means—shooting down drones with guns and missiles—are widely used in Ukraine. Troops are issued shotguns for close-range defense,[88] and most of the defense against Shaheds is indeed kinetic.[89] But small drones are difficult targets. Shotguns may be a useful last-ditch defense, but there are few reports of them being used successfully. They cannot be considered reliable. The only effective use seen so far is with shotguns carried in interceptor drones to shoot down the opponent's Mavics, which appears to have a high success rate.[90]

As mentioned above, legacy air defenses are useful against single Shahed-type drones but will be quickly exhausted against waves of them. Traditional anti-aircraft guns have been widely used in Ukraine for point defense, including everything from the twin 35mm automatic cannon on German Gepard vehicles[91] right down to antique Maxim guns on anti-aircraft mounts.[92] These work because defenders are networked to the command-and-control system, which detects incoming Shaheds with radar, acoustic, and other sensors so that mobile fire teams can be positioned to tackle them.[93]

Perhaps the most promising protection against Shahed-type drones is new interceptor drones.[94] These vary from basic FPVs to larger fixed-wing models, but are still all essentially small, portable drones, generally with explosive warheads, that can bring down a drone from several miles away. Again, effectiveness relies on a good sensor network so the interceptor can be vectored in on a target in good time. Such drones may be safer in a counterterrorism context than guns or missiles in civilian areas. In particular, net-firing interceptors like those supplied by Fortem[95] (and used successfully in Ukraine) offer a minimum risk of unintended damage. In general, military planners favor a layered kinetic defense incorporating multiple C-UAS weapon types across different ranges. In the very near future, they are likely to be augmented by high-energy laser and microwave weapons with a low cost-per-shot.

Conclusion

Drone warfare has evolved fast during conflict between Russia and Ukraine, and the war has generated drone weapon systems that are directly applicable to terrorism. It is clear from the foregoing analysis that drones present a variety of new threats ranging from an intercontinental drone strike to a mass attack using smuggled drones similar to Ukraine's Operation Spiderweb, right down to domestic terrorists carrying out individual attacks of opportunity with consumer quadcopters.

Countering each of these threat types will require a wide range of responses, and there is considerable work ahead. This will require at a minimum: a comprehensive review of the current threat and how it is likely to change with emerging technologies such as AI-enabled autonomous drones and long-range drones with global reach; a consideration of the threats that these pose and what vulnerable targets need to be protected; a review of the defensive measures that are available and emerging; and a plan of action to put these measures in place and ensure that they are regularly reviewed in line with the changing threat. Plus, of course, adequate funding is required for all these efforts. CTC

Citations

1 "Operation Spiderweb: How Ukraine's Drones Are Pushing Russian Aircraft Back – Visual Guide," *Guardian*, June 2, 2025.
2 Don Rassler and Yannick Veilleux-Lepage, "On the Horizon: The Ukraine War and the Evolving Threat of Drone Terrorism," *CTC Sentinel* 18:3 (2025).
3 Mark Pomerleau, "How $650 Drones Are Creating Problems in Iraq and Syria," C4ISRNET, January 5, 2018.
4 Don Rassler, Muhammad al-`Ubaydi, and Vera Mironova, "The Islamic State's Drone Documents: Management, Acquisitions, and DIY Tradecraft," CTC Perspectives, January 31, 2017.
5 Jack Watling and Nick Reynolds, "Tactical Developments During the Third Year of the Russo–Ukrainian War," Royal United Services Institute, February 2025.
6 David Albright and Sarah Burkhard, "Electronics in the Shahed-136 Kamikaze Drone," Institute for Science and International Security, November 14, 2023; "Dissecting Iranian drones employed by Russia in Ukraine," Conflict Armament Research, November 2022; "Documenting the domestic Russian variant of the Shahed UAV," Conflict Armament Research, August 2023.
7 Benjamin Jensen and Yasir Atalan, "Assessing Russian Firepower Strikes in Ukraine," Center for Strategic & International Studies, October 23, 2024; Benjamin Jensen and Yasir Atalan, "Drone Saturation: Russia's Shahed Campaign," Center for Strategic & International Studies, May 13, 2025.
8 Arno Van Rensbergen, "The EU's defence push risks neglecting drone revolution," *Parliament Magazine*, July 1, 2025.
9 "Connected Commercial Drones Report 2025: Asia-Pacific Leads in Drone Adoption, with DJI Holding a Dominant 70% Global Market Share," Global Newswire, April 8, 2025.
10 See "DJI Phantom 1 Specifications," Dofly, February 26, 2023.
11 "DJI Mavic 4 Pro," Heliguy, accessed July 4, 2025.
12 Sean Hollister, "DJI is skipping the US with its most advanced drone yet," Verge, May 13, 2025.
13 David Hambling, "DJI Mavic Consumer Drones Are Still Russian Soldiers' Favorite," *Forbes*, March 10, 2025.
14 Ibid.

15 David Hambling, "Russia Wants a Pretext for War and These Drones Could Supply It," *Forbes*, February 18, 2022.
16 See, for example, "Mavic Pro - Electronic Payload Release System For DJI MAVIC PRO," Gannet Release Systems, accessed July 2, 2025.
17 "Modified VOG-17 30mm grenades integrated with commercial drones for Russian troops," Army Recognition Group, August 24, 2023.
18 Roman Kretsul, Alexey Ramm, and Dmitry Astrakhan, "[Lightweight - up and running: FPV drones are now producing standard ammunition]," *Izvestia*, December 1, 2023.
19 David Hambling, "Steel Hornets: Inside Ukraine's Amazon For Drone Bombs," *Forbes*, April 2, 2024.
20 Vadim Kushnikov, "Defense forces use Ukrainian-made thermobaric grenades," Militarnyi, February 20, 2023.
21 Thomas Gibbons-Neff and Natalia Yermak, "In a Ukraine Workshop, the Quest to Build the Perfect Grenade," *New York Times*, January 7, 2023.
22 Felix Hoske, Anastasiia Malenko and Sofiia Gatilova, "Ukraine says Russia steps up illegal use of tear gas to clear trenches," Reuters, April 17, 2024.
23 Bruce Crumley, "Ukraine reportedly adapts small drones to drop Molotov cocktails in war with Russians," DroneDJ, March 11, 2022.
24 Roy, "An electronic Molotov cocktail. This Ukrainian incendiary FPV drone …," X, July 24, 2024.
25 Brian Bull, "Drones with incendiary "ping pong balls" are helping crews fight fire with fire," KLCC, September 12, 2022.
26 "Russians Develop New Drone System for Dropping PFM-1 Mines," Defense Express, September 29, 2024.
27 David Hambling, "How Can Ukrainian Drones Keep Dropping Grenades into Open Tank Hatches?" *Forbes*, May 10, 2024.
28 David Hambling, "Russians Field Sawn-Off Shotgun Attachment for Consumer Quadcopters," *Forbes*, May 16, 2025.
29 David Hambling, "Ukraine's Elegantly Simple Recoilless Shotgun Drone," *Forbes*, March 11, 2025.
30 David Hambling, "Ukraine Racing Drone Converted into Loitering Munition Makes Precision Strike through Doorway," *Forbes*, August 1, 2022.
31 David Hambling, "Ukraine Launches Queen Hornet Supersized FPV Bomber Drone," *Forbes*, May 30, 2024.
32 See David Hambling, "The Key Is Pilots, Not Drones: Ukraine's Escadrone on the Skill of Flying FPV Kamikazes," *Forbes*, May 5, 2023.
33 Tim Zadorozhnyy, "Ukraine to buy 4.5 million FPV drones in 2025," *Kyiv Independent*, March 10, 2025.
34 David Hambling, "Spiking the Guns: Precision Drone Strikes Destroy Russian Artillery," *Forbes*, November 6, 2024.
35 David Hambling, "Thermobaric Drones Blast Russian Positions," *Forbes*, January 23, 2024.
36 Howard Altman and Tyler Rogoway, "Thermite-Spewing 'Dragon' Drones Are Ukraine's Newest Battlefield Innovation," TWZ, September 4, 2024.
37 David Hambling, "Ukraine's Flying Claymore Mines Cut Down Russian Infantry," *Forbes*, March 12, 2024.
38 Vlada Toporkova, "Drone-On-Drone War: How Ukraine's FPV Interceptors Are Beating Russia in the Sky," UNITED24 Media, April 22, 2025.
39 Martin Fornusek, "Ukrainian FPV drone hit Russian Mi-28 helicopter in 'historic' feat, source says," *Kyiv Independent*, July 2, 2025.
40 David Hambling, "How Ukraine Is Building a Drone Army at Its Kitchen Tables," *Forbes*, March 7, 2024.
41 Maria Brovinska, "A citizen of Aitivka and an editor assemble drones in their own kitchen: first-hand experience of creating flying weapons," dev.ua, March 2, 2024.
42 "Ukraine launches production of thermal imaging cameras for FPV drones," Militarnyi, October 24, 2024.
43 David Hambling, "How an American Volunteer Helped Kickstart Ukraine's Unstoppable Drone," *Forbes*, December 9, 2024.
44 Vlad Litnarovych, "Ukrainian FPV Drone Sets Record With 42-Kilometer Strike on Russian Tank, Video," UNITED24 Media, May 27, 2025.
45 David Hambling, "Destroying Russian Tanks Is Just the Start for U.S. AI Drone Autopilot," *Forbes*, July 10, 2024.
46 David Hambling, "Cinder Is a New American Autonomous Attack Drone," *Forbes*, May 20, 2025.
47 David Hambling, "Ukrainian AI attack drones may be killing without human oversight," *New Scientist*, October 13, 2023.
48 Artem Mazhulin, Oliver Holmes, Lucy Swan, Laure Boulinier, and Arnel Hecimovic, "Operation Spiderweb: How Ukraine's Drones Are Pushing Russian Aircraft Back – Visual Guide," *Guardian*, June 2, 2025.
49 "Ships, trucks, and suitcases: How Israel reportedly got its attack drones into Iran," *Times of Israel*, June 15, 2025.
50 Uzi Rubin, "Russia's Iranian-Made UAVs: A Technical Profile," RUSI, January 13, 2023.
51 Sofiia Syngaivska, "Russia Reportedly Upgrades the Kometa Navigation Chip for Improved Precision and EW Resilience in its Munition and Shahed Drones," Defense Express, April 25, 2025.
52 "New thermobaric warhead discovered in Shahed," Militarnyi, November 9, 2024.
53 Vadim Kushnikov, "Russian Forces Employ Stealth Tactics: Shahed Drones Go Black to Elude Ukrainian Air Defense," Militarnyi, November 25, 2023.
54 Martin Rosenkranz, "What is the SIM card doing in the Shahed drone?" Militar Aktuell, September 14, 2024.
55 Neil Hollenbeck, Muhammed Hamza Altaf, Faith Avila, Javier Ramirez, Anurag Sharma, and Benjamin Jensen, "Calculating the Cost-Effectiveness of Russia's Drone Strikes," Center for Strategic & International Studies, February 19, 2025.
56 "Lockheed Martin secures US Army Patriot missile production contract," Defense Connect, November 15, 2024.
57 "Missile Interceptors by Cost," Missile Defense Advocacy Alliance, updated February 2024.
58 See Shahed Tracker, "Shahed type OWA-UAS stats Mar2025 [per UA Air Force Reports] …," X, March 31, 2025.
59 Ivan Khomenko, "Ukrainian AN-196 Liutyi Drone, Dubbed 'Ukrainian Shahed,' Receives Major Upgrade," UNITED24 Media, November 25, 2024.
60 "UJ-26 Bober," Metis, n.d.
61 "Drone attack sparks fire at Russian site, reports say oil depot ablaze," Reuters, January 17, 2025.
62 See, for example, "AQ 400 Scythe: Strategic range, Precision munition," Terminal Autonomy, n.d.
63 David Hambling, "Ukraine Launched More Long-Range Attack Drones Than Russia in July," *Forbes*, August 1, 2024.
64 Natasha Bertrand, "CNN Exclusive: A single Iranian attack drone found to contain parts from more than a dozen US companies," CNN, January 4, 2023; "Dissecting Iranian drones employed by Russia in Ukraine;" "Documenting the domestic Russian variant of the Shahed UAV."
65 "Northampton County Man Sentenced to Five Years for Using Drone to Harass Ex-Girlfriend, Illegally Possessing Bombs and Guns," U.S. Attorney's Office, Eastern District of Pennsylvania, September 24, 2020.
66 See, for example, "DJI Terra: Make the World Your Digital Asset," DJI Enterprise, n.d.
67 David Hambling, "What Really Happens When a Drone Strikes an Airplane," *Popular Mechanics*, December 22, 2016.
68 Francis Farrell, "As Russia's fiber optic drones flood the battlefield, Ukraine is racing to catch up," *Kyiv Independent*, May 20, 2025.
69 Aziz El Yaakoubi and Maha El Dahan, "Saudi Aramco petroleum storage site hit by Houthi attack, fire erupts," Reuters, March 26, 2022; "Shrapnel injures 12 at Saudi Abha airport as drone intercepted," Reuters, February 10, 2022; "16 hurt as drone targets Saudi airport; Yemen's Iran-backed Houthis blamed," *Times of Israel*, February 22, 2022.
70 Ghaida Ghantous and Alexander Cornwell, "U.S. condemns deadly Houthi attack on Abu Dhabi; UAE reserves right to respond," Reuters, January 17, 2022; "Timeline: UAE under drone, missile attacks," Al Jazeera, February 3, 2022.
71 See "Topic number AF171-124," SBIR/STTR Transition Program Success Story, U.S. Department of the Navy, 2023.
72 For background, see Don Rassler, "Going the Distance: The Emergence of Long-Range Stand-Off Terrorism," *CTC Sentinel* 17:2 (2024).
73 Samuel Bendett, "Explanation for major volunteer/DIY efforts on both sides in this war …," X, October 12, 2024.
74 "Threefold rise in vehicular attacks in Western countries indicates cars are terrorists' weapon of choice," Henry Jackson Society, n.d.
75 Yevheniia Martyniuk and Ekonomichna Pravda, "The EW backpack revolution: How Ukrainian portable tech jams Russian drones," Euromaidan Press, May 17, 2024.
76 See, for example, "Ex-Pentagon Electronic Warfare Specialist Highlights Implications of Russia's EW Advantage," Military Watch Magazine, May 29, 2024.
77 Rusty Rumley, "Can I Shoot Down Drones Flying over my Property?" National Agricultural Law Center, December 17, 2024.
78 Ashley Deeks and Madison Rinder, "Are Domestic Drone Shoot-Downs Lawful?" Lawfare, February 5, 2025.
79 "Timmons Opens Hearing on Addressing Unauthorized Drone Activity Over Military Installations," Committee on Oversight and Government Reform, U.S. House of Representatives, April 29, 2025.

80 "Unjammable: Ukraine's Blue Arrow Forges a New Path in Drone Warfare with GPS-Free Navigation," Tech Ukraine, June 13, 2025.
81 "Field in Ukraine covered with fiber-optic cables from FPV drones [1125x1500]," Reddit, June 2025.
82 Kateryna Stepanenko, "The Battlefield AI Revolution Is Not Here Yet: The Status of Current Russian and Ukrainian AI Drone Efforts," Institute for the Study of War, June 2, 2025.
83 "Counter Drone Nets," Think Defence, December 26, 2024.
84 WarTranslated, "Ukrainian fighters are once again showcasing a anti-drone corridor …," X, April 4, 2025.
85 Pelusium OSINT, "According to MoD the building in question had drone cage …," X, January 29, 2023.
86 See, for example, "Ukrainian Drone Operator Found a Gap in the Anti Drone Net and Hit the Target," UNITED24 Media, YouTube, June 6, 2025.
87 David Hambling, "Ukrainian Drone Pilots Unimpressed by Russia's Anti-FPV Tunnel," *Forbes*, February 17, 2025.
88 Roman Pryhodko, "28th Mechanized Brigade Begins Training Recruits to Shoot at Plates as Countermeasure Against FPV Drones," Militarnyi, March 16, 2025.
89 See, for example, Aurora Borealis, "How #Shahed launched by the #ruZZian occupiers in #Ukraine are shot down …," X, October 6, 2024.
90 Slava, "The shotgun drone is on the hunt for Russian Mavic again …," X, January 19, 2025.
91 Yuri Zoria, "Gepard flak tank praised as most reliable German weapon in Ukraine," Euromaidan, April 12, 2025.
92 Daryna Vialko, "Ukrainian forces shoot down Shahed drone with rare machine gun," RBC-Ukraine, October 23, 2024.
93 See Lucile Brizard, "Sky Fortress—Ukraine's Acoustic Detection System That Tracks Drones Cheap and Fast," UNITED24 Media, July 1, 2025.
94 Dmytro Shumlianskyi, "First Footage Appears of Ukrainian Interceptor Drone Targeting Shahed," Militarnyi, May 19, 2025.
95 Danny Romano, "What Is a Drone Interceptor?" Fortem Technologies, August 8, 2024.

A View from the CT Foxhole: Adam Hadley, Executive Director, Tech Against Terrorism

By Don Rassler

Adam Hadley CBE is the Founder and Executive Director of Tech Against Terrorism, a public-private partnership dedicated to disrupting terrorists online. Tech Against Terrorism was established as an initiative of the United Nations Counter-Terrorism Committee Executive Directorate (CTED). Hadley is also the CEO of QuantSpark, an AI innovation consultancy.

CTC: You founded and serve as the Executive Director of Tech Against Terrorism and as the founder and CEO of QuantSpark, a consultancy focused on driving innovation through applied analytics and AI. What led you to the field of terrorism studies and the counterterrorism area?

Hadley: My role in establishing Tech Against Terrorism was entirely unexpected and was born out of work that I was doing, studying in a master's program at King's College London. My background is rather eclectic, having studied physics, Middle Eastern studies, Arabic language, and I worked in a range of public and private sector roles over the years in a number of start-ups and consultancies. But I was studying for a master's in Middle Eastern Studies and found myself focused particularly on analyzing Dabiq magazine. Part of my academic background had been in physics and computer science. So, it's trivial to do some natural language processing, and the idea behind my work at King's was to try to understand the nature of how Islamic scripture had been instrumentalized by jihadists and the topic of abrogation within Islamic jurisprudence and in particular how different parts of the Qur'an and Hadith are used selectively or idiosyncratically by political Islam, and in particular violent Islamism. So, my initial work was focused on this crossover between computer science and Islamic theology and terrorism studies. I think this speaks to what I find interesting and innovative, which is cross-disciplinary work. Much of my professional background has been this mix of social sciences and the physical sciences. This is borne out by a lot of what I've done subsequently.

My dissertation was spotted by an official working at the U.N. Security Council. This was at the heyday of the use of the internet by the so-called Islamic State, of course, and the United Nations Counter-Terrorism Committee, which exists underneath the Security Council, had just started a project looking at how the internet was being used by terrorists. Bear in mind, this is 2016. The sheer volume of terrorist content online was really out of control. So, it's serendipitous in the sense that I was working on a simple computational approach to understand and detect Islamic State propaganda, and I was asked to join a research project working with the U.N., which at the time was just a very small initiative funded by the government of Switzerland.

One thing led to another, and eventually, I grew this project into Tech Against Terrorism. Around the same time, I was also working as a freelance data scientist—working on applying data science, analytics, and some basic artificial intelligence techniques to solve various commercial problems within a few private sector businesses in London. It was a very busy year, the result of which ended with me founding Tech Against Terrorism and bootstrapping QuantSpark.[a] Tech Against Terrorism was accidental in a sense, but I suppose, looking back, its establishment was sort of inevitable given the environment at the time and the need to bridge the gap between government and tech platforms and bridge effectively the intelligence gap with regards to understanding how terrorists were using the internet and what we should do about it.

CTC: Can you talk about Tech Against Terrorism—its mission, where it's been, key accomplishments, and what's next for it?

Hadley: For me, Tech Against Terrorism, whilst its establishment—or at least the initial genesis of the work—was unexpected, environmentally, it was almost inevitable that someone would create this type of organization because there's *such* a gap. There are a number of gaps, really. One is how to work alongside government and tech platforms in a non-combative, collaborative fashion, how to bridge that divide. The other is how to bridge this policy and tech divide, which exists within government, within platforms as well. 'Is there a way of using tech within the social sciences or humanities?' With Tech Against Terrorism, that's what I've been trying to do—trying to create a new type of organization that isn't a not-for-profit, isn't a start-up, but is a combination of these two things that's mission-driven, that's purpose-driven, but also operates a lot like a start-up and operates on the basis of trying to understand what outcome it can achieve before it starts doing things.

Tech Against Terrorism is a very small, lean organization. I set out trying to create a small not-for-profit that behaved like a start-up and was incredibly focused on building technology, using technology well, and trying to cut through the noise that often comes with very large, bureaucratic initiatives that governments and large companies are involved with. What I wanted to create was the antithesis of a normal public-private partnership, the antithesis of a normal not-for-profit, an organization focused on operational impact first and foremost. This ethos, I'd like to think, has been a large part of why Tech Against Terrorism has been extraordinarily successful despite being a very small team with very limited funding. And to be clear, I don't want a bigger team. I don't want more funding. The fact that we have this limited budget and limited team size forces us to be more thoughtful about how we can be effective. It's a paradox with organizations that the bigger you get, the less effective you become. With Tech Against Terrorism, being lean is an essential part of our effectiveness.

a Editor's Note: Tech Against Terrorism and QuantSpark were founded in 2016.

