COMBATING TERRORISM CENTER AT WEST POINT

CTC SENTINEL

OBJECTIVE · RELEVANT · RIGOROUS | MARCH 2025 · VOLUME 18, ISSUE 3

FEATURE ARTICLE

The Ukraine War and the Evolving Threat of Drone Terrorism

DON RASSLER AND YANNICK VEILLEUX-LEPAGE

A VIEW FROM THE CT FOXHOLE

Christian Klos

DIRECTOR GENERAL OF PUBLIC SECURITY, GERMANY'S FEDERAL MINISTRY OF INTERIOR AND COMMUNITY

Contents

FEATURE ARTICLE

INTERVIEW

ANALYSIS

FROM THE EDITOR

The March issue focuses in particular on the drone threat. In the feature article, Don Rassler and Yannick Veilleux-Lepage examine the evolution of terrorist drone usage and forecast its future trajectory in light of the tactical and technological innovations emerging from the Russo-Ukrainian War. They write that "the conflict has become a critical 'innovation hub' for drone warfare, accelerating advancements in the scale, speed, and range of drone operations. These developments are not only transforming the modern battlefield but also creating new opportunities for violent extremist organizations (VEOs) to enhance their operational capabilities." They assess that "in particular, the war has normalized large-scale drone deployment, demonstrating the feasibility of launching coordinated drone swarms and phased attacks capable of overwhelming existing defenses" and note that the potential future pairing of high-speed First-Person View (FPV) drones with emerging technologies such as AI-assisted targeting "could significantly increase the precision and impact of future attacks." In a similar vein, Jake Dulligan, Laura Freeman, Austin Phoenix, and Bradley Davis, in assessing the threat posed by commercial drones, write that the biggest concern "is that drone swarms could dramatically increase the impact of bad actor drone operations, be it kinetic strikes, ISR, or psychological warfare."

This month's interview is with Dr. Christian Klos, the Director General of Public Security at Germany's Federal Ministry of Interior and Community. He says that "when it comes to the external threat, I would agree with the assessment that ISIS-K is in Germany as well. What we observe from the intelligence side is that there are clear indications that the group intends to conduct attacks in Europe, and this can also include Germany and therefore we are very much aware of this threat, and we have seen also travel activities. So, it's not just some minor indications."

Aaron Zelin assesses the new Syrian government's efforts to counter the Islamic State, Hezbollah, and the captagon trade. He writes: "Unlike the Assad regime—which did little to fight the Islamic State, was closely aligned with Hezbollah, and produced captagon on an industrial scale—HTS in its guise as the new government of Syria is taking on these challenges assertively, and has a significant track record in doing so previously. Not only are these efforts a benefit to Syrian society and the security and stability of the country, but they also align with the interests of the United States and U.S. regional allies."

Alexandre Rodde and Justin Olmstead examine the evolution of vehicular ramming attacks and prevention efforts. They write that "when it comes to indicators and warnings of future attacks, the demonstration effect created by high-casualty vehicle-ramming attacks has in the past seemingly produced a surge in copycat attacks, which means the security agencies should be particularly vigilant given the recent uptick in high-profile attacks, including the New Orleans attack."

Paul Cruickshank, *Editor in Chief*

CTCSENTINEL

Editor in Chief

Paul Cruickshank

Managing Editor

Kristina Hummel

CONTACT

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

SUBMISSIONS

The *CTC Sentinel* welcomes submissions.

Contact us at ctc@westpoint.edu.

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

Cover: AI-generated image of a drone flying over city streets (TP71/Adobe Stock)

On the Horizon: The Ukraine War and the Evolving Threat of Drone Terrorism

By Don Rassler and Yannick Veilleux-Lepage

This article analyzes the evolution of terrorist drone usage and forecasts its future trajectory in light of the tactical and technological innovations emerging from the Russo-Ukrainian War. The conflict has become a critical "innovation hub" for drone warfare, accelerating advancements in the scale, speed, and range of drone operations. These developments are not only transforming the modern battlefield but also creating new opportunities for violent extremist organizations (VEOs) to enhance their operational impact and engage in surprise. This, it is argued, will lead to a new burst of terror drone activity across key threat vectors. In particular, the war has normalized large-scale drone deployment, demonstrating the feasibility of launching coordinated drone swarms and phased attacks capable of overwhelming existing defenses. Likewise, the widespread use of high-speed First-Person View (FPV) drones in Ukraine highlights the tactical value of speed and agility—capabilities that are increasingly within reach for terrorist actors. When paired with emerging technologies such as AI-assisted targeting, these systems could significantly increase the precision and impact of future attacks. The article also emphasizes the growing threat of long-range drone operations. To help contextualize these shifts, the article introduces the VEO Drone Capability-Impact Framework, which illustrates how both component- and system-level advances continue to lower the barriers to entry for extremist actors. The convergence of drone warfare with other disruptive technologies—such as additive manufacturing and artificial intelligence—is also explored, as the fusion of these capabilities creates even more opportunities for extremists to be creative and to innovate with drones in the future. The article also discusses how counter-UAS systems and legal frameworks that guide their use are struggling to keep pace with these changes and challenge the ability of governments to respond quickly and effectively.

The Russo-Ukrainian War has emerged as an innovation hub. While "every war offers a window into how future wars will be waged,"[1] the case of Ukraine stands apart as particularly unique. The conflict has revolutionized the role and scope of drone warfare and the operational use of artificial intelligence, pushing the boundaries of applied warfare in human-machine teaming. In addition, the sourcing of materiel inputs for the war has involved a combination of state-level assistance and the widespread, scaled, and innovative use of commercially available systems and components. This ranges from the deployment of thousands of DJI drones[2] to the critical integration of commercial components in state-produced systems, such as Iran's Shahed drones.[3] The war has also been unique due to the diverse mix and convergence of actors who are supporting the two warring parties. General Bryan Fenton, the leader of U.S. Special Operations Command, recently noted that the conflict exemplifies a form of adversarial convergence: "This is not just Russia fighting Ukraine ... It's Russia, backed by Iranian drones, North Korean personnel and indirect Chinese contributions."[4] Faced with these developments, the United States and its allies are closely monitoring the innovations and advancements resulting from the war. Many of these innovations are not only worth emulating but may also pose challenges that Western forces will need to contend with in the future.[5] However, other actors, including violent extremist organizations (VEOs), are also observing these developments, and it is likely that they will inspire new terror drone tactics and strategies.

This article traces the evolution of terrorist use of drones and forecasts how the ongoing conflict in Ukraine will likely shape the future trajectory of terrorist drone usage. To achieve this, the article analyzes five key trends affecting the drone landscape, focusing on critical concerns, capabilities, and risks relevant to the future of drone terrorism. The article is organized into three parts. Part I provides a high-level overview of the past and present state of the terrorist drone threat, arguing that terrorist drone usage follows a pattern of relative stability punctuated by bursts of rapid innovation. Part II introduces the novel VEO Drone Capability-Impact Framework, which situates drone use developments during the Ukrainian conflict in relation to component and system level changes and their associated potential for surprise and impact.

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

Yannick Veilleux-Lepage, Ph.D., is an Assistant Professor in the Department of Political Science and Economics at the Royal Military College of Canada. His research focuses on the intersection of technology, terrorism, and the evolution of terrorist tactics. He is also the Scientific Director of Pier Point Consulting, a firm specializing in providing analysis and threat assessment related to misuse of emerging technology.

This article utilizes this framework to highlight how changes across these areas continue to reduce barriers to entry for state and non-state actors to access and operationalize scale, speed, and range as threat vectors. The authors argue that understanding these ongoing changes are essential to forecasting how advancements in drone warfare from the Russo-Ukrainian war will create new opportunities for VEOs to deploy drones in attacks, enhance their operational capabilities, and expand the range of potential threats. Part III explores the implications of drone-related innovations that have emerged from the Russo-Ukrainian War for the future of terrorism. The article concludes with high-level takeaways.

Part I: The Early Evolution of Drone-Related Terrorism - From Then to Now

Terrorist innovation is not a linear or sequential process, but a dynamic and non-linear phenomenon shaped by social, technological, and environmental factors. The evolution of terrorist interest in and operational use of drones is best understood through the evolutionary biology concept of punctuated equilibrium.[6] Unlike gradualism—which suggests that change occurs through the slow, steady accumulation of small genetic modifications over long periods—punctuated equilibrium is characterized by long periods of stability, during which an organism's traits remain largely unchanged.[7] These stable phases are occasionally disrupted by short, intense bursts of rapid change, leading to the emergence of new forms or adaptations. Figure 1 shows how this has applied to VEOs when it comes to their operationalization of drones.

Early interest in drones among non-state violent actors marked a period of relative stability, during which drones were recognized for their potential but had not yet been operationalized due to technical and logistical limitations. This stable phase was disrupted by state-supported groups such as Hezbollah and Hamas.[8] These organizations, benefiting from greater resources and technological expertise, pioneered the use of drones for reconnaissance, propaganda, and targeted attacks. In doing so, they demonstrated operational possibilities and created new capability pathways that influenced the strategies of other non-state actors, facilitating broader adoption and adaptation among terror networks.

During the mid-2010s, groups such as the Islamic State and al-Qa`ida rapidly weaponized commercially available drones, employing them for surveillance, bomb delivery, propaganda, and psychological operations.[9] These developments—the sudden introduction of new capabilities that transformed operational practices—represent the 'short bursts of rapid change' that disrupted the existing status quo or equilibrium. Following this wave of innovation, a new equilibrium emerged, as many terror groups refined their drone strategies, adopting methods similar to those of the Islamic State and al-Qa`ida, while others lagged due to resource constraints.

In many ways, the current state of the VEO drone threat—excluding the notable exception of the Houthis' use of long-range drones[10]—remains relatively stable and aligned with the status quo established by the Islamic State and al-Qa`ida during the 2015-2017 period. However, a core argument of this article is that the Russo-Ukrainian War and the associated bursts of innovation in state-level military conflict—particularly advances in artificial intelligence and autonomous systems—constitute shocks that will irreversibly disrupt the existing equilibrium for both states and violent non-state actors. These advancements are set to usher in a new era of VEO drone exploitation, fundamentally diverging from previous patterns and introducing unprecedented capabilities that will redefine the threat landscape.

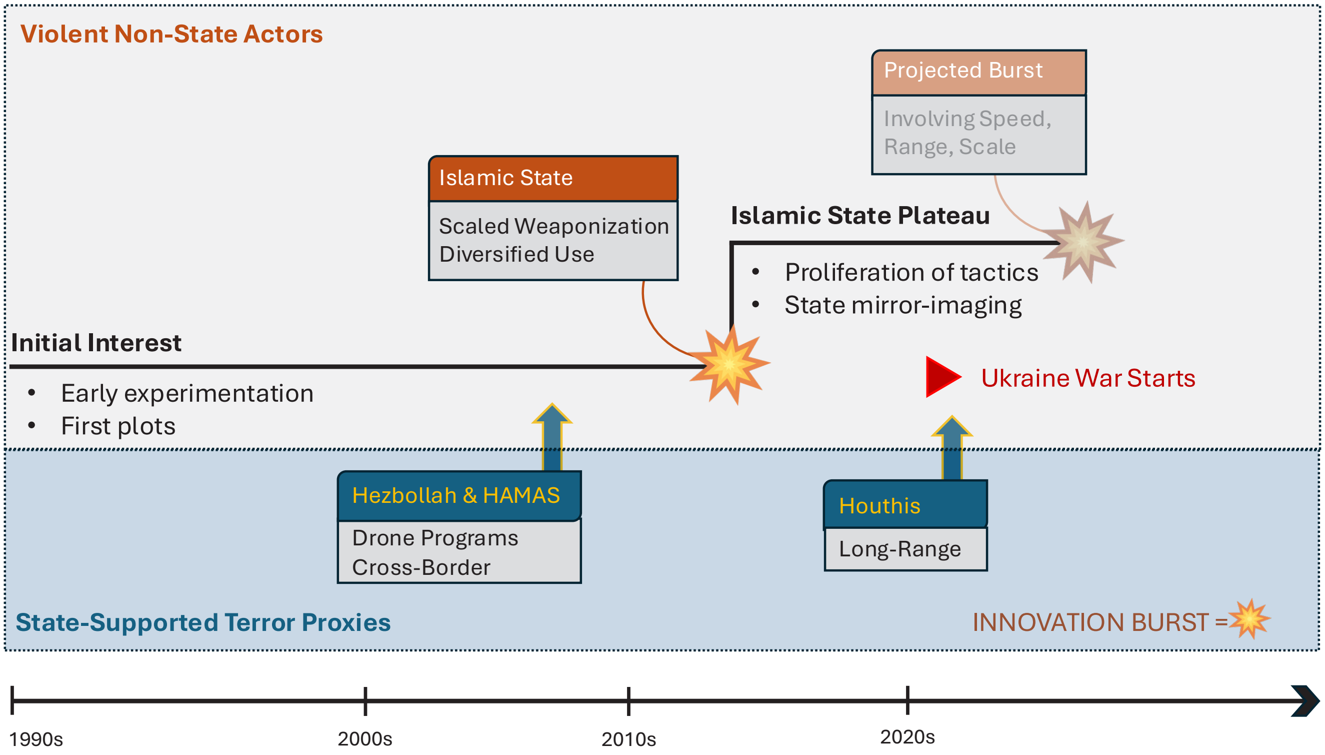

Figure 1: The Punctuated Evolution of Drone Terrorism[11]

> **"The Russo-Ukrainian War and the associated bursts of innovation in state-level military conflict—particularly advances in artificial intelligence and autonomous systems—constitute shocks that will irreversibly disrupt the existing equilibrium for both states and violent non-state actors. These advancements are set to usher in a new era of VEO drone exploitation, fundamentally diverging from previous patterns and introducing unprecedented capabilities that will redefine the threat landscape."**

First Period of Stability: Discovery and Initial Experimentation - 1990s-2014

With the exception of a few abortive plots and difficult-to-substantiate reports, early attempts by terrorist groups to weaponize drones were limited in both scope and success. The first stable plateau of terrorist drone use, spanning from the 1990s to 2014, was marked by limited yet significant experimentation and conceptual exploration. During this phase, five major focus areas emerged: (1) the potential use of drones for chemical or biological attacks, (2) cross-border operational applications, (3) drone weaponization, (4) structured program development, and (5) hacking or intercepting adversarial drone systems.[12] Though rudimentary, these early efforts laid the foundation for later advancements and demonstrated the utility of drone technology for violent non-state actors.

Arguably, one of the key catalysts for VEOs adopting drones was their own exposure to the technology as targets of it. In the late 1990s, state-supported groups such as Hezbollah demonstrated the growing feasibility of drone operations by leveraging both their own innovations and the unintended consequences of state actors' use of the technology.

Hezbollah's initial exposure to drones occurred in 1992, when Israel used a UAV to guide an airstrike that killed Abbas al-Musawi, Hezbollah's general secretary.[13] Israel's drone operations against Hezbollah continued, notably during 'Operation Accountability' in 1993, when Israeli forces conducted 27 UAV flights over Lebanon in coordination with airstrikes on militant positions.[14] By 1997, Hezbollah had reportedly intercepted unsecured video feeds from Israeli UAVs, which were extensively used for reconnaissance over southern Lebanon, providing real-time intelligence to Israeli forces.[15] This ability to exploit drone surveillance culminated in the Ansariya ambush on the night of September 4, 1997, in southern Lebanon.[16] By intercepting UAV feeds, Hezbollah ambushed an Israeli commando unit from Shayetet 13, the Israeli Navy's elite special operations force.[17] The meticulously planned attack resulted in the deaths of 12 Israeli soldiers, marking one of the earliest documented cases of a non-state actor successfully leveraging drone technology for a decisive tactical advantage.

It is highly likely that Hezbollah's formal UAV program began shortly after the 1997 Ansariya ambush. According to an Israeli intelligence source, Hezbollah had already "begun to experiment with unmanned aerial vehicles" around the time of the al-Aqsa Intifada (2000-2005).[18] Hezbollah's entry into the UAV space was significantly bolstered by its close relationship with Iran, which has maintained its own UAV program since the Iran-Iraq War.[19] Iranian officials have openly acknowledged sharing UAV technology with Hezbollah,[20] helping to explain why Hezbollah's drone program is more advanced than those of other non-state actors. In 2004, Hezbollah flew a drone—dubbed the Mirsad-1, believed to be a variant of the Iranian-produced Mohajer-4 or Ababil-T—across the Israeli border from southern Lebanon.[21] During its 15- to 30-minute flight, the UAV passed over the northern Israeli town of Nahariya before returning to Lebanese territory. Hezbollah later released a grainy video of the flight, boasting that the aircraft could fly 'deep' into Israel, marking a significant public relations victory for the group.[22] In April 2005, Hezbollah flew another UAV into Israeli airspace.[23] Following this, Hezbollah's then secretary general, Hassan Nasrallah, claimed that the group's drones could carry 40-50 kilograms of explosives and could be used to attack targets inside Israel.[24] The following year, during the 2006 war with Israel, Hezbollah launched at least three drones into Israeli airspace, all of which were intercepted and shot down by the Israel Defense Forces (IDF). Notably, one of these drones was reportedly loaded with approximately 30 kilograms of explosives, intended for use as a guided bomb.[25] During this period, Hezbollah's UAV incursions into Israeli airspace became a recurring feature of its operations. However, with the exception of a few daring missions, these activities generally remained relatively muted compared to the perceived magnitude of the threat.[26]

Hamas' drone program followed a trajectory similar to Hezbollah's but with more limited capabilities and a slower progression toward developing its own drone technology. Like Hezbollah, Hamas initially focused on reconnaissance and psychological impact during this early period of stability. However, it faced significant setbacks, including the loss of key personnel due to Israeli counterterrorism operations.

Hamas' interest in drones dates back to at least early 2003, though its capabilities at the time were rudimentary. In January 2003, reports surfaced that Fatah had allegedly purchased remote-control toy planes from Europe, intending to use them as explosive-laden devices for attacks.[27] While uncorroborated, this claim reflected broader interest among Palestinian groups in drone technology.[28] Around the same time, an Israeli newspaper reported that Hamas members had been discussing the development of model airplane bombs on online forums for months.[29] Despite Hamas' early interest in drone technology, its initial efforts were hampered by significant setbacks and limited technical capabilities. For example, in 2004, an unsourced report claimed that six Hamas operatives were killed while attempting to construct an explosive-laden drone.[30] Similarly, in 2005, Israeli intelligence dismantled a cell attempting to transfer UAV technology from the United Arab Emirates to Hamas.[31]

Like Hezbollah, whose early ventures into UAV technology were driven by being targeted by Israeli drones, Hamas likely gained insights from studying Israeli UAVs that malfunctioned, crashed, or were shot down in Palestinian territory.[32] These incidents provided valuable intelligence that Hamas could use to re-engineer drone technology or develop countermeasures. By the early 2010s, Hamas' drone program displayed increasing sophistication and operational activity. In 2012, as part of Operation Pillar of Defense, the IDF conducted strikes against Hamas facilities suspected of developing drones capable of carrying explosives.[33] The IDF later released a video showing Hamas members test-flying a UAV, underscoring the group's growing ambitions.[34] By October 2013, Palestinian security forces in the West Bank disrupted an advanced Hamas plot to launch a UAV into Israel after the group had reportedly conducted multiple test flights and planned to attach explosives to the drone.[35] Leveraging its ties to Iran as a catalyst for innovation, Hamas further advanced its drone program during the 2014 'Fifty-Day War' with Israel. During this conflict, Hamas launched at least two drones into Israeli airspace. One of these, an Ababil A1B—believed to be modeled after the Iranian Ababil drone series, such as the Ababil-T and Mohajer-4—reportedly carried four air-to-ground missiles in addition to a camera.[36] Hamas publicized the event by releasing pictures and videos from the UAV on Twitter.[37] However, these flights were largely unsuccessful; one drone was shot down over Ashdod, and another was intercepted over Ashkelon.[38] There was also speculation that the missiles were inert and that the display was just a publicity stunt by Hamas.[39]

Domestically, in the United States, the period before 2014 saw drone-related terrorist plots that were limited in scope, largely aspirational, and shaped by the post-9/11 security environment.[40] Examples include the Virginia Jihad Network's attempt in the 2000s to acquire range-extending technology for Lashkar-e-Taiba, which involved procuring autopilot modules and wireless video transmission equipment compatible with unmanned aerial systems,[41] and Rezwan Ferdaus' thwarted 2011 plan to attack federal buildings with remote-controlled aircraft.[a] Although these efforts were unsuccessful, they contributed to a heightened sense of fear and vulnerability in the post-9/11 era, amplified by media coverage that emphasized their novelty and potential danger, even when the actual threat remained minimal.[42] The focus on 'lone wolf' threats further fueled alarm, despite the lack of true innovation and the plateauing of the drone threat during this period due to significant technical limitations.[43] However, the intent behind these plots was often taken seriously, reinforcing the perception of an imminent and pervasive threat.[44]

Rapid Change: The Islamic State's Breakthrough Innovation (Weaponization at Scale) - 2014-2018

The equilibrium that defined the first decade of the century was shattered by the Islamic State's ability to successfully weaponize commercial drones, and to do so at scale.[45] The diverse ways that the Islamic State used drones—including for surveillance and reconnaissance, attack coordination and command, weaponization, as well as propaganda and external communication—was also a notable development.