CTC: A central part of Tech Against Terrorism's work is the development of tools such as the Terrorist Content Analytics Platform (TCAP). Can you share a bit about Tech Against Terrorism's core tools, who uses them, and their practical real-world value?

Hadley: Tech Against Terrorism is not just focused on working with tech platforms to improve content moderation with regards to terrorist content but also trying to understand how we can use and deploy technology to do it. We have a small engineering team that builds tools, and the Terrorist Content Analytics Platform is one of them. It provides enormous value to hundreds of platforms and is a very simple idea well implemented, which is to support the workflow of our open-source intelligence analysts, speed up the verification of terrorist content, and then alert platforms. Over time, what we've done is built in various tools to archive this material, to hash this material, and to feed this into an automated pipeline of processing leading to alerts, hashing, and archiving. The Terrorist Content Analytics Platform essentially serves to help report verified examples of terrorist content created by organizations that have been designated as terrorist organizations in the U.S. It's a very high threshold for reporting content created by actual terrorists. Through doing this, we've reported hundreds of thousands of pieces of content across the internet, and this is going from strength to strength as we're building out a network of trusted flaggers who can help expand the aperture of this intelligence collection activity.

In addition to this, we're building tools using generative AI, using large language models to determine when content has been removed because we want to understand which platforms need more support or maybe where there's ambiguity or where terrorists are particularly congregating online. We use technology all the time not to replace what we do—human-in-the-loop[b] integration of AI is very important—but to increase the productivity of our team by 10x, which means that whilst we may only have a team of five to 10 people, we're as productive as you might expect from 50 or 100. We also use this technology not only to collect intelligence on where terrorist content is, but to summarize this activity, to analyze this activity, and to produce intelligence assessment products for our stakeholders and partners.

CTC: Can you tell us a little bit about your work at QuantSpark and synergies that might exist between your role there and your role at Tech Against Terrorism?

Hadley: Having the ability to tap into a deep expertise in terms of software engineering, data science, and AI is certainly very helpful. Tech Against Terrorism and QuantSpark are separate entities, but certainly Tech Against Terrorism wouldn't have survived this long were it solely relying on government grants and tech companies. The fact that we've had access to an almost pro bono pool of technical specialists has meant that Tech Against Terrorism has been able to punch above its weight technically. Were we to try and do this at commercial day rates and go to market, it simply would not have been viable.

Long gone are the days when you could just have conferences or just have reports or just have research. You've got to build software these days, even as a not-for-profit. Your primary activity should be building software because, let's face it, the only way you're going to have impact in the world—especially when you're dealing with technology—is if you yourself are a technologist and using technology to have that degree of impact. When I look around the community and look around the space, I wonder if only more people were product managers, if more people had experience building software, we'd be much more productive as a sector.

CTC: With the work that you do at QuantSpark and Tech Against Terrorism, it gives you a unique vantage point of the field. In efforts to combat terrorist use of the internet or online activity, if you had to evaluate the field and community of practice that's focusing on this area, where has it performed well? What are its problems or core challenges? And where does it need to improve?

Hadley: This might sound like a strange thing to say considering I've been doing this for more than a decade, but I still feel like an outsider from the counterterrorism community. Whether that's about me or about the community or something else, I'm not sure. But having a slightly different perspective means that it's a bit easier to see where there are opportunities to do things better. We've got to focus on outcomes first and work backwards. This requires rigorous critical reasoning and analytical faculties and the application of intelligence assessment techniques. Counterterrorism is a space that is quite contested as well, with a very large amount of academic and research interest. This will be a controversial thing to say, but I don't think counterterrorism is a single academic discipline. I think it's quite a complex discipline that involves psychology, sociology, criminology, theology, and all these other 'ologies.'

Now, in terms of what the community could do better, we've all got to acknowledge the fact that counterterrorism is no longer a popular pursuit politically. And terrorists often benefit from complacency. Right now, of course, counterterrorism has been comprehensively defunded within governments, within tech companies. Only last week, a major government counterterrorism team was just fired.[1] At tech companies, this is not a major focus anymore. Yet, regrettably, if we look at the statistics in terms of the prevalence of terrorist content online, it's abundantly clear that terrorist activity has returned with a vengeance on the internet, even though probably the kinetic threat to the U.S. and the U.K. and E.U. is lower than it has been for a while. The use of the internet by terrorist groups operating in other parts of the world has never been higher, and the destabilizing impacts of terrorist groups in Africa, Central Asia, the Middle East, Southeast Asia is peaking. So, I think there is a strategic confusion—I would say in the U.S., in Europe, in the U.K.—that there are just so many state threats and non-state threats for policymakers to digest that counterterrorism has basically, in my view, been completely forgotten. The community is under threat from complacency. It needs to get better at articulating the nature of that threat, and you could argue that this is an overcorrection from a few years ago when there were simply too many people in the counterterrorism space. So, the first thing I would say is there is a risk in my opinion of overcorrecting and there being almost zero capacity to look at over-the-horizon threats

b Editor's Note: "Human-in-the-loop (HITL) machine learning is a collaborative approach that integrates human input and expertise into the lifecycle of machine learning (ML) and artificial intelligence systems." "Topics: Human in the Loop," Google Cloud, accessed July 15, 2025.

Adam Hadley

where terrorism is concerned.

I do think we've lost focus as a community, and we need to refocus on the most egregious threats. And this is a rather crude word, but we need to think about return on investment. We need to think about what our objectives are and how we evidence this. At Tech Against Terrorism, we have an abundance of evidence: content removal, disruption of terrorist-operated websites, and increasingly disruption of live terrorist attacks and threat to life. So, in summary, I would say broadly that the policy-making community has lost interest in counterterrorism and that is a strategic error, but at the same time, the community hasn't helped itself by losing focus and forgetting to work backwards from the intended outcomes.

CTC: Do you think that part of the challenge in the counterterrorism space, particularly when it comes to terrorist use of digital technologies, is just the fragmentation of the landscape, of the different equities that different players have, whether that's government or platforms themselves or those that operate outside of those areas? When I look at the community and the landscape, there are a lot of solutions, and it could be so much more powerful if there was more collaboration in areas where that collaboration made sense. Do you feel the same?

Hadley: Answering that backwards, I'd say that the word 'collaboration' or 'public-private partnerships' are often used quite loosely. We also have to recognize that as a community, there's an extraordinary amount of competition. I run a for-profit company, QuantSpark. I run a not-for-profit NGO Tech Against Terrorism. And I must say, the environment that Tech Against Terrorism operates in is significantly more competitive than a private company. It's a lot less collaborative than the private sector. It's in some ways more ruthless. Especially when funding is so restricted, it's very easy for people in the community to undermine one another by accident. We as a community need to get a lot better at focusing on what we're trying to achieve, and it might be sometimes *not* doing a project because someone else is better at it. Or it might be collaborating. Part of that is the dynamics of this community, and I largely hold funders responsible for this where funders often don't really know enough about the area and fund conflicting programs of activity and don't focus on synergy. And the reason for that is geopolitical: Countries don't want to collaborate. They want to be seen to be doing things. Often, the problem starts because funders want talking points, and that can cause a lot of inefficiency in terms of delivery.

You could argue that the word 'fragmentation' is the word of the decade. We have a fragmented political landscape—internationally, domestically—fragmented technology and tech stack. Certainly, the fragmentation of terrorists to the internet is a function of adversarial shift, which in a sense is a sign that we've all been doing some good stuff. A lot of the low-hanging fruit has already been disrupted, apart from terrorist-operated websites, which is more like 'back to the future.' But a challenge that we're all facing in many disciplines is that the technical complexity of what we're trying to do is increasing faster than our ability as professionals to learn the new technologies. It's almost like technology is alienating ourselves from our own disciplines, and therefore, you might be an expert in counterterrorism and you may be steeped in the theology of a particular organization or the ideology of an organization, but how on Earth can you keep up with the exponential growth created by generative AI? I think *that*, singly, is the bigger challenge we all face as knowledge professionals: How can we keep up with this terrifying pace of technological progress? This is more generally a problem with generative AI. Technology is racing ahead of humanity, and the experts are struggling to keep up.

CTC: It's interesting to hear your comment previously about feeling like an outsider in the counterterrorism field. Because what you just mentioned about the complexity, if you project forward, it really seems as though organizations like Tech Against Terrorism that are trying to bridge the gap and create synergies between social sciences approaches and more technical physical science approaches, computer science, leveraging technology, that's the way we're going to get a better handle on this complexity.

Hadley: The nature of complexity is something we *all* need to be thinking about more and so-called wicked problems.[2] There are so many more wicked problems we have to deal with now, without almost recognizing them as such. Part of this is that quite a few traditional ways of working—let's say in the intelligence community or the counterterrorism community or in government in general—themselves need to be disrupted. This seeming cultural aversion to open-source intelligence is part of the problem. This almost obsession with secret intelligence may have made sense pre-AI, but we're now approaching a singularity where it's possible to gather such a vast array of data, publicly available or commercially available data, that when you combine that with fairly basic approaches and techniques with large language models and agentic AI—again, another controversial thing potentially to say—the entire intelligence enterprise is ripe for disruption. The combination of gathering very large amounts of data and treating it with AI is so

formidable, but there's so much cultural resistance to this that that's the biggest barrier to adoption for technology. It's not actually the technology, but rather change management, fear of the unknown, and individuals perhaps being slightly frightened of things they don't understand.

All of us as professionals need to recognize that our knowledge will become irrelevant and useless more quickly than ever before, that our own kind of utility as knowledge professionals is atrophying with an increasingly limited or short half-life. The way forward really is for all of us to focus on not just keeping up with the news about technology but also embracing studying the application of AI and how to build software that applies this. I firmly believe that pretty much in every discipline, the primary way you're going to have impact is by coding. It's by building software, which is such a radical shift from what we are used to. And generative AI is making it much more accessible as well. You don't really need to be a coder anymore to build software; you just need to have a good idea and access to generative AI tools that can help you prototype software quickly. So, I'm rather hoping that the expertise and creativity that we have in the community can be applied in a more practical and operational sense with regards to software development, because that's really going to be the only way we can deal with the complexity.

Unless we vastly accelerate the pace of our own understanding in this area, hostile nation-states will overtake us, and the more sophisticated terrorist organizations will as well. It is a race against time. It behooves all of us to promote education in this space because there is a very real risk as we go into quite a dangerous geopolitical era that our generals and our policymakers are thinking about bombs and bullets[3] instead of bytes and bits.

"Unless we vastly accelerate the pace of our own understanding [of AI tools], hostile nation-states will overtake us, and the more sophisticated terrorist organizations will as well. It is a race against time. It behooves all of us to promote education in this space because there is a very real risk as we go into quite a dangerous geopolitical era that our generals and our policymakers are thinking about bombs and bullets instead of bytes and bits."

CTC: When it comes to terrorist use of technology and online aspects, what trends or use cases concern you the most? Which do you feel are underappreciated in our community?

Hadley: There are two sides to this. One is, there are push and pull factors. What theoretically could terrorists do? What do they actually do? And what explains the gap between the two? There are lots of things that terrorists *could* be doing, but they appear not to be. A lot of the conversation is about the emerging threats. That's relevant, I suppose, because it's novel, it's new, it's interesting, and we all like to think about the new and the novel. But the reality is the terrorists' use of the internet is pretty similar to what it has been for quite a long time. And yes, there are some qualitative improvements to how they're using technology to produce content, but we haven't seen a big shift with AI.

What I would say is, probably the most concerning trend—which is still very low baseline—is the increased personalization of content for radicalization and mobilization journeys. However, this is still 0.01 percent of activity. Most of the terrorist activity online is quite simple, quite rudimentary. It's sharing content, it's having conversation, it's looking for bomb-making materials, it's doing basic ISR work. An example of this is terrorist-operated websites. We're tracking 400 websites that we assess all of them to be almost certainly owned or operated by a designated terrorist organization. This is terabytes of freely accessible information online, and very little is being done about it. So, there's a lot of hue and cry about AI, but when it comes down to it, the basics have been forgotten. The debate about generative AI seems to be to the exclusion of focusing on common sense, which is terrorist-operated websites and the sharing of obvious content on major social media platforms. So, yes, the trend is towards more personalized content. Generative AI can help that. The trend you've outlined is towards fragmentation across a greater number of platforms, but fundamentally not a lot has changed. We just need to remain alert to terrorists following the path of least resistance.

Not wanting to contradict myself, but one big threat down the line is the use of agentic AI. This is when it becomes easy to create your own bots where you can create your own distributed network of 10,000 social media profiles, posting nonsense and doing so automatically. The barrier to entry for the more technical work is being lowered both for us as specialists in this area but also for terrorists, which means that the use of agentic AI and circumvention techniques to create tens of thousands of accounts online and create terrorist content with abundance is not so far away. We must hope that the major platforms are a few steps ahead and are using generative AI to get ahead of the threat. Because unfortunately, the future is one in which we have many orders of magnitude more content on the internet and many orders of magnitude less authentic content on the internet. And that applies to terrorist content and disinformation.

The final thing I'll say on this in terms of emerging threat is not actually about the terrorist use of the internet, but the increased convolution of hostile nation-state activity online and the role that terrorist content may or may not play in that. Many of our nation-state adversaries are quite opportunistic. Many of them are very thoughtful and within their published doctrine include information operations. Now obviously in the West—in the U.S., in the U.K., in the E.U.—the information environment is largely completely ignored. I suppose the extent to which traditional military think about information operations is dropping fliers from aircraft. It's embarrassingly primitive, but adversaries have information operations at the core of their own military doctrine. As a result of this, we are seeing examples in the public domain of hostile nation-states encouraging terrorist acts, encouraging polarization, creating fake networks of terrorist content. So, talking about the complexity, it's not just about the technology, it's also about the operating environment, where it's going to become increasingly difficult to

distinguish between a nation-state actor pretending to be a terrorist and a terrorist being supported by a nation-state actor. It's going to become much more ambiguous and gray. I think with the specter of hybrid warfare we are experiencing right now, I worry that our doctrine, our investment, our technology, our policy focus is simply not equipped to deal with that degree of ambiguity.

CTC: Speaking of hybrid warfare, we don't hear a lot about the Houthis' online presence and their use of digital platforms and technologies. In prior conversations, the Tech Against Terrorism team has mentioned that the issue deserves more attention. Can you unpack that a little bit?

Hadley: The Houthis have certainly surprised the counterterrorism community with their military ingenuity, but despite their tenacious efforts attacking Israel from Yemen, their kinetic impact remains pretty limited. What demands attention is their full spectrum media strategy across social media and their own websites; they're not trying to terrorize but rather tap into anti-Israel domestic sentiment and shore up their own political support. Their use of the internet also represents a significant intelligence collection opportunity that we're simply not exploiting. Their overarching objective is recognition and international legitimacy as they aspire to control Yemen, which means their military actions are as much about symbolic projection of power as they are about military effect. Here's the glaring contradiction: Whilst they're designated as a Foreign Terrorist Organization under U.S. law, the Houthis operate completely uncontested across digital platforms, producing sophisticated propaganda that directly supports their strategic goals. We're not just missing an opportunity by ignoring the information environment; we're fundamentally misunderstanding how kinetic operations can undermine strategic intent when their propaganda machine transforms every strike into a recruitment tool and legitimacy claim. Since their online information operations are so aligned with their military activity—both serving the same strategic goal of projecting legitimacy—this represents a profound strategic misunderstanding of how to counter organizations like the Houthis. We're ceding the information domain whilst pursuing kinetic solutions that feed directly into their narrative, which shows we've failed to grasp the very nature of this conflict.

This applies to al-Shabaab as much as anyone else. Al-Shabaab's internet activity is one of the most prolific of all terrorist organizations with vast global reach, extensive financial networks, and connections to diaspora communities worldwide. Yet senior policymakers in military and foreign affairs circles seem to completely ignore hybrid warfare as a concept with regards to the terrorist use of the internet. The moment hot conflicts erupted in various parts of the world, everyone forgot about hybrid warfare and the critical role the information environment plays within it. Here's a provocative question: What proportion of defense spending goes on understanding and disrupting the information environment? Is it one percent? A tenth of one percent? A hundredth of one percent? I don't know what it is, but I know it should be significantly more than it currently is. What I do know is that in any serious hostilities, the information environment would be the first battleground—and probably the first one we'd lose.

CTC: You talked about generative AI and AI and terrorism. Specifically related to counterterrorism, what are some of the more important and most interesting use cases that you've come across in that area, and what more needs to be done?

Hadley: I'd split this into three separate buckets. The first is generative AI as a force multiplier for an individual analyst. The second is thinking through generative AI to supercharge organizational processes. And the third is emergent use cases that would never have been possible previously. So, the first one is as an individual analyst or researcher, off-the-shelf generative AI tools when used well, can and do increase productivity, when summarizing content, translating content, extracting information from content. I'm sure many of your readers have spent days upon days transcribing material or coding text or extracting information from screenshots or PDFs; you could argue 90 percent of time doing research historically has been manual grunt work. All of that can be done in milliseconds now, where you can just throw primary research at large language models and you can just structure information and extract information. That's a massive force multiplier. That's already 10x to a good analyst or good researcher, whether in government, academia, or tech companies. There's a misnomer that generative AI is about generating output. Generative AI is good at transforming one format of information to another format of information. So, the primary benefit to all of us now is getting this technology used in our day-to-day workflows as researchers and as analysts. For instance, if you're an intelligence assessment professional, you can even use generative AI to support analytical techniques such as Analysis of Competing Hypotheses (ACH) or you can draft a Cone of Plausibility in seconds, whereas historically that would have taken you days to do and therefore wouldn't have been done in an operational environment.

That's the first wave of things: analysts getting more comfortable using this technology and being allowed to use it and stopping laggards in bureaucracies from stopping the adoption of this technology because there are very safe ways of using large language models. There are open-source, large language models like Llama that you can install locally in an air-gapped environment. So, a lot of the concerns about privacy, about information exfiltration are, in my opinion, overblown and are stopping analysts using this amazing technology, which means that government circles are way behind the private sector, and they're way behind our adversaries.

The second is about workflow. Generative AI is useful to bridge the gaps between systems, to translate information from one type to another, to convert handwritten notes or voice notes into something. A lot of operational processes in the police, intelligence, and wherever is essentially a web of different processes, and generative AI can sit above all of this and fill in the gaps and accelerate existing processes, especially when you're triaging radicalization or mobilization leads. So, especially in the threat space, generative AI can vastly reduce the burden of form-filling and connecting one system to another because it can connect all these things up.

The third is what I call emergent use cases, particularly using agentic AI, where you have a large language model that has its own thought process so it can manage other agents or other technologies. It's almost a metaphysical layer of abstraction above technology where you can get AI to orchestrate other technologies and instruct other tools and technologies to do things. What this means is you can have hundreds, if not thousands of 'workers.' Give it a couple of years and you could probably get an agentic system to do the work of 400 people, provided you are able to describe their

"My hope comes from the fact that the sophistication of the new technologies that are emerging is so great that despite the inertia and lack of focus, the technology will be so powerful that it will provide several orders of magnitude more productivity. My hope is that the scale and the power of generative AI and the data sets that are increasingly available and the ease with which it is possible to build technology to counter terrorism will make up for any deficits and deficiencies in the current counterterrorism landscape."

work clearly enough that it could be delegated. Therefore, a lot of AI adoption is about being very good at delegation. It's trying to explain how to solve a problem clearly with enough context and clarity that an AI can replace that particular process. The third wave is truly mind-bogglingly exciting. If you know how to design these systems and have an abundance of imagination and experience and contextual understanding, you could build an analytical system that could replace 400 analysts. This is potentially extremely interesting with regards to triaging content at scale, in order to find threat to life indicators or even radicalization indicators. If you can get an AI system to do something 80 percent as well as an intern but you can have tens of thousands of them, you then have emergent capability that's unlike anything you have seen previously. That's very hard for people to get their head around because as humans, we believe that a tool must be 99 percent as effective as a human. It doesn't. It needs to be a bit better than an intern. But at scale, it can be incredibly powerful. That's the third wave, which is probably a few years away. I very much doubt government is going to support that sort of work. I'd imagine that innovation will come from the private sector.

CTC: You've talked about how various parts of intelligence process are ripe for disruption, how governments are behind, and the different risks and cultural factors that shape adoption of AI. And then, we have the speed of AI and how things are moving. Do you think that governments are too far behind given where this is going?

Hadley: Yes, undoubtedly. But you never entirely know what's going on inside governments. So, there may well be islands of secret innovation, but certainly, I would sincerely doubt that governments have progressed particularly far. I think it's a combination of lack of funding, lack of imagination, and excessive caution with regards to the legal infrastructure. And in America, you don't really have GDPR or RIPA.[c] Part of the problem with the internet is going on someone's social media profile in some circumstances is considered legally equivalent to in-person surveillance in someone's garden. So, the legal infrastructure is, in my view, really backwards. And what this does is create a climate of inertia. And let's face it, government is already inertial. But combined with this fear about AI, fear about the internet, fear about conducting surveillance, it's a somewhat toxic formula, which is militating against innovation in this space at the very time that we need government to be doing more. And the fact that so many of the leading NGOs in this space are almost bankrupt suggests that there isn't really funding to solve these problems; that many of the social problems we're facing, there aren't many companies prepared to invest in that. There aren't many corporate philanthropists anymore. There aren't many businesses that are prepared to pay to solve the social problems that they help create. So, there is a market failure here as well; I don't think we can assume that the private sector will pick up all the slack.