One of the earliest and most effective ways the Islamic State employed drones was for intelligence gathering. By deploying UAVs for reconnaissance, the group improved its ability to plan attacks, monitor enemy movements, and gain real-time situational awareness on the battlefield. Drones were used to scout enemy positions, identify weak points, and conduct pre-attack reconnaissance. Before capturing Tabqa Air Base in Syria in August 2014, the Islamic State released footage obtained from a drone,[46] showcasing its ability to conduct aerial surveillance ahead of an assault. Similarly, drones were used against the Baiji Oil Refinery[47] and during the battle for Mosul[48] to track enemy positions in real time. The intelligence gathered through drone surveillance enhanced the Islamic State's coordination, making its attacks more precise and increasing their overall effectiveness.[49]

Beyond intelligence gathering, the Islamic State integrated drones into its command-and-control structures to coordinate battlefield operations. Drones provided real-time footage that allowed the Islamic Strate commanders to monitor attacks, guide Vehicle-Borne Improvised Explosive Devices (VBIEDs), and direct mortar and artillery fire. By using drones to scout urban landscapes, the Islamic State improved the accuracy of its suicide attacks and artillery strikes. In Mosul, drones were used to map out VBIED routes, enabling the Islamic State to navigate congested urban streets and strike high-value targets with precision.[b] In some cases, Islamic State drones helped adjust artillery fire mid-battle, ensuring more effective bombardments.[50]

The Islamic State expanded its drone operations by modifying commercial UAVs to carry and drop explosive payloads.[51] This tactic transformed drones into 'flying artillery,' allowing the group to strike targets from above.[52] The Islamic State developed rudimentary but effective mechanisms to drop grenades, mortar shells, and improvised explosive devices on enemy positions.[53] In some instances, it also employed loitering munitions, flying drones directly into targets.[54] Notably, in October 2017 the Islamic State released footage of a drone-launched munition destroying a Syrian military munitions depot,[55] highlighting the destructive potential of its aerial attacks. These weaponized drones provided the Islamic State with a low-cost, high-impact method of striking both military and civilian targets while adding a psychological dimension to its warfare tactics.[56]

Drones also played a crucial role in the Islamic State's

[a] In 2011, Rezwan Ferdaus, a U.S. citizen and physics graduate student at Northeastern University in Boston, planned to attack the Pentagon and the U.S. Capitol Building using remote-controlled model aircraft filled with explosives. His plan involved using three drones: one to strike the Capitol dome and two to target the Pentagon. These attacks were intended to create chaos, allowing other members of his group to carry out additional attacks on survivors. Despite its ambition, the plot faced considerable technical challenges, such as the need for a long runway, payload limitations of the model aircraft, and issues with flight stability. Experts noted that the drones Ferdaus intended to use could carry only a small amount of explosives and would likely have been uncontrollable with the added weight. The case was further complicated by an FBI sting operation, which provided Ferdaus with the necessary materials to carry out his plans. This raises the question of whether he could have implemented his scheme without the FBI's involvement. Additionally, Ferdaus' lawyers argued that his plot was a "fantasy" fueled by mental illness, adding another layer of complexity and making the true threat more difficult to ascertain. See Ros Krasny, "Massachusetts Man Pleads Guilty in Plot to Attack Pentagon, Capitol," Reuters, July 11, 2012; Don Rassler, *Remotely Piloted Innovation: Terrorism, Drones and Supportive Technology* (West Point: Combating Terrorism Center, 2016); Jess Bidgood, "Massachusetts Man Gets 17 Years in Terrorist Plot," *New York Times*, November 2, 2012; Paul Harris, "FBI Faces Entrapment Questions over Rezwan Ferdaus Bomb Plot Arrest," *Guardian*, September 29, 2011.

[b] At least 47 such attacks have been displayed in Islamic State propaganda. Emil Archambault and Yannick Veilleux-Lepage, "Drone Imagery in Islamic State Propaganda: Flying like a State," *International Affairs* 96:4 (2020): pp. 955-973.

propaganda efforts, enabling the group to capture high-quality footage of armed engagements and attacks for recruitment and psychological warfare.[57] Drone footage provided a first-person perspective of attacks, making the Islamic State's propaganda videos more compelling and cinematic.[58] By filming combat operations with drones, the Islamic State exaggerated its military capabilities, intimidated enemies, and attracted new recruits. The group's videos frequently featured precision drone strikes, VBIED explosions, and aerial surveillance footage—all designed to project an image of military strength.[59]

The Islamic State's adoption and use of drones can be attributed to a combination of technological advancements, organizational capabilities, and strategic imperatives. From a technological perspective, the proliferation of affordable, advanced commercial drones—easily retrofitted or modified—allowed the Islamic State to overcome barriers that had previously constrained non-state actors from effectively utilizing unmanned systems, despite lacking the state sponsorship that benefited groups such as Hezbollah and Hamas.[60] Parallel advancements in cameras, sensors, and end-to-end encryption further enhanced the Islamic State's capabilities, improving operational precision, surveillance effectiveness, and secure communication. Organizationally, the Islamic State centralized its uncrewed aerial system (UAS) program under the Committee of Military Manufacturing and Development (CMMD), assigning it to the Al-Bara' bin Malik Brigade.[61] This ensured standardization in munition production and promoted interoperability. Additionally, the group developed a sophisticated supply chain network to procure drones and components from commercial sources, using legitimate businesses as fronts to facilitate procurement and shipping.[62] Strategically, the Islamic State exploited the largely uncontested territory in Syria and Iraq, leveraging the region's deserts and urban areas to experiment with and conduct drone operations—often with little opposition—for reconnaissance, weaponization, and propaganda purposes.[63]

Second Period of Stability: Post Islamic State "Plateau" - 2018-2024

With the emergence of the Islamic State's drone program, the group disseminated its tactics, techniques, and procedures globally, often through propaganda that exaggerated the tactical effectiveness of its drone operations. As a result, various terrorist and insurgent groups worldwide have adopted similar practices, establishing a new equilibrium in the use of drones by violent non-state actors.

This proliferation is most evident among Islamic State and al-Qa`ida affiliates in Africa, where commercial drone systems have become integral to intelligence, surveillance, reconnaissance, propaganda, and attack coordination. In Somalia and Kenya, al-Shabaab uses drones to monitor security forces and identify strategic targets.[64] Similarly, Ahlu Sunna wal-Jama'a in Mozambique and Islamic State's West Africa Province (ISWAP) in Nigeria and the Lake Chad Basin employ drones to gather intelligence and direct fire during attacks.[65] Other groups, such as the Allied Democratic Forces (ADF) in the Democratic Republic of the Congo and Jama'at Nusrat al-Islam wal-Muslimin (JNIM) in the Sahel, have integrated drones for reconnaissance and operational planning.[66]

Similarly, on October 7, 2023, Hamas used commercial drones as a pivotal component of its attack on Israel, disabling key Israeli defenses and facilitating subsequent incursions.[67] A first wave of small, explosive-laden commercial drones targeted surveillance infrastructure, including observation towers, cameras, sentries, and communication systems along the Gaza border.[68] This effectively blinded the IDF, reducing their situational awareness and creating confusion and delays in Israel's response, allowing Hamas fighters to breach the border and overrun Israeli military positions. Beyond disabling surveillance systems, Hamas used drones as aerial munitions platforms, often modifying RPG-7 warheads to be dropped on Israeli tanks, armored vehicles, infantry, and civilian targets.[69] In at least one instance, documented in Hamas propaganda, drones were used to strike an ambulance responding to the attacks.[70] Similar to the Islamic State, Hamas deployed small, off-the-shelf commercial drones in overwhelming numbers, making them an affordable and scalable air force alternative.[71] The group also integrated drones with other military platforms, including infantry and rocket barrages, demonstrating a high level of tactical coordination.[72] The sophistication of Hamas' drone operations on October 7 is further evidenced by reports suggesting that Palestinian Islamic Jihad maintained a dedicated drone operations room during the attack, facilitating real-time coordination and reconnaissance missions.[73]

Hamas' adoption of small, off-the-shelf commercial drones—a tactic favored by the Islamic State—does not mean it abandoned efforts to develop indigenous drone capabilities. During the October 7 attack, Hamas also deployed 35 Zouari drones,[74] a new loitering munition named after Tunisian aerospace engineer Mohammed Zouari, who pioneered Hamas' drone program before his assassination in 2016, an operation widely attributed to Mossad.[75] The Zouari drones function similarly to Iranian Shahed drones, loitering over targets before striking them with explosive payloads.

Before taking control of Syria and disbanding, Hay'at Tahrir al-Sham (HTS) increasingly relied on drones as a key component of its military strategy, using them for both reconnaissance and targeted attacks.[76] During its offensive in Syria during the fall of 2024, HTS deployed kamikaze first-person view (FPV)[c] drones and long-range rocket-propelled UAVs to strike Syrian regime tanks, artillery positions, and command centers.[77] These drones provided HTS with a crucial tactical advantage, allowing it to disrupt enemy defenses and leadership structures before ground forces advanced. The group's Al-Shaheen Brigade, a specialized drone unit, carried out targeted assassinations, including the killing of Uday Ghossah, the regime's commander of military security, in Hama.[78] Additionally, HTS used secondary reconnaissance drones to enhance strike accuracy and produce propaganda videos, amplifying its successes on social media.[79]

Like Hamas' actions on October 7, HTS' drone strategy has been heavily influenced by the Islamic State. Initially, HTS modified consumer drones to drop grenades and small explosives, mirroring Islamic State tactics.[80] However, over time, it has developed more advanced and specialized drone units. The influence of the Islamic State was particularly evident in HTS' use of suicide drones and drone "swarms," both tactics pioneered by the Islamic State in Syria and Iraq. Additionally, before it overthrew the Assad regime, HTS mirrored the Islamic State's approach of integrating drones into

[c] First-Person View (FPV) refers to drone operations where the pilot controls the aircraft using a live video feed transmitted from an onboard camera, typically viewed through goggles or a screen. This immersive perspective allows for precise maneuvering and is widely used in racing, recreational flying, and increasingly in military applications.

broader combat operations, using them in combined arms assaults alongside infantry and artillery.[81] However, HTS took drone warfare a step further by establishing dedicated drone production facilities in Idlib, employing 3D printing and clandestine supply chains to manufacture drone components.[82]

A rare innovation during this period came from the Houthi movement, which initially relied on shorter-range stand-off weapons, primarily targeting areas within Yemen and southern Saudi Arabia. However, by 2018, its drone and missile capabilities had expanded significantly in both range and complexity. This transition was marked by the development and deployment of long-range drones, such as the Samad-3, which the group claimed to have used in an attack on Dubai International Airport, approximately 1,200 km away.[83] A U.N. panel later confirmed that the Samad-3 incorporated internationally sourced components and had an estimated range of 1,500 km.

With continued technical and logistical support from Iran, the Houthis have further extended the operational range of their UAVs. A February 2024 assessment by the Defense Intelligence Agency (DIA) estimates the range of key Iranian-supplied Houthi drones as follows: Shahed 131 (Waid 1) at 900 km, Samad at 1,800 km, and Shahed 136 (Waid 2) at 2,500 km.[84] These extended-range drones have been instrumental in attacks on strategic targets in Saudi Arabia, the UAE, and Israel,[d] demonstrating a continued effort to push the boundaries of their strike capabilities. This rare departure from the Islamic State's evolutionary plateau can be attributed primarily to Iranian support. The Islamic Revolutionary Guard Corps (IRGC) has played a crucial role in providing technological assistance, platform designs, and operational training to the Houthis. Additionally, access to commercial technologies has facilitated further improvements, as the Houthis have sourced drone components from the global market, leveraging dual-use technology to enhance their long-range attack capabilities.

Poised for Another Burst: The Next Coming Wave of Rapid Change

Over the past decades, drone innovations have significantly shaped the operational capabilities of extremist groups, enabling them to conduct reconnaissance, deliver explosives, and disrupt conventional military forces using relatively low-cost technology. However, the adoption of Islamic State-inspired drone tactics has not been limited to non-state actors. Both Ukraine and Russia have integrated similar techniques into their military operations, adapting them to fit the scale and complexity of state-level warfare.

While it is widely recognized that non-state actors often borrow tactics from state militaries, the potential for bi-directional learning—where states also adopt innovations from terrorist organizations—should not be overlooked. The literature on terrorist tactical innovation suggests that VEOs are not passive observers in modern warfare but actively monitor, study, and incorporate military advancements into their own strategies.[85] As Ukraine and Russia refine their drone tactics in ongoing conflict, it is highly likely that terrorist groups will learn from and repurpose these innovations for asymmetric warfare.

"VEOs are not passive observers in modern warfare but actively monitor, study, and incorporate military advancements into their own strategies."

Historically, insurgent and terrorist groups have consistently demonstrated the ability to borrow, adapt, and repurpose military innovations to suit their needs. Some of the most striking examples include the appropriation of orange jumpsuits by the Islamic State in execution videos, deliberately mimicking imagery associated with detainees in U.S. military custody to maximize psychological impact.[86] Similarly, aerial hijacking—first used as a state tactic in 1930s Peru—was later seized upon, refined, and expanded by numerous non-state actors, ultimately becoming a hallmark of modern terrorism.[87] Another example is the systematic destruction of hijacked planes by the Popular Front for the Liberation of Palestine (PFLP) and its sympathizers, a tactic influenced by Israel's Operation Gift, which destroyed 12 passenger airplanes.[88] More recently, the proliferation of the U.S. Army Sabotage Manual on extremist sites has provided non-state actors with a blueprint for disruption, demonstrating how military doctrine can be repurposed for insurgent operations.[89]

Given this well-documented pattern, the Russo-Ukrainian War is likely to serve as the next major catalyst, disrupting the current evolutionary plateau in terrorist drone use. As violent extremist organizations adapt and repurpose drone innovations emerging from the conflict, the world may soon witness a new era of asymmetric warfare characterized by the widespread use of swarm tactics, FPV drone strikes, and advanced drone countermeasures. These techniques, initially developed for state-led combat, will likely be integrated into the arsenals of extremist groups.

Furthermore, recent reports suggest formal bi-directional exchanges of drone warfare tactics between state and non-state actors, particularly involving Russian and Ukrainian advisors collaborating with various groups. Following Hamas' October 2023 attack on Israel, Kyrylo Budanov, Ukraine's military intelligence chief, suggested that Hamas' sophisticated drone operations closely mirrored tactics used by Russian forces in Ukraine,[90] implying potential Russian training or Hamas learning from drone activity from that conflict. Conversely, in late 2024, reports emerged that Ukrainian intelligence operatives supplied approximately 150 FPV drones and deployed around 20 experienced drone operators to assist HTS.[91] This support aimed to enhance HTS' drone capabilities against forces of the Russia-allied Assad regime.

Part II: Introducing the VEO Drone Capability-Impact Framework

The Russo-Ukrainian War has already triggered rapid evolutionary shifts in drone warfare for both Ukraine and Russia. This transformation will have lasting implications—not only shaping how both states leverage drone technology in future conflicts but also providing a blueprint for how VEOs might operationalize drones.

[d] For example, on July 19, 2024, the Israeli city of Tel Aviv was attacked by a long-range drone. The Houthis claimed responsibility for the attack and the Israeli military assessed that the drone used "was an upgraded Iranian-made Samad-3 model ... that arrived from Yemen." See Rami Amichay, "Tel Aviv hit by drone attack claimed by Iranian-backed Houthis," Reuters, July 19, 2024.

This section introduces the VEO Drone Capability-Impact Framework (Figure 2), which conceptually maps how both component-level and system-level advancements are creating new opportunities for VEOs to enhance their impact and engage in surprise. At the component level, the framework focuses on advancements in three key drone capabilities: scale (economies of scale and operational scaling), speed (physical speed and tactical agility and speed in decision making), and range (physical range and range of control). The colored arrows that appear in Figure 2 and which trend upward are used to illustrate how advancements in commercial technologies are enabling access to scale (red arrow), speed (blue arrow), and range (green arrow). These three capability areas are also mapped onto a quad chart that evaluates these advancements in relation to their impact and surprise potential. The outer box (the system level) visually highlights two other critical trends—how the cost of capable commercial UAS systems continue to drop (downward arrow) while other forms of integrated technology are simultaneously making those systems easier to use (upward arrow).

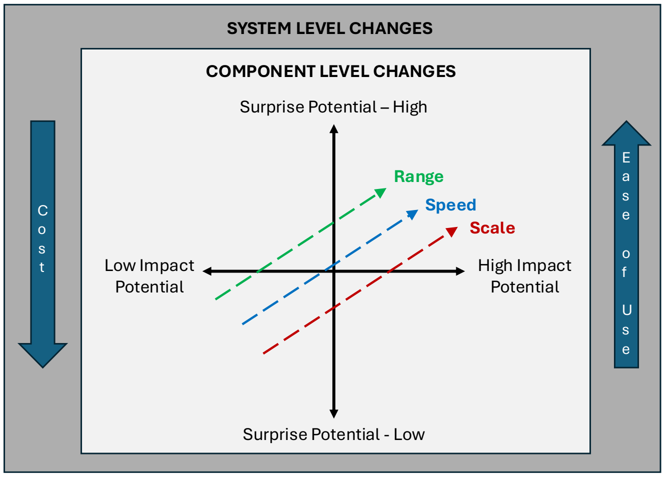

Figure 2: VEO Drone Capability-Impact Framework

When viewed holistically, the framework illustrates how component- and system-level advancements interact synergistically, allowing VEOs to enhance both the effectiveness and unpredictability of their drone operations. For example, in today's environment it is easier and cheaper for VEOs to gain access to a commercial drone that has the ability to fly at speeds in excess of 80 miles per hour and that can be controlled with limited training or experience (ease of use). The affordability of these types of commercial drones also means that it is easier for VEOs to acquire a collection or fleet of increasing capable commercial drones, illustrating the synergistic interplay between costs and scale. These dynamics create new opportunities for VEOs to amplify operational effects, execute rapid precision strikes against targets, and exploit vulnerabilities in conventional defense systems. These developments, in turn, complicate the threat landscape and elevate the risks associated with future drone-enabled terrorism.

Component and System Level Changes Through the Lens of the Russo-Ukrainian War

The following discussion examines how these component- and system-level changes have manifested in the Russo-Ukrainian War and how they have transformed both the conflict and drone capabilities. The subsection is organized around scale, speed, and range, and it examines the two system level changes—reduction in cost and enhanced ease of use—as cross cutting themes that are touched on throughout. While both military-grade and commercially available drones and components are considered, this analysis places particular emphasis on commercial systems. Since most VEOs have limited or no access to military-grade platforms or restricted technologies, their drone operations will primarily depend on commercially available solutions.

Scale

One of the most profound developments to emerge from the Russo-Ukrainian War is the utilization of drones by both Ukraine and Russia at an unprecedented scale. The concept of scale is a foundational element across various disciplines, encompassing spatial, temporal, analytical, and operational dimensions. In economics and business literature, scale is central to achieving efficiencies and optimizing resource allocation. It operates as a dynamic process of adaptation and optimization that shapes production and strategy (economies of scale), organizational expansion (operational scaling), and technological advancement. In the context of drone warfare, scale manifests in how drone technologies are developed, deployed, and refined over time. The discussion below explores drone use in the Russo-Ukrainian war through the lens of two of these primary categories—economies of scale and operational scaling, as they provide insights into how mass production, technological advancements, and strategic integration have been transforming battlefield operations in profound ways.

Economies of Scale

Economies of Scale refers to the reduction of costs through fixed distribution, supply chain optimization, and process standardization. The rise in the capabilities and accessibility of commercial UAS and other add-on technologies, combined with the rise of decentralized manufacturing (e.g., 3D printing), which has further enabled mass production, has made scaling a more important vector, or arena, where state and non-state entities can compete to economically weaken or outperform their adversary.

The Russo-Ukrainian War has exemplified this principle, with both sides dramatically increasing drone production to sustain high-intensity operations. In fact, the war has featured "the most intensive use of drones in a military conflict in history."[92] While estimates of the total number of drones used by both countries vary, the overarching picture is staggering. According to one estimate, Ukraine has been losing 10,000 drones per month, more than 100,000 drones per year.[93]

Other data points suggest that the number of drones used by Ukrainian forces are even higher, and with production continuing to accelerate. In early 2024, *Forbes* noted how the Ukrainian military partnering "with a growing network of small civilian workshops … quickly ramped up" production of FPV drones last year.[94] This surge in production has been driven by significant Ukrainian investment and resource allocation to drone procurement. In 2024, "the Ukrainian government allocated $2 billion to produce at least 1 million … FPV drones," signaling a major commitment to sustaining large-scale drone warfare.[95] By March 2024, the Ukrainian military was "acquiring at least 50,000 FPVs a month at a cost of just a few hundred dollars per drone," amounting to 600,000 FPV drones annually.[96] In October 2024, President Zelensky claimed "that the country had already surpassed" that number and that "Ukraine is now capable of producing 4 million drones annually."[97]

The high numbers are not limited to FPV drones: Economies of scale have also been a key feature of the production of longer-range drone attacks. During the conflict, both Ukraine and Russia have ramped up production of long-range attack drones. In December 2024, for instance, the Ukrainian Defense Ministry announced "plans to deliver more than 30,000 long-range attack drones in 2025, with production partially financed by international partners."[98]

The rise of decentralized manufacturing has enabled this mass production, which is further facilitated by additive manufacturing, open-source designs, and modular components, which has allowed for customization and the rapid replenishment of drone stockpiles at relatively low costs. This has been particularly evident in Ukraine's ability to produce long-range attack drones, such as the AQ400 Scythe, a wooden drone designed for low-cost, scalable production. The founder of Terminal Autonomy, the company behind the AQ400, described the drone as "basically flying furniture – we assemble it like Ikea,"[99] emphasizing its rapid assembly process, which takes roughly an hour to construct the fuselage and even less time to integrate the electronics, motor, and payload.

The high burn through rate of UAS during the war has made large-scale drone production not just an advantage, but an operational necessity. The ability for Russia and Ukraine to quickly manufacture and replace drones at minimal cost has allowed both countries to sustain their drone warfare capabilities despite heavy losses, highlighting the central and strategic role of economies of scale in this conflict.

Operational Scaling

Operational scaling refers to the number and frequency by which drones, and drone countermeasures, are deployed in combat. The Russo-Ukrainian War has demonstrated an unprecedented level of drone deployment, with both sides using thousands of drones per month in increasingly complex and large-scale operations. Drones are no longer occasional battlefield assets; they have become integral to daily offensive and defensive actions, saturating the battlespace.