CTC: When you look out over the horizon and think about how the intersection between terrorism and technology is going to evolve, what concerns you and what gives you hope?

Hadley: What concerns me is that in the absence of a recent major terrorist attack in the West, we've lost leadership. It seems to me that the only way, unfortunately, that this community can focus is through tragedy, and I really hope that we're able to focus based on an objective appreciation of the threat, on things that matter. We shouldn't have to wait for a big terrorist attack to start thinking about counterterrorism. I fear that that is inevitable, that the community will only focus after the next attack, by which point it would be too late.

My hope comes from the fact that the sophistication of the new technologies that are emerging is so great that despite the inertia and lack of focus, the technology will be so powerful that it will provide several orders of magnitude more productivity. My hope is that the scale and the power of generative AI and the data sets that are increasingly available and the ease with which it is possible to build technology to counter terrorism will make up for any deficits and deficiencies in the current counterterrorism landscape.

CTC: Is there anything that we haven't talked about that you want to cover?

Hadley: The key thing is that when countering terrorists, we have to uphold the fundamental values in our society. This is an ethical position, but it's also a pragmatic one because if we dilute our standards, then we let the terrorists win. What the terrorists want really, and what many nation-states want as well, is to undermine

c Editor's Note: "The General Data Protection Regulation, or GDPR, is a European Union (EU) law that governs how organizations within and outside the EU handle the personal data of EU residents. GDPR was adopted by the European Parliament and Council of the EU in 2016 and took effect on 25 May 2018." "What is the General Data Protection Regulation (GDPR)?" IBM, accessed July 15, 2025. The Regulation of Investigatory Powers Act 2000 (RIPA) is U.K. legislation that governs the use of surveillance and investigatory powers by public bodies. It was enacted to ensure that such powers are exercised in a manner compatible with the European Convention on Human Rights, particularly the right to privacy. See "Regulation of Investigatory Powers Act 2000 (RIPA)," U.K. Home Office, updated July 25, 2025.

our collective security and stability and our effectiveness as democracies. In designing counterterrorism programs, respect for human rights and fundamental freedoms—the U.S. Constitution, for instance—is not a nice-to-have; it's a necessity. Otherwise, it undermines everything we are doing from a moral and practical standpoint. We've got to make sure that we don't dismiss parts of counterterrorism that have become a bit distracted by non-core terrorism issues.

And we've got to make sure that policymakers in companies and in government don't dismantle counterterrorism for political purposes, because if they do, we know that terrorists will rebound. There are many areas of contestation in the world, the Sahel, North Africa is one of these areas where there is, without a doubt, state collapse across many countries. It's easy to imagine a world in which we have another Afghanistan, in the Sahel, at a time when governments have lost focus and tech companies are not being held to account. We've got to focus on the threat; we've got to focus on the hard counterterrorism work before it's too late. CTC

Citations

1 Editor's Note: See Jory Heckman, "State Dept lays off 1,350 employees as reorganization nears final phase," Federal News Network, July 11, 2025.

2 Editor's Note: As defined in Horst W.J. Rittel and Melvin M. Webber, *"Dilemmas in a General Theory of Planning,"* Policy Sciences 4:2 (1973): pp. 155-169.

3 Editor's Note: See Adam Hadley, "We Need to Move Beyond Bombs and Bullets to Counter Terrorism," RUSI, September 6, 2024.

From TikTok to Terrorism? The Online Radicalization of European Lone Attackers since October 7, 2023

By Nicolas Stockhammer

The October 7, 2023, Hamas attack on Israel marked a pivotal moment not only in Middle East security policy but also in the global Islamist and particularly jihadi propaganda landscape. This article examines how the ensuing digital "victimhood-revenge" narrative rapidly spread across platforms like TikTok, fueling a new wave of radicalization among adolescents in Europe. Drawing on six European case studies from 2023 to 2025—including foiled and executed attacks in Vienna, Solingen, and Zurich—this article identifies a recurring radicalization pattern involving emotionally vulnerable, digitally native individuals exposed to algorithm-driven Islamist content in social media, but predominantly on TikTok. The analysis conceptualizes this process through the lens of a "Virtual Caliphate Complex" and explores TikTok's role as a low-threshold gateway into extremist ecosystems. By analyzing cross-platform mobilization dynamics, aesthetic framing, and the hybridization of lone-actor terrorism with online support networks, the article underscores the urgency of adapting P/CVE strategies to algorithmic environments. The conclusion suggests possible policy emphasis on content moderation, digital literacy, and platform accountability—particularly in the context of the European Union's Digital Services Act legislation. The article contends that today's prevailing Islamist radicalization pattern reflects not only ideological motivations but also youth-online-culture dynamics and algorithmic influence.

The October 7, 2023 attack against Israel marked a watershed moment not only in the escalation of violence in the Middle East but also in the global jihadi propaganda matrix.[1] Immediately, radical Islamist and jihadi propagandists launched a potent "victimhood-revenge" narrative that was rapidly disseminated across digital platforms.[2] Within hours of the initial attack and the subsequent Israeli counteroffensive, they began framing the events through the lens of victimhood, occupation, and defense of the *umma*.[3] Social media platforms—especially TikTok, Telegram, Instagram, and X—were flooded with images and videos from Gaza, often faked or stripped of context and repackaged with emotionally charged slogans, Qur'anic references, and graphic calls for revenge.[4] Hashtags such as #GazaUnderAttack, #FreePalestine, and #MuslimBrothersInGaza were co-opted by salafi-jihadi influencers to increase visibility among broader Muslim audiences, particularly adolescents. The framing of the war in Gaza as a Western-backed "genocidal" war against Islam served to intensify the perceived moral urgency of jihad, with many posts suggesting that passivity was equivalent to complicity.[5] This message resonated strongly with disaffected or already ideologically primed individuals in the West, some of whom viewed the unfolding conflict as a personal call to action or, as Alexander Ritzmann coined it, a "tribal call to arms."[a]

Crucially, jihadi propaganda portrayed local attacks in Europe as retaliation against direct accomplices of the "Zionist enemy," not as isolated acts of violence, but as acts of transnational solidarity and religious duty."[6] This catalyzed a new wave of online radicalization, particularly among digitally native, under-25 audiences.[7] The dynamic gave rise to a hybrid mobilization dynamic, blending traditional anti-colonial, antisemitic, and pan-Islamist narratives with high-speed, algorithm-driven dissemination models.[8] Without doubt, this has led to a significant expansion of the digital recruitment pool and lowered the threshold for ideological entry into jihadi milieus—especially among lone actors.[9] Salafi-jihadi groups have leveraged this renewed momentum to disseminate a form of a "virtual caliphate,"[10] not only through seemingly innocuous Islamist content on platforms such as TikTok, YouTube, 4Chan, and Reddit, but also via overtly violent jihadi propaganda circulated through Telegram channels and other encrypted communication platforms.[11] On a "lower extremist scale," self-declared Islamist online "influencer preachers" are increasingly emerging as central figures in the phenomenon often referred to as "TikTok radicalization."[12]

This massive digital shift aligns with the broader trend that transnational terrorism in the 2020s has become ubiquitous.[13] Particularly within the jihadi attack spectrum, terrorist acts are no longer confined to major European urban environments but are now occurring even in medium-sized towns and small municipalities, some of them in Germany, Belgium, France, and elsewhere. A

a On January 4, 2024, the Islamic State issued a direct call for a global campaign of violence. In an audio message titled "And Kill Them Wherever You Overtake Them," the group's official spokesperson, Abu Hudhayfah al-Ansari, urged followers to carry out attacks against Christian and Jewish targets. He explicitly instructed Islamic State militants to make no distinction between civilian and military "apostates," reinforcing the group's commitment to indiscriminate violence. See also Muhammad Makmun Rasyid, "How global fatwas on Gaza challenge national religious authority," Middle East Monitor, June 1, 2025; Alexander Ritzmann, "A Tribal Call to Arms: Propaganda and What PVE Can Learn from Anthropology, Psychology and Neuroscience," VOX-Pol, January 2, 2024.

Nicolas Stockhammer is Director of the Research Cluster "Counter-Terrorism, CVE (Countering Violent Extremism) and Intelligence" at Danube-University Krems (Austria). X: @Nic_Stockhammer

striking recent example is Villach, a mid-sized Austrian city in the state of Carinthia with approximately 65,000 inhabitants—best known for its carnival tradition and local ice hockey derbies. In mid-February 2025, Villach suddenly made international headlines when an Islamist-inspired knife attack occurred, allegedly committed by a self-radicalized Syrian asylum seeker. For many observers, the attack there was completely surprising, as Villach is not known for hosting a significant Islamist scene. Yet, the incident raised urgent questions about online radicalization on spaces like TikTok and its impact on extremist violence. Initial evidence suggests that the attacker may have undergone a process of TikTok radicalization.[14]

The constant availability and proliferation of extremist content online has increased substantially and is now easily accessible.[15] The range of such content spans from initially low-threshold and seemingly harmless life advice delivered in Q&A-style videos by salafi influencer preachers (e.g., "Should one shake hands with unbelievers?") to brutal execution footage released by Islamic State militants.[16] Jihadi terrorist organizations have continuously expanded their capabilities in the digital sphere[17] and increasingly use the virtual space to propagate their extremist ideology, often framed through grievance and victimhood narratives that should justify revenge and violence.[18] At the same time, demand for such content has grown steadily, particularly among digitally native demographics such as Generation Z and Generation Alpha.[19]

The threat emanating from Europe today is no longer just about the possible return of foreign terrorist fighters or transnationally active, structured local extremist networks. Conceivably, it is shaped by a pernicious convergence of religiously motivated extremist ideology, digital platform mechanisms, and contemporary Western online youth culture. What is emerging is not merely the diffusion of radical content, but the progressive cultural normalization of extremist narratives, articulated through online formats that align with the affective and identity-forming dynamics of a digitally native youth. This convergence has transformed contemporary jihadism into a fluid, networked, and increasingly aestheticized movement—one capable of inspiring violence not through clandestine training camps, but through swipeable videos, viral slogans, and online 'tribalism.' Dealing with such a new threat landscape, Europe's counterterrorism challenge is therefore as much youth-cultural and algorithmic as it is operational and ideological.

To investigate this multifaceted dynamic in more detail, this article is organized into four main sections, each examining a distinct facet of contemporary Islamist/jihadi radicalization dynamics. Part I explores the concept of the Virtual Caliphate Complex, focusing on the decentralized and transnational nature of online jihadi ecosystems. Part II investigates the role of TikTok and short-form video platforms in shaping visual radicalization patterns, aesthetic appeal, and algorithmic amplification. Part III presents a selection of empirical case studies of European individual attackers since 2023, with verified indicators of online radicalization, including thwarted plots. Part IV provides a comparative analysis of these cases, identifying shared behavioral patterns, online platform trajectories, and ideological markers. The analysis concludes with a reflection on structural detection gaps and potential strategic implications for a more effective European/Western preventing and countering violent extremism (P/CVE) policy.

"Dealing with such a new threat landscape, Europe's counterterrorism challenge is … as much youth-cultural and algorithmic as it is operational and ideological."

Part I: The "Virtual Caliphate Complex"

The virtual caliphate promoted by Islamic State outlets and affiliates has fundamentally transformed jihadi terrorism into a phenomenon that is decoupled from geography—enabled by global digital connectivity, encrypted communication, and on-demand propaganda.[20] It no longer refers to a territorial entity but to a transnational digital ecosystem: a loosely organized but (from the jihadi perspective) ideologically coherent online network, which operates on the macro level through shifting social media platforms and on the meso/micro levels via encrypted messaging apps. A wide variety of digital formats—ranging from propaganda videos, jihadi podcasts to sort of 'e-learning' modules on 3D-gun printing or bomb-making are increasingly replacing or complementing real-world interactions with propagandists, agitators, or recruiters. In such a manner, the jihadi digital value chain, i.e., the exploitation of online propaganda, virtual recruitment, and processing of attacks in closed communication spaces, is growing ever more fluid, autonomous, and globally diffused.[21]

The systemic complexity of the "virtual caliphate" rests on three key pillars: First, it aims at low-threshold engagement of individuals vulnerable to radicalization—particularly adolescents—through emotionally charged content, music, memes, and pop cultural aesthetics that are subtly or overtly aligned with jihadi ideology. Platforms such as TikTok, Instagram, and YouTube serve as ideal vectors for these narrative framings, as they combine algorithmic virality with visual immediacy and cultural relatability.

Second, the virtual caliphate enables targeted selection and outreach to potential attackers via encrypted platforms such as Telegram or Rocket.Chat. These channels are often accompanied by "cyber coaching"[22] or even "plotting hubs,"[23] in which more experienced jihadi operatives provide virtual mission briefings or act as digital mentors. This pseudo-mentorship may include logistical advice, ideological justification, or psychological reinforcement, all delivered remotely and anonymously.

Third, this strategy constructs a transnational ideological identity space that allows even socially isolated or psychologically unstable individuals to feel embedded in a global jihadi struggle[24]—without the need for physical integration into real-world networks. In this way, the virtual caliphate functions not as a command structure, but as a decentralized ecosystem for ideological mobilization and operational facilitation.

This Islamist virtualization strategy, as a defining expression of what is increasingly referred to as "mutant jihadism,"[25] has profound implications for the contemporary threat landscape: It significantly lowers the barriers to entry into extremism, complicates law enforcement detection and prevention efforts, and enables asymmetric mobilization even in the absence of formal organizational structures. It also contributes to the rise of so-called 'do-it-yourself jihadis'—individuals who radicalize autonomously

through online content, operate independently, and can execute attacks within extremely short timeframes. Numerous recent cases across Europe exemplify this ongoing dynamic. A particularly illustrative example is the opportunistic lone actor attack in Villach mentioned earlier. The alleged perpetrator, Ahmad G., reportedly radicalized via TikTok and is said to have been triggered into violence by watching a specific piece of Islamist online propaganda. His exposure to this material likely increased his propensity for violence and may have served as a direct catalyst for the attack.

The rapid, borderless availability of such inciting content has enabled jihadi networks to efficiently expand the reach and influence of the 'virtual caliphate.' It adapts quickly to platform restrictions, evades traditional forms of surveillance, and empowers lone actors by connecting them to a transnational jihadi narrative—anytime, anywhere. In this regard, it is less a platform of hierarchical command than a flexible and resilient infrastructure for ideological mobilization, operational guidance, and psychological embedding.

Part II: TikTok as a Gateway

Social media platforms have become indispensable tools for extremist actors across ideological spectrums.[26] Their unrestricted global reach, low entry barriers, and capacity for anonymity make them ideal environments for spreading propaganda, recruiting followers, and exchanging operational knowledge. Extremists particularly exploit platforms with algorithm-driven content delivery—such as TikTok, YouTube, and Instagram—where emotionally charged or sensationalist material can quickly gain visibility. Short-form videos, memes, and similar stylized imagery allow radical messages to be disguised in appealing formats, making them especially effective for engaging younger, digitally native audiences.

This exploitation becomes most effective under specific conditions: during periods of geopolitical crisis, in politically polarized environments, and where digital literacy is low. Weak content moderation and poorly regulated or encrypted platforms further facilitate the spread of extremist narratives. In such an environment, social media serves not only as a broadcasting tool but as a powerful force multiplier—enabling the rapid radicalization of individuals, the creation of virtual ideological communities, and the decentralized planning of extremist acts.

TikTok is a Chinese short-form video platform launched globally in 2018 that enables users to create and engage with videos—mostly under a minute—across genres such as music, comedy, politics, and lifestyle. Driven by user-generated trends and a highly personalized algorithm, especially popular among Gen Z and Gen Alpha, TikTok aligns closely with current youth *zeitgeist*. Against this backdrop, its influence on adolescents has grown swiftly, turning it into both a powerful tool for creativity and, increasingly, a contested space for disinformation, populist messaging, and extremist propaganda.[27]

Social media platforms such as TikTok have emerged as critical first contact gateways for the radicalization of young individuals susceptible to all facets of extremist and radical Islamist ideologies in particular. Content creators strategically exploit TikTok's algorithm, its emotional aesthetics, and its popularity among adolescents to disseminate polarizing, ideologically charged material.[28] This includes martyrdom narratives, anti-Western rhetoric, and religious interpretations of global conflicts—particularly the war in Gaza.[29]

TikTok plays a seminal role in this digital radicalization ecosystem: It lowers the entry threshold,[30] amplifies identity-based grievances, and connects teenage users with radical salafi symbolism (e.g., the raised index finger as gesture for *tawhid* or the celebratory grin of attackers such as the alleged Villach perpetrator),[31] ideological codes, and narrative shortcuts. Short-form videos blend radical Islamist as well as jihadi references, graphic content, and familiar cultural cues to create a virtual identity space for potential young attackers. Gradual exposure through comments, algorithms, and cross-platform links leads to recruitment and access to encrypted channels, sometimes via QR codes.[32]

The following paraphrased excerpt from an anonymized interrogation protocol of a teenager who had planned—but ultimately abandoned—a terrorist attack in Vienna in September 2023 illustrates how continuous exposure to extremist content on social media can significantly reinforce the radicalization process.[33] In his statement, the teenager describes how he was influenced by radical online propaganda. He claims that salafi online preachers convinced him that Muslims were "superior to non-believers" and that only the strictly observant would go to paradise. According to his statement, his radicalization was driven primarily by salafi and jihadi content on TikTok, while Instagram and Telegram served as platforms for networking with ideological peers and sharing footage of terrorist attacks. Furthermore, he recounts that he watched many videos of an Islamic State-affiliated hate preacher, which convinced him to become a follower of the Islamic State, believing it to be the "most religious group in the world." During the interrogation, he denied that the Islamic State would kill innocent people, claiming instead that it would target only non-believers. He aspired to become a martyr like them and decided to plan an attack. The teenager bought a knife guided by the intention to kill as many *kafir* (non-believers) as possible. He considered acquiring a gun but could not afford one. Also, the adolescent had planned to wear a fake suicide belt to instill fear and panic during the attack. His ultimate goal was to be shot by the police to become a martyr and go directly to paradise, where he imagined there would be only peace and no more conflict. He claimed that he boarded the subway intending to carry out the attack upon arrival but lost his courage at the last moment. Allegedly, he became afraid that he might not die in the attack and thus would not reach paradise.[34]

This hybrid form of radicalization—emotionalized, decentralized, and digitally embedded—poses a serious challenge for Western security services. The so-called 'TikTok Jihad' is no longer a fringe phenomenon but has evolved as a strategic toolkit component of the jihadi value chain.[35] Recent cases such as the foiled ISK-inspired Taylor Swift concert attack in Vienna (2024) illustrate convincingly how TikTok serves as an emotional incubator, catalyst, and ideological gateway, while Telegram becomes the operational communication space.[36] Security authorities across Europe now recognize TikTok not only as a tool of propaganda but as a direct accelerant of radicalization and operational readiness.[37]

Radicalization on TikTok

Radical Islamist hate preachers are increasingly leveraging TikTok to disseminate antisemitic, homophobic, and other extremist enemy narratives, alongside martyrdom myths and a rigid, binary worldview rooted in the strict dichotomy of "*halal*" versus "*haram*."[38] The content they promote advocates a strictly sharia-compliant way of life that is deliberately austere, deeply fundamentalist, and explicitly anti-modern—rejecting liberal Western values such as

"Recent cases such as the foiled ISK-inspired Taylor Swift concert attack in Vienna (2024) illustrate convincingly how TikTok serves as an emotional incubator, catalyst, and ideological gateway, while Telegram becomes the operational communication space."

individual freedom, democracy, pluralism, and gender equality as corrupt, decadent, and incompatible with an alleged 'true' Islamic identity.[39] At first glance, this messaging appears paradoxical: highly stylized and digitally savvy in its format yet promoting an ideology that is deeply anti-modern. However, this contradiction is strategic rather than accidental. The modern aesthetic—short videos, viral music, meme culture, influencer language—is deliberately employed to lower access barriers and resonate with digitally native, identity-seeking youth.[40] Once engaged, viewers are gradually introduced to a rigid ideological framework that presents the rejection of modernity not as a loss, but as moral superiority and spiritual clarity. A deceitful sleek digital packaging thus serves as a gateway into a worldview that ultimately demands the wholesale rejection of the very cultural environment it initially mimics.

The rise of radical salafi online influencer preachers marks a pivotal shift in the way Islamist ideologies—particularly those aligned with the violent salafi-jihadi spectrum—are disseminated, consumed, and internalized by young, often digitally native audiences.[41] These figures blend religious authority with the aesthetics of digital populism, delivering highly stylized content via social media platforms such as TikTok, Instagram, YouTube, and Telegram. Such activities also generate revenue. Notably, the presence of crowdfunding and donation links on many of these accounts indicate that TikTok is increasingly leveraged as a promotional tool for fundraising and financial support[42]—not only for ideological outreach, but also for the personal benefit of the preachers themselves, who often market pilgrimage packages, *halal* products, or other religiously branded goods.

TikTok's Problematic Messengers

When it comes to radicalization, the major challenge with TikTok is that users themselves, especially the self-declared "preachers," produce their problematic content, akin to a "do-it-yourself *dawa*"—a form of religious outreach or proselytizing that individuals essentially carry out on their own.[43] Unlike traditional mosque-based *dawa*, their digital preaching is personalized, emotionally charged, and algorithmically amplified, allowing them to potentially reach millions of users across linguistic, national, and cultural boundaries. The salafi TikTokers messaging often operates within the gray zone between legality and radicalization, making it especially challenging for regulatory or intelligence frameworks to address.

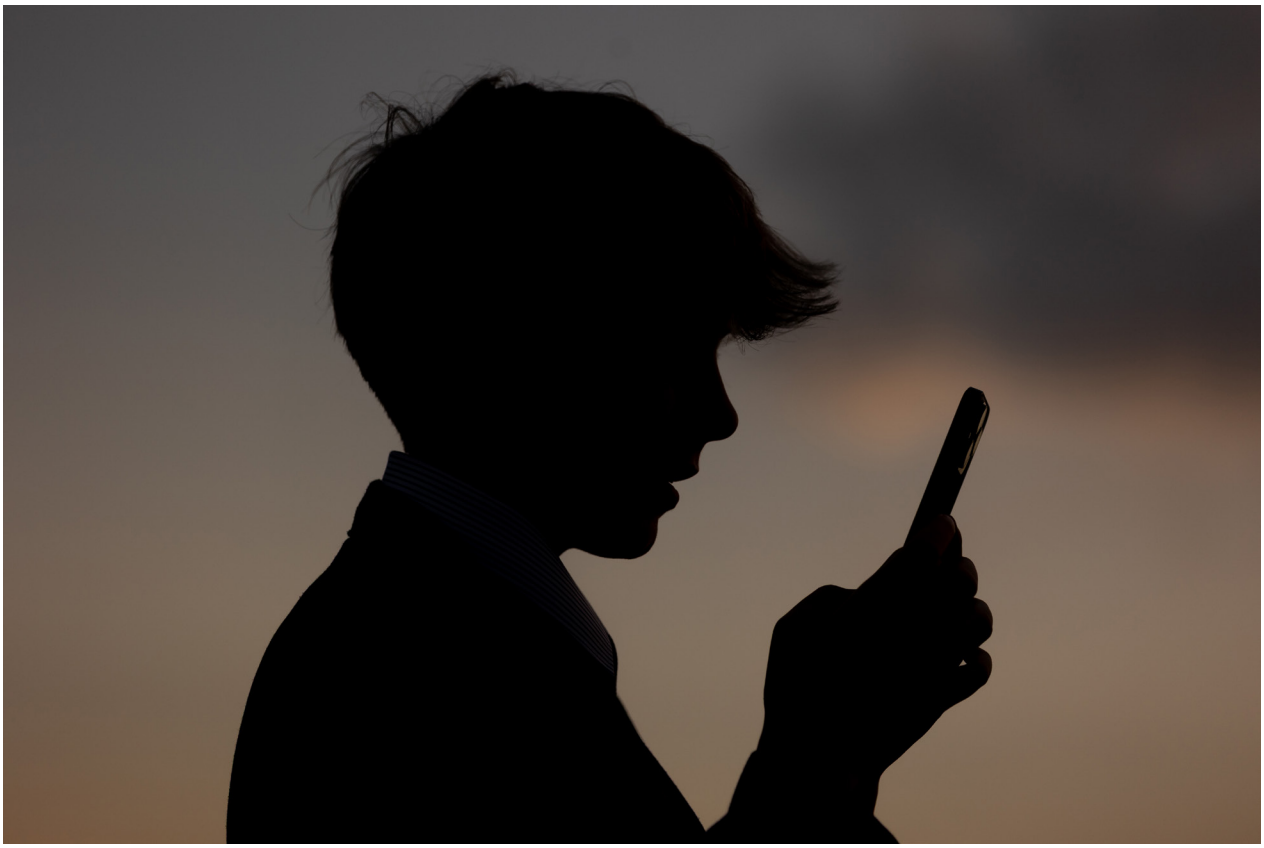
Some of the most prominent figures in this space are Abul Baraa (104,000 followers on TikTok); Marcel Krass (160,000 on Instagram, 91,000 on YouTube, and 13,000 followers on TikTok, where he has recently been more active); Deran A., known as "Abdelhamid" (580,000 followers on TikTok); and Ibrahim El Azzazi (600,000 followers on TikTok)—all German-speaking salafi online preachers with extensive reach among youth audiences in Europe.[44]

Abul Baraa, widely known within the German-speaking radical salafi scene, is notorious for theological justifications of religiously motivated violence, the rejection of democracy, and antisemitic or anti-Western nuances couched in religious rhetoric.[45] This "rock star" among the German-speaking salafi influencer preachers promotes an intimidating interpretation of Islam, marked by threatening undertones, in which—according to his rhetoric—individuals are granted little to no legitimate personal autonomy.[46] He reportedly dismisses the life choices of those who do not strictly adhere to Islamic commandments as invalid or inferior.[47] His content appears to remain mostly within the boundaries of what is legally permissible but is frequently referenced in jihadi contexts, including in legal proceedings involving radicalized individuals.[48] Marcel Krass, although presenting himself as more moderate in tone, has propagated similar narratives, particularly around the rejection of Western political systems, gender roles, and Islamic orthopraxy.[49] Both individuals are frequently named in jihadi investigation files as influential voices in the radicalization histories of young suspects.[50]

The third highly relevant persona, "Abdelhamid," an Islamist "TikTok star" gained notoriety in a recent trial in Düsseldorf: He is alleged to have pocketed donations for children in need on a grand scale.[51] The North Rhine-Westphalia Office for the Protection of the Constitution describes "Abdelhamid" as a top salafi online influencer with hundreds of thousands of followers and 10 million likes—a lifestyle preacher in a sports jersey who radicalizes young people.[52] Ibrahim El-Azzazi, the fourth significant person in this category, has more than 600,000 followers on TikTok, where he is known as "Sheik Ibrahim."[53] The preacher, who grew up in Munich, had been under surveillance by the Bavarian Office for the Protection of the Constitution.[54] According to the authorities El-Azzazi espouses "anti-democratic, misogynistic, and homophobic views."[55]

What distinguishes these preachers from traditional religious authorities is not merely their ideology but their comprehensible use of modern digital communication. Their videos, livestreams, and interactive formats employ techniques common to influencers: direct eye contact, emotional storytelling, relatable language, and rapid-response interaction with viewers. They simplify complex theological concepts and link them to everyday struggles of identity, discrimination, or personal crisis. The result is a highly adaptable and seemingly authentic message that is deeply resonant with alienated or identity-seeking youth,[56] especially those from Muslim diaspora communities.[57] This modern media-affine approach makes them "valuable" ideological bridges between mainstream conservative Islam, radical Islamism, and jihadi radicalism.[58]

Crucially, these preachers do not typically call for violence directly. Rather, they create a radical Islamist 'environment' in which dichotomous thinking, exclusivist religious identity, and resentment toward Western norms are normalized and theologically legitimized. In this atmosphere, jihadi propaganda can flourish, as it builds on the ideological foundations laid by such influencers. Repeatedly, jihadi attackers or suspects in recent years have cited initial exposure to online preachers such as Abul Baraa as an early stage in their radicalization process—before transitioning



A teenage boy looks at a iPhone screen display on May 21, 2025. (Anna Barclay/Getty Images)

to encrypted channels or more explicit jihadi content.[59] In this sense, radical salafi influencer preachers function as gatekeepers or facilitators of ideological escalation, making them a critical node in the hybrid radicalization pathway that increasingly defines the terrorist threat landscape in Europe.

The TikTok Dilemma

German domestic intelligence agencies have issued warnings that TikTok functions as a "radicalization accelerant" for vulnerable youth.[60] While the use of social media by Islamists is not a new phenomenon, the agencies emphasized that the app TikTok—due to its "addictive potential" driven by constantly refreshed, algorithm-based video suggestions—had led to a "dramatic acceleration" of radicalization.[61]

In response to such risks, the European Union is establishing age restrictions for TikTok referring to child protection reasons. In several states such as India, China, and Pakistan, access is either temporarily banned or heavily restricted due to national security concerns.[62] Consequently, TikTok has taken measures—through automated moderation, NGO partnerships, and policy updates—to reduce the spread of extremist content.[63] The European Digital Services Act (DSA) can be regarded as a game-changing enforcement tool in this context: For the first time, TikTok must legally assess, mitigate, and be audited on systemic risks, including online radicalization. The European Commission has launched formal investigations under the DSA, examining TikTok's handling of youth protection, harmful content, addictive algorithmic design, and election-related risks.[64] TikTok continues to struggle with detecting coded or "softer" Islamist content, such as charismatic preachers who use religious language to promote radical ideas. Content removal is often delayed, especially for non-English or regional-language videos.

As right- and left-wing extremists also try to exploit the social media platform, which is particularly popular among young people, the trend is most pronounced in radical Islamist circles. TikTok plays a "central role" in the staging and dissemination of Islamist content.[65] Meanwhile, the platform's algorithm may amplify borderline material, exposing vulnerable youth to extremist narratives tied to identity, belonging, or grievance. Through ongoing exposure to algorithmically promoted content and interaction with salafi online influencer preachers, users—especially susceptible adolescents—are potentially drawn into increasingly extreme ideological ecosystems. This process is often facilitated not only by public posts but also by anonymous users operating in comment sections, livestreams, or encrypted group chats. Sometimes, within a few hours, users may be confronted with highly problematic material or even be invited—through links on TikTok—to encrypted chat formats.[b] A common next step in this radicalization trajectory involves direct invitations to migrate to alternative platforms such as Instagram, Telegram, or Rocket.Chat.[66] Online environments such as these offer more privacy and lower levels of content

b One Austrian investigative journalist has reported troubling insights into the immersive dynamics of TikTok-driven radicalization, documenting how rapidly users can be exposed to extremist content and how such material is algorithmically promoted and reinforced within the platform's ecosystem. See Leo Eiholzer, "Das Jihadisten–Protokoll: Auf TikTok gerät man in drei Stunden von Katzenvideos in eine Terroristen Chat–Gruppe," *NEWS* (Vol. 9), February 27, 2025, pp. 21-26.

moderation,[c] which makes them attractive for the continuation of communication in closed or encrypted channels. Such "safe spaces" provide fertile ground for harder to monitor indoctrination, ideological reinforcement, and even operational planning.

Platform migration remains a serious challenge in the radicalization process—where ideological exposure facilitates more opportunities for deeper commitment and exposure to content or interactions that lay the groundwork for terrorism. In this environment, users have opportunities to become active participants in clandestine digital subcultures, where ideological boundaries blur and violent action is increasingly framed as a legitimate and even obligatory expression of faith. Thus, TikTok is not merely a platform for ideological outreach—it can serve as a gateway to a broader radicalization infrastructure that extends across digital ecosystems.

While other platforms also play roles in extremist recruitment, TikTok's design and demographic focus amplify risks for youth, supported by both case evidence and expert analysis.[67] However, radicalization increasingly continues across platforms; TikTok frequently serves as the gateway rather than the sole venue. The German Bundesamt für Verfassungsschutz (BfV) has also called for closer monitoring of digital radicalization patterns, particularly among socially isolated individuals with migration backgrounds, and warned of the increasing role of TikTok in jihadi recruitment across Europe.[68]

Part III: Case Studies of Lone Actors and Online-Driven Attacks (2023-2025)

The selected six attack cases (both foiled and executed) span four Western European countries (Austria, Germany, Belgium, and Switzerland) from 2023 to 2025, demonstrating a growing trend of TikTok-linked radicalization. They involve varied attack types, backed by investigations confirming TikTok exposure. Common features include young perpetrators under 25 who self-radicalized mainly through TikTok where they had been exposed to radical Islamist content from salafi influencers. TikTok's algorithm may have accelerated their move from passive viewing to violence, with many shifting to encrypted messaging apps such as Telegram for deeper indoctrination.

Vienna, Austria – Foiled Attack on Pride Parade (June 2023)

In June 2023, Austrian security authorities foiled a jihadi terrorist plot targeting the Vienna Pride Parade, a major LGBTQ event held annually in the Austrian capital.[69] The three suspects—a 14-year-old of Chechen descent and two brothers aged 17 and 20 of Bosnian origin, all residing in Lower Austrian capital St. Pölten—were arrested on June 17, just days before the parade.[70] The group had reportedly planned to carry out a coordinated assault involving an AK-47 assault rifle, a machete, and potentially a vehicle-ramming attack.[71] In preparation for the attack, the 14-year-old suspect reportedly used the encrypted messaging app Threema to request bomb-making instructions from an unknown online contact.[72] In response, he received a link to detailed instructions.

Omar Haijawi-Pirchner, head of Austria's State Protection and Intelligence Directorate (DSN), stated that the individuals had radicalized themselves on TikTok, noting that their profile closely aligned with the target demographic of certain salafi online preachers: "The suspects belong exactly to the target audience of these preachers. They are young and self-radicalized via TikTok or other social media platforms."[73] The now 19-year-old suspect reportedly adopted Islamic State ideology as early as March 2022, actively promoting it on platforms such as TikTok and Telegram, as well as through his PlayStation profile, where he glorified the group and disseminated its ideology.[74]

According to investigative findings, the youngest suspect did not merely consume jihadi "TikToks;" he consequently actively engaged in creating, curating, and disseminating content via Telegram, essentially moving from passive consumer to propagandist. Investigations revealed that he allegedly established a Telegram channel for jihadi networking, fundraised for weapons, and planned to travel to ISK territory in Afghanistan.[75] His radicalization pathway exemplifies how TikTok increasingly serves as a soft entry zone, from which vulnerable teens are drawn into more secure and operational platforms (e.g., Telegram, Threema). The plot also offers a sobering illustration of how jihadi propaganda increasingly resonates with a new, very young generation (teenagers) of digital natives.

Brussels, Belgium – Shooting Attack (October 2023)

On October 16, 2023, a 45-year-old Tunisian national, Abdesalem Lassoued, perpetrated a terrorist shooting in Brussels, fatally targeting two Swedish nationals and wounding a third.[76] All three victims were reportedly enroute to a UEFA EURO 2024 qualification match, visibly identifiable by their yellow Swedish football jerseys.[77] The attack occurred in the context of growing hostility toward Sweden, which had intensified over several months following public burnings of the Qur'an—first by far-right activist Rasmus Paludan and later by Iraqi protester Salwan Momika.[78] As a result, Sweden increasingly became a symbolic target in jihadi narratives. In this context, Magnus Ranstorp, a Swedish terrorism researcher, noted, "We are among the top countries in the West perceived as being at war with Islam and identified as priority targets."[79]

The attacker, who was illegally residing in Belgium after prior convictions and a failed asylum claim in Italy, was already known to Belgian authorities.[80] Critically, investigators later confirmed his recent activity on TikTok, where he had consumed videos promoting radical Islamist narratives, including claims about Sweden's alleged mistreatment of Muslim children—a conspiracy theory widely circulating in Arabic-language videos at the time.[81]

The attacker's ideological motivation was clearly articulated in a video message he posted shortly before the attack, in which he pledged allegiance to the Islamic State. He claimed that he "targeted Swedes" as "revenge in the name of Muslims" allegedly oppressed by Western governments, specifically citing Sweden.[82] The narrative he referenced—that Swedish authorities were removing Muslim children from their families to "Christianize" them—had been widely amplified on TikTok and Telegram, often in highly emotional and decontextualized formats.[83] While there is no evidence of direct contact with Islamic State operatives, the attack aligns with the model of 'inspired terrorism'—acts carried out independently but ideologically aligned with jihadi groups.[84] The Islamic State later claimed responsibility via its official channels, hailing the attacker

c Since the start of Trump's second administration, Instagram's content moderation has shifted toward a more permissive, user-driven model—marked by the removal of fact-checkers, relaxed hate speech policies, and reduced proactive enforcement—while remaining subject to E.U. oversight under the Digital Services Act. See Jess Weatherbed, "Meta abandons fact-checking on Facebook and Instagram in favor of Community Notes," Verge, January 7, 2025.

as a "soldier of the Caliphate."[85]

The attack prompted high-level political discussions in both Belgium and across the European Union, focusing on systemic failures in addressing radicalization, shortcomings in deportation and asylum enforcement mechanisms, and the increasingly critical role of social media platforms in amplifying jihadi propaganda and facilitating online mobilization.[86] The Brussels case strikingly illustrates that social media platforms like TikTok can serve as entry points into (more) extreme ideological spheres. While the perpetrator did not match the typical 'teenage TikTok jihadi' profile age-wise, his case shows that the platform's algorithmic exposure model can radicalize even older individuals—especially when conspiratorial content intersects with identity-based grievance.

Zurich, Switzerland – Knife Attack (March 2024)

In March 2024, a 14-year-old male of Swiss-Tunisian background carried out a brutal knife attack in central Zurich, severely injuring an Orthodox Jewish man in what authorities described as a religiously motivated and explicitly antisemitic assault.[87] The teenage attacker stabbed the man multiple times, leaving him critically injured. Passersby managed to overpower the assailant, who continued to issue threats, declaring it was his Muslim duty to kill Jews.[88] Witnesses told the Jewish magazine *Tachles* that he allegedly shouted: "I am Swiss. I am Muslim. I'm here to kill Jews." According to *20 Minuten*, he also yelled "Allahu Akbar" and "Death to all Jews."[89] The victim survived the attack, but the incident sent shockwaves through Switzerland due to the young age of the perpetrator, the clear jihadi motive, and the weaponization of antisemitic narratives.[90]

The assailant reportedly declared his motivation to be religious, framing the act as part of his perceived duty to defend Islam against its enemies.[91] Investigators soon discovered that the teenager was not merely exposed to extremist ideas but was deeply embedded in a growing online subculture known as "Alt-Jihad" (also known as "Islamogram")—a digital phenomenon inspired by the far-right "Alt-Right" movement "Terrorgram."[92] This specific subculture merges traditional Islamist/jihadi narratives with meme culture, gamer aesthetics, and content strategies tailored to engage adolescents on platforms such as TikTok and Instagram.[93]

The attacker was a highly active user of TikTok and Instagram, where he both consumed and created jihadi propaganda. His social media profiles featured Islamic State-related symbolism, martyrdom references, Qur'anic excerpts, and videos referencing the destruction of Israel and Western society.[94] Moustafa Ayad, a researcher focusing on the virtual dimension of jihadism, stated in an interview with the Swiss daily *Tagesanzeiger* that he had never seen an attacker like the one in Zurich who was so directly connected to the online ecosystem of salafism and the visual world of Islamogram.[95] In Ayad's view, the case of the Zurich teenage perpetrator confirmed what his study suggested: This disturbing online matrix could have catastrophic consequences in reality.[96]

The attacker's online activity revealed frequent interaction with content from jihadi influencers, as well as aestheticized propaganda videos set to *nasheeds*, interspersed with memes that mocked Western values and glorified violence against non-Muslims, particularly Jews.[97] This style of content is characteristic of "Alt-Jihad"—a decentralized, digitally native form of extremist expression that appeals to digitally literate Gen Z users by using humor, cultural references, and simplified theological rhetoric.[d] Swiss investigators also discovered that the boy had begun to produce his own content,[98] reposting jihadi videos and even creating "remixed" TikToks that adapted Islamic State propaganda into stylized edits specifically for his peer teenagers audience. These included short videos with motivational captions about "fighting injustice," condemning "Zionists," and presenting the attacker's religious identity as incompatible with Western life.

What is particularly concerning about this case is the apparent absence of direct personal contact with jihadi recruiters. The teenager appears to have radicalized entirely online, in what Swiss security services described as a "closed-loop digital ecosystem" of echo chambers and extremist comment threads.[99] Investigators linked his radicalization timeline to online exposure to jihadi content during the Gaza conflict escalation post-October 7, 2023, during which he increasingly engaged with accounts promoting antisemitic and violent rhetoric.[100] The suspect had also joined private group chats on Instagram and Telegram, where users shared pro-Islamic State memes, antisemitic tropes, and glorifications of lone-actor attacks.[101]

Vienna, Austria – Thwarted Islamic State-Inspired Attack on Taylor Swift Concert (August 2024)

In August 2024, Austrian authorities foiled a jihadi-inspired terrorist plot targeting a Taylor Swift concert in Vienna, one of the highest-profile entertainment events of the summer.[102] The three suspects, aged between 17 and 19, were arrested before they could carry out the attack, which, according to investigators, was intended to cause mass casualties and garner maximum media attention in the name of the Islamic State, specifically Islamic State Khorasan.[103]

The TikTok radicalization aspect of the foiled Taylor Swift concert attack in Vienna in August 2024 is a textbook example of how jihadi propaganda increasingly leverages youth-focused platforms to manipulate and mobilize vulnerable individuals.[104] According to his own testimony, the main suspect, Beran A., a 19-year-old with Macedonian-Albanian roots, was radicalized in part by regularly consuming TikTok videos of the aforementioned German salafi preacher Abul Baraa, the charismatic influencer on the platform.[105] His TikTok content—stylized, youth-focused, and emotionally charged—served as an accessible entrance point to more hardcore jihadi ideology, including videos glorifying violence and martyrdom.