Operational data refines the picture of how drones are being deployed at scale and how their use has evolved beyond sporadic strikes into a continuous and high-volume form of warfare. Data compiled by Kateryna Bondar for Breaking Defense (Figure 3) highlights—in a broad way—how Russia has scaled its use of Shahed type drones over the 2022-2024 period.

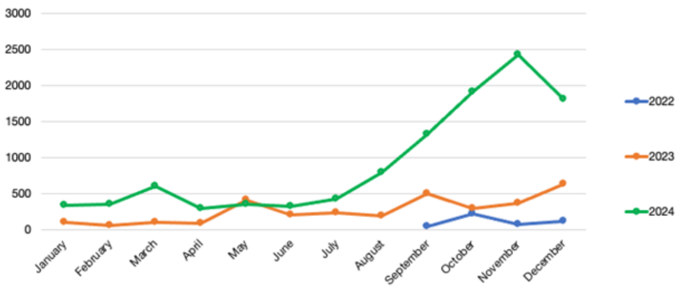

Figure 3: Number of Russian Shahed or Shahed-type drone attacks on Ukraine, by year and month[100]

Information compiled by ShahedTracker (Figure 4) provides an even more granular view. This data shows how Russia deployed, and tried to attack Ukraine, with more than 1,000 Shahed long-range one-way attack drones per month from September 2024 – February 2025,[101] illustrating the extent to which drones are being used as a primary attack method, rather than a supplementary tool. On November 26, 2024, Russia reportedly reached a high-water mark in its daily deployment of Shahed drones, as the Ukrainian government claimed Russia had launched "188 drones against most regions of Ukraine in a nighttime blitz… a record number of drones deployed in a single attack."[102] The sheer number of drones deployed on that day serves as a valuable data point, as it reflects not only Russia's reliance on Shahed drones but also the broader scale of its drone warfare. Importantly, this figure only accounts for one type of drone and does not include the numerous FPV drones and other UAVs that Russia has also deployed in high numbers in Ukraine.[103] Moreover, it serves to highlight how scale is not only about production numbers but also about how drones are deployed in overwhelming numbers to achieve battlefield objectives.

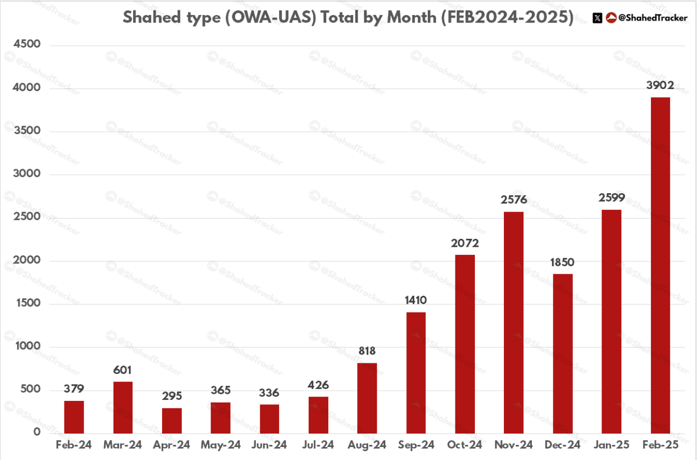

Figure 4: Data on Russian Shahed drones used in Ukraine, compiled by @ShahedTracker[104]

Ukraine has responded with similarly high-volume drone operations. The commander of a Ukrainian long-range drone unit interviewed by CNN "said he had personally overseen more than 500 long-range drone attacks into Russia since its full-scale invasion of Ukraine in February 2022."[105] As part of this strategy, Ukraine has increasingly employed large-scale drone attacks, often launching dozens or even hundreds of drones in a single wave. On September 29, 2024, for instance, CNN reported that Ukraine launched more than 100 drones overnight on a single mission into Russia."[106] [e]

These numbers are not anomalies but rather part of a broader shift toward continuous, high-intensity drone usage, where drones are deployed in coordinated salvos, overwhelming enemy defenses and complicating traditional methods of countering aerial threats. Indeed, one of the most striking examples of how scale and innovation intersect in the Russo-Ukrainian War is the way both

[e] Ukraine is reported to have used more than 100 drones during another long-range attack against Russia on September 18, 2024. For background, see Peter Dickinson, "Ukraine's Expanding Drone Fleet Is Flying Straight through Putin's Red Lines," Atlantic Council, September 21, 2024.

Russia and Ukraine have integrated deception, mass deployment, and multi-role drone tactics into their campaign. Rather than relying solely on individual high-tech platforms, both sides have leveraged volume, adaptability, and tactical ingenuity to maximize the effectiveness of their drone arsenals.

During the early part of the conflict, it was believed that many, "possibly the majority, of the drones used by Ukrainian forces were originally designed for commercial purposes or for hobbyists."[107] This may still be the case; however, over time, the UAS systems employed by Ukraine have become increasingly diverse, incorporating different materials and structural designs. As reported by David Hambling:

> *Ukraine has produced a huge variety of long-range attack drones, HI Sutton of CovertShores has documented 23 different types but this may not be exhaustive. The drones are produced by a variety of different groups, and range from the primitive but effective "drainpipe drone" with a fuselage made from plastic piping, to converted light aircraft to sophisticated models like the Lyuty ("Fierce") fielded by Ukrainian Military Intelligence. There are also the foreign-supplied models, including the Dominator from the U.S. provided as part of the Phoenix Ghost program.*[108]

Russia has similarly employed scalable drone innovation, particularly in its Shahed campaign, where unarmed decoy drones have been deployed in scale to conceal "a small number of highly destructive thermobaric drones."[109] The approach is reportedly "intended to force Ukraine to expend scarce resources to save lives and preserve critical infrastructure, including by using expensive air defence munitions."[110] Ukraine has also been using large-scale deployment of drones and decoys to achieve its objectives. For example, for longer-range drone attacks against Russia, Ukraine has deployed smaller Rubaka one way attack drones[111] in combination with its more capable Liutyi drone.[112] As explained by a commander of a Ukrainian unit focused on long-range drone operations, the use of the smaller Rubaka "drones are crucial to the success of any mission. The aim is simple: to overwhelm the air defenses and draw Russian fire away from the Liutyi, which often carries a payload as great as 250 kilograms (550 pounds)."[113] According to this commander, "some 30% of all the drones being launched" for long-range missions "will be on decoy missions … We try to mix them, and we try to send them from different distances, different launch places … they try to destroy them."[114]

This strategy has heightened concerns about the potential use of drone swarms.[115] As explained by Stacie Pettyjohn, "swarms typically consist of a greater number of [drone] units that autonomously coordinate their behavior."[116] [f] However, despite reports on social media over the past year that Ukrainian forces have "been deploying smarms of 3 to 10 drones,"[117] the "vast majority of drones in the war in Ukraine are remotely piloted and humans not machines remain the interface that manually coordinates the actions of multiple drones. Thus, there … [have been] no true drone swarms or cooperative autonomy."[118] Instead, it is more accurate to describe drones being "operated in stacks" controlled by humans aided by software, artificial intelligence, and other forms of technology "rather than swarms."[119] Pettyjohn explains the distinction:

"While true drone swarms have not arrived yet, some observers believe that drone swarms are not that far away and that Ukraine and Russia are getting closer to being able to deploy swarms."

> *In a stack, drones are layered in the same vicinity but at different altitudes to prevent collision. Longer-range and endurance drones with better sensors are at the top of the stack providing persistent coverage of the battlespace and cueing other drones if a potential target is spotted. Below them, there is another intelligence drone that obtains precise targeting information. A separate drone will often pass that information to ground-based fires units or to kamikaze drone operators, which will then strike the target. Drones provide intelligence, including battle damage assessment, and determine if the target needs to be reengaged. In contrast, swarms typically consist of a greater number of units that autonomously coordinate their behavior.*[120]

Nevertheless, drones utilizing AI or autonomous features and/or technology have been operationally used in Ukraine,[121] and large numbers of drones have also been used in specific attacks.[122] As noted by Reuters, "AI drone development in Ukraine is broadly split between visual systems helping identify targets and fly drones into them, terrain mapping for navigation, and more complex programmes enabling UAVs to operate in interconnected 'swarms'."[123] There are various private companies active in the space, including the large U.S. technology company Palantir,[124] which has been reportedly helping Ukrainian UAS teams to "skirt around Russia's electronic warfare and air defence systems"[125] and smaller Ukrainian firms such as Swarmer that have "developed AI software that allows a single operator to control up to seven drones on bombing and reconnaissance missions."[126] While true drone swarms have not arrived yet, some observers believe that drone swarms are not that far away and that Ukraine and Russia are getting closer to being able to deploy swarms, and that this might happen in 2025.[127]

This growing reliance on mass drone deployments has, in turn, necessitated adaptations in counter-drone tactics, demonstrating how the scalability of innovation applies not only to offensive drone strategies but also to defensive responses. This has led to a scaled Ukrainian counter-UAS response, an effort just as noteworthy, as it highlights how counter-drone systems and methods used to disable drones have been evolving over the course of the conflict. For example, according to reporting by *Le Monde* and Defense Post, out of the total 188 Shahed drones that Russia launched on November

[f] Another definition offered by Zachary Kallenborn and Philipp Bleek defines a drone swarm as "multiple unmanned platforms and/or weapons [being] deployed to accomplish a shared objective, with the platforms and/or weapons autonomously altering their behavior based on communication with one another." See Zachary Kallenborn and Philipp C Bleek, "Drones of Mass Destruction: Drone Swarms and the Future of Nuclear, Chemical, and Biological Weapons," War on the Rocks, February 14, 2019.

26, 2024, "a total of 76 were downed kinetically by Ukrainian air defenses using fighter jets, helicopters, mobile air defense batteries, and surface-to-air missiles"[128] and through electronic jammers.[129] Ninety-five additional drones were "diverted by 'spoofing' their satellite coordinates."[130] Out of the 188 drones Russia launched, only 17 were able to evade C-UAS countermeasures. To further mitigate the threats posed by Shahed and other types of drones utilized by Russia, the Ukrainian government has been testing German[131] and American[132] interceptor drones. Ukraine has also been developing and deploying its own interceptor drones to take down rival FPV drones for some time.[g]

Nevertheless, the diversity of UAS platforms—whether originating from commercial and hobbyist designs or military-grade systems—on the battlefield presents distinct challenges and complicates efforts by both Russian and Ukrainian forces to scale their counter-UAS responses. In addition, the more recent introduction of fiber optic FPV drones (which will be discussed in greater detail in the section of this article focusing on range, highlighting the interplay between different component-level changes), which rely on cables to transmit data instead of radio or satellite signals, further compounds the counter-UAS challenge. These drones have a lower electromagnetic signature, making them more difficult to detect, and the closed nature of their data transmission renders them less susceptible—some even argue immune[133]—to electronic warfare measures.

Speed

Speed in drone warfare is not just about how fast a drone can move; it encompasses multiple dimensions that affect how drones are deployed, operated, and adapted for military use. Broadly, speed can be categorized into two main types: physical speed, which affects flight performance, and speed in decision-making, which accelerates battlefield response times.

Physical Speed and Tactical Agility

This refers to the raw velocity and maneuverability of a drone in flight. Drones optimized for speed, such as FPV drones, have reshaped battlefield dynamics, outrunning both soldiers and vehicles. Originally developed for recreational racing, commercial FPV drones have been repurposed as kamikaze weapons, carrying explosives and flying at high speeds. Ukrainian troops report that these small FPV kamikaze drones are so fast that "it is impossible to outrun them—you have to shoot them down."[134] On the other end of the spectrum, large loitering munitions trade speed for endurance, cruising slowly before executing high-speed dives onto targets, much like precision-guided missiles.

Before the war, FPV drones were mainly used for racing competitions and high-speed aerial cinematography.[135] The rise of organized drone racing leagues in 2015, along with improvements in compact, high-definition cameras, led to widespread commercial availability.[136] Platforms like YouTube and Vimeo enabled a growing community of FPV pilots to share footage, exchange knowledge, and refine piloting techniques. This accessibility played a significant role in their military adaptation. Unlike conventional military drones, which require lengthy procurement processes, commercial FPV drones could be purchased directly by soldiers and modified in the field. Their open-source nature allowed for rapid customization—whether by attaching explosives, installing thermal optics, or enhancing maneuverability for combat scenarios. FPV drones thus became one of the most cost-effective and adaptive aerial assets in modern warfare. Ukrainian and Russian forces alike have benefited from the vast knowledge base in the civilian FPV community, using forums, video tutorials, and trial-and-error engineering to optimize their performance for combat.

Arguably, one of the greatest advantages offered by FPV drones is their speed, which can be leveraged effectively to gain tactical advantages on the battlefield. Due to their small size and ability to reach speeds of up to 160 km/h, FPV drones are challenging to detect and intercept using conventional air defense systems. Their rapid maneuverability makes them extremely difficult to shoot down, as traditional anti-aircraft systems struggle to accurately target such small, fast-moving objects, forcing belligerents to rely largely on small arms—with limited effectiveness. The ability of FPV drones to engage targets rapidly has been a true game-changer. Highly maneuverable, an FPV operator can steer the drone around obstacles to strike at the weakest points of a vehicle or trench. Additionally, their speed has enabled FPV drones to catch up to and strike moving targets, even fast-moving vehicles and a helicopter.[137]

Low-flying FPV drones are fleeting targets that are difficult to destroy with small arms fire. Ukrainian soldiers have likened the sound of incoming drones to bees or hornets, providing little warning before an FPV drone strikes a position. However, if a drone can move faster than repositioning troops, it gains a significant advantage. Moreover, higher speed shortens the time from launch to impact, giving the enemy less warning. Agility is equally important for mission success, allowing an FPV drone to pop out from cover, adjust its course, and exploit gaps in defenses. Videos released by both sides of the conflict have shown operators loitering around a target, searching for weak spots such as an open hatch, a window, or thin top armor. This tactic leverages the ability to loiter slowly while attacking quickly, combining patience with bursts of speed—an approach that has proven extremely effective.

Across all categories of drones, speed and maneuverability translate directly into battlefield outcomes. This is especially evident in the case of loitering drones such as the Russian ZALA Lancet and the U.S.-supplied Switchblade. These drones often cruise slowly while searching for targets, then attack with a high-speed dive. The Lancet, for instance, cruises at around 110 km/h but can reach speeds of up to 300 km/h in its final attack,[138] giving targets little time to escape or deploy countermeasures.

In addition to their offensive use, speed is also critical for reconnaissance platforms such as Russia's Orlan-10 recon UAV and Turkey's Bayraktar, used by Ukraine. Both are fixed-wing drones with moderate speed. The Orlan-10 can cruise at around 110 km/h and accelerate in bursts up to 150 km/h, allowing it to scan wide areas quickly and, perhaps most importantly, evade small commercial quadcopters trying to intercept it.[139] Finally, in response to the growing use of reconnaissance and loitering

[g] For example: "In April 2024, Ukraine launched a competition to identify the most effective interceptor drone solutions, with dozens of Ukrainian drone manufacturers participating. One of these models is already credited with around twenty confirmed hits on enemy spy drones and is now being used by Ukrainian drone units on the Kursk, Kharkiv, and Zaporizhzhia fronts." For background, see Peter Dickinson, "Missiles, AI, and Drone Swarms: Ukraine's 2025 Defense Tech Priorities," Atlantic Council, January 2, 2025, and "Ukraine Introduces New Mavik Interceptor Drones to Counter Russian Quadcopters," Global Defense News, November 4, 2024.

munitions by Russia, Ukraine has begun developing specialized anti-drone FPVs capable of reaching speeds of up to 315 km/h in tests, aiming to intercept and target drones like the Orlan and the Iranian Shahed.[140]

Speed in Decision-Making

Speed is not limited to airspeed but also relates to the speed of the kill chain—essentially, how drones and their operators process and act on information in real time. Traditional drone operations require human pilots to manually navigate and engage targets, but advancements in AI and autonomous targeting systems are dramatically increasing reaction times. Both Ukraine and Russia are making significant advances in artificial intelligence, automation, and human-machine teaming to compress decision cycles from minutes to seconds. This includes using AI to analyze targets in live video feeds, networking drones and operators for instant communication, and enabling drones to autonomously identify and strike targets. The ability to make decisions—or enable humans to make decisions—faster than the adversary provides a critical advantage on the battlefield.

According to reporting from Reuters, Ukrainian drone teams often work together, with one soldier operating the remote controller and wearing FPV goggles, while another monitors a tablet with a digital map.[141] This setup allows the pilot to focus on flying the drone at high speed and maneuvering toward targets, while their teammate provides navigation updates or coordinates new targets. This form of human-machine teaming dramatically speeds up decision-making. The moment an enemy target appears on a map or screen, the drone can be redirected or guided in for a strike. By splitting tasks between crew members and relying on live data feeds, FPV units can react in seconds to battlefield changes, improving their strike success against dynamic targets.

A major boost to reaction speed comes from the integration of AI systems that assist or even replace human eyes in spotting and fixing targets. Instead of a human operator manually scanning a drone feed for a camouflaged target—which could be time intensive—to quickly identify targets, AI technology can aid and enable that task. Ukraine has invested heavily in such technology. For example, its military's experimental "Avengers" system uses AI-driven image recognition to scan drone and CCTV feeds; it has been spotting roughly 12,000 Russian pieces of equipment per week automatically,[142] a volume no team of humans could process in real time. This automation ensures that the moment enemy assets, such as tanks, become visible, the AI promptly flags their location on commanders' displays, facilitating rapid and precise decision-making.[143] On the Russian side, similar advancements are underway; Russia has touted the use of AI for target recognition in its Lancet strike drones.[144] This capability allows the Lancet to autonomously detect and lock onto specific targets, such as Ukrainian armored vehicles, during its terminal phase, enhancing strike precision and reducing the likelihood of human error.[145] Notably, investigations have revealed that the Lancet incorporates foreign technology, including components from U.S. companies. Specifically, the drone is equipped with Nvidia's Jetson TX2 AI module, a high-performance computing device designed for AI applications, and Xilinx's Zynq system-on-chip, which integrates programmable logic with processing systems.[146] The integration of such sophisticated AI modules enables the Lancet to process complex algorithms for image recognition and target tracking, facilitating real-time decision-making during missions. The result: faster and more accurate strikes. In general, these AI targeting systems have significantly accelerated the "observe-orient" phases of the decision-making process in military operations, commonly referred to as the OODA loop (Observe, Orient, Decide, Act)—thus, compressing the time from seeing a target to attacking it.[147] What might take a human 30 seconds to confirm (or a chain of command several minutes to approve), an AI system can decide in a flash.

The widespread adoption of AI-assisted targeting systems has not only enhanced strike precision but also transformed how battlefield intelligence is processed and acted upon. While AI-driven recognition technologies improve individual targeting capabilities, real-time data integration has emerged as another critical force multiplier, ensuring that battlefield information is rapidly shared and utilized across multiple units. According to reports from the frontline, real-time data integration in drone platforms has significantly sped up battlefield decision-making.[148] Using tools like Ukraine's Kropyva,[149] frontline observers and drone operators can instantly share reconnaissance data. When a drone marks an enemy position on a map, artillery batteries or loitering munitions receive precise coordinates and can engage the target within moments, as networked units seamlessly share information.[150] This streamlining of the kill chain eliminates the need for laboriously calling in targets over radios. Instead, soldiers observing a drone feed can simply tap a screen and targeting data flows directly to gunners. According to Ukrainian forces, this integration has had a significant impact, allowing them to turn drone sightings into artillery strikes with remarkable efficiency.[151]

Many domestically produced drones now feature AI-guided navigation, enabling them to "reach targets on the battlefield without being piloted," according to Ukraine's digital transformation minister.[152] Practically, this means if Russian jammers disrupt the control link, an AI-powered drone can still maneuver and strike based on preloaded target data or real-time visual recognition. By late 2024, reports indicated that "thousands of drones" were already flying themselves into targets without direct human control.[153] Ukrainian companies such as Vyriy and Saker are at the forefront of these advancements, developing AI-driven software capable of autonomously tracking targets using cameras and onboard computers—eliminating the need for constant human oversight.[154] These systems leverage computer vision algorithms and, in some cases, deep learning to interpret visual data, allowing for rapid and precise decision-making in both targeting and movement.[155]

A notable example is the Saker Scout, a domestically developed quadcopter designed to be compact enough to fit in a suitcase-sized container. Initially intended for commercial AI applications, the Saker Scout pivoted to military use following Russia's invasion in February 2022.[156] The drone can recognize 64 types of Russian military equipment and execute lethal strikes autonomously.[157] This level of autonomy not only allows drones to function independently in heavily jammed environments—an increasingly common feature of electronic warfare—but also enhances operational speed and reducing the need for constant human oversight frees operators to focus on higher-level strategic tasks, such as battlefield analysis and mission planning.

On the Russian side, many of the "Geran-2" (Shahed-136) kamikaze drones attacking Ukrainian cities are pre-programmed to follow waypoints and then dive on a GPS coordinate autonomously, functioning as a low-cost, long-range loitering munition rather than an AI-adaptive system.[158] These Iranian-designed drones rely on Global Navigation Satellite Systems (GNSS) and Inertial Navigation Systems (INS) for guidance, allowing them to execute precision strikes on fixed targets without direct human control.[159] However, unlike more sophisticated UAVs, it cannot dynamically adjust its flight path or seek out new targets mid-flight. This makes it highly effective against stationary infrastructure and military positions but less suitable for engaging mobile or time-sensitive targets.[160]

The trend is clearly toward more self-directed drones that can make split-second adjustments in flight. Ukraine is even testing drone swarms, where multiple drones coordinate attacks as a group with minimal human input. In a swarm, drones would share data and react to targets collectively at machine speed: If one drone's camera picks up an enemy radar, all drones in the swarm can instantly reposition to swarm it. Developers in Ukraine have created AI software (like the "Swarmer" system) to network drones in this way, allowing decisions to be executed instantly across a swarm of drones with almost no human involvement.[161]

Indeed, the acceleration of decision-making in drone operations has fundamentally altered the dynamics of the Russia-Ukraine war. The ability to observe, process, and engage targets at unprecedented speed has become a decisive factor in battlefield success. The integration of drones with AI-driven analytics has significantly reduced the sensor-to-shooter timeframe. In some cases, Ukrainian artillery units have neutralized targets within two to three minutes of identification by reconnaissance drones—an operational tempo that previously required hours.[162] The rapidity of drone-assisted targeting has greatly increased lethality, particularly against exposed personnel and equipment. According to *The New York Times*, "drones now kill more soldiers and destroy more armored vehicles in Ukraine than all traditional weapons of war combined."[163] A tank operating without adequate concealment, for instance, can now be detected, confirmed, and destroyed by a precision-guided loitering munition before its crew is even aware of its vulnerability.[164] As one analysis notes, this war is "taking warfare into uncharted territory" through the increasing autonomy and networking of drone systems.[165] At the core of this transformation is human-machine teaming, which is crucial to enhancing operational efficiency.[166] This collaboration ranges from soldiers sharing FPV drone piloting responsibilities to AI systems assisting human operators by filtering data and optimizing targeting decisions.