It seems that Beran A. did not merely consume this content passively. Inspired by such material and driven by a personal crisis that included social alienation and mental health issues, he fully embraced jihadi ideology.[106] In his own words during interrogation, he had "dedicated his life to Allah" and advocated for sharia law

d Alt-jihadis blend far-right culture war narratives with support for jihadi groups such as Hezbollah, Hamas, al-Qa`ida, and the Islamic State. While they glorify 9/11 as proof of Western vulnerability, many also embrace conspiratorial "truther" narratives blaming Jews or Western elites. Ideologically inconsistent, they denounce white supremacists yet flirt with ethno-state rhetoric. What unites them is a toxic, viral-ready rejection of liberalism, multiculturalism, and democratic values. See Scott Atran, "Alt-Right or jihad? Unleashed by globalisation's dark side and the collapse of communities, radical Islam and the alt-Right share a common cause," AEON, November 6, 2017; Moustafa Ayad, "Teenage Terrorists and the Digital Ecosystem of the Islamic State," *CTC Sentinel* 18:2 (2025); and Moustafa Ayad, "An 'Alt-Jihad' is rising on social media," Wired, December 8, 2021.

while distancing himself from "sinful" peers.[107] This process of ideological transformation was definitely facilitated by TikTok's algorithmic amplification, which exposed him to increasingly radical material.[108] He eventually pledged allegiance to the Islamic State via Telegram and began tactical preparations for a mass-casualty attack.[109]

When Beran A. transitioned to Telegram, he allegedly coordinated operational details, sought weapons, and communicated with other extremists.[110] Nevertheless, based upon what is known about his background, TikTok served as the initial ideological vector.[111] This example starkly illustrates how "hipster Salafism"[112] and borderline content[113]—mixing memes, slang, and pop culture— is exhibited on platforms like TikTok attempting to reach Gen Z audiences. Such content is often difficult to moderate because it appears initially benign or coded. But it regularly serves as an ideological "on ramp," directing viewers to more radical material on encrypted platforms.[114] Sometimes, it is directly by means of QR codes leading to "closed" Telegram groups.[115]

Solingen, Germany – Knife Attack at City Festival (August 2024)

On August 24, 2024, the German city of Solingen—ironically renowned for its blade manufacturing—became the scene of a deadly jihadi knife attack.[116] During the "Festival of Diversity," held to commemorate the city's 650th anniversary, 26-year-old Syrian asylum seeker Issa Al H. launched a stabbing attack on festival visitors, killing three people and injuring eight others—many of whom sustained severe wounds to the neck and upper body.[117]

According to federal prosecutors, Issa Al H. was driven by radical Islamist convictions and sought to kill as many "unbelievers" as possible.[118] Prior to the attack, he reportedly recorded a video pledge of allegiance to the Islamic State and sent it to a contact associated with the terrorist group, indicating pre-meditation and ideological alignment.[119] In initial statements to investigators, Issa Al H. framed the attack as an act of religious duty, declaring that those attending the multicultural festival were enemies of Islam.

The assault bore hallmarks of Islamic State-inspired lone actor terrorism. Prosecutors, however, claim that prior to the enabled attack, he reached out to Islamic State affiliates via jihadi social media channels, where he allegedly received support in planning the assault and selecting the weapon used to carry out the killing.[120] Undoubtedly, the attack fits the broader pattern of digitally mediated radicalization without direct organizational involvement. Investigators believe he had contact via chat with an unknown jihadi entrepreneur with a *nom de guerre* "Abu Faruq," who could have served as facilitator.

It is worth noting that the Solingen attack marks the first instance since the 2016 Berlin Breitscheidplatz Christmas market vehicle-ramming attack that the Islamic State officially issued a statement of responsibility for a terrorist act on German soil.[121] In its Solingen communiqué, promulgated via its Amaq channel, the Islamic State explicitly referenced the situation in Gaza.[122]

Investigations revealed that Issa Al H. had consumed extensive amounts of jihadi propaganda on platforms such as YouTube, but also on TikTok and ultimately Telegram, including videos that glorified martyrdom, justified attacks against civilians, and promoted Islamic State narratives of vengeance and religious duty.[123] German intelligence services confirmed that his radicalization occurred primarily online and in isolation, with short videos playing a notable role in the early stages. From at least June 2024 onward, he immersed himself in jihadi ideology, particularly consuming propaganda from al-Qa`ida.[124] He watched videos of Usama bin Ladin, listened to podcasts linked to the Islamic State, and installed software on his smartphone that allowed him to access jihadi forums anonymously.[125] Telegram probably played a central role in his radicalization. He followed jihadi channels, and allegedly, he even created his own channel on the platform in February 2024.[126] According to investigators, he is believed to have shared Islamic State-related videos—such as beheading footage—and published Islamist propaganda, although apparently without much response.

It was reportedly the Gaza conflict that further radicalized Issa Al H., according to his own messages. He allegedly searched online for locations such as the Israeli embassy in Berlin, a chapel in Cologne, and a German military training ground—possibly as potential targets.[127] On one of these channels, Al H. received advice on how to behave covertly.[128] In his confession video, he vowed "revenge for our people" and referred to himself as a "soldier of the IS."[129] Al H.'s consumption of Islamic State propaganda material is believed to have reinforced his extremist worldviews and specifically intensified his hostility toward secular and pluralistic societies, such as that symbolized by the festival in Solingen.[130]

The attack also reignited national debate over immigration enforcement and deportation policy. Al H.'s asylum claim in Germany had been rejected, and he was scheduled for deportation to Bulgaria—his first country of entry into the European Union under the Dublin Regulation.[131] However, like many failed asylum seekers, he evaded removal, reportedly due to bureaucratic obstacles and the lack of travel documents.[132] Following the attack, then German Chancellor Olaf Scholz vowed to introduce stricter knife laws, speed up deportation processes for rejected asylum seekers, and strengthen the powers of immigration enforcement.[133]

Villach, Austria – Knife Attack (February 2025)

Just days after a 14-year-old, who allegedly had been rapidly radicalized after watching Islamist videos on TikTok, was arrested on February 10, 2025, in Vienna for planning an Islamist-motivated attack on a train station,[134] a deadly jihadi-inspired knife attack took place on February 15 in Villach, Carinthia. There, 23-year-old Syrian asylum seeker Ahmad G. randomly assaulted passersby with a folding knife near the Draubrücke bridge.[135] A 14-year-old boy was killed, and five others were injured, some critically. Witnesses reported hearing "Allahu Akbar," and Ahmad G. later declared allegiance to the Islamic State.[136]

A search of his apartment revealed jihadi writings, an improvised Islamic State flag using black plastic trash bags, and evidence of frequent consumption of extremist propaganda, particularly via social media.[137] Authorities concluded that he had undergone a rapid and largely isolated process of online radicalization, primarily through consumption of radical Islamist TikTok content.[138] According to his own statement, his turn toward jihadism occurred within just three months, heavily influenced by salafi influencer preachers.[139] He told investigators that a specific Islamist propaganda video, viewed four days before the attack, served as the decisive trigger.[140]

This pattern of online radicalization has repeatedly been observed across Europe and is clearly exemplified by the Villach case.

It also raises the issue of "stochastic terrorism"[e]—a form of indirect incitement where mass-distributed extremist content increases the likelihood of violent acts, even without explicit calls to action.[141] This tactic, which can be extended to manifestations of jihadi violence, relies on suggestive messaging, broadly disseminated across digital platforms, where vulnerable individuals interpret and act on the content independently.[142]

Ahmad G. had recorded a pledge of allegiance to the Islamic State on the morning of the assault but did not publish it, assuming he would die in the attack and that the video would be released posthumously.[143] During his arrest, he showed no remorse, reportedly taunting police officers and smiling while raising his index finger in the *tawhid* gesture—a symbol widely used in jihadi iconography.[144] His apprehension was made possible by the swift intervention of a Syrian-born food delivery driver, who used his vehicle to stop the attacker.[145] During interrogations, Ahmad G. told authorities he saw himself as a "warrior of the Islamic State" and had planned the attack earlier that day.[146] His case has since become emblematic of hybrid or dual radicalization,[147] where online jihadi narratives fuse with personal crises and real-life encounters, leading to sudden acts of targeted violence.[148] [f] The Villach attack has sparked intense public debate in Austria over preventive counterterrorism measures, surveillance of the asylum system,[149] and the growing threat posed by digitally radicalized lone actors.

Ahmad G.'s radicalization trajectory illustrates how the virtualization strategy—consistent with the "virtual caliphate" approach—profoundly affects the terrorist threat landscape.[150] It lowers the threshold for entry into extremism, complicates surveillance, and allows for asymmetric mobilization, even in the absence of organizational structures. It also fosters "do-it-yourself jihadis" who radicalize online, act autonomously, and can mobilize sometimes even within weeks. The phenomenon has taken on a hydra-like manifestation—each incident giving rise to new expressions, echoes, and imitations across digital platforms.

Almost immediately after the attack, TikTok saw a wave of posts that either endorsed, referenced, or framed the act within a broader jihadi narrative, demonstrating how online ecosystems not only reflect but actively amplify acts of terrorism.[g] This digital resonance underscores the self-replicating nature of contemporary jihadi propaganda, where one act can rapidly generate ideological validation, aesthetic celebration, and emotional mobilization in real time. For example, a TikTok user with over 2,000 followers shared a picture of the grinning attacker, tagging it in Arabic with "#Mosul #Austria_Vienna #Syrian_in_Austria" and adding a soundtrack. This posting illustrates vividly how the radicalization spiral on TikTok unfolds.

In the comments section, users praised the attacker, writing phrases such as "May God release him from captivity"—a common jihadi expression. Another commenter referred to him as a "brother in tawhid." The TikTok account was linked to an Instagram profile featuring an Islamic State-produced video glorifying suicide bombers as "frontline warriors of death." Suggested TikTok content included *nasheeds*, stories from early Islamic history accompanied by Islamic State imagery, prayer calls, anti-Western clips like "Lost in the land of disbelief," and even a football-themed video. Ahmad G. exemplifies the currently prevailing profile of contemporary jihadi lone actors: a young, unemployed male asylum seeker originally from a conflict zone—socially isolated and radicalized online via TikTok.

Part IV: Cross-Case-Analysis - Common Radicalization Patterns

The examined attack cases share key features of TikTok-facilitated radicalization: All involve young, digitally native perpetrators—predominantly under 25—who were exposed to emotionally charged radical Islamist content on TikTok. Further online engagement, often algorithmically reinforced, escalated into more extreme material and led some to migrate to encrypted platforms such as Telegram. European lone attackers/attack plotters typically lacked ties to organized terrorist groups, pointing to immersive self-radicalization. Several among them consumed Islamic State-style propaganda that glorified revenge, martyrdom, and violence, with their opportunistic attacks reflecting an increasingly decentralized threat landscape.

Young Age, Digital Isolation, and Ideological Drift

Across almost all presented attack scenarios, perpetrators, plotters, or suspects were notably young, typically in their teens to early twenties, reflecting an alarming trend of youth radicalization. For instance, thwarted attack plots such as the one focusing on the Vienna Taylor Swift concert involved suspects aged 15, 17, and 19, while the Vienna Pride Parade plot included a 14-year-old suspect among the other conspirators. These cases suggest that attack plans involving teenagers may be more likely to be intercepted at an earlier stage, possibly due to operational inexperience or heightened digital visibility of their communications. The Brussels shooter, a 45-year-old Tunisian, was an outlier, but his radicalization was also digitally mandated.

Young age correlates with vulnerability to online extremist content due to identity formation and emotional predisposition. Prolonged isolation and excessive digital immersion—intensified by post-COVID social fragmentation—emerged as key factors in increased susceptibility to online extremist narratives. Many suspects, such as those in Zurich and Solingen, were described as socially withdrawn, spending extensive time online. The Zurich attacker, a 15-year-old Swiss Tunisian, and the Solingen perpetrator, a 26-year-old Syrian, exhibited signs of self-radicalization via online platforms, drifting toward Islamic State-inspired ideology fragments. TikTok's appealing and emotive format lowers barriers to radical content, making its short videos a potent tool for recruitment and mobilization.

TikTok and Short-Form Content as Emotional Gateway

TikTok emerged (among several others, including Instagram and

e This term is, in current academic debates, usually limited to cases of right-wing extremism and/or conspiracy-driven extremist violence. See James Angove, "Stochastic terrorism: critical reflections on an emerging concept," *Critical Studies on Terrorism* 17:1 (2024): pp. 21-43; Mark S. Hamm and Ramón Spaaij, *The Age of Lone Wolf Terrorism* (New York: Columbia University Press, 2017); and Karina Biondi and Jennifer Curtis, "From Structural to Stochastic Violence," Association for Political and Legal Anthropology, 2018.

f A recent psychiatric evaluation confirmed that his actions were not due to mental illness, but were ideologically motivated, and he was deemed fit to stand trial. The Klagenfurt public prosecutor's office continues to treat the incident as a lone-actor attack. See Manuela Kaiser, "Terroranschlag in Villach: Syrer war bei Tat zurechnungsfähig," *Kleine Zeitung*, May 20, 2025, and "Villach-Anschlag: Attentäter fühlte sich 'stark' und stach zu," PULS24 News, May 8, 2025.

g A similar dynamic has been observed in far-right extremist circles. See Amarnath Amarasingam, Marc-André Argentino, and Graham Macklin, "The Buffalo Attack: The Cumulative Momentum of Far-Right Terror," *CTC Sentinel* 15:7 (2022).

YouTube) as a critical platform for radicalization, particularly in the presented Viennese cases. Its short-form, algorithm-driven content served as an emotional gateway, amplifying extremist narratives through engaging, bite-sized videos. In the Vienna Pride Parade plot, the 14-year-old suspect was exposed to jihadi TikTok content glorifying violence. Similarly, the Taylor Swift plot suspects allegedly consumed videos of salafi online influencer preachers and Islamic State propaganda on TikTok, which emotionally charged their radicalization process. TikTok's algorithm prioritizes user engagement and creates echo chambers by recommending increasingly radical/extreme content based on prior interactions.[151] This mechanism exploits emotional vulnerabilities, particularly among susceptible teenagers like the Viennese Pride, the Zurich or the Taylor Swift plotters, fostering rapid ideological shifts.[152] Unlike platforms such as Meta or YouTube where illicit content removal has become relatively effective, TikTok has not yet achieved comparable standards.

Hybridization of Lone Actor Terrorism and Virtual Community Support

The selected cases illustrate a hybridization of lone actor terrorism and virtual community support, blurring traditional distinctions between solitary and group-based violent extremism. While perpetrators such as the Brussels shooter and Solingen attacker acted alone in terms of tactics, their radicalization was strongly supported by online communities. The Brussels suspect consumed Islamic State propaganda online and interacted with peers on closed channels, while the Solingen attacker engaged with extremist forums.

In the Viennese plots, suspects collaborated in small, digitally connected cells, coordinating via encrypted platforms such as Telegram but (allegedly) radicalizing through open platforms such as TikTok. Virtual communities provided ideological reinforcement, tactical knowledge, and emotional validation, reducing the isolation typically associated with lone actors. This hybridization is evident in the Zurich case, where the teenage attacker, though acting alone, drew inspiration from global jihadi networks online. The interplay of lone action and virtual support enhances the unpredictability and scalability of threats, as individuals can radicalize independently but draw on collective resources.

Conclusion and Policy Implications

The cross-case analysis identifies a recurring radicalization pattern: young, socially isolated individuals drawn into extremism via TikTok's emotionally charged content, driven by perceived injustices, and reinforced through virtual peer networks. Key risk factors include emotional vulnerability, algorithmic overexposure, and digital isolation. Effective P/CVE strategies must address these dimensions by aligning with the digital behaviors and identity needs of susceptive adolescents. Early-stage interventions—capable of detecting non-violent but ideologically loaded content—are essential. This demands greater digital literacy among educators and parents, alongside support structures for disengagement. At the policy level, stronger enforcement of content moderation/removal and algorithmic transparency under the European Union's Digital Services Act is critical. Public-private partnerships and investments in counter-narratives are vital to disrupt the online ecosystems in which radicalization proliferates.

"The interplay of lone action and virtual support enhances the unpredictability and scalability of threats, as individuals can radicalize independently but draw on collective resources."

Strengthening AI-based Early Warning Systems in Digital Environments: The centrality of platforms such as TikTok and Telegram in recent radicalization trajectories—e.g., Vienna and Zurich—underscores the need for robust, AI-supported early warning capabilities. Governments and security agencies should develop real-time monitoring tools to detect behavioral indicators such as increased interaction with extremist content or migration to encrypted platforms, as seen in the Vienna Taylor Swift concert plot. Collaboration with open-source intelligence (OSINT) communities can further enhance detection capacities, potentially averting attacks like the one in Solingen.

Counter-Radicalization and Digital Literacy for Youth: Given the young age profile of many suspects (14-19), counter-radicalization efforts must prioritize adolescent-focused interventions. Integrating digital literacy into school curricula can help students critically assess online content and recognize manipulative algorithmic patterns. Community initiatives such as mentorship programs may mitigate social withdrawal, while counter-narrative campaigns—culturally tailored and delivered via youth-relevant platforms—can offer positive alternatives. Engaging trusted figures like moderate religious leaders and local influencers enhances credibility and reach.

Platform Accountability and Algorithm Transparency: TikTok's function as an emotional entry point into extremist ecosystems highlights the urgency of platform accountability. The DSA should be rigorously applied to ensure algorithmic transparency and the timely removal of extremist content. Regular audits of moderation practices and the development of AI tools to flag borderline content—without infringing on free expression—are essential. Initiatives such as the Global Internet Forum to Counter Terrorism (GIFCT) and Tech Against Terrorism (TAT) provide best-practice models for cross-platform collaboration, industry standards, and threat intelligence sharing, thereby supporting both tech companies and law enforcement in addressing digital radicalization while upholding fundamental rights. CTC

Citations

1 Daniele Garofalo, "Jihadist reactions to the conflict between Israel and the Joint Palestinian Operations Room," Daniele Garofalo Monitoring, October 21, 2023.
2 Tricia Bacon, "The Jihadist Landscape Amidst Israel-Hamas War: Five Critical Factors," International Centre for Counter-Terrorism (ICCT) Analysis, December 2023.
3 David D. Kirkpatrick and Adam Rasgon, "The Hamas Propaganda War. Across the Arab world, the group is successfully selling its narrative of resistance," *New Yorker*, October 30, 2023; Garofalo.
4 Elizabeth Dwoskin, "A flood of misinformation shapes views of Israel-Gaza conflict," *Washington Post*, October 14, 2023.
5 Peter R. Neumann, *Die Rückkehr des Terrors. Wie uns der Dschihadismus herausfordert* (Berlin: Rowohlt, 2024), p. 84.
6 Eva Berendsen and Deborah Schnabel eds., "Die TikTok-Intifada – Der 7. Oktober & die Folgen im Netz," in *Analysen & Empfehlungen der Bildungsstätte Anne Frank*, Report #Nahostkonflikt, Bildungsstätte Anne Frank, 2024; Brian Michael Jenkins, "The Israel-Hamas War Has Upended the Terrorist Threat Matrix," Hill, November 22, 2023.
7 Clara Broekaert, Colin P. Clarke, Michaela Millender, Annika Scharnagl, and Joseph Shelzi, "Accelerating Hate: The Impact of the Israel-Hamas War on the Terrorist Threat Landscape on the West," Soufan Center Intel Brief, September 10, 2024, p. 9.
8 Neumann, *Die Rückkehr des Terrors*, p. 85.
9 Broekaert, Clarke, Millender, Scharnagl, and Shelzi, p. 7.
10 Maura Conway, Moign Khawaja, Suraj lakhani, Jeremy Reffin, Andrew Robertson, and David Weir, "Disrupting Daesh: Measuring Takedown of Online Terrorist Material and Its Impacts," *Studies in Conflict and Terrorism* 42 (2018): pp. 141-160; Charlie Winter, "The Virtual 'Caliphate': Understanding Islamic State's Propaganda Strategy," Quilliam, 2015.
11 Abdullah Alrhmoun, Charlie Winter, and János Kertész, "Automating Terror: The Role and Impact of Telegram Bots in the Islamic State's Online Ecosystem," *Terrorism and Political Violence* 36:4 (2023): pp. 409-424.
12 Nicolas Stockhammer, "European Trend Report on Terrorism 2025," European Institute for Counter Terrorism and Conflict Prevention (EICTP), April 2025, pp. 91-91.
13 Martha Crenshaw, "Rethinking Transnational Terrorism: An Integrated Approach," *Peaceworks* 158, United States Institute of Peace, February 2020; Nicolas Stockhammer ed., *The Routledge Handbook of Transnational Terrorism* (London: Routledge, 2023).
14 "Attentäter von Villach streamte vor dem Anschlag Propagandavideos," *Der Spiegel*, February 19, 2025.
15 Bennett Clifford, "Moderating Extremism: The State of Online Terrorist Content Removal Policy in the United States," Program on Extremism, George Washington University, December 2021; Tamar Mitts, "Why the Fight Against Online Extremism Keeps Failing," *Time*, March 6, 2025.
16 Maura Conway et al. eds., "Terrorists' Use of the Internet: Assessment and Response," *NATO Science for Peace and Security Series – E: Human and Societal Dynamics* 136 (Amsterdam: IOS Press, 2017); Rita Katz, *Saints and Soldiers. Inside Internet-Age Terrorism, From Syria to the Capitol Siege* (New York: Columbia University Press, 2022), pp. 157-168.
17 Winter, "The Virtual 'Caliphate.'"
18 Liam Duffy, "Gradualists to Jihadists. Islamist Narratives in the West," Counter Extremism Project, December 2020.
19 Stockhammer, *European Trend Report on Terrorism 2025*.
20 Winter, "The Virtual 'Caliphate.'"
21 Stockhammer, *European Trend Report on Terrorism 2025*.
22 John Mueller, "The Cybercoaching of Terrorists: Cause for Alarm?" *CTC Sentinel* 10:9 (2017): pp. 29-36.
23 Reuben Dass, "Islamic State-Khorasan Province's Virtual Planning," Lawfare, May 19, 2024.
24 Stefan Malthaner, Francis O'Connor, and Lasse Lindekilde, "Scattered Attacks: The Collective Dynamics of Lone-Actor Terrorism," *Perspectives on Politics* 22:2 (2024): pp. 463-480.
25 Armen Georgian, "'Mutant jihadism' spreading across borders and online: EU's anti-terrorism coordinator," France24, May 10, 2023.
26 Daniele Valentini, Anna Maria Lorusso, and Achim Stephan, "Onlife Extremism: Dynamic Integration of Digital and Physical Spaces in Radicalization," *Front. Psychol.* 11:524 (2020); Julia Ebner, *Going Mainstream: how extremists are taking over* (London: Ithaka Press, 2023); Kate Gunton, "The Impact of the Internet and Social Media Platforms on Radicalisation to Terrorism and Violent Extremism" in Reza Montasari, Fiona Carroll, Ian Mitchell, Sukhvinder Hara, and Rachel Bolton-King eds., *Privacy, Security and Forensics in the Internet of Things (IoT)* (New York: Springer, 2022).
27 "IntelBrief: National Security Concerns Continue to Grow Over the Use of Social Media App TikTok," Soufan Center, January 23, 2023; Moustafa Ayad, "CaliphateTok: TikTok continues to host Islamic State propaganda," ISD Digital Dispatches, June 13, 2023.
28 Erich Vogl, "Islamism on the net. The gateway drug TikTok: Calls for a ban are getting louder," *Kronen Zeitung*, February 18, 2025.
29 Drew Harwell and Taylor Lorenz, "Israel-Gaza war sparks debate over TikTok's role in setting public opinion," *Washington Post*, November 2, 2023.
30 Stefan Kaltenbrunner and Clemens Neuhold, *Allahs mächtige Influencer. Wie TikTok-Islamisten unsere Jugend radikalisieren* (Wien: edition a GmbH, 2025), p. 7 (translated and paraphrased by the author).
31 "Grinse-Terrorist: 'Wollte so viele töten wie möglich!'" *Kronen Zeitung*, February 17, 2025.
32 Ayad, "CaliphateTok: TikTok continues to host Islamic State propaganda."
33 Kaltenbrunner and Neuhold, p. 7.
34 Ibid., p. 7.
35 "TikTok Jihad: Terrorists Leverage Modern Tools to Recruit and Radicalize," Soufan Center, Intel Brief, August 9, 2024.
36 Nicolas Stockhammer and Colin P. Clarke, "The August 2024 Taylor Swift Vienna Concert Plot," *CTC Sentinel* 18:1 (2025).
37 "Verfassungsschutz warnt vor 'Tiktokisierung des Islamismus,'" Zeit Online, April 21, 2024.
38 Kaltenbrunner and Neuhold, p. 37.
39 Ibid.
40 Julian Lanchès, "Radicalisation and Repercussions: Contextualising the Mannheim Knife Attack," ICCT Short Read, June 6, 2024.
41 Stockhammer, "European Trend Report on Terrorism 2025;" Mustafa Ayad, "Islamogram: Salafism and Alt-Right Online Subcultures," Institute for Strategic Dialogue, November 16, 2021.
42 Jakob Guhl and Milo Comerford, "Understanding the Salafi Online Ecosystem: A Digital Snapshot," Institute for Strategic Dialogue, 2021.
43 Lisa Haberkorn, "Islamismus auf Tiktok: Wenn Prediger zu Influencern werden," *Der Standard*, May 24, 2024.
44 Stockhammer and Clarke.
45 Jan Michael Marchart, "Wie die Radikalisierung zum Islamisten auf TikTok funktioniert," *Der Standard*, August 11, 2024.
46 Salma Abdelaziz, Florence Davey-Attlee, and Nina Avramova, "The 'rock star' preacher influencing young people online," CNN, August 15, 2024.
47 Lino Klevesath, Annemieke Munderloh, Joris Sprengeler, Florian Grahmann, and Julia Reiter, "Radikalislamische YouTube-Propaganda: Eine qualitative Rezeptionsstudie unter jungen Erwachsenen," Studien des Göttinger Instituts für Demokratieforschung zur Geschichte politischer und gesellschaftlicher Kontroversen, 2021, p. 74.
48 Marchart, "Wie die Radikalisierung zum Islamisten auf Tiktok funktioniert."
49 Lino Klevesath, Annemieke Munderloh, Joris Sprengeler, Florian Grahmann, and Julia Reiter, "3.1. Marcel Krass und sein Video 'Was ist Scharia?'" in *Radikalislamische YouTube-Propaganda: Eine qualitative Rezeptionsstudie unter jungen Erwachsenen*, 45-55. Bielefeld: transcript Verlag, 2021; Jan Michael Marchart, "Deutscher Salafistenstar trat in Wien auf, Gastgeber sitzt bei Rassismusevent der Uni Wien," *Der Standard*, April 19, 2024.
50 "Berliner Imam soll Terrorismus finanziert haben," Vice, December 18, 2018; Oliver das Gupta, "Der Radikalisierung auf der Spur. Terrorpläne gegen Swift-Konzerte: Deutsche Salafisten distanzieren sich von Beran A.," *Der Standard*, August 13, 2024.
51 "It's about donation fraud. Salafist Tiktok star on trial in Germany," Bluewin.ch, June 20, 2025.
52 "'Abdelhamid'. Islamistischer TikTok-Prediger gesteht Spendenbetrug im großen Stil," *Die Welt*, July 1, 2025.
53 Neumann, *Die Rückkehr des Terrors*, pp. 88-99.
54 Joseph Röhmel, "Volksverhetzung: Münchner TikTok-Salafist angeklagt," BR24, October 23, 2024.
55 Ibid.
56 Marchart, "Wie die Radikalisierung zum Islamisten auf TikTok funktioniert."
57 Anna Wintersteller, "Die Tricks der Islamisten: So radikalisieren sie Junge im Netz," *Profil*, June 22, 2023; Haroro Ingram, "Learning from ISIS's virtual propaganda war for Western Muslims: A comparison of Inspire and Dabiq," International Center for Counter Terrorism, July 26, 2017.

58 Kaltenbrunner and Neuhold; Angela Gendron, "The Call to Jihad: Charismatic Preachers and the Internet," *Studies in Conflict & Terrorism* 40:1 (2016): pp. 1-18. For the ideological transitions, see Magnus Ranstorp, Filip Ahlin, Peder Hyllengren, and Magnus Normark, "Between Salafism and Salafi-Jihadism. Influence and Challenges for Swedish Society," *Swedish Defence University Report*, 2018; Mohamed-Ali Adraoui, "Borders and sovereignty in Islamist and jihadist thought: past and present," *International Affairs* 93:4 (2017) pp. 917-935.
59 Das Gupta, "Der Radikalisierung auf der Spur;" Kaltenbrunner and Neuhold, pp.16-17, 22-32.
60 "Verfassungsschutz warnt vor 'Tiktokisierung des Islamismus.'"
61 "Radikalisierung – Verfassungsschützer warnen vor 'TikTokisierung des Islamismus,'" Deutschlandfunk, April 21, 2024.
62 "EU to launch age-check app as pressure builds on Big Tech," *Financial Times*, May 30, 2025.
63 "Digital Services Act: Our fourth transparency report on content moderation in Europe," TikTok, February 28, 2025.
64 "Commission opens formal proceedings against TikTok under the Digital Services Act," European Commission, February 19, 2024.
65 "Radikalisierung – Verfassungsschützer warnen vor 'TikTokisierung des Islamismus.'"
66 "Rocket.Chat Remains One of the Most Resilient Platforms for Jihadists," Flashpoint, December 20, 2020.
67 "'Five Eyes' Powers Warn of Rise in Online Youth Extremism," Defense Post, December 6, 2024; Cathrin Schaer, "The teenage terrorists of the 'Islamic State,'" Deutsche Welle, November 9, 2024; Moustafa Ayad, "Teenage Terrorists and the Digital Ecosystem of the Islamic State," *CTC Sentinel* 18:2 (2025).
68 "Verfassungsschutz warnt vor 'Tiktokisierung des Islamismus,'" *Die Zeit*, April 21, 2024.
69 "Anschlag auf Wiener Regenbogenparade durch Verfassungsschutz vereitelt," Austrian Federal Ministry of the Interior, June 18, 2023.
70 "Erster konkreter Hinweis auf geplanten Anschlag bei der Pride in Wien," *Die Presse*, November 7, 2023.
71 Stockhammer and Clarke.
72 "Geplanter Pride-Anschlag: Chats verdeutlichen Interesse an Bombenbau," *OÖ-Nachrichten*, July 1, 2023.
73 "Geplanter Pride-Anschlag. Experte Neumann: 'Islamisten werden immer jünger,'" *Kleine Zeitung*, June 19, 2023; "Austrians say they foiled possible attack on Vienna's Pride parade by alleged IS sympathizers," *Independent*, June 18, 2023 (quote translated by author).
74 "Trial After Planned Attack on Vienna Pride Parade Begins on July 15," vol.at, April 22, 2025.
75 Natalia Anders, "DSN: 'Latentes Gefahrenpotenzial' bei Regenbogenparade," *Profil*, June 7, 2024.
76 George Wrigth, "Brussels Shooting: Suspect at Large after Two Swedes Killed in Terror Attack," BBC, October 16, 2023.
77 "Two Swedes fatally shot in central Brussels in a terrorist attack," *Monde*, October 16, 2023; James Robinson, "Brussels 'on highest terror alert' and football fans told to stay in stadium after two shot dead," Sky News, October 17, 2023.
78 Karl Ritter, "Why does Sweden allow Quran burnings? Like much of West, it has no blasphemy laws," Associated Press, July 20, 2023.
79 Charlie Duxbury, "After Brussels attack, Swedes fear becoming a target for terrorists," Politico, October 20, 2023.
80 Ella Joyner, "Belgium: Terrorist shooting underlines tense mood in Europe," Deutsche Welle, October 18, 2023.
81 Johan Wikén, Oskar Jönsson, Kovan Alshawish, and Filip Brusman, "Han misstänks för attacken mot svenskar i Bryssel," SVT Nyheter, October 17, 2023; "Sweden battles disinformation on 'kidnappings' of Muslim children," France24, February 23, 2022; "Deux supporters suédois tués à Bruxelles: voici l'auteur présumé, il se revendique membre de l'État islamique," *Libre Belgique*, October 16, 2023.
82 Duxbury.
83 Wikén, Jönsson, Alshawish, and Brusman; "Sweden hits out at 'disinformation' on child kidnappings," Associated Press, February 3, 2023.
84 For the "inspired terrorism" model, see Boaz Ganor, "Understanding the Motivations of 'Lone Wolf' Terrorists: The 'Bathtub' Model," *Perspectives on Terrorism* 15:2 (2021): pp. 23-32.
85 "Attentat à Bruxelles: l'Etat islamique revendique l'attaque," *Soir*, October 17, 2023.
86 "Policymakers want stricter return policies after the terrorist attack in Brussels," European Migration Network, October 18, 2023; "Belgium: Extremism and Terrorism," Counter Extremism Project– Report, March 2024.
87 "Ein Jahr nach dem Messerangriff – Was hat sich verändert?" Schweizerischer Rundfunk (SRF), March 1, 2025.
88 Tobias Marti, Jan Hudec, and Fabian Baumgartner, "Ein Zürcher Teenager verbreitet ein verstörendes Video. Dann begibt er sich auf Mordmission im Namen des Terrors," *Neue Zürcher Zeitung*, March 2, 2024.
89 Tobias Marti, Jan Hudec, Fabian Baumgartner, and Forrest Rogers, "Was treibt einen 15-Jährigen an, mit solchem Hass zu einer Bluttat zu schreiten? Rekonstruktion eines IS-inspirierten Anschlags in Zürich," *Neue Zürcher Zeitung*, March 5, 2024.
90 Ibid.
91 Ibid.
92 Anielle Peterhans and David Sarasin, "Wie Jihadisten mit Mangas und Memes Teenager rekrutieren," *Tagesanzeiger*, March 25, 2024; Ayad, "Islamogram: Salafism and Alt-Right Online Subcultures."
93 Guhl and Comerford.
94 Peterhans and Sarasin.
95 Ibid.; Moustafa Ayad, "An 'Alt-Jihad' is rising on social media," Wired, December 8, 2021.
96 Ibid.; Milo Comerford, Moustafa Ayad, and Jakob Guhl, "Generation Z & Das Salafistische Online Ökosystem," Institute for Strategic Dialogue, 2021.
97 Peterhans and Sarasin.
98 Ayad, "Teenage Terrorists and the Digital Ecosystem of the Islamic State."
99 Ibid.
100 Peterhans and Sarasin.
101 Ibid.
102 Stockhammer and Clarke.
103 Aaron Katersky, Felix Franz, Will Gretsky, Emily Shapiro, Josh Margolin, and Luke Barr, "Taylor Swift shows in Vienna canceled after 2 arrested for planning ISIS-inspired terror plot," ABC News, August 8, 2024; Souad Mekhennet and Joby Warrick, "Inspired by ISIS: From a Taylor Swift plot in Vienna to carnage in New Orleans," *Washington Post*, January 3, 2025.
104 Stockhammer and Clarke.
105 Abdelaziz, Davey-Attlee, and Avramova. See also Stockhammer and Clarke; Florian Hartleb and Nicolas Stockhammer, "'Ich hätte den Sprengstoff in der Menschenmenge platziert'. Eine Analyse des vereitelten Terroranschlages auf die Massenveranstaltung 'Taylor-Swift-Konzert' im August 2024 in Wien," EICTP Research Paper, September 2024, p. 13; and "Nur ein Maus-Klick bis zur Bombe," *Focus Magazin* 34 (2024).
106 Patrick Wammerl, "Der komplette Akt des Beran A.: Bomben, Exorzismus und Taylor Swift," *Kurier*, August 22, 2024; Jan Michael Marchart, Fabian Schmid, and Birgit Wittstock, "Auf den Spuren des Ternitzer Anschlagsplaners Beran A.," *Der Standard*, August 9, 2024. See also Stockhammer and Clarke; Wintersteller.
107 "Details über Terrorverdächtigen: Sprengfallenbasteln in der Küche," *Die Presse*, August 15, 2024.
108 Wintersteller.
109 Deborah Cole, "Taylor Swift concert plot: Austrian police find bomb chemicals in suspect's home," *Guardian*, August 8, 2024, "Verhindertes Attentat auf Swift-Konzert in Wien: Weitere Festnahme," *Die Presse*, April 24, 2025.
110 "Terrorpläne bei Swift-Konzert: Verdächtigem war Sprengstoff-Herstellung geglückt," *Kurier*, October 29, 2024. See also "Anschlag auf Taylor-Swift-Konzert: 'Sehe viele potenzielle Opfer,'" *Kurier*, October 20, 2024.
111 Stockhammer and Clarke.
112 "Dokumentationsstelle Politischer Islam warnt vor 'Hipster-Salafisten,'" *Die Presse*, June 17, 2024.
113 Erin Saltman and Micalie Hunt, "Borderline Content: Understanding the Gray Zone," Global Internet Forum to Counter Terrorism, GIFCT Insight, June 29, 2023.
114 Stockhammer and Clarke.
115 Giorgia Cascone and Marina Mancuso, "Online radicalisation, extremism and terrorism," Key results of the research conducted under the EU-funded project ALLIES, Milan: Transcrime – Joint Research Centre on Innovation and Crime 2025, p. 7.
116 Paul Kirby, "Syrian admits triple murder at trial for German knife attack," BBC, May 27, 2025.
117 For a detailed analysis of the Solingen attack in the light of inner-German political perceptions, see Julika Enslin, "The Evolution of the Islamist Terror Threat Landscape in Germany Since 2020," *CTC Sentinel* 18:5 (2025), p. 41.
118 "Beweise 'erdrückend' - worum es im Solingen-Prozess geht," Tagesschau, May 27, 2025.
119 "Planvoll, zielgerichtet - eng abgestimmt mit dem IS," Tagesschau, May 22, 2025.

120 "Terroranschlag auf Stadtfest von Solingen: Generalbundesanwalt erhebt Anklage wegen Mordes," Legal Tribune Online, February 27, 2025.
121 "'Islamischer Staat' reklamiert Anschlag in Solingen für sich," Tagesschau, August 24, 2024.
122 Michael Götschenberg, "Ein Anschlag im Namen des IS?" Tagesschau, August 26, 2024.
123 Marcel Fürstenau, "Solingen: Radikalisierung durch Social Media?" Deutsche Welle, August 29, 2024.
124 Wolf Wiedmann-Schmidt, "Treueschwur im Dönerimbiss," *Der Spiegel*, May 17, 2025, pp. 38-39.
125 Ibid.
126 "Planvoll, zielgerichtet - eng abgestimmt mit dem IS."
127 Ibid.
128 "Messeranschlag von Solingen: Angeklagter gesteht die Tat," WDR, May 27, 2025.
129 "'Es ist definitiv ein Video, das den Attentäter zeigt,'" Tagesschau, August 27, 2024.
130 Wiedmann-Schmidt.
131 Manuel Bewarder and Florian Flade, "Solingen: Hat der Tatverdächtige falsche Asylangaben gemacht?" Tagesschau, August 26, 2024.
132 "NRW-Flüchtlingsministerin gesteht Systemversagen bei Abschiebung des Solingen-Attentäters," *Die Welt*, August 28, 2024.
133 "Regierung einigt sich auf Sicherheits- und Asylpaket," Tagesschau, August 29, 2024.
134 "Austria arrests teen over foiled plot to attack Vienna station," Voice of America, February 19, 2025.
135 "Brutale Attacke in Österreich. IS-Messerangreifer von Villach wollte nach Deutschland, wurde aber abgewiesen," *Focus*, February 18, 2025.
136 "Messerangriff in Villach 'islamistischer Anschlag mit IS-Bezug,'" *Der Standard*, February 16, 2025.
137 Ibid.
138 "Grinse-Terrorist: 'Wollte so viele töten wie möglich!'"
139 Ibid.
140 "Attentäter von Villach streamte vor dem Anschlag Propagandavideos."
141 Stefan Goertz and Nicolas Stockhammer, *Terrorismusbekämpfung und Extremismusprävention* (Wiesbaden: Springer 2023), p. 219.
142 James Angove, "Stochastic terrorism: critical reflections on an emerging concept," *Critical Studies on Terrorism* 17:1 (2024).
143 "Villach-Anschlag: Attentäter fühlte sich 'stark' und stach zu," PULS24 News, May 8, 2025.
144 "Grinse-Terrorist: 'Wollte so viele töten wie möglich!'"
145 "Warum nun gegen den 'Helden von Villach' ermittelt wird," *Die Presse*, February 26, 2025.
146 "Messerangriff in Villach 'islamistischer Anschlag mit IS-Bezug.'"
147 Valentini, Lorusso and Stephan, pp. 1-15; Charlie Winter, Peter R. Neumann, Magnus Ranstorp, Lorenzo Vidino et al., "Online Extremism: Research Trends in Internet Activism, Radicalization, and Counter-Strategies," *International Journal of Conflict and Violence* 14:2 (2020): p. 2.
148 Joe Whittaker, "Onlife Radicalisation: Understanding the Online/Offline Nexus," ECTC Advisory Network Conference, The Hague, 2023.
149 "Minister fordert 'anlasslose Massenüberprüfung,'" Tagesschau, February 17, 2025.
150 Stockhammer, "European Trend Report on Terrorism 2025."
151 Victoria Joshua and Juliana George, "Echo Chambers in 15 Seconds: How TikTok Algorithms Create Isolated Realities for Gen Z Audiences," available via ResearchGate, February 5, 2025.
152 Joe Whittaker, Sean Looney, Alastair Reed, and Fabio Votta, "Recommender systems and the amplification of extremist content," *Internet Policy Review* 10:2 (2021); Gabriel Weimann and Natalie Masri, "Research Note: Spreading Hate on TikTok," *Studies in Conflict & Terrorism* 46:5 (2023): pp. 752-765; Areeba Shah, "TikTok's algorithm is pushing out extremist and violent content to 13-year-olds," Salon, March 25, 2023.