Range

Since the start of the conflict, range—and the ability for both Ukraine and Russia to conduct long-range stand-off attacks using drones and other weapons—has "become an increasingly prominent part of the Russia-Ukraine war."[167] It has become a strategic arena through which the war is being fought. When it comes to drones, range can be understood in two ways. First is the physical range of a drone—how far a specific drone can travel. Second is the range of control—the distance over which an operator can control a drone and provide operational inputs to modify a drone's behavior.

Physical Range

Over the past two years, Ukraine has progressively been able to fly one-way attack (OWA) drones further into Russia, and to expand the pace of those efforts. It is believed that the "first recorded incident involving a suspected Ukrainian long-range OWA drone came in June 2022, with an attack on a Russian oil refinery in Rostov."[168] [h] The facility that was struck was located "around 10 kilometers (6 miles) from the Russo-Ukrainian border and over 200 kilometers (120 miles) from the front line."[169] Six months later in December 2022, Ukraine reportedly used drones to attack two Russian airbases located deep inside Russia—more than 500 and 700 kilometers from Ukraine.[170] Then, in May 2023, Ukraine flew drones to Moscow and attacked the Kremlin.[171] A little more than a year later in July 2024, Ukraine conducted its longest-range drone attack to date when it used drones to attack an airfield in Russia's Arctic, more than 1,700 kilometers from Ukraine.[172]

As noted earlier, Ukraine has used a diverse mix of drones for long-range attacks. This includes commercial and military grade drones, UASs produced and supplied by foreign partners, and modified light aircraft. Public information detailing the design and components and sensors that are incorporated into Ukraine's long-range drones are lacking, which makes it hard to discern which systems could be recreated using commercial technology. More simple variants, such as the AQ Scythe drone, provide a window into how long-range drones could be developed by VEOs and other types of non-state actors, however. As noted by Terminal Autonomy—the company that produces the AQ Scythe—the drone "is the culmination of … efforts to offer strategic capabilities at the very lowest prices."[173] The Scythe, whose fuselage is "made from milled sheets of plywood from Ukrainian furniture factories … a more scalable alternative to 3-D plastic printing," has a small gas engine, boasts a 750km range, and has the capability to carry a "total payload of 94 pounds."[174] Reporting from 2023 suggests that each AQ Scythe costs between $15,000 to $25,999 to produce.[175] While not as capable as more advanced drones, such as the Liuty, that Ukraine uses for long-range missions, the AQ Scythe drone would be easier for a VEO to reverse-engineer and manufacture.

More detailed public information exists about the components found in long-range Iranian Shahed and Russian-produced Shahed variants, the primary long-range drone platform that Russia has been using to attack Ukraine. The results from multiple Conflict Armament Research (CAR) field investigations have revealed how Shahed variant drones recovered in Ukraine are developed around commercial components produced in other countries that either Russia or Iran have sourced. For example, in November 2022 CAR reported that four UAS recovered in Ukraine—one Shahed-131, two Shahed-136, and one Mohajer-6 UAS—were "made almost exclusively of components produced by companies based in Asia, Europe, and the United States."[176] During its investigation, CAR documented 495 components found in the four UAS. It discovered that more "than 70 manufacturers based in 13 different countries and territories produced these components, with 82 per cent of them manufactured by companies based in the United States."[177] Or, put another way, a key and strategic "military grade" long-range UAS that Iran developed, and shared with Russia, has largely been constructed around commercial technology acquired from U.S. companies.

[h] As noted by Reuters at the time, Russia was "also investigating the cause of a large fire that erupted at an oil storage facility in the city of Bryansk, 154 km (96 miles) northeast of the border with Ukraine, in late April [2022]." So, it is possible that the June 2022 attack may not have been the first. See "Russian Refinery Says It Was Struck by Drones from Direction of Ukraine," Reuters, June 22, 2022.

"A key and strategic 'military grade' long-range UAS that Iran developed, and shared with Russia, has largely been constructed around commercial technology acquired from U.S. companies."

In August 2023, CAR examined two additional Shahed variants recovered in Ukraine. It concluded that the two UAS recovered were likely produced by Russia and not Iran. But CAR also found that the "Russian-produced Geran-2 UAVs are almost exclusively made of components bearing the marks of companies based outside the Russian Federation," specifically "companies headquartered in China, Switzerland, and the United States."[178] Further, a third of the components CAR traced had been manufactured between 2020-2023, including 12 components that "were manufactured after the start of the invasion in February 2022."[179] These findings put a finer point on how U.S. adversaries are leveraging dual-use technologies, including recently manufactured components, to develop long-range UAS platforms used to attack Ukrainian forces and civilians. There is also evidence that U.S. technology was used in the Shahed drone that killed three U.S. servicemembers in the "Tower 22" attack in Jordan in January 2024.[180] In December 2024, the Department of Justice indicted two individuals, one of whom was arrested in the United States, for conspiring "to evade U.S. export control and sanctions laws by procuring U.S. origin goods, services and technology from" a U.S. company and illegally exporting those items to Iran to develop a navigation system.[181] The indictment further alleges that "the same navigation system … was determined to be used in the drone that struck Tower 22 and caused the death of three U.S. service members."[182]

Additional reporting highlights how Russia has been working to diversify and augment its production of long-range UAS through partnerships with companies based in China. In 2023, Russia began producing and deploying "a new long-range attack drone called the Garpiya-A1."[183] In October 2024, the U.S. Treasury Department sanctioned two companies based in China, another company based in Russia, and a Russian national for the roles they played in the production and deployment of this new drone.[184] In its press release, the U.S. Treasury Department claimed that the Garpiya was "designed and developed by People's Republic of China (PRC)-based experts" and that the Garpiya drones were "produced at PRC-based factories in collaboration with Russian defense firms before transferring the drones to Russia for use against Ukraine."[185] The two China-based companies—Xiamen Limbach Aircraft Engine Co., Ltd. (Limbach) and Redlepus Vector Industry Shenzhen Co Ltd (Redlepus)—reportedly produced the L550E engine for the Garpiya and supplied "electronic and mechanical components with UAV applications such as aircraft engines, parts of automatic data processing machines, and electrical components."[186] The Garpiya case illuminates how Russia has outsourced the production of some long-range UAS, and the role that China-based companies have played in producing a new type of drone and in providing key UAS components.

Range of Control

For drones that have less range, but that provide other advantages such as speed (e.g., FPV variants), Ukrainian and Russian forces have been utilizing and developing methods to both extend the distance FPV drones can travel and the range of control—the distance over which an operator can control a drone and provide operational inputs to modify a drone's behavior. There are simple methods, such as upgrading the antenna and optimizing its placement, and incorporating signal boosters, that can marginally extend the range of drones,[187] that have been utilized in Ukraine. But two other methods—one that is more well known and another that has reportedly started to emerge in Ukraine—hold potential and are important to watch. The first method is utilizing repeaters to extend a drone's range. This can be done by pre-positioning relay devices/repeaters located at a distance in the field or by leveraging forward-deployed drones to function as repeaters to receive and transmit data from the drone's controller. This method, which can involve the use of one or multiple repeaters, enables the operator to control and provide instructions to a drone over greater distances.[i] Given the nature of frontline warfare in Ukraine, pre-positioning repeaters across enemy lines can be an exceptionally risky task for soldiers to execute. To lower the risk, Russian and Ukrainian forces have been using FPV drones to function as flying repeaters for other FPV attack drones.[188] While just how much additional range FPV repeaters provide likely varies, some argue that repeaters can "double the range of FPVs," enabling "them to reach targets which would otherwise be inaccessible."[189]

In January 2024, reporter David Hambling provided an inside look at a Russian FPV repeater that was recovered in Ukraine.[190] The repeater was paired to work with the Russian Ghoul FPV drone, "a small, fast quadcopter able to carry an RPG warhead."[191] Similar to other Russian repeater drones, the recovered device "doubles the range of the Ghoul by relaying control signal from the operator to the FPV and video signals from the FPV to the operator."[192] What made the discovery of the recovered FPV stand out was its make-up and components. It "was smarter-looking than many other locally-made drones," was designed using CAD software, included custom 3D-printed parts, and made "effective use of off-the-shelf commercial components."[193] Some of more noteworthy commercial components that the drone included were an outsized antenna, a SpeedyBee flight controller, commercial radio and video transmitters, and a commercial SAW filter.[194] The SAW filter found on the drone "costs $2 and blocks radio frequencies outside a certain narrow range" limiting the frequencies where the receiver would be vulnerable to jamming."[195] Posts with photos and videos of Ukrainian FPV repeater drones are also available online,[196] highlighting how both sides of the conflict are using and developing FPV repeaters to enhance range.

The other noteworthy method that has started to emerge in Ukraine is the reported development and use of 'drone carriers' to transport FPV drones. The idea is similar to initiatives being pursued by the United States and other nations whereby a collection of smaller drones would be transported to an operational

[i] Another method commonly referred to as daisy-chaining involves the use of different operators separated by distance, such as being located at opposite ends of a drone's range, who use separate controllers and hand the drone off to one another.

area in a fixed-wing 'mothership' drone and launched from it.[197] One of the primary benefits of such an approach is that it allows operators to preserve limited FPV battery life; in Ukraine, "FPV flights typically last 15 minutes or less, even with the best batteries available, so the maximum possible range is perhaps 20 miles."[198] So, instead of the FPV drones using their own power to arrive at a target location, the drone carrier uses its power to transport them, which enables the FPV drones to fly and conduct operations at even greater distances. According to reporting by David Hambling, in September 2024, Russian developers showcased a drone carrier called the Burya-20.[199] It is believed that the Burya-20 "can fly more than 40 miles from ground control, and release a number of FPV attack drones."[200] The new drone carrier, which Russian developers claim is in small-scale production, can reportedly carry a payload "over 30 pounds, enough for several FPVs" and also has the ability to function "as a relay station, directing the FPVs from up to 9 miles away."[201]

The ongoing reduction in barriers to entry to increasingly capable commercial unmanned systems and components has revolutionized the Russo-Ukrainian War and how it is being executed, especially as it relates to speed, range, and scale. As many observers have noted, the full impact of the Russo-Ukrainian War's drone developments will be much broader, more profound, and longer-lasting. Various nation-states, such as the United States, have been paying close attention to what is going on in Ukraine and have recognized how the war will transform future wars—and how future conflicts will be dominated by the scaled and integrated use of unmanned systems combined with other forms of technology. This recognition is not just casual; it is disrupting and driving change across the U.S. defense enterprise.[202]

But, since most of the drone innovations taking place in Ukraine have been widely shared and discussed online, states are not the only actors paying attention. VEOs have been taking note, too. For example, jihadi and far-right extremist networks online have both been sharing information about drone systems and the evolution of drone tactics in Ukraine.[203] While a successful terror drone attack has not happened yet in the United States—or another Western nation—in 2024, the FBI observed "a concerning increase in the use of UAS in the commission of crimes with the intent to cause injury to U.S. persons on U.S. soil."[204]

Part III: Terrorism Implications

This section, Part III, examines the terrorism implications of the drone developments and innovations that have emerged from the Russo-Ukrainian War, and it provides a perspective on the dangers those developments pose for terrorism and how they are likely to shape future terror activity. For parity with Part II, emphasis is placed on evaluating the terrorism implications associated with the scaled use of drones in Ukraine, and the broad deployment of commercial and mixed-makeup drones that operate at greater speeds and extended ranges. This includes a short discussion of how drone capability and use trends in Ukraine introduce new terrorism risks and are likely to complicate the ability of governments to identify and effectively mitigate future terror drone threats, *and* potentially other adversarial drone threats, through the deployment of counter-small unmanned aerial systems (C-sUAS) and other approaches. Noteworthy areas where there is convergence between drones deployed in Ukraine, drone and component supply chains, and VEO use of drones are also discussed.

Scale

There are important differences between what state and violent non-state actors can achieve with drones, especially when it comes to scale. This is because it is usually easier for states to gain access to military-grade systems and technologies. States also have more resources, which they can use to develop or purchase equipment and systems, such as drones, at scale. So, as a starting point it is important to remember that terror groups usually operate from a weaker, disadvantaged position—a factor that informs the choices and strategies terror groups pursue and what terrorist use of drones at scale would look like.

Prior to the Islamic State's breakthrough weaponization of drones during 2015-2016, terror groups' application of drones typically involved the use of one or a few commercial or 'homemade' drones. For state-supported entities such as Hezbollah and Hamas, their drone efforts also included more capable military systems provided by Iran. While commercial drones were becoming more available and sought after by VEOs in the lead up to 2016, drones were not widely integrated by VEOs as a common tool or capability. As a result, the pace or scale of terror network operations that involved drones remained low.

The Islamic State dramatically changed these dynamics and was able to develop an arsenal of drones and significantly increase the scale of its drone operations. At its peak in the spring of 2016, the organization was conducting at least 60-100 aerial drone bombing attacks per month across Iraq and Syria.[205] Further, as highlighted by General Raymond Thomas, there was a day in early 2017 during the fight to recapture Mosul "where literally over 24 hours there were 70 [Islamic State] drones in the air ... At one point, there were 12 'killer bees' if you will, right overhead and underneath our air superiority."[206] There is also evidence that speaks to how the Islamic State operated drones in a stack during this period.[207]

Multiple factors enabled the Islamic State to deploy drones at this type of scale, many of which would be difficult for other VEO groups to replicate. This included the Islamic State's control of a broad swath of territory and key cities such as Mosul, which contained manufacturing facilities, universities, and many other resources. The Islamic State also had access to, and recruited, specialists with technical expertise and individuals who were either based in, or could acquire drone systems and components from, foreign countries.[208] It leveraged some of these individuals and their access and developed a global and layered supply chain to source drones and other related components. For example, during the group's heyday one key node of the Islamic State's supply chain network acquired commercial technology from "at least 16 different companies that were based in at least seven different countries."[209]

The Islamic State also devoted considerable financial resources to its drone efforts. In 2018, the U.S. Treasury Department designated Yunus Emre Sakarya and an ISIS front company that he ran—Profesyoneller Elektronik—that was "involved in the procurement of UAV-related materials."[210] During the first half of 2016, Profesyoneller Elektronik "was involved in transactions for UAV-related equipment that totaled over $500,000 for ISIS."[211] Another key factor that helped the Islamic State to scale its drone efforts was that it took all of these inputs and developed standardized methods to creatively and cheaply transform stock quadcopters into aerial bomb dropping weapons of war, an approach that was complemented by drone-related training. Since that time, besides the Houthis—whose drone capabilities vastly exceed those ever possessed by the Islamic State—no other non-state terror group has come close to obtaining the scale or sophistication of what the Islamic State achieved through its drone program during the 2016-2017 period. It is also important to keep in mind that the Houthis' ability to deploy drones at greater scale and conduct long-range drone attacks has been strategically enabled by the equipment, systems, resources, and training that Iran has provided.

VEO networks that do not have control of territory (or some element of safe-haven), developed and resilient supply chains, or state-level assistance will be hard-pressed to develop and deploy attack drones at large scale as part of a longer-term operational drone campaign. What is arguably more likely and possible for a terror network to achieve over the next several years is for it to deploy a large number of stockpiled drones either as part of a single attack or as part of a more limited, phased, or 'wave-type' operational campaign executed over a limited span of time. It is also possible that a capable, radicalized individual or small cell could also deploy a collection of armed drones as part of an attack or series of attacks. For example, one scenario to consider is what the D.C. sniper attacks would have looked like if weaponized drones were used instead of a long-range rifle to attack random, dispersed, and unsuspecting civilian targets. Since the ability to deploy drones at scale is dependent on the ability of a VEO to acquire a sizable collection of drones, a key variable for counterterrorism practitioners to pay attention to are those VEO networks that are strategically patient and that have the discipline to stockpile a collection of drones rather than use them not long after they have been acquired. For the threat posed by individuals, effective 'arming' or weaponization of commercial drones still remains a key hurdle and investigative trip wire.

When it comes to scale, it is also likely that the terror drone threat will look different in different contexts/environments. For example, VEO networks that operate in more permissive areas where local security forces have fewer resources, are less capable, and/or have limited or no access to counter-UAS capabilities will have more opportunities to deploy drones—even less capable variants—at scale, and potentially with effect. As outlined below, reports about the evolving use of drones, including weaponized drones, by Islamic State and al-Qa`ida affiliates in Africa, is particularly concerning, and a 'watchout' area, in this regard.

It is hard to predict what the scaled terror drone operations will look like in the future. While the threat lurks on the horizon, it is also hard to know when that moment will arrive. The increase in the scale of drone use by cartels along the southern border of the United States[j] and the number of unidentified drones flown over stadiums during NFL games over the past several years highlights how scale has already evolved as a problem for other categories of non-state actors. These cases also illustrate how scale has stressed C-UAS coverage in the United States and how it can complicate the ability for security personnel to identify:

> *In 2022, we experienced 2,537 rogue drone flights into the restricted air space above stadiums during NFL games, and in 2023, the number of incursions grew to 2,845. To put these numbers in context, when I testified in 2018, we had tracked about a dozen incursions by drones at stadiums during games in the 2017 season. In the 2018 season, we tracked 67 drone incursions at games. Even accounting for the increased sophistication of our drone tracking abilities today, these statistics almost certainly understate the total number of events. Yet, even with that limitation, these statistics demonstrate the dramatic increase in drone incursions*—rising by more than 20,000 percent between 2017 and 2023.[212]

Over the short term, it is reasonable to expect that the threat area will follow a progression, with VEOs experimenting with or deploying drones in a coordinated stack—with heavy dependence on human control and human-machine teaming, versus an autonomous drone swarm. This could take various forms. VEOs could look to asymmetrically mirror the stacked use of drones in Ukraine. For example, a VEO could deploy many 'decoy' drones to distract an adversary or to hide or protect a drone that is more capable of delivering more lethal or strategic effects as part of an attack. It is also possible that VEOs could use and deploy many low-cost drones over time as a form of economic asymmetric warfare with the intent to deplete, and over time attrit, the resources of a more well-resourced state adversary. The broad use of cheap improvised explosive devices (IEDs) by terror groups during the wars in Iraq and Afghanistan provide one example of how terror entities, at low cost, made those wars much more costly for the United States and its partners. The broad use of IEDs during those conflicts also constrained the mobility of U.S. and partner forces, and it is possible that a fleet of cheap weaponized drones could be used by VEOs in a similar way in the future. There is already precedent for this as during the 2016 period, the Islamic State used drones to complicate the activity and mobility of Iraqi security force units.

When it comes to scale, a core security implication for the United States and its partners is that the potential for a scaled terror drone threat increases the need to be able to deliver a scaled response. The issue of speed only compounds that challenge.

Speed

As discussed above, speed—through the broad-scale deployment of commercial FPV drones that operate and can more effectively be controlled at high speeds—is another vector that has been revolutionizing the Russo-Ukrainian War. While FPV drones have not been broadly adopted or deployed by VEOs, there is a growing corpus of evidence that VEOs recognize the value of these types of systems; that they are trying to acquire them; and that several VEOs are already deploying FPV drones, including weaponized versions. One way to characterize the moment is that we are at the beginning phase of FPV drones being more widely adopted by terrorist groups. Given the wide availability of commercial FPV drones, and how easy it is to observe and collect information online about their weaponized use in Ukraine, it is highly likely that over the next several years that FPV systems will be deployed by more

[j] For example, as noted by CBP during congressional testimony in December 2024, "During a recent six-week period, CBP recorded more than 6,900 drone flights within close proximity of the Southwest Border It is these flights, particularly those in areas of high illicit activity, that pose the greatest risk to CBP's – and our partners' – operations, personnel, and crewed aircraft." The CBP official also stated that "the volume of [UAS] activity within 500 yards of our contiguous border … is staggering." "Counterterrorism, Innovation, and Threats: Military and Security Testimony Before the House Committee on Homeland Security," U.S. House of Representatives, Committee on Homeland Security, 118th Congress, 2nd session, December 10, 2024,

"It is important that the counterterrorism community think through the threat implications associated with high-speed drones, and how defensive approaches can identify and mitigate these types of threats."

and more VEOs, including by networks operating in different areas and who are motivated by different causes. The primary danger is that this will enhance the ability of VEOs to conduct stand-off attacks at speed and to engage in surprise. Thus, it is important that the counterterrorism community think through the threat implications associated with high-speed drones, and how defensive approaches can identify and mitigate these types of threats.

Terrorist group interest in developing or acquiring high-speed drones is not entirely new. Nearly a decade ago in August 2015, an Islamic State network that procured drones and other components for the group, purchased a plan for a "valved pulsejet engine capable of approximately 222 N (50 lbs) of thrust" from a U.S. company.[213] As explained by Conflict Armament Research (CAR): "Pulsejets are a type of acoustic jet engine originally developed for World War II-era V1 'flying bomb' cruise missiles … They remain inexpensive and [are a] technically unsophisticated jet engine, which some amateur model aircraft enthusiasts use to construct jet-powered model aircraft capable of speeds of 250 km/hr and more."[214] Two years after the Islamic State purchased the pulsejet engine plan, a "fully constructed pulsejet engine" was recovered by CAR at a complex in Mosul, Iraq, that the Islamic State had used to store weapons and ammunition and "as a production facility for airborne IEDs and a range of other weapons."[215] The discovery demonstrated how the Islamic State was experimenting with the technology for potential future use and how the group was looking at speed as an attack vector.