The Escalation of U.S. Airstrikes in Somalia and the Role of Perceived Threats to the U.S. Homeland

By David Sterman

In 2025, the United States substantially increased the pace of its airstrikes in Somalia. At the same time, it increasingly cited not just regional security rationales for the increased pace of strikes but also rationales rooted in an assessed potential threat to the U.S. homeland from Somalia—in particular from the Islamic State-Somalia's recruitment of foreign fighters. This article examines the increased pace of strikes, the rationales that have been cited to explain the increase, and what existing evidence reveals about the potential threat to the U.S. homeland. It also underscores the need for greater clarity from the U.S. government regarding its assessment of the extent of such a threat.

The United States is currently waging a stepped-up air campaign against jihadi groups in Somalia. According to information released by United States Africa Command (AFRICOM), between February 1, when the Trump administration conducted the first strike in Somalia of 2025, and June 10, the United States conducted 38 strikes against the Islamic State in Somalia and al-Shabaab. Additional strikes after June 10 have also been conducted.[a] The rationales surrounding the increase in strikes relate to concerns about regional security (including the threat to Somalia's federal government), but also exhibit an increasingly prominent discussion of the potential threat to the U.S. homeland. Both rationales are driven in part by the perceived role that foreign fighters play in the Islamic State in Somalia.

To shed light on the escalation of the U.S. airstrike campaign in Somalia and the role of homeland security rationales in motivating the increase in strikes, this article proceeds in five parts. First, it provides an account of the escalation in strikes this year. Second, it examines the rationales behind this increase, looking at the distinct roles of homeland security and regional security rationales. Third, it considers the specific though fragmentary reporting on the role of foreign fighters. Fourth, it examines what can be gleaned about the homeland security threat from a review of cases of Americans seeking to join jihadi groups in Somalia since the fall of the Islamic State's capital in Syria in 2017. Finally, it concludes with a short discussion of the importance of greater clarity regarding the government's assessment of the threat to the homeland from Somalia—and the disaggregation of homeland security from regional security rationales in analyzing the escalated use of air strikes.

A Stepped-Up U.S. Air Campaign in Somalia

When President Trump took office for his second term, it was far from clear how his administration would approach the issue of U.S. counterterrorism operations in Somalia.[1] At the end of his first term, Trump had ordered the withdrawal of U.S. advisory forces from Somalia—a position that former members of his administration linked to a view that key U.S. interests were not at risk in the country.[2] Debate over the extent of U.S. commitment in Somalia has continued into the second Trump administration.[3]

Then, on February 1, AFRICOM conducted its first strike in Somalia of 2025, targeting Islamic State-Somalia in a series of caves southeast of Bossaso, a major port city in the semi-autonomous Puntland state of Somalia.[4] In the aftermath of that strike, it was still not clear whether it was a one-off operation or the beginning of a larger escalation. Mohamed Mubarak, the head of Puntland's security coordination office, told the BBC, "We don't know if the Americans will conduct more than one airstrike."[5] Matt Bryden, a longtime analyst of the situation in Somalia, likewise told the BBC, "The strike does not mean that the US government is going to step up its military engagement in Somalia."[6] A *Washington Post* profile later that month on the rise of the Islamic State in Somalia and the semi-autonomous Somali state of Puntland's military campaign against it cited an anonymous AFRICOM official as saying that Puntland counterterrorism operations were not receiving support from AFRICOM. The piece stated, "Beyond the strike, the Trump

a The strike tallies examined here are based upon AFRICOM's declared strikes, drawing from the following sources: author correspondence, AFRICOM Public Affairs, May and June 2025, and Peter Bergen, Melissa Salyk-Virk, and David Sterman, "America's Counterterrorism Wars: The War in Somalia," New America, accessed July 2, 2025. As the analysis here relies on AFRICOM's own declared count of strikes, strikes are defined using the command's definition, which can include the use of multiple munitions. The one exception is that for ease of reference, ground raids are counted as a single strike. AFRICOM does not count ground operations as strikes. The only ground operation in the data analyzed here (covering 2021 through June 10, 2025) is the January 25, 2023, raid that killed Bilal al-Sudani. It is worth noting that there is a question as to whether some strikes that AFRICOM has counted as single strikes might be better understood as having been multiple strikes hitting distinct targets rather than a single strike using multiple munitions. On this question, see the discussion of reporting around the February 1, 2025, strike in Caleb Weiss, "Trump Admin Ups the Tempo of Airstrikes against Jihadist Groups in Somalia," FDD's Long War Journal, March 30, 2025.

David Sterman is Deputy Director of the Future Security program at New America. His current research focuses on terrorism and violent extremism in America, immigration and terrorist threats, foreign fighter recruitment, and the effectiveness and consequences of American counterterrorism efforts. Sterman's writing on terrorism has appeared in CNN, Foreign Policy, Time, *and* The Washington Post *among other outlets, and his research has been cited by CNN, FOX, MSNBC,* The New York Times, The Washington Post, *and* The Wall Street Journal.

administration has not detailed its plans for Somalia. Africom said it was unable to comment on future policy."[7]

It has since become clear that there has been a significant escalation in strikes. By June 10, 2025, AFRICOM had conducted 38 strikes in Somalia—almost four times the number that it conducted in all of 2024, and more than it had conducted in any year during the Biden administration.[8] The increase should be examined as two distinct sets of strikes: those against the Islamic State in Somalia and those against al-Shabaab.

U.S. Strikes Against Islamic State-Somalia

First, the United States has substantially escalated its operations against the Islamic State in Somalia, moving from a position of targeting senior leaders to a posture of supporting a large counterterrorism operation by Somalia's semi-autonomous Puntland state.

Of the 38 strikes AFRICOM conducted through June 10, 22 targeted the Islamic State in Somalia. In 2024, the United States conducted only one strike targeting Islamic State-Somalia.[9] Moreover, U.S. strikes against Islamic State-Somalia appear to have gone beyond the targeting of senior leaders.

AFRICOM issued six press releases regarding strikes targeting Islamic State-Somalia that labeled the seven strikes they covered as collective self-defense strikes, a category that is meant to focus on disrupting threats to U.S. or partner forces rather than offensively striking high-value targets or generalized enemy formations.[10] The other 15 strikes against Islamic State-Somalia may have targeted senior leaders (as appears to have been the case with the February 1, 2025, strike), involved offensive targeting of the group's forces beyond its senior leadership, or even been collective self-defense strikes that were not labeled as such.

In contrast, the United States declared only two strikes or operations against Islamic State-Somalia during the Biden administration, and both targeted senior Islamic State-Somalia leaders. Neither operation was framed as collective self-defense. The first occurred on January 25, 2023, when the United States conducted a ground raid in northern Somalia, targeting and killing Bilal al-Sudani, who the United States described as "an ISIS leader in Somalia and a key facilitator for ISIS's global network"[11] (more on al-Sudani below). The other occurred on May 31, 2024, when the United States conducted a strike "targeting ISIS militants ... in a remote area in the vicinity of Dhaardaar, approximately 81 km southeast of Bosaso, Somalia."[12] This strike was widely reported as having targeted Abdulqadir Mumin, an Islamic State-Somalia leader who also holds a senior role in the Islamic State's global architecture and who was even rumored to be the new overall Islamic State leader.[13]

U.S. Strikes Against al-Shabaab

AFRICOM conducted 16 strikes against al-Shabaab in 2025 through June 10. This constitutes an increase from the nine strikes that AFRICOM declared conducting against al-Shabaab in 2024.[14] In 2023, the United States declared 18 strikes against al-Shabaab.[15] Since the cut-off for the data examined in this article, the United States has already surpassed the number of strikes conducted against al-Shabaab in 2023 despite there being still several months left in the year.

However, the number of strikes against al-Shabaab so far in 2025 increased less sharply than those against the Islamic State. In addition, at least during the first months of this year, U.S. strikes against al-Shabaab did not appear to be deadlier than previous strikes.

Assessing the U.S. CT campaign in Somalia based on the death tolls from U.S. strikes is difficult because independent reporting on the toll of strikes is minimal to non-existent in many cases. Moreover, AFRICOM, which was already inconsistently reporting assessed death tolls in its press releases, stopped providing death toll assessments in response to queries as a matter of policy at some point in April or May 2025, telling reporters that "we are temporarily refraining from publishing casualty estimates while the new administration finalizes its policy."[16]

However, one can analyze AFRICOM's assessed death tolls for its early strikes. Of the 16 strikes against al-Shabaab declared by AFRICOM in the time period examined here, New America received information on initial death toll assessments for eight. The average initial AFRICOM assessed death toll for these strikes was about 1.4 militants per strike.[17] This is a lower government-assessed deaths per strike average for strikes targeting al-Shabaab than in 2023 (about 6.1 militants per strike) or 2024 (about 4.2 militants per strike).[18] These numbers suggest that at least in the first months of 2025, U.S. strikes against al-Shabaab did not see a shift to major offensive strikes on massed al-Shabaab forces of the kind that killed tens or even in one case more than 100 militants during the escalation of strikes in the first Trump administration.[19] However, that may have changed.

Regional and Homeland Security Rationales

When the United States initiated its war against the Islamic State in Iraq and Syria in 2014, its decision-making was influenced by a range of rationales, including the group's direct threat to regional security and the perception of a potential threat to the U.S. homeland if the group's capabilities were allowed to grow.[20] As the United States steps up its strikes against the Islamic State in Somalia (and against al-Shabaab), a similar mix of rationales focused on the regional security threat and a potential threat to the homeland appears to be influencing decision-making.

The United States has long viewed al-Shabaab primarily through the lens of its threat to regional security. For example, the intelligence community's 2010 Worldwide Threat Assessment assessed "most Al-Shabaab and East Africa-based al-Qa'ida members will remain focused on regional objectives in the near-term," and the 2012 version assessed that "most al-Shabaab members in 2012 will remain focused on battling AMISOM, TFG, and Ethiopian/Kenyan-backed forces in Somalia."[21] Michael Vickers, who served in senior government roles between 2007 and 2015 and oversaw key raids in Somalia, wrote in his memoir, "Al-Shabaab was mostly a regional threat, so it received far less of my attention than AQAP and al-Qai'da in Syria."[22]

In 2016, when AFRICOM began issuing press releases on its website regarding strikes, the press releases emphasized regional security.[23] For example, a press release for a September 26, 2016, strike stated, "The U.S. remains committed to our partners in eliminating terrorism and advancing security in the region. Violent extremists endanger the safety and stability of the Somali people; countering these threats remains in our common interests," but did not include a reference to the U.S. homeland.[24]

The United States' stepped-up strikes against al-Shabaab in 2025 are likely driven by conditions on the battlefield and an

Carrier Air Wing (CVW) 1 conducts routine flight operations from the Nimitz-class aircraft carrier USS Harry S. Truman (CVN 75) in the U.S. Central Command area of responsibility on February 1, 2025, the date U.S. Africa Command stated it had conducted airstrikes against Islamic State-Somalia. (U.S. Navy)

increased perception of a regional security threat. In 2025, al-Shabaab mounted an offensive that at the least reversed some of the Somali government's gains in prior offensives and, according to at least some analysts, may pose a threat to Mogadishu itself, the Somali government's seat of power.[25] Notably, other non-U.S. partners of the Somali government also stepped up their activity in response to the offensive.[26]

In addition, the assertion that al-Shabaab has developed ties over the past couple years with Yemen's Houthi rebels further contributes to the regional security rationale for strikes.[27] During his testimony on AFRICOM's 2025 Posture Statement, General Michael Langley, AFRICOM's commander, stated, "Al-Shabaab is especially a heightened terrorist threat, namely because they're colluding with the Houthis across from Yemen."[28]

While historically regional security has been the main concern regarding jihadi groups in Somalia, in recent years, concerns about a potential threat to the U.S. homeland have grown in prominence. In 2019, the Philippines arrested a Kenyan national who received training from al-Shabaab and who the United States later charged and convicted of plotting a 9/11-like attack that would have involved crashing a hijacked plane into a building.[29] In the wake of news of the arrest, then-Commander of AFRICOM General Stephen J. Townsend testified to Congress in 2020 that "Shabab is a very real threat to Somalia, the region, the international community and even the U.S. homeland," although the Defense Intelligence Agency still assessed that al-Shabaab posed a low threat to the homeland.[30]

The emergence of the Islamic State in Somalia likewise contributed to a growing perception of a homeland threat. Islamic State-Somalia posed a far lesser threat to regional security in territorial terms than al-Shabaab.[31] Initially, the Islamic State did not even acknowledge those who had declared an Islamic State group in Somalia under Mumin's leadership as an official province, but when it officially recognized them, it did so in a December 2017 video promoting attacks in the West.[32] While its ability to pose a territorial threat was limited, Islamic State-Somalia's connection to global Islamic State networks and the role of foreign fighters in its ranks amplified concern about threats beyond Somalia.[33] These connections not only bolstered concern about potential attacks on the U.S. homeland but also the ways Islamic State-Somalia could pose a regional security threat without threatening Somalia's control of territory by providing financial and other support to other parts of the Islamic State's network.[34]

Concern about the presence of foreign fighters in Somalia and the potential for attacks against the U.S. homeland is not entirely new nor a product solely of the Islamic State's mobilization. In the aftermath of the 2006 Ethiopian invasion of Somalia, the FBI began paying close attention to a flow of foreigners to Somalia, including Americans.[35] This mobilization, and the networks it

revealed, did raise concern among American policymakers, but these concerns were primarily in the realm of the potential for a larger, future threat rather than a perception of an existing direct threat. As Philip Mudd, then Associate Executive Assistant Director of the FBI's National Security Branch, testified in 2009, "While there are no current indicators that any of the individuals who traveled to Somalia have been selected, trained, or tasked by al-Shabaab or other extremists to conduct attacks inside the United States, we remain concerned about this possibility and that it might be exploited in the future if other U.S. persons travel to Somalia for similar purposes."[36]

In addition, the earliest U.S. counterterrorism operations and strikes in Somalia sought to eliminate al-Qa`ida's East African hub. This network hub was made up mainly of the local remnants of the 1998 East Africa Embassy Bombing network. One figure tied to the network hub—Saleh Nabhan, a Kenyan—was killed in a helicopter raid in September 2009.[37] After his death, American officials noted his reported connection to the training of foreign militants, including Americans.[38] In 2011, Fazul Harun, a figure within the network who hailed originally from the Comoros Islands, was not killed by a U.S. strike but by Somali forces at a checkpoint.[39] He reportedly had documents on him suggesting he may have been planning an attack in the United Kingdom and was considering using British foreign fighters who had traveled to Somalia to carry out the attack.[40] Just the previous year, the travel of U.K. residents to Somalia led Britain's then-head of MI5 to state, "I am concerned that it's only a matter of time before we see terrorism on our streets inspired by those who are today fighting alongside al-Shabaab."[41]

As noted, U.S. intelligence assessments from this period still viewed jihadis in Somalia as primarily a regional threat, but they also revealed broader concerns. For example, in 2010, the intelligence community assessed: "East Africa-based al-Qa'ida leaders or al Shabaab may elect to redirect to the Homeland some of the Westerners, including North Americans, now training and fighting in Somalia."[42] In 2012, the intelligence community assessed that "members of the group—particularly a foreign fighter cadre that includes US passport holders—may also have aspirations to attack inside the United States; however, we lack insight into concrete operational plans outside the Horn of Africa."[43]

This year, 2025, appears to mark a shift in the United States' perception or at least its presentation of the threat to the homeland from Somalia. In 2025, AFRICOM adopted language in its press releases regarding strikes in Somalia that raises the specter of a potential threat to the U.S. homeland. With the exception of the first strike on February 1, 2025,[b] and one strike against vessels in Somali territorial waters that were allegedly carrying "advanced conventional weapons" to al-Shabaab, every press release announcing a strike in Somalia during the period examined in this article included a variation of the following lines: "Degrading ISIS and other terrorist organizations' ability to plot and conduct attacks that threaten the U.S. homeland, our partners, and civilians remains central to U.S. Africa Command's mission" or "Degrading al Shabaab and other terrorist organizations' ability to plot and conduct attacks that threaten the U.S. homeland, our partners, and civilians remains central to U.S. Africa Command's mission."

In 2024, AFRICOM only referred to threats to the homeland in one of its 10 press releases regarding strikes in Somalia, the press release for the strike that reportedly targeted Abdulqadir Mumin, who plays a senior role in the Islamic State's global activity and is even rumored by some to be the Islamic State's latest "caliph."[44]

In his April 2025 statement before the Senate Armed Services Committee, General Michael E. Langley, AFRICOM's commander, made five references to the threat that jihadi groups in Africa might pose to the "homeland."[45] He emphasized, "We are acutely aware that if ISIS and al-Qaeda groups continue their expansion, they will pose a direct threat to the U.S. homeland."[46] He also specifically referenced the aforementioned "9/11 style terror attack on the U.S."[47] Langley's phrasing suggests that U.S. efforts are still—to some extent—preventive with the main threat lying in the future if action is not taken to prevent Islamic State-Somalia and al-Shabaab's growth.

The question of foreign fighter recruitment played an important role in General Langley's discussion of such expansion and its relation to a threat to the homeland. His 2025 AFRICOM Posture Statement directly connected Islamic State-Somalia's foreign fighter recruitment to concerns about potential threats to the homeland, stating, "For now, ISIS and al-Qaeda groups are focused on local interests, but they continue to expand and recruit fighters from around the world to position themselves to attack the Homeland. The dangerous capabilities of these groups, if not addressed, will continue to threaten U.S. interests."[48]

Historically, foreign fighter recruitment has played a similar role in perceptions of threats to the homeland and their mobilization to support the use of force based in preventive logic. When President Obama announced his decision to expand the counter-Islamic State war into Syria and beyond initially limited objectives in Iraq, a key part of his argument that "if left unchecked, these terrorists could pose a growing threat beyond that region, including to the United States" was that "our Intelligence Community believes that thousands of foreigners -- including Europeans and some Americans -- have joined them in Syria and Iraq. Trained and battle-hardened, these fighters could try to return to their home countries and carry out deadly attacks."[49] General Langley's testimony on Somalia closely resembles this phrasing.

Foreign Fighter Dynamics

Reporting on the number and role of foreign fighters in the Islamic State in Somalia's structure is fragmentary and incomplete. However, numerous reports suggest they play an important role. In February 2025, *The Washington Post* wrote, "according to U.S. Africa Command (Africom), and local officials estimate there are as many as 1,000 militants under its command," adding that "large numbers of foreign fighters have flowed into Somalia, establishing a formidable force that now threatens Western targets."[50] More recently, a U.S. defense official estimated that Islamic State-Somalia's force had grown from around 500 fighters to 1,600 with about 60 percent being foreign fighters.[51]

b While the initial press release for the February 1, 2025, strike did not include such a reference, a later update announcing that the strike had killed a senior Islamic State-Somalia operative did. See "Update: U.S. Forces Strike on ISIS-Somalia," U.S. Africa Command, February 11, 2025. There is also one declared strike in 2025 that was not reported via a press release and thus is not applicable to this analysis of the language used in press releases. "2025 Airstrikes," United States Africa Command, n.d.; "U.S. Forces Strike ISIS-Somalia," U.S. Africa Command, February 16, 2025; "Federal Government of Somalia Engages al Shabaab with Support from U.S. Forces," U.S. Africa Command, February 22, 2025; "U.S. Forces Conduct Strike Targeting al Shabaab," U.S. Africa Command, April 18, 2025.

Insight into the alleged role of foreign fighters in Islamic State-Somalia is provided by fragmentary reports regarding those killed and imprisoned as part of Puntland's counterterrorism operations.[52] *The Washington Post* noted that Puntland's prisons held numerous foreigners accused of joining Islamic State-Somalia, including a group of six Moroccans one of whom told the *Post*, "We trained with Kalashnikovs, in a group of around 30 people — Algerians, Moroccans, Tunisians, Somalis and two Palestinians."[53] Likewise, in February 2025, Voice of America reported that Puntland authorities claimed dozens of the some 200 Islamic State-Somalia fighters they had killed were foreigners.[54]

In addition, some of Islamic State-Somalia's senior figures, who have been targeted or killed by U.S. strikes in recent years, are foreign fighters, Somalis who have spent significant time outside of Somalia, and/or those who have allegedly played roles in the recruitment of foreign fighters. For example, Ahmed Maeleninine, who was reportedly killed in the February 1, 2025, strike, was born in Oman, according to Puntland officials.[55] The U.S. press release on his death did not mention his nationality, but did emphasize his role as a "key ISIS recruiter."[56] Likewise, Bilal al-Sudani, who was killed in a U.S. ground raid in 2023, was a Sudanese man, sanctioned in 2012 for activity dating back to 2007 where he would act as a "facilitator for the entry of foreign fighters and extremists into Somalia" including a 2010 case where he "facilitated the travel of extremists from Chad to Somalia."[57] When he was killed, the United States emphasized his role in enabling "ISIS's expansion and activities across Africa and beyond the continent, in particular by providing funding to sustain the operational capabilities of ISIS elements around the world" including in Afghanistan via support for the Islamic State-Khorasan branch.[58] Abdulqadir Mumin, who was the target of the May 31, 2024, strike in Somalia, was born in Puntland, but spent time in Sweden and the United Kingdom, where some reports speculated he crossed paths with militants and may have been involved in a recruitment and radicalization network, before returning to Somalia.[59]

Al-Shabaab also historically sought to recruit and benefit from foreign fighters, including those from Europe and the United States, sparking somewhat similar concerns (albeit concerns generally discussed with more circumspection) about potential homeland attacks. It is worth noting that the Islamic State's recruitment of foreign fighters can be seen in part as a continuation of activity under al-Shabaab. Until 2015, the Islamic State in Somalia's key members were still mainly associated with al-Shabaab. For example, when the United States sanctioned al-Sudani in 2012, it described his activity as being "on behalf of al-Shabaab."[60] However, al-Shabaab's efforts to take advantage of foreign fighter recruitment stumbled in the 2010s for a variety of reasons, including in-fighting, law enforcement and military pressure, and the rising prominence of the Islamic State in Iraq and Syria and other groups/locations as preferred destinations for and influence upon foreign fighters.[61] Today, it is the perceived growth in the Islamic State's foreign fighter cadre rather than foreigners fighting with al-Shabaab that has dominated discussion of the extent of the threat to the U.S. homeland from Somalia.