Commercial FPV drones have made speed, and the ability to navigate a UAS at speed, much more accessible, and it did not take long for armed actors in other conflicts, to include proxies and terrorist groups, to adopt and try to replicate how FPV drones have been used in Ukraine. For example, in September 2023, David Hambling noted how the Sudanese Armed Forces were attacking Rapid Support Forces units with small weaponized FPV drones.[216] More recently, FPV and long-range drones are reported to have played an important role in helping the coalition led by the now disbanded group Hayat Tahrir al-Sham (HTS) to capture Aleppo, Hama, and Syria's capital, Damascus. FPV drones "enabled HTS and its allies to accurately strike tanks, artillery positions, and individuals behind enemy lines," activity which was also complemented by HTS' deployment of longer-range fixed wing drones.[217]

The Washington Post has also reported that prior to HTS' capture of Damascus, the Ukraine government gave 150 FPV drones to HTS and sent "20 experienced drone operators" to share and advise HTS in drone tradecraft.[218] It has also been reported that HTS developed and used turbo-jet powered, fixed-wing drones to attack Assad's forces.[219] (Turbo-jet engines acquired by the Houthis have also been recovered in Yemen.[220]) Not surprisingly, terror group interest in FPV drones in the Levant is not limited to HTS and other militant groups that collaborated with it. Islamic State networks online have been sharing information about FPV drones on Telegram,[221] an indicator which suggests that the Islamic State inside Syria and Iraq will soon deploy weaponized FPV drones, if this has not happened already.

There is a growing corpus of evidence that Islamic State- and al-Qa`ida-affiliated terror groups operating in different regions of Africa have either sought to acquire or have been using FPV drones, too.[222] For example, in the fall of 2023 three Kenyan nationals were reportedly "charged with eight counts of terror-related charges" for importing "a DJI Matrice drone from South Africa" for al-Shabaab.[223] A mix of reports from more reliable press articles to unverified social media posts suggest that FPV drones are an increasing capability of emphasis for Islamic State-Somalia. In January 2025, for instance, Defense Post reported that the Somali Army "shot down around nine drones loaded with explosives which IS tried to attack and detonate on the security forces during the fighting."[224] Nine days later, the Somali Guardian claimed that Islamic State-Somalia used a weaponized FPV drone to kill a Somali soldier.[225] Unverified photos of commercial drones, including FPV variants, that have allegedly been recovered by Puntland security personnel have also been posted online.[226] In Nigeria, the government has acknowledged that ISWAP has been using weaponized drones to attack military bases.[227] There is also evidence that JNIM has been deploying weaponized drones in Mali.[228]

As these examples highlight, VEO interest in, experimentation with, and adoption of commercial FPV drones has already begun to proliferate. Several factors—the way the Russo-Ukrainian War continues to highlight the power and value of commercial FPV drones, and the ongoing reduction in barriers to entry (e.g., accessibility, ease of use, and cost)—make it highly likely that proliferation and VEO adoption of FPV drones will both broaden and intensify over the coming years. Due to this, it is probable that speed will evolve as a more important terrorism threat vector.

The ability for VEOs to access and deploy commercial UAS platforms, and—in turn—enhance their capability to conduct aerial operations at speed presents several security challenges. One core challenge is whether counter-UAS platforms have the ability to detect *and* mitigate small commercial high-speed drones. This is particularly relevant to commercial FPV drones that VEOs or individual extremists have weaponized, as if a C-sUAS platform cannot detect *and* mitigate a hostile drone at a commensurate speed, then it creates space—a gap in coverage and response—that extremists can exploit. C-UAS systems also need to keep pace with evolving tactics, such as the deployment of fiber optic FPV drones,[k] which—given the closed nature of how those types of drones communicate—are harder to mitigate. For example, it is possible that even well-defended sites, such as the White House, could face challenges in mitigating a weaponized fiber optic FPV drone attack. Since scale is also a potential threat variable, it is important to evaluate whether C-sUAS platforms can defeat attacks that

[k] Fiber optic FPV drones are UAS that include a spool of fiber optic cable, which is used to transmit data, that has been attached and/or integrated onto the drone. For background, see Roman Pahulych, "Fiber-Optic Drones The New Must-Have In Ukraine War," Radio Free Europe/Radio Liberty, March 12, 2025.

involve multiple or the phased deployment of hostile fast-moving drones. This is because the Russo-Ukrainian War has demonstrated how mass and scale can be utilized to confuse defensive systems or to 'hide'/provide cover to a drone that can deliver more powerful effects.

A second related challenge is the context in which C-UAS platforms are deployed and the statutory frameworks that legally govern their practical use, as C-UAS technologies are only as good, or only as capable, as *how*, *where*, and *when* they can be used. This varies country by country. The current statutory framework that guides the deployment of C-UAS platforms in the United States highlights some of this capability-authority tension, and the vulnerabilities and response limitations it enables. Various federal statutes, for example, "provide four federal departments—DHS, DOJ, DOD, and DOE—express statutory authority to conduct drone detection and counter-drone operations" in the United States.[229] While DOD and DOE have the authority to detect and mitigate drones that are determined to be threats to their facilities in the United States,[230] DHS and DOJ have been vested with broader authority to mitigate hostile drones operating in the country, specifically at airports.[231] The Federal Aviation Administration, which regulates civil aviation activity in the United States, has more limited authority to "test and evaluate technologies/systems that detect and/or mitigate risks posed by UAS at five airports," but it does not have the authority to mitigate a hostile, unauthorized drone "that poses a risk to aviation safety" unless it is discovered as part of C-UAS testing and evaluation.[232]

In the United States, local law enforcement—those who are "expected to be the first to respond to a drone sighting"[233]—do not have the legal authority to use C-UAS platforms to mitigate drone threats. As noted by government witnesses during congressional testimony in December 2024, the "absence of such authority has hamstrung their efforts."[234] It has also led to C-UAS response challenges, as neither "DOJ nor DHS has the resources to fill the thousands of requests each year we receive to use our authority to assist our SLTT [state, local, tribal, and territorial] partners."[235] Or, as was stated by another participant in the hearing, "The demand for [C-UAS] protection ... vastly exceeds federal resources."[236]

The current legal framework is designed to protect the privacy and civil liberties of individuals, and it is guided by "several federal criminal laws, such as laws relating to electronic surveillance, signals interference, aircraft piracy, and aircraft sabotage."[237] While well intentioned, the current C-UAS statutory framework in the United States creates various gaps. These seams make it hard for the U.S. government to quickly respond to drone threats that operate at speed; against targets where C-UAS systems are not in place, or where DHS or DOJ are not postured, well postured, or are allowed under existing law to provide coverage; and against geographically dispersed drone threats. For example, "current law does not contain clear authority for the federal government, SLTT law enforcement, or the private sector to mitigate or, for certain technologies, even detect UAS that threaten critical infrastructure ... Gaps in legal authorities [also] leave sensitive federal facilities, such as CIA Headquarters vulnerable to both intelligence collection by foreign states and physical attacks by hostile actors."[238] This significantly limits the ability of the United States to respond to hostile drone threats launched by terrorists and other actors, especially high-speed ones.

There has been recognition—from Congress, the DOJ, FBI, Customs and Border Protection, industry, and other entities—that the "current legal authorities are insufficient to deal with drones."[239][l] For example, the need for the United States to bolster its C-UAS posture was reflected in 2022 in the Domestic Counter-Unmanned Aircraft Systems National Action Plan that the Biden Administration released.[240] The need is also reflected in bills that have been introduced in the Senate (S.1631) and House or Representatives (H.R. 8610 and H.R. 4333) that "would renew and reform counter-UAS legal authorities."[m] The two leading bills making their way through Congress share a lot of common ground and would extend, in a limited and measured way over a defined period, the ability for some federal, state, local, territorial, or tribal law enforcement agencies to acquire and deploy counter-UAS systems under specified conditions.[241][n] Both bills would create a pilot C-UAS program for local law enforcement. For example, under the bipartisan Counter-UAS Authority Security, Safety, and Reauthorization Act (H.R. 8610), a limited C-UAS mitigation law enforcement pilot program would be created "to assess the efficacy of approved counter-UAS mitigation systems at covered sites and determine the appropriate policies, procedures, and protocols necessary to allow State and covered local law enforcement agencies… to acquire, deploy, and operate approved counter-UAS mitigation systems and mitigate unauthorized UAS operations on behalf of covered entities."[242]

The ideas expressed in these bills would enhance the United States' C-UAS posture, and it is a step in the right direction. But the scale and scope of change that the current versions of the bills would enable will also be constrained, as the pilot programs are limited. For example, under the current version of H.R. 8610, the pilot program would initially be limited for the first 18 months to "not more than 5 State or covered law enforcement agencies" that can only operate C-UAS mitigation systems at four covered sites.[243] After the initial 18-month test period, the number of law enforcement agencies participating in the program could be expanded to 10.[244] And after three years, the number of covered sites could include "not more than 20."[245] Under H.R. 4333, the Homeland Security Secretary and Attorney General can initially select "a combined total of not more than 12" SLTTs "for participation in the pilot program, and may designate 12 additional SLTTs each year thereafter," but the total number of SLTTs that are allowed to participate in five-year pilot is capped at 60.[246] These proposed pilot programs would expand C-UAS coverage in a limited way over a multi-year

[l] As noted by the FBI during recent Congressional testimony: "The FBI strongly supports pursuing expanded counter UAS authorities for State, Local, and Tribal as robustly and swiftly as is prudently possible." "Counterterrorism, Innovation, and Threats: Military and Security Testimony Before the House Committee on Homeland Security," U.S. House of Representatives, Committee on Homeland Security, 118th Congress, 2nd session, December 10, 2024.

[m] This includes, for example, the "Safeguarding the Homeland from the Threats Posed by Unmanned Aircraft Systems Act of 2024," a House companion bill filed under the same name, and the House's Counter-UAS Authority Security, Safety, and Reauthorization Act. For background on these bills, see "Counter-Drone Expansion Depends on Congressional Compromise and NDAA Passage This Fall—Here's What to Expect," Commercial UAV News, October 3, 2024, and Matt Bracken, "Federal law enforcement officials make the case for expanded drone authorities," FedScoop, December 11, 2024.

[n] As noted during Congressional testimony, "The legislation would authorize all SLTT law enforcement as well as the owners or operators of airports or critical infrastructure to use federally vetted UAS detection-only capabilities, subject to conditions and safeguards."

span, and if deemed successful, they could also open the door to the broader distribution of C-UAS authorities to other local law enforcement entities across the country. But without broader and timely distribution of C-UAS authorities, terror adversaries will be able to find seams, as according to DHS there are approximately 18,000 law enforcement agencies in the United States.[247]

Range

Ongoing advancements of commercial drone platforms, powering technologies, and software is also making range, and the extension of range, more accessible as a capability. For example, today's "commercially available drones ... are more efficient, more capable, and can fly farther, faster, longer, and with heavier payloads than drones that were available to consumers a decade ago."[248] Further, "stepwise and more radical advancements in consumer UAS will continue to elongate range and make longer-range UAS attack pathways more viable for violent non-state actors."[249] One could make the case, as one of the authors has argued elsewhere, that the era of long-range drone terrorism has already arrived. For example, the Houthis' long-range drone strikes are arguably "just an early manifestation, or leading-edge indicator, or a broader, coming problem."[250] While much less capable, HTS reportedly developed and used one-way fixed-wing attack drones to strike Syrian regime targets at more extended ranges as part of its campaign to overthrow Bashar al-Assad last year.[251] The HTS drones were in part modeled on "captured Iranian and Russian suicide drones that did not explode."[252]

The decision of VEOs to pursue and engage in long-range drone operations will be shaped by several factors that have the potential to accelerate and constrain adoption. Innovative achievements by experienced remote-control hobbyists have already demonstrated that "commercial technologies and systems can be leveraged" and repurposed by nefarious actors "to execute long-range missions."[253] But just because range has become more accessible to VEOs, and likely will become even more accessible in the years ahead, does not mean that VEOs will broadly pursue or develop long-range UAS capabilities. VEOs will need to navigate technical feasibility, resources, and operational tradeoffs (e.g., the benefits and risks involved, especially when other types of tried-and-true weapon systems are easily available). As a result, as one of the author's has previously noted, the approach will likely:

> *only appeal to those types of extremist networks that have an interest in attacking targets from a long range, and that believe such an attack would advance their specific cause and/or goals. Terror networks, for example, that are more concerned with local issues ... would likely not want to expend the resources or take on added risk to experiment with and develop the capability. But terror networks, or regimes, that have more resources, that have key enemies located a great distance away, and/or that embrace a 'far-enemy' targeting mindset would likely be more interested in long-range stand-off terrorism.*[254]

"Given that resources will be a key determining factor for first movers,"[255] it is important that emphasis be placed on more well-resourced VEOs and on movements and proxies that receive support from states such as Iran. Another key area that requires scrutiny and monitoring are areas where there is convergence between state and VEO activity in relation to drones, and specifically the procurement and development of long-range UAS systems and related technologies. The discussion in Part II about Iranian Shahed and Russian Garpiya long-range drones used in Ukraine highlights two important points of convergence in this regard. The first is a focus on drones, including long-range variants, and related components that have been designed and produced by companies based in China. Given that the UAS market is dominated by firms based in China and that the country is a key global manufacturing hub, it is not surprising that VEOs would seek out drones manufactured by Chinese companies, or that VEOs would seek to develop direct supply-chain links with Chinese companies that produce drones and other key components. But, as outlined below, the nature and type of support that some China-based companies have been providing to VEOs is enabling their capabilities, which is a concern.

Like Russia, the Houthis have developed ties with companies based in China that produce and/or supply key dual-use and military grade components used in Houthi UAS and missiles. These relationships are part of a broader "network of international shipping and logistics companies" that the Houthis have used to transport commercial and "military-grade components from third-country suppliers to their forces in Yemen."[256] For example, in October 2024, the U.S. Treasury Department sanctioned three companies based in China for helping the Houthis to procure weapons and smuggle materiel. This included two companies—Shenzhen Jinghon Electronics Limited and Shenzhen Rion Technology Co., Ltd.—that supplied dual-use and other critical components that "Houthi forces have used to advance their domestic missile and UAV production efforts."[257] The third China-based firm engaged in similar activity and was used by "Houthi logistics operatives ... to transport ... important dual-use and military grade items via commercial methods in an effort to evade interdiction."[258] The U.S. Treasury Department's press release also noted how "Houthi operatives located in Iran and elsewhere manage an array of supply chains and smuggling networks to transport dual-use materials and other lethal aid into Houthi-controlled territory,"[259] highlighting how Iran and the Houthis have been collaborating to acquire and smuggle UAS components.

In August 2024, maritime security forces of the Yemeni National Resistance Forces interdicted a dhow associated with the Houthis that contained a considerable amount of UAS and related materiel. CAR's field investigators were given access to the seized items, which included:

- Hundreds of airframes and fins for use in the local assembly of 270mm Badr-class precision-guided artillery rockets
- Small turbojet engines manufactured by a European company
- Hundreds of commercial-off-the-shelf UAVs
- Maritime radar and automatic identification system units
- UAV detection and electronic countermeasure equipment[260]

Of broader concern, however, is that the CAR team also documented what it believes were parts of a commercially produced hydrogen fuel cell system that had been acquired from a company in China. This included "9-, 12-, and 20-litre carbon-fibre wrapped pressurised gas tanks mislabelled as 'oxygen cylinders', a 'tank-valve for hydrogen fuel cell systems,' a 'pressure transformer connector,' and written 'transfer documentation packed with the components,' 'which also clearly indicated the intended use in UAVs.'"[261] What

CAR did not find and document was the presence of fuel cell stack modules.[o]

As noted by one of the authors elsewhere, the discovery of these components is concerning because "UAS powered by hydrogen fuel cell technology are attractive because they are 'smaller, lighter, more versatile and more resilient than alternatives like batteries or small gasoline and diesel engines,' offering what is claimed to be 'three times the range of flight time of lithium battery powered drones.'"[262]

Over the past several years, there has also been reporting coming out of Somalia about the recovery of Chinese-made drones imported under suspicious circumstances. One of the first cases occurred in November 2021, when Somali security forces seized a shipment of six Mugin-2 drones imported from Turkey.[263] According to Mugin's website, the Mugin 2 has a three-hour flight endurance and can carry a 6kg payload.[264] As a point of reference, it is believed that other more capable Mugin variants—such as the Mugin-5, which has a longer flight endurance—have been operationally used during the Russo-Ukrainian War, including for long-range operations.[265] The Mugin-2 drones that were recovered in Somalia were reportedly imported by a former member of Somalia's parliament, and it was claimed that the drones would be used for "agricultural" purposes.[266] The Somali security services had concerns that the drones were imported for other purposes, however, to potentially include being used in some type of attack.[267]

In 2023, there was another case in Somalia that involved the import of Chinese drones under suspicious circumstances with an even closer, alleged nexus to terrorism. The case involved the arrest of a businessman whom Somali authorities believed was "importing military equipment from China on behalf of Al Shabaab."[268] As part of their investigation, Somali authorities seized five "high specification JS crop drones with the capacity to carry 10 liters of liquid" in addition to other military equipment.[269] The drones and other military equipment were reportedly "hidden in containers discussed as legitimate goods."[270]

More recent reporting from the United Nations in July 2024 provides additional data points that speak to the intent of al-Shabaab and Islamic State affiliates to acquire "sophisticated unmanned aerial systems for surveillance and attacks."[271] According to U.N. member state reporting:

> *Al-Shabaab's external operations cell in Jilib has intensified efforts to acquire unmanned aerial systems with greater payload capacity for attacks. Al-Shabaab seeks to procure advanced long-distance UAS with thermal capability to enhance nighttime surveillance and fix accurate target coordinates. External operations cells, supported by local logistical facilitators, procure unmanned aerial systems online and ship through international commercial couriers.*[272]

In mid-January 2025, reports and photos appeared online that claimed the Islamic State in Somalia had acquired "a significant number" of Evo Max 4T drones, produced by Autel, a company headquartered in Shenzen, China.[273] While the Evo Max 4T is not a long-range UAS platform, it has a 12.4-mile transmission range and a 42-minute flight endurance. It also comes stock with a thermal camera and reportedly includes some autonomous features.[274]

The second point of convergence between Russia's long-range drone activity in Ukraine and VEO use of drones is the proliferation, and extended chain of proliferation, of Iranian UAS and components. It has been well established that Iran provides drones, other materiel, and technical assistance to the Houthis and Hezbollah, and that Iranian assistance and technology has enabled the Houthis to extend the range of weaponized drones and to deploy long-range drones at greater scale. Over the past year, reports have emerged that the Houthis have engaged in deeper practical cooperation with al-Shabaab, al-Qa`ida in the Arabian Peninsula (AQAP), and local smuggling networks that also work with or have ties to these two terror groups.[275] Analysts believe this activity by the Houthis is being motivated by a desire to "build-out their presence in the Horn of Africa" and the Red Sea, to diversify and help secure supply chains so the Houthis can "further facilitate the movement of illicit and licit goods" in the region, and to increase their political leverage and reduce their dependence on Iran.[276]

While collaboration between these various entities might seem far-fetched, Michael Horton has explained how the "Houthis, AQAP, al-Shabaab, Iran, and smugglers have developed a relationship oriented around common objectives where all can benefit."[277]

> *Iran continues to provide the Houthis with needed components for their vital UAV and missile programs, in addition to some small arms. In exchange, Iran gets the leverage that comes with a well-armed and capable proxy that shares a long border with Saudi Arabia and occupies land near the strategic chokepoint of the Bab al-Mandeb. Iran and Hezbollah, both of which have advisers in Houthi-controlled Yemen, also benefit from being able to collect data from the Houthis' use of what are primarily Iranian-designed UAVs and missiles against multiple targets, including U.S. and allied warships. Al-Shabaab benefits from acquiring small arms, UAVs, and, potentially, war-fighting expertise from the Houthis. All these parties benefit financially. Al-Shabaab has long been involved in human trafficking, which generates tens of millions of dollars for the networks that facilitate the movement of men, women, and children from multiple Horn of Africa nations to Yemen. The Houthis and AQAP receive fees from Yemen-based smugglers who move the refugees from southern Yemen toward the Saudi and Omani borders.*[278]

In June 2024, the U.S. intelligence community assessed that the Houthis were in discussions with al-Shabaab to provide the latter group with weapons.[279] Since that time, there has been a mixture of reporting of different levels of reliability about practical cooperation—and the tit-for-tat support—between the Houthis, al-Shabaab, and AQAP. This has included statements about collaboration,[p] unverified reporting that the Houthis have sent engineers to Somalia to help al-Shabaab develop sophisticated weapons,[280] suggestions that AQAP has received drones from the

[o] As noted by CAR: "Such modules transform the hydrogen gas into electric power and are essential for the effective deployment of this technology. It is unclear why the stack modules were not included in the cargo." "Hydrogen-Powered Houthi Drones," Conflict Armament Research - Field Dispatch, March 2025.

[p] For example, in June a senior U.S. defense official interviewed by Voice of America stated the following: "They are working with the Houthis. It's a bit of a surprise … It's quite concerning." See Carla Babb, "Al-Shabab Reverses Somali Force Gains, Now Working with Houthis in Somalia," Voice of America, June 17, 2024.

Houthis, and U.N. member state reporting from October 2024 that claims there has been an increase in "smuggling activities involving small arms and light weapons ... between the Houthis and al-Shabaab, with indications of shared military supplies or a common supplier."[281] Yemen's National Resistance Forces (NRF) have also observed an increase in coordination between the Houthis and al-Shabaab and outlined how "al-Shabaab operatives ensure that shipments of drone and missile components are safely offloaded in Somalia or its waters and then loaded onto smaller boats that take the contraband to Yemen."[282] Al-Shabaab reportedly "receives money, small arms, and guidance from the Houthis" in exchange for this support.[283] The NRF also claims that it has "intelligence that indicates that the Houthis intend to supply al-Shabaab with more advanced weaponry that might enable them to target shipping in the Gulf of Aden."[284]

Conclusion

This article provided an overview of the early evolution of the terrorism drone threat—where the threat has been. Through the lens of the VEO Drone Capability-Impact Framework and the transformative case of Ukraine, it has also explored how advancements in commercial technologies and effective operational deployment of UAS at scale, at greater speeds, and enhanced ranges is likely to shape the future of drone related terrorism. In Part I, the authors utilized the idea of punctuated equilibrium to describe how the phenomenon of drone terrorism has remained mostly stable across time, and to show how those periods of stasis were punctuated by key innovations—bursts—that significantly altered and set a new level for VEO drone use. Given the nature of drone-related innovations that are emerging from the Russo-Ukrainian war, the authors also argued that the terror drone landscape is poised for another burst, and that the coming burst would include scale, speed, and range as key threat vectors.

In Part II, the authors introduced the VEO Drone Capability-Impact Framework to situate how component and system level changes continue to reduce barriers to entry to scale, speed, and range as more accessible capabilities, which in turn broadens opportunities for VEOs to leverage commercial systems and other add-on technologies to engage in surprise and enhance their impact. The Ukraine case demonstrates, in a profound way, how the boundaries of speed, range, and scale—and what is possible in each of these areas—continues to shift. It also highlights how the creative convergence, or blended use, of unmanned systems with other disruptive commercial technologies—primarily additive manufacturing and artificial intelligence—have been a driver of operational drone innovations and tactics. Thus, as the counterterrorism community looks forward and prepares for drone-related 'outputs' from the Ukraine war, it should be concerned not just about speed, range, and scale, but also about the creative convergence of these technologies—a fourth cross-cutting future threat vector.

Part III examined the terrorism implications of the Russia-Ukraine war's drone-related outputs in greater detail. It highlighted how scale will look different in a terrorism context: how it will likely be more limited and follow a progression oriented more around the deployment of drones in numbers, or multiple drones operated in a coordinated stack, with heavy dependence of human-machine teaming instead of autonomous swarms, at least over the near term. When it comes to speed, various VEOs have already acquired and deployed FPV drones, highlighting how the operational and weaponized use of fast-moving commercial UAS is a desired terror network capability *and* how adoption has already begun to proliferate across terror networks operating in different theaters—a trend that will likely intensify over the coming years.

The combined challenges posed by scale and speed introduce new risks and VEO attack pathways, and they raise serious questions about whether C-sUAS—and statutory frameworks that guide the ability of security personnel to identify and mitigate fast-moving terror drone threats, including those that involve some element of scale—are keeping pace with the threat. Various data points illustrate, not surprisingly, that key terror networks also have a desire to utilize UAS to attack from greater stand-off distances. Several terror networks have been 'eyeing' and appear to be actively working to acquire or develop commercial UAS, or related technology, that will enable them to elongate range and strike from further afield. Of particular concern in this regard is the discovery off the coast of Yemen of what is believed to be parts of a commercial hydrogen fuel cell tied to the Houthis. The case illustrates how ongoing advancements in UAS technologies and related systems that affect range are going to compound other C-sUAS challenges. The primary danger when these three elements (speed, range, and scale) are blended in a convergent way with other disruptive technologies is that the advantage favors the creative, which creates more space and opportunity for terrorists to engage in surprise or use UAS for impact. It is important that Western governments use this period—before another terror drone burst arrives—to adequately prepare for those malign use cases. The pace of drone innovations in Ukraine, and the expansion of terror plots that include interest in weaponized drones, such as the one tied to a returned jihadi foreign fighter who was arrested in France in March 2025,[285] suggests that there might not be much time. CTC

Citations

[1] "'The Future Character of War': Keynote Address by Deputy Secretary of Defense Kathleen H. Hicks," Royal United Services Institute, December 10, 2024.

[2] Greg Myre, "A Chinese drone for hobbyists plays a crucial role in the Russia-Ukraine war," NPR, March 28, 2023.

[3] "Dissecting Iranian drones employed by Russia in Ukraine," Conflict Armament Research, Ukraine Field Dispatch, November 2022.

[4] Wes Shinego, "Adversarial convergence raises alarm, warns Socom general at Reagan Defense Forum," DoD News, December 9, 2024.

[5] Ibid.

[6] Niles Eldredge and Stephen Jay Gould, "Punctuated Equilibria: An Alternative to Phyletic Gradualism" in Thomas J. M. Schopf, *Models in Paleobiology* (San Francisco: Freeman Cooper, 1972), pp. 82-115.

[7] Stephen Jay Gould, *The Structure of Evolutionary Theory*, illustrated edition (Cambridge, MA: Belknap Press, 2002).

[8] Don Rassler, *Remotely Piloted Innovation: Terrorism, Drones and Supportive Technology* (West Point: Combating Terrorism Center, 2016); Yannick Veilleux-Lepage and Emil Archambault, "A Comparative Study of Non-State Violent Drone Use in the Middle East," International Centre for Counter-Terrorism, December 9, 2022.

[9] Kerry Chávez and Ori Swed, "Off the Shelf: The Violent Nonstate Actor Drone Threat," *Air & Space Power Journal* (2020): pp. 29-43; Emil Archambault and Yannick Veilleux-Lepage, "The Islamic State Drone Program," in James Patton Rogers ed., *De Gruyter Handbook of Drone Warfare* (Berlin: De Gruyter, 2024), pp. 243-254; Rassler, *Remotely Piloted Innovation*.

[10] Don Rassler, "The Emergence of Long-Range Stand-Off Terrorism," *CTC Sentinel* 17:2 (2024).

[11] For an additional analytical perspective, see Daveed Gartenstein-Ross, Colin P. Clarke, and Matt Shear, "Terrorists and Technological Innovation," Lawfare, February 2, 2020.

[12] For background, see Don Rassler, "Back to the Future: The Islamic State, Drones, and Future Threats" in Georgia Harrigan ed., *On the Horizon: Security Challenges at the Nexus of State and Non-State Actors and Emerging/Disruptive Technologies* (Boston: Strategic Multilayer Assessment (SMA) Periodic Publication, 2019).

[13] Tamir Libel and Emily Boulter, "Unmanned Aerial Vehicles in the Israel Defense Forces: A Precursor to a Military Robotic Revolution?" *RUSI Journal* 160:2 (2015): pp. 68-75.

[14] David Rodman, "Unmanned Aerial Vehicles in the Service of the Israel Air Force: 'They Will Soar on Wings Like Eagles,'" *Middle East Review of International Affairs* (2010): pp. 77-84.

[15] Carl Anthony Wege, "Hizballah's Counterintelligence Apparatus," *International Journal of Intelligence and CounterIntelligence* 25:4 (2012): pp. 771-785.

[16] Rassler, *Remotely Piloted Innovation*.

[17] Roee Nahmias, "Nasrallah Describes 1997 Ambush," YNET News, September 8, 2010.

[18] "Homeland Security: The 9/11 Commission and the Course Ahead," U.S. Government Printing Office, September 14, 2004.

[19] Rassler, *Remotely Piloted Innovation*; Arthur Holland Michel, "Iran's Many Drones," Center for the Study of the Drone at Bard College, November 25, 2013.

[20] "Iran: Hezbollah Drone Proves Our Capabilities," Washington Examiner, October 14, 2012.

[21] "Hezbollah Flies Unmanned Plane over Israel," CNN, November 7, 2004.

[22] Rassler, Remotely Piloted Innovation.

[23] "Hezbollah Drone Airstrip in Lebanon Revealed," YNET News, April 25, 2015.

[24] Milton Hoenig, "Hezbollah and the Use of Drones as a Weapon of Terrorism," Federation of American Scientists, June 5, 2014.

[25] Arthur Holland Michel and Dan Gettinger, "A Brief History of Hamas and Hezbollah's Drones," Center for the Study of the Drone at Bard College, July 14, 2014.

[26] Yannick Veilleux-Lepage and Emil Archambault, "Étude Comparative de l'usage des drones par des groupes armés non étatiques au Moyen-Orient," International Centre for Counter-Terrorism - ICCT, 2023.

[27] "Arafat's New Terror Weapon: Exploding Toy Planes," Debka Files, January 14, 2003.

[28] Rassler, *Remotely Piloted Innovation*.

[29] Ibid.

[30] Janes Goodman, "Attack of the Drones: The Dangers of Remote-Controlled Aircraft," Jane's Intelligence Review, December 16, 2011; Rassler, *Remotely Piloted Innovation*.

[31] Rassler, *Remotely Piloted Innovation*.

[32] Jonathan Beck, "Drone Intercepted by Hamas Is Elbit Skylark 1," *Times of Israel*, August 12, 2015; "Israel Denies Palestinians Shot Drone down over Gaza," BBC, November 3, 2013.

[33] "Hamas Fajr-5 Missiles and UAV Targets Severely Damaged," Israel Defense Forces, November 17, 2012; Gili Kohen, "HAMAS Has More Drones Up Its Sleeve, Defense Officials Say," Haaretz, July 14, 2014.

[34] Rassler, *Remotely Piloted Innovation*.

[35] Avi Issacharoff, "PA Forces Thwart Hamas Attack Drone Plot in West Bank," *Times of Israel*, October 25, 2013.

[36] David Cenciotti, "Hamas Flying an Iranian-Made Armed Drone over Gaza," Aviationist, July 14, 2014; Rassler, *Remotely Piloted Innovation*.

[37] Cenciotti.

[38] Hana Levi Julian, "IDF Shoots Down Iranian-Made Hamas UAV Over Ashkelon," Jewish Press, July 17, 2014; Leo Giosuè, "Gaza Drone Enters Israel, Is Shot down over Ashdod by IAF," *Jerusalem Post*, July 14, 2014.

[39] Rassler, *Remotely Piloted Innovation*.

[40] Veilleux-Lepage and Archambault, "A Comparative Study of Non-State Violent Drone Use in the Middle East;" Rassler, *Remotely Piloted Innovation*.

[41] Simon Freeman, "Judge Pleads for Power to Jail Terror Fundraisers for Life," *Times*, March 17, 2006.

[42] Rassler, *Remotely Piloted Innovation*.

[43] Rassler; Veilleux-Lepage and Archambault, "A Comparative Study of Non-State Violent Drone Use in the Middle East."

[44] Ibid.

[45] Daveed Gartenstein-Ross, Matt Shear, and David Jones, "Virtual Plotters. Drones. Weaponized AI?: Violent Non-State Actors as Deadly Early Adopters," Valens Global & Organization for the Prevention of Violence, November 20, 2019.

[46] Emil Archambault and Yannick Veilleux-Lepage, "Drone Imagery in Islamic State Propaganda: Flying like a State," *International Affairs* 96:4 (2020): pp. 955-973.

[47] Caleb Weiss, "Islamic State Uses Drones to Coordinate Fighting in Baiji," FDD's Long War Journal, April 17, 2015; Bill Roggio and Caleb Weiss, "Islamic State Assaults Baiji Oil Refinery," FDD's Long War Journal, April 13, 2015.

[48] Archambault and Veilleux-Lepage, "Drone Imagery in Islamic State Propaganda."

[49] Veilleux-Lepage and Archambault, "A Comparative Study of Non-State Violent Drone Use in the Middle East."

[50] Archambault and Veilleux-Lepage, "The Islamic State Drone Program."

[51] Nick Waters, "Types of Islamic State Drone Bombs and Where to Find Them," Bellingcat, May 24, 2017.

[52] Ben Kesling, "Islamic State Drones Terrorize Iraqi Forces as Mosul Battle Rages," *Wall Street Journal*, February 26, 2017.

[53] "Islamic State's Multi-Role IEDs," Frontline Perspective, Conflict Armament Research, April 2017.

[54] Veilleux-Lepage and Archambault, "A Comparative Study of Non-State Violent Drone Use in the Middle East."

[55] Mansij Ashthana, "Watch: How A $500 Drone Annihilates A $500 Million Stadium In Syria," Eurasian Times, October 28, 2020; "Footage Shows Islamic State Drone Blowing up Stadium Ammo Dump," ABC News, October 25, 2017.

[56] Thomas Gibbons-Neff, "ISIS Drones Are Attacking U.S. Troops and Disrupting Airstrikes in Raqqa, Officials Say," *Washington Post*, June 14, 2017.

[57] Archambault and Veilleux-Lepage, "Drone Imagery in Islamic State Propaganda."

[58] Yannick Veilleux-Lepage, Chelsea Daymon, and Emil Archambault, *Learning from Foes: How Racially and Ethnically Motivated Violent Extremists Embrace and Mimic Islamic State's Use of Emerging Technologies* (London: Global Network on Extremism and Technology, 2022).

[59] Ibid.

[60] Veilleux-Lepage and Archambault, "A Comparative Study of Non-State Violent Drone Use in the Middle East."

[61] Don Rassler, Muhammad Al-'Ubaydi, and Vera Mironova, "The Islamic State's Drone Documents: Management, Acquisitions, and DIY Tradecraft," Combating Terrorism Center at West Point, January 31, 2017.

[62] Don Rassler, *The Islamic State and Drones: Supply, Scale, and Future Threats* (West Point, NY: Combating Terrorism Center, 2018).

[63] Veilleux-Lepage and Archambault, "A Comparative Study of Non-State Violent Drone Use in the Middle East."

[64] Håvard Haugstvedt, "A Flying Threat Coming to Sahel and East Africa? A Brief Review," *Journal of Strategic Security* 14:1 (2021): pp. 92-105; Ana Aguilera,

"Drone Use by Violent Extremist Organisations in Africa: The Case of Al-Shabaab," GNET, July 5, 2023.

65 Haugstvedt; Barbara Morais Figueiredo, "The Use of Uncrewed Aerial Systems by Non-State Armed Groups: Exploring Trends in Africa," UNIDIR, January 30, 2024; Francis Okpaleke, "Eyes in the Sky: The Innovation Dilemma of Drone Proliferation among Violent Non-State Actors in the Sahel," Global Network on Extremism and Technology, April 10, 2024.

66 Haugstvedt; Figueiredo.

67 Daniel Byman, Riley McCabe, Alexander Palmer, Catrina Doxsee, Mackenzie Holtz, and Delaney Duff, "Hamas's October 7 Attack: Visualizing the Data," Center for Strategic & International Studies, December 19, 2023.

68 Elisabeth Gosselin-Malo, "Hamas Drones Helped Catch Israel off Guard, Experts Say," C4ISRNet, October 18, 2023.

69 Dylan Malyasov, "Hamas Drone Strikes Israeli Merkava Tank," Defence Blog, October 20, 2023.

70 Emanuel Fabian, "Hamas Publishes Footage of Drone Attack on IDF Ambulance," *Times of Israel*, October 7, 2023.

71 Antebi Liran and Matan Yanko-Avikasis, "Life and Death in the Hands of the Drone: The Small, Cheap Devices Early in the Swords of Iron War," Institute for National Security Studies, accessed March 20, 2025.

72 Byman, McCabe, Palmer, Doxsee, Holtz, and Duff; Patrick Sullivan and John Amble, "What Happened to Iron Dome? A Lesson on the Limits of Technology at War," Modern War Institute, October 10, 2023.

73 Kerry Chávez, and Ori Swed, "How Hamas Innovated with Drones to Operate like an Army," Bulletin of the Atomic Scientists, November 1, 2023.

74 Dmytro Kaniewski, "Hamas: Learning about Drone Warfare from the War in Ukraine," Deutsche Welle, October 20, 2023.

75 Dov Lieber, "Hamas Officially Blames Mossad for Death of Tunisian Drone Maker," *Times of Israel*, November 16, 2017.

76 Broderick McDonald, "The Drones of Hayat Tahrir Al-Sham: The Development and Use of UAS in Syria," GNET, December 20, 2024.

77 Rueben Dass, "Hayat Tahrir Al-Sham's Drone Force," Lawfare, December 13, 2024.

78 McDonald.

79 Dass.

80 Ibid.

81 McDonald; Dass.

82 McDonald; Robert Tollast, "Militias in Syria Show Chilling Future of Guerrilla War with 3D Printed Drones and Night-Vision Units," National, December 4, 2024.

83 Don Rassler, "Going the Distance: The Emergence of Long-Range Stand-Off Terrorism," *CTC Sentinel* 17:2 (2024).

84 "Iran: Enabling Houthi Attacks Across the Middle East," Defense Intelligence Agency, February 2024.

85 Veilleux-Lepage, Daymon, and Archambault.

86 "U.S. Official: 'No Coincidence' Islamic State Victims in Guantanamo-like Jumpsuits," Reuters, February 5, 2015.

87 Yannick Veilleux-Lepage, *How Terror Evolves: The Emergence and Spread of Terrorist Techniques* (Lanham, MD: Rowman & Littlefield Publishers, 2020).

88 Ibid.

89 Bennett Clifford, "'Trucks, Knives, Bombs, Whatever:' Exploring Pro-Islamic State Instructional Material on Telegram," *CTC Sentinel* 11:5 (2018): pp. 23-29.

90 "Budanov: Hamas' Use of Drones Clear Sign of Russian Involvement," Kyiv Independent, October 12, 2023.

91 "Ukrainian Operatives Aided Syrian Rebels with Drones, Washington Post Reports," Reuters, December 11, 2024.

92 Ulrike Franke, "Drones in Ukraine and Beyond: Everything You Need to Know," European Council on Foreign Relations, August 11, 2023.

93 David Hambling, "Ukraine Drones Losses Are '10,000 Per Month' Ten Thousand Russian Jamming," *Forbes*, May 22, 2023.

94 Ibid.

95 Joanna Kakissis and Claire Harbage, "Ukraine Is Amping up Drone Production to Get an Edge in the War against Russia," NPR, October 15, 2024.

96 David Axe, "In The Hottest Sector of the Ukraine War, The Ukrainians Might Deploy as Many Drones as the Russian Deploy Soldiers: That's a Lot of Drones," *Forbes*, March 10, 2024.

97 Joe Saballa, "Zelensky Says Ukraine Can Now Produce Four Million Drones a Year," Defense Post, October 3, 2024.

98 Peter Dickinson, "Ukraine Is Expanding Its Long-Range Arsenal for Deep Strikes inside Russia," Atlantic Council, December 10, 2024.

99 Jonathan Beale and Thomas Spencer, "Ukraine's Long-Range Strikes Bring War Home to Russia," BBC, August 29, 2024.

100 Kateryna Bondar, "Inside Russia's Plan to Build Autonomous Drone Swarms," Breaking Defense, January 8, 2025.

101 Shahed Tracker, "Shahed type OWA-UAS stats Feb2025," X, March 1, 2025. See also David Hambling, "Russia's Rapidly Intensifying Shahed Offensive Threatens a Dark Winter," *Forbes*, November 4, 2024. For a perspective on the number of Ukrainian drones flown into Russia per month, see David Hambling, "30,000 Ukrainian Attack Drones To Hammer Russian Strategic Targets," *Forbes*, December 4, 2024.

102 Hanna Arhirova, "Ukraine Says Russian Attack Sets a New Record for the Number of Drones Used," Associated Press, November 26, 2024.

103 Verity Bowman, "Russian drones designed to maim not kill overwhelm Ukrainian medics," *Telegraph*, March 10, 2025.

104 Tracker.

105 Sebastian Shukla, Daria Tarasova-Markina, Victoria Butenko, Frederik Pleitgen, and Claudia Otto, "Exclusive: CNN Sees inside Elite Ukrainian Drone Mission Flying Deep into Russia," CNN, October 16, 2024.

106 Ibid.

107 Franke.

108 Hambling, "30,000 Ukrainian Attack Drones To Hammer Russian Strategic Targets."

109 Daniel Bellamy, "Russia's New War Tactic: Hiding Deadly Drones in Swarms of Decoys," Euro News, November 16, 2024. See also Hambling, "30,000 Ukrainian Attack Drones To Hammer Russian Strategic Targets."

110 Bellamy.

111 Chloé Hoorman, "Kamikaze Drones Attack Russian Rear Bases in Ukraine," *Monde*, December 14, 2024.

112 Mia Jankowicz, "One Type of Ukrainian Drone Is Responsible for 80% of Successful Strikes on Russian Oil Refineries: Report," Business Insider, May 15, 2024.

113 Shukla, Tarasova-Markina, Butenko, Pleitgen, and Otto.

114 Ibid.

115 Vikram Mittal, "Swarming Drones Will Be On The Russian-Ukrainian Battlefield In 2025," *Forbes*, January 2, 2025.

116 Stacie Pettyjohn, "Evolution Not Revolution," Center for a New American Security, February 8, 2024.

117 Mittal.

118 Stacie L. Pettyjohn, "Drones Are Transforming the Battlefield in Ukraine But in an Evolutionary Fashion," War on the Rocks, March 5, 2024.

119 Pettyjohn, "Evolution Not Revolution," p. 1.

120 Ibid., pp. 39-40.

121 "The Era of Killer Robots is Here," Daily Podcast, New York Times, July 9, 2024.

122 "Russia and Ukraine Launch Drone Swarms in New Offensive," Al Jazeera, November 10, 2024; Amos Chapple, "Swarm Wars: The Shaky Rise Of AI Drones In Ukraine," Radio Free Europe/Radio Liberty, August 14, 2024.

123 Max Hunder, "Ukraine Rushes to Create AI-Enabled War Drones," Reuters, July 18, 2024.

124 "Artificial Intelligence Raises Ukrainian Drone Kill Rates to 80%," Kyiv Post, October 14, 2024.

125 Beale and Spencer.

126 Paul Mozur and Adam Santariano, "A.I. Begins Ushering In an Age of Killer Robots," *New York Times*, July 12, 2024.

127 Bondar; Mittal.

128 Inder Singh Bisht, "Ukraine Spoofs Nearly 100 Shahed Drones to Head Back to Russia," Defense Post, December 5, 2024.

129 Emmanuel Grynszpan, "Guerre en Ukraine : la Russie multiplie les attaques de saturation de l'espace aérien ukrainien," *Monde*, November 26, 2024.