"Today, it is the perceived growth in the Islamic State's foreign fighter cadre rather than foreigners fighting with al-Shabaab that has dominated discussion of the extent of the threat to the U.S. homeland from Somalia."

Aspiring and Actual American Foreign Fighters and Somalia

When AFRICOM announced that senior Islamic State-Somalia figure Ahmed Maeleninine had been killed in its February 1, 2025, strike, it alleged that one of his roles was as an "external operations leader responsible for the deployment of jihadists into the United States and across Europe."[62] This is a significant allegation about potential direct threats to the United States, but AFRICOM has not provided further details on the nature of the alleged U.S. nexus.

There have been reports of alleged Islamic State-Somalia links to terrorism cases in Europe—specifically in Sweden in 2024 and in Italy in 2018.[63] Of the case in Italy, a United Nations Panel of Experts on Somalia report stated that the arrested individual, Omar Moshin Ibrahim, had entered Italy in 2016, received training in Libya prior to his entry, and "during his time in Italy, he maintained communication with ISIL affiliates in Somalia and Kenya."[64] However, the report also stated that "intercepted communications" suggested that the actual plot he was arrested for "was not directly tasked by ISIL operatives outside the country" and "was rudimentary and had little chance of success."[65]

A review of cases of Americans (and others present in the United States) accused of jihadi terrorism-related criminal activity since the fall of the Islamic State's capital of Raqqa in October 2017 provides seven cases of Americans who have either traveled or sought to or aided travel to Somalia.[66] What it does not seem to provide is any case of an individual who received training from Islamic State-Somalia being deployed back to the United States. Further, all but one case involved failed attempts to travel to Somalia.

On February 27, 2025, the United States arrested Abdisatar Ahmed Hassan, a 22-year-old Minnesota resident and ethnic Somali born in Kenya, charging him with attempting to provide material support to a foreign terrorist organization in relation to two unsuccessful attempts "to travel from Minnesota to Somalia to join ISIS."[67] Beyond his attempted travel, the complaint alleges that he posted a video praising the deadly January 1, 2025, attack in New Orleans, which was seemingly inspired by the Islamic State.[68] The criminal complaint in the case alleges that Hassan consumed a range of Islamic State-Somalia and al-Shabaab propaganda online and interacted with a Facebook account named the Manjaniq Media Center, which per the complaint describes itself as "a media organization that nurtures the righteous youth of the Islamic Caliphate" and whose posts encourage "Somali-speaking individuals to travel and fight on behalf of ISIS."[69] Hassan appears to have been on law enforcement's radar screen before both of his attempts to join Islamic State-Somalia, both of which were closely monitored, due in part to his activity online.[70]

About four months earlier, in October 2024, the United States arrested Michael Sam Teekaye, Jr., a 21-year-old Maryland resident, alleging that he had attempted to travel to join the Islamic State in Somalia, and had told an undercover officer that he "was in contact with a Somali ISIS fighter regarding his plans to travel to Somalia

to join ISIS" and that his "'plan B' was to carry out an attack in the United States against people who support Israel."[71] However, it is worth noting that in addition to being monitored by an undercover officer, Teekaye had a reported history of mental health issues including a diagnosis of schizophrenia and two hospitalizations.[72]

The year before Teekaye's arrest, in December 2023, the United States charged Karrem Nasr, a 23-year-old U.S. citizen, with allegedly trying to join al-Shabaab.[73] The individual who Nasr believed to be an al-Shabaab facilitator helping him plan his trip from Egypt, where he was living, to Kenya (where he was arrested) and onto Somalia, was in fact an informant.[74] Nasr pled guilty in January 2025.[75]

In 2019, the United States charged three men, all Kenyan-born men holding U.S. citizenship and connected by family ties, with attempting to travel (or supporting members of the group's travel) to Somalia to join the Islamic State.[76] The case involved monitoring of social media activity and the use of undercover officers dating back years.[77] All three men were convicted and sentenced for their involvement.[78]

The only case involving an individual who succeeded in joining Islamic State-Somalia is also the oldest case. In January 2018, the United States filed a criminal complaint alleging that Harafa Hussein Abdi, a U.S. citizen, left the United States in 2015 (prior to the fall of the Islamic State's capital in Raqqa), traveled to Somalia, and received training from an Islamic State group affiliated with the aforementioned Mumin in Puntland.[79] Notably, while with the Islamic State in Somalia, Abdi promoted travel to join the group via social media and appeared in Islamic State propaganda, according to the complaint.[80] The United States also alleged that Abdi distributed a rap whose lyrics praised violence inside the United States before a dispute led him to leave the group, leading to his arrest in East Africa.[81] Yet, the case does not provide clear evidence that the group managed to train recruits and send them back to the United States. The case appears to be evidence of, as another article examining the Islamic State-Somalia global threat has put it, "the potential danger Islamic State-Somalia poses in encouraging terror plots abroad."[82] Now, more than a half a decade after Abdi was arrested and charged, caution is merited when citing his case to assess the state of that potential threat today given the seeming paucity of similar cases and the possibility that the conditions that made his journey possible may have changed.

The cases examined above do provide reason to pay attention to Islamic State-Somalia and the involvement of Americans or other foreign fighters in its activity. There does appear to be continuing interest among some Americans in joining jihadi groups (including Islamic State-Somalia) in Somalia. At least some of those who have considered fighting in Somalia have also allegedly expressed support for attacks inside the United States,[83] and there does appear to have been an effort on the part of Islamic State-Somalia to reach out and encourage travel.

However, the cases that have been charged so far in the United States do not suggest an imminent threat. While it is possible that there are individuals who have not been charged, the known cases do not show a developed capability or effort to send fighters back to the United States to conduct attacks. Moreover, the cases suggest that Americans who seek to join Somali jihadi groups face challenges in avoiding detection.

Conclusion

In 2025, the United States has substantially escalated its strikes in Somalia and embarked on a new campaign aimed at the Islamic State in Somalia. This escalation has been justified in part by references to the threat posed by foreign fighters in the Islamic State-Somalia's ranks along with an increase in references to a potential threat to the U.S. homeland. While there is reason to believe that the potential threat to the homeland from Somalia may have grown in recent years, the American public and policymakers would benefit from greater clarity on the basis for any such assessment. CTC

Citations

1 See, for example, David Sterman, "What Is the Future of American Counterterrorism Strikes in Somalia?" Just Security, December 19, 2024.
2 Christopher C. Miller, *Soldier Secretary* (Nashville: Center Street, 2023), pp. 192-193; Mark Esper, *A Sacred Oath: Memoirs of a Secretary of Defense during Extraordinary Times* (New York: William Morrow, an imprint of HarperCollins Publishers, 2022), p. 604.
3 Charlie Savage and Eric Schmitt, "Trump Team Divided Over Future of U.S. Counterterrorism Operations in Somalia," *New York Times*, April 10, 2025.
4 "U.S. Forces Conduct Strike Targeting ISIS-Somalia," U.S. Africa Command, February 1, 2025; "Update: U.S. Forces Strike on ISIS-Somalia," U.S. Africa Command, February 11, 2025.
5 Mary Harper, "Why Trump Is on the Warpath in Somalia," BBC, February 6, 2025.
6 Ibid.
7 Katharine Houreld, "The Islamic State Has Regrouped in Somalia — and Has Global Ambitions," *Washington Post*, February 11, 2025.
8 Author correspondence, AFRICOM Public Affairs, June 2025; Bergen, Salyk-Virk, and Sterman.
9 "2024 Airstrikes," United States Africa Command, accessed June 25, 2025; "U.S. Forces Conduct Strike Targeting ISIS," U.S. Africa Command Public Affairs, May 31, 2024; Bergen, Salyk-Virk, and Sterman.
10 The press releases in question are: "U.S. Forces Conduct Strike against ISIS-Somalia," U.S. Africa Command, April 1, 2025; "Federal Government of Somalia Engages ISIS-Somalia with Support from U.S. Forces," U.S. Africa Command, April 18, 2025; "U.S. Forces Conduct Strike Targeting ISIS-Somalia," U.S. Africa Command, April 21, 2025; "U.S. Forces Conduct

Strike Targeting ISIS-Somalia," U.S. Africa Command, April 24, 2025; "U.S. Forces Conduct Strike Targeting ISIS-Somalia," U.S. Africa Command, June 4, 2025; "U.S. Forces Conduct Strike Targeting ISIS-Somalia," U.S. Africa Command, June 10, 2025. The press release on April 1 covered two strikes. Author correspondence, AFRICOM Public Affairs, May 2025. On collective self-defense strikes and an analysis of the historical distinctions between kinds of strikes, see David Sterman, "The Three Kinds of Declared U.S. Strikes in Somalia in 2023," New America, January 10, 2024; Sarah Harrison, "What the White House Use of Force Policy Means for the War in Somalia," Just Security, October 20, 2022; and Oona A. Hathaway and Luke Hartig, "Still at War: The United States in Somalia," Just Security, March 31, 2022.

11 "Background Press Call by Senior Administration Officials on a Successful Counterterrorism Operation in Somalia," The White House, January 26, 2023; "Statement by Secretary of Defense Lloyd J. Austin III on Somalia Operation," U.S. Department of Defense, January 26, 2023.

12 "U.S. Forces Conduct Strike Targeting ISIS," May 31, 2024.

13 Courtney Kube, "Global Leader of ISIS Targeted and Possibly Killed in U.S. Airstrike," NBC, June 15, 2024.

14 "2024 Airstrikes;" Bergen, Salyk-Virk, and Sterman.

15 Sterman, "The Three Kinds of Declared U.S. Strikes in Somalia in 2023;" Bergen, Salyk-Virk, and Sterman.

16 The quote is from "AFRICOM Halts Disclosure of Somalia Airstrike Casualties amid Trump Policy Review," Shabelle Media Network, May 20, 2025. The author received a similar, though slightly differently worded, response to a query about death tolls on May 7, 2025. Author correspondence, AFRICOM Public Affairs, May 2025.

17 For details, see David Sterman, "AFRICOM Provides Death Tolls for 2025 Strikes," New America, April 3, 2025; and Bergen, Salyk-Virk, and Sterman.

18 David Sterman, "How Many People Does the U.S. Assess It Killed in Somalia in 2023?" New America, April 2, 2024; Sterman, "What Is the Future of American Counterterrorism Strikes in Somalia?"; "2024 Airstrikes."

19 Sterman, "The Three Kinds of Declared U.S. Strikes in Somalia in 2023."

20 David Sterman, "Decision-Making in the Counter-ISIS War: Assessing the Role of Preventive War Logic," New America, November 15, 2019.

21 Dennis C. Blair, "Annual Threat Assessment of the US Intelligence Community for the Senate Select Committee on Intelligence," Office of the Director of National Intelligence, February 2, 2010, p. 11; James R. Clapper, "Unclassified Statement for the Record on the Worldwide Threat Assessment of the US Intelligence Community for the Senate Select Committee on Intelligence," Office of the Director of National Intelligence, January 31, 2012, p. 4.

22 Michael G. Vickers, *By All Means Available: Memoirs of a Life in Intelligence, Special Operations, and Strategy* (New York: Alfred A. Knopf, 2023), p. 255.

23 "2016 Airstrikes," United States Africa Command, accessed June 26, 2025.

24 "U.S. Self-Defense Strikes in Somalia," U.S. Africa Command, September 27, 2016.

25 Ashley Jackson, "Flailing State: The Resurgence of al-Shabaab in Somalia," War on the Rocks, June 3, 2025; Daisy Muibu and Yayedior Mbengue, "Somalia at a Crossroads: Resurgent Insurgents, Fragmented Politics, and the Uncertain Future of AUSSOM," *CTC Sentinel* 18:5 (2025).

26 Kathryn Tyson, Yale Ford, and Liam Karr, "Africa File, May 1, 2025: AU, Turkey, and United States Surge to Halt al Shabaab; DRC Peace Talks; Uganda's Role in the Eastern DRC," Critical Threats Project, May 1, 2025.

27 "Expanding Al Shabaab–Houthi Ties Escalate Security Threats to Red Sea Region," Africa Center for Strategic Studies, May 28, 2025; Ibrahim Jalal and Adnan al-Jabarni, "Dhows, Drones, and Dollars: Ansar Allah's Expansion into Somalia," Carnegie Endowment for International Peace, March 14, 2025; "Thirty-Fifth Report of the Analytical Support and Sanctions Monitoring Team Submitted Pursuant to Resolution 2734 (2024) Concerning ISIL (Da'esh), Al-Qaida and Associated Individuals and Entities," United Nations Analytical Support and Sanctions Monitoring Team, February 6, 2025, p. 10.

28 "To Receive Testimony on the Posture of United States European Command and United States Africa Command in Review of the Defense Authorization Request for Fiscal Year 2026 and the Future Years Defense Program," U.S. Africa Command, April 3, 2025, p. 42.

29 "Kenyan National Indicted for Conspiring to Hijack Aircraft on Behalf of the Al Qaeda-Affiliated Terrorist Organization Al Shabaab," U.S. Department of Justice, December 16, 2020; "Cholo Abdi Abdullah Convicted for Conspiring to Commit 9/11-Style Attack at the Direction of Al Shabaab," U.S. Department of Justice, November 4, 2024.

30 Eric Schmitt and Abdi Latif Dahir, "Al Qaeda Branch in Somalia Threatens Americans in East Africa — and Even the U.S.," *New York Times*, March 21, 2020.

31 "The Islamic State in Somalia: Responding to an Evolving Threat," Crisis Group Africa Briefing, International Crisis Group, September 12, 2024, p. 3.

32 Ibid., footnote 2, p. 2; Thomas Joscelyn and Caleb Weiss, "Islamic State Video Promotes Somali Arm, Incites Attacks during Holidays," FDD's Long War Journal, December 27, 2017.

33 "The Islamic State in Somalia: Responding to an Evolving Threat," pp. 2-4; Caleb Weiss and Lucas Webber, "Islamic State-Somalia: A Growing Global Terror Concern," *CTC Sentinel* 17:8 (2024).

34 Adam Rousselle, "Combating the Islamic State Finance: Somalia and the Pan-African Nexus," GNET, February 17, 2025; Jessica Davis, "The Financial Future of the Islamic State," *CTC Sentinel* 17:7 (2024).

35 Andrea Elliott, "Charges Detail Road to Terror for 20 in U.S.," *New York Times*, November 23, 2009.

36 Philip Mudd, "Statement Before the Senate Committee on Homeland Security and Governmental Affairs," FBI, March 11, 2009.

37 Vickers, pp. 256-257; William H. McRaven, *Sea Stories: My Life in Special Operations*, First edition (New York: Grand Central Publishing, 2019), Kindle Location 3,299-3,528; Jeffrey Gettleman and Eric Schmitt, "U.S. Kills Top Qaeda Militant in Southern Somalia," *New York Times*, September 14, 2009.

38 Gettleman and Schmitt.

39 Malkhadir M. Muhumed, "Young Somali Soldier: I Killed Top al-Qaida Operative," NBC, June 14, 2011; Jeffrey Gettleman, "Somalis Kill Mastermind of 2 U.S. Embassy Bombings," *New York Times*, June 11, 2011.

40 Paul Cruickshank, Tim Lister, and Nic Robertson, "Evidence Suggests That Al-Shabaab Is Shifting Focus to 'Soft' Targets," CNN, September 26, 2013.

41 Richard Norton-Taylor, "MI5 Chief Warns of Terror Threat from Britons Trained in Somalia," *Guardian*, September 17, 2010; Alexander Meleagrou-Hitchens, "Al-Shabab's Western Recruitment Strategy," *CTC Sentinel* 5:1 (2012).

42 Blair, p. 11.

43 Clapper, p. 4.

44 "2024 Airstrikes;" "U.S. Forces Conduct Strike Targeting ISIS," May 31, 2024.

45 "Statement of General Michael E. Langley, United States Marine Corps Commander, United States Africa Command Before the United States Senate Committee on Armed Services," U.S. Africa Command, April 3, 2025.

46 Ibid., p. 1.

47 Ibid., p. 3.

48 Ibid., p. 3.

49 "Statement by the President on ISIL," The White House, September 10, 2014.

50 Houreld, "The Islamic State Has Regrouped in Somalia — and Has Global Ambitions."

51 Author correspondence, U.S. defense official, April 2025.

52 See, for one example, "Somalia: Puntland Forces Capture Turkish ISIS Fighter Amid Major Anti-Terror Offensive," Garowe Online, June 14, 2025.

53 Houreld, "The Islamic State Has Regrouped in Somalia — and Has Global Ambitions."

54 Mohamed Olad Hassan, "Somali Officials: US Airstrike against Islamic State Kills 16 Militants," Voice of America, February 17, 2025.

55 Mohamed Olad Hassan and Jeff Seldin, "Key Islamic State Planner Killed in Airstrike, US and Somali Officials Say," Voice of America, February 12, 2025.

56 "Update: U.S. Forces Strike on ISIS-Somalia."

57 "Treasury Targets Regional Actors Fueling Violence and Instability in Somalia," U.S. Department of the Treasury, July 5, 2012; Katherine Houreld, "Killing of Top ISIS Militant Casts Spotlight on Group's Broad Reach in Africa," *Washington Post*, February 3, 2023.

58 "Background Press Call by Senior Administration Officials on a Successful Counterterrorism Operation in Somalia."

59 Austin Doctor and Gina Ligon, "The Death of an Islamic State Global Leader in Africa?" *CTC Sentinel* 17:7 (2024).

60 "Treasury Targets Regional Actors Fueling Violence and Instability in Somalia."

61 Jeremy Scahill, "The Purge," Intercept, May 19, 2015; Hansen, p. 113.

62 "Update: U.S. Forces Strike on ISIS-Somalia."

63 Weiss and Webber.

64 "Letter Dated 1 November 2019 from the Chair of the Security Council Committee Pursuant to Resolution 751 (1992) Concerning Somalia Addressed to the President of the Security Council," United Nations Security Council, November 1, 2019, pp. 19-20.

65 Ibid., pp. 19-20.

66 This is based on a review of the data collected in Peter Bergen and David Sterman, "Terrorism in America After 9/11," New America, April 23, 2025. On the Islamic State's loss of Raqqa, see Hilary Clarke, Nick Paton Walsh, Eliza Mackintosh, and Ghazi Balkiz, "ISIS Defeated in Raqqa as 'Major Military Operations' Declared Over," CNN, October 18, 2017.

67 "Minneapolis Man Arrested for Attempting to Provide Material Support to ISIS," U.S. Department of Justice, February 28, 2025.

68 "Criminal Complaint United States of America v. Abdisatar Ahmed Hassan," United States District Court for the District of Minnesota, February 27, 2025, pp. 26-27.
69 Ibid., pp. 11-15.
70 Ibid., pp. 5-6.
71 "Maryland Man Charged With Attempting To Provide Material Support To Isis," U.S. Attorney's Office, District of Maryland, October 16, 2024.
72 Mike Hellgren, "Howard County Man Allegedly Joining ISIS Terror Organization Arrested at BWI, FBI Says," CBS Baltimore, October 19, 2024.
73 "New Jersey Man Charged With Attempting To Provide Material Support To Al Shabaab," U.S. Attorney's Office, Southern District of New York, December 29, 2023.
74 "United States of America v. Karrem Nasr [Sealed Complaint]," United States District Court Southern District of New York, December 14, 2023.
75 "New Jersey Man Pleads Guilty to Attempting to Provide Material Support to Al Shabaab," U.S. Attorney's Office, Southern District of New York, January 27, 2025.
76 "United States of America v. Muse Abdikadir Muse, Mohamed Salat Haji & Mohamud Abdikadir Muse [Criminal Complaint]," United States District Court for the Western District of Michigan, January 21, 2019.
77 Ibid.
78 "Mohamed Haji Sentenced To 130 Months In Prison For Conspiring To Provide Material Support To Isis," U.S. Attorney's Office, Western District of Michigan, September 22, 2021.
79 "United States of America v. Harafa Hussein Abdi [Sealed Complaint]," Southern District of New York, January 9, 2018, pp. 11-12.
80 Ibid., p. 7.
81 "U.S. Citizen Charged with Providing Material Support to Isis And Receiving Military-Type Training at Isis Fighter Camp," U.S. Department of Justice, February 16, 2024.
82 Weiss and Webber.
83 "Criminal Complaint United States of America v. Abdisatar Ahmed Hassan," pp. 26-27; "Maryland Man Charged With Attempting To Provide Material Support To Isis;" "U.S. Citizen Charged with Providing Material Support to Isis And Receiving Military-Type Training at Isis Fighter Camp."