130 Bisht; Grynszpan. For background on Russian UAS takedowns, see Hambling, "30,000 Ukrainian Attack Drones To Hammer Russian Strategic Targets."

131 Abhishek Bhardwaj, "186 Mph Interceptor UAV: Ukraine's New Defense against Russian Shahed Drones," Yahoo News, December 31, 2024.

132 Joe Saballa, "US Tech Firms Test Hitchhiker Interceptor Drone on Ukraine Frontline," Defense Post, November 28, 2024.

133 David Hambling, "Ukraine Fields Unjammable Fiber Optic FPV Attack Drone," *Forbes*, November 7, 2024.

134 Dan Sabbagh, "'It Is Impossible to Outrun Them': How Drones Transformed War in Ukraine," *Guardian*, January 4, 2025.

135 Nick Jones, "Threat Trajectories: Cinema, FPV Drones, and Pandemic Anxiety" in Elisa Serafinelli ed., *Drones in Society: New Visual Aesthetics* (Switzerland: Springer Nature, 2024), pp. 25-38.

136 Erik Olsen, "Gentlemen, Start Your Drones," *New York Times*, November 11, 2015.

137 Martin Fornusek, "Ukrainian FPV Drone Hit Russian Mi-28 Helicopter in

'historic' Feat, Source Says," Kyiv Independent, August 7, 2024.

138 Artem K., "Lancet 3: Russia's Spear in the Sky," Grey Dynamics, November 1, 2024.

139 "Orlan-10 Uncrewed Aerial Vehicle (UAV)," Airforce Technology, March 24, 2023.

140 "325 km/h: While Ukraine Breaks New Speed Record For Armed FPV Drone, Let's Take a Look at the World's Fastest," Defense Express, September 15, 2024.

141 Mariano Zafra, Max Hunder, Anurag Rao, and Sudev Kiyada, "How Drone Combat in Ukraine Is Changing Warfare," Reuters, March 26, 2024.

142 Max Hunder, "Ukraine Collects Vast War Data Trove to Train AI Models," Reuters, December 20, 2024.

143 "Ukraine's AI Spots 12,000 Enemy Vehicles Weekly," Ministry of Defence of Ukraine, September 23, 2024.

144 David Hambling, "Russian Kamikaze Drone Now Seems To Identify Its Own Targets," *Forbes*, March 1, 2024.

145 "Russia's Lancet Drone May Have Autonomous Targeting Capabilities," SOFX, March 1, 2024.

146 David Hambling, "Russia's Smartest Weapon May Have An American Brain," *Forbes*, March 28, 2023.

147 Wes Haha and Courtney Crosby, "AI's Power to Transform Command and Control," National Defense Magazine, November 13 2020.

148 Tom Cooper, "Kropyva: Ukrainian Artillery Application," Medium, June 10, 2022.

149 "Tactical Unit Combat Control System 'Kropyva,'" Design Bureau LOGIKA LLC, March 31, 2021.

150 Audrey Macalpine, "Ukraine's Secret Weapon, 'Kropyva' Software," UNITED24 Media, November 29, 2024.

151 "'Kropyva' Operates Aptly," Defence Intelligence of Ukraine, February 20, 2017.

152 Tom Balmforth, "Ukraine Sees Use of Uncrewed Ground Vehicles, AI-Targeting Drones Surging next Year," Reuters, December 2, 2024.

153 Max Hunder, "Ukraine Rolls out Dozens of AI Systems to Help Its Drones Hit Targets," Reuters, October 31, 2024.

154 Serge Havrylets, "Ukraine's Defense Ministry Approves Innovative Drone with AI Elements for Mass Production," Euromaidan Press, April 9, 2023.

155 Elisabeth Hoffberger-Pippan and Anja Dahlmann, "Digital Battlefield: Concept, Technology and Prospects" in by Robin Geiß and Henning Lahmann eds., *Research Handbook on Warfare and Artificial Intelligence* (Cheltenham, U.K.: Edward Elgar Publishing, 2024), pp. 76-98.

156 "Saker Scout UAV," Automated Decision Research, accessed March 20, 2025.

157 Hoffberger-Pippan and Dahlmann.

158 Uzi Rubin, "Russia's Iranian-Made UAVs: A Technical Profile," Royal United Service Institute, January 13, 2023.

159 "Shahed-136 Series," Open Source Munitions Portal, accessed March 20, 2025.

160 Andrew E. Kramer, "At Least Two Drones Appeared to Target a City Heating Station in Central Kyiv," *New York Times*, October 17, 2022.

161 David Kirichenko, "The Rush for AI-Enabled Drones on Ukrainian Battlefields," Lawfare, December 5, 2024.

162 Dominika Kunertova, "The War in Ukraine Shows the Game-Changing Effects of Drones Depends on the Game," Bulletin of the Atomic Scientists, March 13, 2023.

163 Marc Santora, Lara Jakes, Andrew E. Kramer, Marc Hernandez, and Liubov Sholudko, "A Thousand Snipers in the Sky: The New War in Ukraine," *New York Times*, March 3, 2025.

164 Hattie Lindert, "This Ukrainian Software Engineer Uses Drones to Help Destroy Russian Tanks," *People*, April 13, 2022.

165 Hunder, "Ukraine Rushes to Create AI-Enabled War Drones."

166 Peter Layton, "Human-Machine Teaming's Shared Cognition Changes How War Is Made," Royal United Service Institute, March 19, 2025.

167 Shukla, Tarasova-Markina, Butenko, Pleitgen, and Otto.

168 Marcel Plichta, "Ukraine Strikes Back against Russia as World's First Drone War Escalates," Atlantic Council, August 15, 2023.

169 Martin Fornusek, "Ukraine Strikes 'only Oil Refinery Operating' in Russia's Rostov Oblast, Military Says," Kyiv Independent, December 19, 2024.

170 Anastasiia Malenko, "Ukraine Says It Attacked Oil Depot Serving Air Base for Russian Nuclear Bombers," Reuters, January 8, 2025; "Three Dead in Explosions at Russian Airbases," New Voice of Ukraine, December 5, 2022.

171 Will Vernon, "Analysis: Kremlin Drone Attack Is Highly Embarrassing for Moscow," BBC, May 3, 2023.

172 Jordyn Dahl, "Ukraine Drones Reportedly Hit Russian Airfield in Arctic," Politico, July 28, 2024.

173 Oliver Parken, "Ukraine's Scythe Drone Is All About Striking Far Away As Cheaply As Possible," Yahoo News, December 19, 2023.

174 Ibid.

175 Ibid.

176 "Dissecting Iranian Drones Employed by Russia in Ukraine."

177 Ibid.

178 Ibid.

179 Ibid.

180 Ibid.; Emil Archambault and Yannick Veilleux-Lepage, "Tower 22: Innovations in Drone Attacks by Non-State Actors," International Centre for Counter-Terrorism - ICCT, February 1, 2024.

181 "Iranian Man Indicted for Providing Material Support to Foreign Terrorist Organization Resulting in Death, and for Scheme To Procure Sensitive U.S. Technology Used in Military Drones," U.S. Department of Justice, December 19, 2024.

182 Ibid.

183 Anthony Deutsch and Tom Balmforth, "Exclusive: Russia Produces Kamikaze Drone with Chinese Engine," Reuters, September 13, 2024.

184 "Treasury Targets Actors Involved in Drone Production for Russia's War Against Ukraine," U.S. Department of the Treasury, October 17, 2024.

185 Ibid.

186 Ibid.

187 For background, see "How Can I Increase The Range Of My RC Quadcopter?" UAV Systems International, accessed March 11, 2025.

188 David Hambling, "Inside The Secret Weapon That Extends The Reach Of Russia's FPV Drones," *Forbes*, January 12, 2024; "Solutions to win: Ukrainian engineers develop new aerial repeater for drones," Rubryka, June 13, 2024.

189 Hambling, "Inside The Secret Weapon That Extends The Reach Of Russia's FPV Drones."

190 Ibid.

191 Ibid.

192 In his report, Hambling also discusses another Russian repeater drone, the Extender Hambling. Hambling, "Inside The Secret Weapon That Extends The Reach Of Russia's FPV Drones."

193 Ibid.

194 Ibid.

195 Ibid.

196 Roy, "A Ukrainian Radio Repeater FPV Carries an Elegant Array of Antennas . . .," X, January 21, 2025.

197 See Jen Judson, "US Army Wants Spy Drones to Launch from High-Altitude Motherships," Defense News, January 10, 2025.

198 David Hambling, "Russian Dolls: FPV Drone-Carrying Drones Are Now In Action In Ukraine," Reuters, January 12, 2024.

199 Ibid.

200 Ibid.

201 Ibid.

202 For background, see Kirsten Errick, "Defense Department's Replicator program must increase its speed," Federal News Network, October 19, 2023; Patrick Tucker, "Newest Replicator drones proven on battlefields of Ukraine," Defense One, November 13, 2024.

203 Telegram posts in possession of the authors.

204 "Safeguarding the Homeland from Unmanned Aerial Systems," U.S. House of Representatives, Committee on Homeland Security, December 10, 2024).

205 Ben Sullivan, "The Islamic State Conducted Hundreds of Drone Strikes in Less Than a Month," Vice, February 21, 2017.

206 David Larter, "SOCOM Commander: Armed ISIS Drones Were 2016's 'Most Daunting Problem,'" Defense News, May 16, 2017.

207 For example, see Pablo Chovil, "Air Superiority Under 2000 Feet: Lessons from Waging Drone Warfare Against ISIL," War on the Rocks, May 11, 2018.

208 For background, see Rassler, *The Islamic State and Drones*.

209 Rassler, *The Islamic State and Drones*, p. IV.

210 "Treasury Sanctions ISIS Facilitators Across the Globe," U.S. Department of the Treasury, February 9, 2018.

211 Ibid.

212 Ibid.

213 "Procurement Networks Behind Islamic State Improvised Weapon Programmes," Conflict Armament Research, December 2020, p. 32.

214 Ibid.

215 Ibid.

216 David Hambling, "Kamikaze Drone Videos From Sudan Conflict Signal Rapid Proliferation (Updated)," *Forbes*, September 15, 2023.

217 For background, see "Amid Military Offensive In Syria, Jihadis Highlight Ability To Modify Commercial Drones For Military Use," MEMRI, December 10,

2024; Tollast; Dass; and McDonald. For background on Ansar al Tawhid's use of weaponized FPV drones, see "Jihad and Terrorism Threat Monitor (JTTM) Weekly: August 30-September 7, 2024," MEMRI, September 6, 2024.

[218] David Ignatius, "Ukraine Helped Syrian Rebels Deliver Blow to Russia," *Washington Post*, December 10, 2024.

[219] Dass.

[220] "Hydrogen-Powered Houthi Drones," Conflict Armament Research - Field Dispatch, March 2025.

[221] Telegram messages seen and in the author's possession. See also "User Of Pro-Islamic State (ISIS) Encrypted Chat Asks For Booklet About Drones; Another Offers Step-By-Step Manual To Build FPV Drone," MEMRI, December 19, 2024.

[222] Figueiredo; Aliyu Dahiru, "How Drones Are Changing The Face Of Terrorism In Africa," HumAngle, February 26, 2024; Aguilera; Timothy Obiezu, "Regional Security Analysts Say Africa at Risk of Drone Terrorism," Voice of America, November 22, 2023.

[223] Mary Wambui, "Three Kenyans Accused of Procuring a Drone to Be Used by Al Shabaab Charged," NTV Kenya, January 25, 2024.

[224] "Several IS Fighters Killed in Somalia's Puntland State," Defense Post, January 14, 2025.

[225] "At least one soldier killed in ISIS drone attack in northeastern Somalia's Puntland state," Somali Guardian, January 23, 2025.

[226] For example, see Daludug Security, "Puntland Intercept ISIS Drones This is a significant development . . .," X, January 9, 2025. For additional background, see "Report of the Security Council Committee Pursuant to Resolutions 1267 (1999), 1989 (2011), and 2253 (2015) Concerning Islamic State in Iraq and the Levant (Da'esh), Al-Qaida and Associated Individuals, Groups, Undertakings, and Entities," United Nations Security Council, February 6, 2025.

[227] Ihotu Okpe, "ISWAP Deploys Armed Drones to Attack Nigeria's Military Base," AIT LIVE, December 26, 2024; Solomon Odeniyi, "Terrorists' Drones Are Toys, Not Effective – DHQ," Punch Newspapers, December 27, 2024.

[228] Robert Bociaga, "Drone Games in the Sahel: Extremist Actors Embrace Aerial Technology," Africa Report, May 14, 2024.

[229] "Aviation Safety: Federal Efforts to Address Unauthorized Drone Flights Near Airports," U.S. Government Accountability Office, March 18, 2024.

[230] Ibid.

[231] For background, see "S.2836 - Preventing Emerging Threats Act of 2018," U.S. Congress, Senate, S. 2836, 115th Congress, introduced May 15, 2018.

[232] "Unmanned Aircraft Systems Detection and Mitigation Systems Aviation Rulemaking Committee Report," U.S. Federal Aviation Administration, February 5, 2024.

[233] "Aviation Safety."

[234] "Counterterrorism, Innovation, and Threats: Military and Security Testimony Before the House Committee on Homeland Security," U.S. House of Representatives, Committee on Homeland Security, 118th Congress, 2nd session, December 10, 2024.

[235] Ibid.

[236] Ibid.

[237] "Unmanned Aircraft Systems Detection and Mitigation Systems Report," U.S. Federal Aviation Administration, 2024.

[238] "Counterterrorism, Innovation, and Threats."

[239] Matt Bracken, "Federal law enforcement officials make the case for expanded drone authorities," FedScoop, December 11, 2024; "Counterterrorism, Innovation, and Threats." See also "Countering Unmanned Aircraft Systems: Securing the Homeland Against Evolving Threats," MITRE Corporation, December 2024.

[240] "Fact Sheet: The Domestic Counter-Unmanned Aircraft Systems National Action Plan," The White House, April 25, 2022.

[241] For background, see "H.R. 8610: Safeguarding the Homeland from the Threats Posed by Unmanned Aircraft Systems Act of 2024," U.S. Congress, House, HR 8610, 118th Congress, introduced July 11, 2024.

[242] For definitions of "covered site" and "covered entity," see Ibid.

[243] Ibid.

[244] Ibid.

[245] Ibid.

[246] "H.R.4333 - Safeguarding the Homeland from the Threats Posed by Unmanned Aircraft Systems Act of 2023," U.S. Congress, House, Counter-UAS Authority Security, Safety, and Reauthorization Act, HR 4333, 118th Congress, introduced June 23, 2023.

[247] "Office for State and Local Law Enforcement," U.S. Department of Homeland Security, accessed March 20, 2025.

[248] Rassler, "Going the Distance," p. 4.

[249] Ibid., p. 4.

[250] Ibid., p. 3.

[251] Dass.

[252] Harun al-Aswad, "What Are Shaheen Drones, the New Rebel Weapon in Syria's Skies?" Middle East Eye, December 3, 2024.

[253] Rassler, "Going the Distance," p. 4.

[254] Ibid., p. 5.

[255] Ibid., p. 5.

[256] "Treasury Targets Actors Involved in Drone Production for Russia's War Against Ukraine."

[257] Ibid.

[258] Ibid.

[259] Ibid.

[260] "Hydrogen-Powered Houthi Drones."

[261] Ibid.

[262] Rassler, "Going the Distance," p. 5.

[263] Harun Maruf, "Somali Security Forces Have Seized a Shipment of Drones at Mogadishu Airport Last Week . . .," X, November 3, 2021.

[264] "Mugin-2 Pro 2930MM H-Tail Full Carbon Fiber VTOL UAV Platform - 2023 Edition," Mugin UAV, accessed March 11, 2025.

[265] Rebecca Wright, Ivan Watson, Olha Konovalova, and Tom Booth, "Chinese-Made Drone, Retrofitted and Weaponized, Downed in Eastern Ukraine," CNN, March 16, 2023; Dan Sabbagh, "Ukraine Strikes Psychological Blows in Drone Warfare over Crimea," *Guardian*, August 22, 2022; H.I. Sutton, "H I Sutton - Covert Shores," Covert Shores, November 21, 2024.

[266] "Somalia: Farmaajo's Ally Linked to Importation of Drones from Turkey," Garowe Online, June 30, 2020.

[267] Ibid.

[268] "Police Probe Kenyan Trader 'for Importing Weapons for Al Shabaab Terrorists,'" East African, June 27, 2023.

[269] Ibid.

[270] Ibid.

[271] "Thirty-Fourth Report of the Analytical Support and Sanctions Monitoring Team Submitted Pursuant to Resolution 2734 (2024) Concerning ISIL (Da'esh), Al-Qaida," United Nations Security Council, July 22, 2024.

[272] Ibid.

[273] Kaab TV, "How Did #ISIS Militants Acquire Drones from China? . . .," X, January 14, 2025.

[274] "Autel Robotics EVO Max 4T Xe Rugged Bundle," Autelpilot, accessed March 20, 2025.

[275] For a recent reflection, see "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, Groups, Undertakings and Entities," United Nations Security Council, February 6, 2025.

[276] Michael Horton, "Looking West: The Houthis' Expanding Footprint in the Horn of Africa," *CTC Sentinel* 17:11 (2024): p. 16.

[277] Ibid., p. 18.

[278] Ibid., p. 18.

[279] Katie Bo Lillis, Kylie Atwood, and Natasha Bertrand, "US Intelligence Assesses Houthis in Yemen in Talks to Provide Weapons to Al-Shabaab in Somalia, Officials Say," CNN, June 11, 2024.

[280] Carla Babb, "Al-Shabab Reverses Somali Force Gains, Now Working with Houthis in Somalia," Voice of America, June 17, 2024.

[281] "Final report of the Panel of Experts on Yemen established pursuant to Security Council resolution," United Nations Security Council, September 15, 2024.

[282] Horton, p. 19.

[283] Ibid.

[284] Ibid.

[285] Julien Constant, "Suspecté de fomenter un attentat par drone, un jeune homme arrêté en Seine-et-Marne," *Parisien*, March 21, 2025.

A View from the CT Foxhole: Dr. Christian Klos, Director General of Public Security, Germany's Federal Ministry of Interior and Community

By Julika Enslin

Director General Dr. Christian Klos took over the leadership of the Department Public Security in the Federal Ministry of the Interior and Community (BMI) at the beginning of 2020. He is in charge of legal and general policy issues at national, E.U., and international level regarding security, including counter-terrorism, extremism and organized crime. In addition, he supervises the Federal Criminal Police Office (BKA) and the Federal Office for the Protection of the Constitution (BfV; the domestic intelligence agency).

Dr. Klos has been working at the BMI since 1998, initially in the Project Group for European Harmonization. From 2000 to 2004, he was a national expert in the Directorate-General for Justice and Home Affairs of the European Commission. After returning to the BMI, he was initially responsible for international counterterrorism before working for six years in the ministry's management staff, including as head of the minister's office under Minister Dr. Wolfgang Schäuble. From 2011, he headed the division on immigration law and was also appointed Commissioner for Return during the refugee and migration crisis in 2015. In 2017, he set up the Directorate on Return Policy, which he headed as Deputy Director General.

CTC: You are the Director General of Public Security at the German Ministry for Interior.[1] How does your Department and the Ministry of Interior fit into Germany's counterterrorism approach? And can you describe for our readers what different entities and agencies in Germany are tasked with counterterrorism and where you fit in with your role in the Ministry of Interior?

Klos: The Directorate General for Public Security consists of two parts: The first part focuses mainly on principal issues of public security and in particular, legislation at a national, European and international level, so this is more the legal part. And the second is the more operational part, and here we deal with different phenomena such as serious and organized crime, counterterrorism, the fight against extremism, be it right-wing or left-wing extremism. We also focus on counter espionage, counterintelligence and last but not least, we protect the confidentiality of classified documents and IT.

I have also the supervision of the Federal Criminal Police Office (*Bundeskriminalamt* or BKA)[2] where they have, for example, departments which deal with state protection and counterterrorism. So the Federal Criminal Police Office is the key police force in Germany for countering terrorism. We have a federal structure here in in Germany and usually police work is with the federal states. But for counterterrorism, the Federal Criminal Police Office, the BKA plays not only a coordinative role but in terms of counterterrorism, the leading role, and is also the interface of the federal states with the international level. So, the BKA deals at a European level, corporation with other European Member States of the European Union, of course Europol, and other international partners, most prominently of course the U.S. partners, namely the FBI and other agencies involved in the fight against terrorism.

In addition, I have the supervision of the domestic intelligence service, the *Bundesamt für Verfassungsschutz* (or BfV), the Federal Office for the Protection of the Constitution.[3] This is an intelligence agency, and it is also very much involved in the fight against terrorism but from the intelligence angle.

And I should also mention that there is one special task of the Ministry, which is quite unusual for a ministry. It is a real operational part, and this is the existence of an instrument to ban organizations. When the strict legal conditions are met, we can ban organizations which either perform extremist or terrorist activities, violating criminal law or are directed against international order. Of course, terrorist organizations would be the target or objective of this legal precondition. Recently, for example, we banned Hamas here,[4] which is of course an already listed terrorist organization for more than 20 years. However, this instrument allows us to better restrict activities of these organizations in Germany. The key objective of banning organizations is to absolutely destroy the organizational structure and to seize all assets of such organizations. Of course, Hamas had no organization here, but the use of symbols, for example, can now be easily addressed by law enforcement after an organization is banned.

That was the advantage of the ban of Hamas, which came after the atrocities by Hamas on the 7th of October 2023, and therefore, this was very important. But there are also other organizations in the Islamist context, for example, Hezbollah[5] or the Islamic Center in Hamburg,[6] which is a key actor in the dissemination of Iranian religious ideology and promoting the caliphate. Therefore, this was also an organization which we recently banned and also seized all assets linked to them. Any further activity which would then be linked to such an organization is then also punishable under criminal law as a consequence.

CTC: With regard to the jihadi threat in Germany, a report published in February 2025 by the U.N. sanctions monitoring team on the global jihadi threat[7] stated that in Europe, regional states assessed Islamic State Khorasan (ISK or ISIS-K) to be the most significant external threat to Europe. What is the ISK threat specifically to Germany right now?

Klos: We had a car-ramming attack perpetrated by an Islamist in Munich on February 13, during the Munich Security Conference which caused two casualties and injured dozens of people.[8] Investigations are still running. So, Islamist terrorism is something we unfortunately still see. We are continuing to see Islamist radicalization in Germany, mostly self-radicalized via online fora so

Christian Klos

that there is not the so-to-speak post 9/11 network structures, which have been dismantled in many cases. We are increasingly seeing in Germany—and in Europe, as a whole—individual actors being radicalized and using means such as cars, knives, etc. These are easily available ways of killing people or injuring people. And this is of course then currently the main "felt threat" and the real threat actually. It is primarily an internal rather than external threat.

When it comes to the external threat, I would agree with the assessment that ISIS-K is in Germany as well. What we observe from the intelligence side is that there are clear indications that the group intends to conduct attacks in Europe, and this can also include Germany and therefore we are very much aware of this threat, and we have seen also travel activities. So, it's not just some minor indications. We really see things happen but we don't know where it would be, so, we try our utmost to prevent this.

CTC: When it comes to the threat of the violent far-right, there have been neo-Nazi groups that have been banned by the German government in the past such as Artgemeinschaft[9] and Hammerskins.[10] But the attacker in Hanau five years ago, for example, was found in investigations to have acted largely alone.[11] How would you classify on the extreme right-wing spectrum the threat from organized groups, versus unaffiliated lone actors? And are you more concerned about one or the other?

Klos: I think I would not try to rank the threats because both are a significant threat. We have right-wing extremists, we have right wing radicals, and this is, I would say, a blurred scene. There are a lot of groups of course. And if you ban organizations, it doesn't mean that people cease to exist. They're still there and they still have the ideology. Therefore, right-wing extremism is really a subject of concern. Just to give you a few numbers, we have around 40,000 people in Germany who we regard as being right-wing extremists. In comparison, the Islamist threat is a bit lower, a little bit less than 40,000 are categorized as extremists. And on the left-wing, we have around 30,000 people categorized as extremists.

When it comes to right-wing extremism, we have singled out serious organizations where we find it necessary to ban them because they are very active with their unlawful undertakings. Possibly they have also a perspective of becoming bigger. Of course, sometimes there are also organizations consisting of very old men and they're just dying out and you don't have to ban them, it's not worth the effort.

That is always the challenge with banning organizations, because you must succeed. It's a very strict procedure. We have to have a very clear order banning them in taking direct legal remedies to the Federal Administrative Court (*Bundesverwaltungsgericht*).[12] You really have to make your case, because if you ban an organization but then lose the case and the ban is lifted by the Federal Administrative Court, then the result is counterproductive and you risk being accused of acting against, for example, the right-wing opposition. So, you have to be really sure if you are going to take such steps against organizations.

When it comes to right-wing extremism, it is true to say that we had a lot of lonesome actors. We convened here in Berlin a bilateral initiative of the U.S. Department of Justice and my Ministry to have a counterterrorism law enforcement forum. Among the challenges this forum looked into was right-wing extremism. When you look at attacks such as the Christchurch, New Zealand, attack, you have a lot of lone-wolf actors around. But these actors also are connected to certain milieu, including, for example a martial arts scene influenced by right-wing extremism.[13] There is also a music scene, very active, where you can find this right-wing extremist music and concerts.[14] And of course, there is online material. There are also international links when it comes to, for example, Hammerskins. So, there are interlinked persons, but those who we have seen take action are not necessarily members of these groups.

One exception, of course, is the so-called National Socialist Underground, the NSU. This was a terrorist group, a right-wing terrorist group in Germany who have targeted in particular people with a migration background. This was already a few years ago, but is still very notable. Therefore, there is no easy way to characterize the threat—there are all kind of layers.

You also have a new-right movement in terms of ideology, and this is of course particularly serious because this lays the foundation for any kind of act which follows. If you have the ideology, then possibly people will follow not only just the buzzwords, but also ideologically and this is also what we see is very dangerous. We look into it. There is a particular magazine, the so-called *Compact* magazine in Germany, which is the voice of this new-right in Germany. We are still in the process of banning this magazine. The Federal Administrative Court has issued a temporary decision (*einstweiliger Rechtsschutz*), which resulted in us giving back the assets to this magazine.[15] But we hope that we will win the court case[16] in the end.

I can assure you that freedom of expression, freedom of press are of equal standard as in the United States, but we are by law eligible to ban also press and media entities, if there is an extremist or terrorist background. We have done it in the past with [the Hezbollah mouthpiece] Al Manar TV[17] and others in the Near and Middle East and also here in Germany. These are propaganda channels which we would like to get rid of.

CTC: Shifting to left-wing extremism, last year *CTC Sentinel* published an article about the rise in violent left-wing extremism in Germany and the "Engel-Guntermann Network."[18] And of course, looking back historically, sometimes when we think of Germany the Red Army Faction (RAF) might be one of the first things that comes to mind in terms of terrorism. But what from your perspective is the current threat posed by left-wing extremist groups? And is it rising, or is it changing a lot in tactics and goals from what you are seeing?

Klos: The left-wing extremist threat has changed over time, particularly in recent years. I quoted the number around 30,000 people that we count as left-wing extremists, of which most would say 10 percent are also willing to use violence. The violence has changed. It was in the past not violence but rather sabotage. There were then attacks against any kind of infrastructure, but not against persons. This has significantly changed. In particular, the network you've mentioned directed their action, their attacks against other individuals, mostly right-wing extremists. But that can also be representatives of big companies. But mostly right-wing extremists, that's their declared enemy. And they target them. And so, this is really a shift of, if I can say, towards more violent activity in which people are being beat up.

They also enter right wing events looking for confrontation. For example, there was a "day of honor" in Hungary,[19] which was a magnet for right-wing extremists, and German left-wing extremists went there and then beat up a number of right-wing extremists in Hungary. So, there's also international activity with the left-wing. And there is a second dimension which is really significant because it has caused the greatest financial damage perpetrated by extremists or terrorists let's put it that way in in the recent past, which is the attack on the energy supply of the Tesla motor factory in Brandenburg.[20] They shut down the whole factory for a number of days, which caused a three-digit million-euro damage for the Tesla company. And of course, this is very bad for the German economy and the signal it sends. But this is not the only incident we had. There have also been attacks against other critical infrastructure, but mostly not very successful, not to this dimension which we have seen with this attack against Tesla. But sometimes it's directed against—which is odd—even public transport, which is hard to understand because usually they're also environmentalists in the left-wing scene and there is no real logic in interfering with some public services like public transportation. This is really illogical, but ok, extremists are never really logical. So, what can I say? And of course, we need to be vigilant about any threats to military installations of our NATO partners. What we really see is that the focus is on critical infrastructure, and this is an upcoming trend.

CTC: Vehicle rammings have been a feature of recent attacks. One of the most devastating attacks in Germany was the Breitscheidplatz attack in 2016 when the attacker drove a truck into a Christmas market in Berlin killing 12 and injuring more than 50.[21] And you mentioned the attack on February 13 in Munich where a man drove into a group of protesters. Then in mid-January, U.S. authorities revealed that the January 1, 2025, New Orleans attacker had researched the car ramming in Magdeburg before his attack.[22] What is your office's approach to countering the threat posed by car rammings, and how can Germany mitigate this threat? Is it in any way more difficult to detect or prevent than others?

Klos: We recently held a special meeting of the Committee on Internal Affairs of the German Parliament (*Bundestag*) on the Munich attack. And not only the Minister of Interior of Bavaria, but also my Minister, the Federal Minister of Interior and others declared there is no 100-percent security possible for people, especially when it comes to soft targets.

Having said this, in the aftermath of the mass-casualty Breitscheidplatz ramming, there have been a lot of changes at such events to protect against such attacks. Car ramming is always an issue. Usually there is a security concept to be presented by the organizer of such an event, to include all kinds of barriers, including mobile barriers. I think in New Orleans this was also a bit of a problem, that there were some barriers missing[23] and this actually was the same in Magdeburg. There was a security concept, there were all these physical barriers, but there was one bit not really fully covered according to the security concept, it was too wide, there was a space in which a car could fit through and that's how the Magdeburg ramming happened.

There is the need for such security concepts, and I think this also has preventive effect. This is not performed at the national level but rather at the municipal level. It should also be stressed we can't change the whole character of Christmas markets where people are coming together to have a good time which is exactly what the terrorists want to destroy.

And if you look at the recent Munich vehicle ramming attack, it targeted a demonstration from the unions to demonstrate for better wages and had nothing to do with the Munich Security Conference. It was just a peaceful demonstration for better wages, and it was protected by police in the front and in the back and with a police car. But this was of course a protection against traffic to allow demonstrations to move forward and to reach their destination. But the car rammer just bypassed the police car and then hit a number of people there. Which means, soft targets are extremely difficult to protect. You can do it for particular events which are located in a certain place where you can have physical protection. But we have to be honest, we cannot protect all our public spaces. It's impossible, especially with spontaneous gatherings. We have to look into this, but no 100-percent security is possible.

CTC: Shifting topics, the German Council on Preventing Extremism, the BAG RelEx (German term: *Bundesarbeitsgemeinschaft religiös begründeter Extremismus*) in one of its recent policy briefs observed a rise in anti-Semitism and anti-Muslim racism after the October 7, 2023, Hamas attack and Israel's military response in Gaza.[24] What is your assessment of the impact of October 7 on the German terrorism landscape?

Klos: It definitely had a major impact here on the security situation. On the day of the attack, we increased the security preparations and measures with regard to Israeli or Jewish facilities here, be it diplomatic representations or synagogues, or municipal or Jewish schools, kindergartens. So, we had really to react. And because we have a higher share of Muslim population—of which, of course, 99.7 percent are absolutely peaceful—but I must admit that of course here, there was also sympathy for the terrorist attack of Hamas. For example, sweets were given out here in Berlin by an organization called Samidoun, which also have affiliates in Canada and the Netherlands, and we banned this organization. They are sympathizers of Hamas and their acts.[25]

And I would actually not name anti-Semitism and antimuslim racism in Germany in one sentence because the scale of anti-Semitism is so much higher. If I look at all extremism, again and again you see the common link is anti-Semitism. So, we do have an increase of anti-Semitism in Germany, but the highest increase of anti-Semitism here comes from pro-Palestinian individuals which are mostly seen in urban areas which have a higher share of Muslim population. Again, this is a minority, but very visible. You see this at universities as well. I spoke with representatives of Jewish student organizations, and they feel threatened. They cannot study or they feel endangered to openly show their belief, which is something I cannot accept. In Germany, everybody has the right to express their belief, and it must be possible to wear a kippah or to have a David Star wherever. If you have on social media on your history, a religious symbol, then you see, a sh*tstorm of hate and actually also criminal offences against these students. So, this is really something which is concerning me. We have a whole range of criminal acts against people of Jewish belief, or Israeli people here in Germany.

We do not see the reverse reaction from the Jewish community because of what happened in Israel that they would attack pro Palestinians here. This we do not see at all. What we do see sometimes is demonstrators who intentionally show up with, for example, the Israel flag, at pro-Palestinian demonstrations. So, this is really a challenge for police to get them separated.

When it comes to anti-Muslim xenophobia, yes, I would say there is an increase, but we have a much more security relevant increase of anti-Semitism in Germany. And this is a key focus of our efforts here these days.

CTC: Last year, there were multiple media reports about intercepted Russian attack plots against German defense industry executives, including the CEO of Rheinmetall.[26] There were also media reports about German police suspecting Iran to have hired a Hells Angel biker to help attack Germany synagogues in 2021.[27] What is your assessment of the counterterrorism challenge posed by states such as Iran and Russia in Germany?

Klos: Of course, when it comes to Russia, and in particular the war of Russia against Ukraine, violating international law, then I cannot be that explicit as I've just been with the other forms of extremism. We do see, of course, efforts of Russia trying, to get information, on the German support of Ukraine in particular of course, military support, and training of Ukrainian soldiers here in Germany. But also information about German industry, defense industry in particular. We have seen individuals doing this. There are also some Germans of Russian origin, who offered their services to Russia to possibly sabotage some things here in Germany. We work to try to dismantle this.

What we do see is, but we cannot actually interpret it for the time being, drone flights. This is something I think you see also in the U.S.—drone flights over military installations or critical infrastructure which might be a surveillance mission. Not all of these are Russian drones, but among them are drones which are not the usually DJI drones of hobby drone pilots but rather a speed and shape and size that would be of a state actor. So, this is something that we see.

We clearly see, and sometimes we attribute also not only to Russia, but also, for example, to China, cyber-attacks on all kinds of be it industry and public infrastructure. This is also very serious. It is always a question of what the objective was. In terms of Russia, it is a clear objective to support the fight against Ukraine. In addition, and we are very concerned about this, of course, possible preparation of military action against NATO. This is extremely serious, but this concerns then Russia. For others, let's say China, it is more industrial espionage. They would like to just get intellectual property from such activity or test our countermeasures.

And then of course, there is also the challenge posed by transnational repression. So other actors like Iran and Turkey but also China and Russia. They target their opposition, in other countries like here in Germany. And here there is also activity and if we learn about it, of course we intervene immediately.

CTC: Incidents such as the Islamic State-inspired deadly knife attack in Solingen by a Syrian asylum seeker last year have prompted larger debates about migration and asylum in Germany.[28] As you are very knowledgeable on this topic, having written a Ph.D. about European migration policy and worked in the German government on migration in very high-level positions, what would you add to that debate in terms of whether migration and asylum in any way intersect with any of your current tasks in looking at counterterrorism in Germany?

Klos: There is an interlinkage, of course. Because you can see that terrorist organizations for example like to hide individuals in certain procedures like asylum procedures, so we could possibly be infiltrated not only by terrorists but also by state actors. So, there is a link, and we have of course then to crosscheck our legal migration channels with the intelligence we have. We have also information exchanges with our international partners on this, which can help in preventing the entry of these people. And I think this is a key task of the European law enforcement and intelligence community to keep or get all these people out. We have our information system in place. We have the Schengen Information System (SIS) and a visa information system, all European systems, which are linked with lists where we can actually exclude people from entry or visa issuance.

So, our security community needs to prevent such people from coming. Of course, smuggling networks play a role. So, the fight against illegal migration and the work on security is very closely linked.

CTC: Coming to that European level, terrorist threats can, of course, extend beyond German borders because attackers or perpetrators might move between European countries or access weapons before in other countries. From your office specifically, what does counterterrorism cooperation look like with other European countries?

Klos: We have a very strong operative cooperation, but also political cooperation across all kinds of counterterrorism issues. It's longstanding. Of course, there was a huge momentum of European cooperation after 9/11, apart from the international dimension and cooperation, in particular with the U.S. But there are major steps forward in terms of cooperation, with Europol at the heart of this. Counterterrorism is actually a key European task. It is just very natural to get in touch with our European colleagues on all kind of things. We also built joint investigation teams, if there are transnational phenomena. International terrorism is international, the networks work across Europe, not only in one country, and therefore you must work together.

CTC: One other partner is, of course, the United States. The U.S. and Germany have worked together in counterterrorism for a long time. Are there any lessons that you've learned from U.S. partners in counterterrorism that have influenced the German approach? Or have you also in your time come across issues where you thought this is maybe something where Germany and the U.S. have to take a different approach in counterterrorism just because of differences in the countries?

Klos: I would definitely underline the things we have in common because I think this outweighs much more the differences. And I hope that this also will continue because I think we rely on each other. As I already mentioned, there's an extremely good cooperation between the FBI and the Federal Criminal Police Office at the operational level—this has been longstanding. I have visited the FBI and the Joint Terrorism Task Force in New York, for example.

There is a permanent operational exchange between both countries and high mutual respect of the work of each other and the counterterrorism units in place. And I think this is extremely positive and really vital for our countries to have such a very close cooperation. This also applies for the cooperation between the two countries' intelligence services. The CIA in cooperation with the German External Intelligence service (*Bundesnachrichtendienst*, BND) or as I already mentioned the Federal Office for the Protection of the Constitution, the internal intelligence service is also very important. And here, I must admit that we are very thankful to our American partners to receive important information, which is sometimes or actually often, much more accessible for American colleagues than for us because of legal reasons and very different perceptions of privacy. Data protection plays a very big role—I would even say from my perspective, an exaggerated role in Europe. Of course, I wouldn't go so far as fully endorsing the American approach but something in between for Europe and Germany would be much better. Therefore, we sometimes rely on information gathered in the online world by our American partners. It's extremely worthwhile. We have prevented a high number of terrorist attacks in Germany due to such information—not only from the U.S. but a large part of this information has come from the U.S. agencies—and this is very important for us.

As part of our cooperation with the United States, we are committed to doing everything to prevent any kind of terrorist threat directed against U.S. interests, be it in the U.S. or be it here in Germany, we have a lot of U.S. military installations. We are vigilant about this. I would regard the cooperation extremely good and valuable for both sides. CTC

Citations

[1] "Structure and organisation," Federal Ministry of the Interior and Community, n.d.

[2] Editor's Note: "The BKA," Bundeskriminalamt, n.d.

[3] Editor's Note: "The German domestic intelligence services," Bundesamt für Verfassungsschutz, n.d.

[4] Editor's Note: "Germany bans Hamas activities, dissolves Samidoun group," Deutche-Welle, November 2, 2023.

[5] Editor's Note: Laurenz Gehrke, "Germany announces total ban on Hezbollah," Politico, April 30, 2020.

[6] Editor's Note: "Germany bans Muslim association for pursuing radical Islam," Reuters, July 24, 2024.

[7] "Thirty-fifth report of the Analytical Support and Sanctions Monitoring Team submitted pursuant to resolution 2734 (2024) concerning ISIL (Da'esh), Al-Qaida and associated individuals and entities," United Nations, February 6, 2025.

[8] Editor's Note: Christopher F. Schuetze, "What We Know About the Munich Car Attack," *New York Times*, February 14, 2025.

[9] Richard Connor and Christoph Hasselbach, "Germany bans neo-Nazi group for 'indoctrination of children,'" Deutsche Welle, September 27, 2023.

[10] Michael Ertl, "Germany bans neo-Nazi group Hammerskins," BBC, September 19, 2023.

[11] Blyth Crawford and Florence Keen, "The Hanau Terrorist Attack: How Race Hate and Conspiracy Theories Are Fueling Global Far-Right Violence," *CTC Sentinel* 13:3 (2020).

[12] Editor's Note: "The Federal Administrative Court," Federal Administrative Court, Supreme Court, n.d.

[13] Editor's Note: Catie Edmondson, "How Germany's Extreme Right Seized on the Martial Arts Scene," *New York Times*, September 17, 2023.

[14] Editor's Note: Soraya Sarhaddi Nelson, "Neo-Nazis In Germany Use Music To Attract Followers," NPR, November 6, 2013.

[15] Editor's Note: Jiahand Li, "German court suspends ban on right-wing Compact Magazine amid ongoing legal proceedings," Jurist, August 15, 2024.

[16] Editor's Note: "German minister defiant after court lifts 'Compact' ban," Deutsche Welle, August 15, 2024.

[17] Editor's Note: "Germany bans Hezbollah television station," Reuters, November 21, 2008.

[18] Christian Jokinen, "Is Left-Wing Terrorism Making a Comeback in Germany? Analyzing the 'Engel – Guntermann Network,'" *CTC Sentinel* 17:1 (2024).

[19] Editor's Note: "The far-right and neo-Nazi gathering in Budapest known as the 'Day of Honour,'" Question for written answer E-000554/2024 to the Commission, European Parliament, February 21, 2024.

[20] Editor's Note: Fred Pleitgen and Olesya Dmitracova, "Tesla's Berlin plant shut after arson attack on electricity pylon. Far-left group claims responsibility," CNN, March 6, 2024.

[21] Editor's Note: Sebastian von Münchow, "Aftermath of the Terror Attack on Breitscheid Platz Christmas Market: Germany's Security Architecture and Parliamentary Inquiries," Marshall Center, July 2017.

[22] Editor's Note: "FBI Releases Investigative Update in Bourbon Street Attack," FBI New Orleans, January 14, 2025.

[23] Editor's Note: "Barriers to stop vehicle attacks were in the process of being replaced in New Orleans," PBS Newshour, January 1, 2025.

[24] Rüdiger José Hamm and Miriam Katharina Heß, "Am Stamm und nicht den Zweigen ansetzen - Der Nahostkonflikt in der Islamismusprävention," BAG RelEx, October 2024.

[25] Editor's Note: "Germany bans pro-Palestinian group Samidoun," Reuters, October 12, 2023.

[26] Csongor Körömi, "NATO: There was officially a Russian plot to kill European weapons chief," Politico, January 28, 2025.

[27] Greg Miller, Souad Mekhennet, and Cate Brown, "Iran turns to Hells Angels and other criminal gangs to target critics," *Washington Post*, September 12, 2024.

[28] Nette Nöstlinger, "Migration smashes into German elections after deadly knife attack," Politico, August 26, 2024; Emmy Sasipornkarn, "Solingen knife attack: IS suspect charged with murder," Deutsche Welle, February 27, 2025.

The New Syrian Government's Fight Against the Islamic State, Hezbollah, and Captagon

By Aaron Y. Zelin

Hayat Tahrir al-Sham's background as a former branch of the Islamic State and al-Qa`ida has created a perception that it is untrustworthy when it comes to security concerns of the United States and its allies. This has come to the fore even more acutely with the fall of the Assad regime. Some of the largest threats to outside countries in Syria remain the Islamic State, remnant Hezbollah networks, and the criminal captagon trade. Although few paid attention when Hayat Tahrir al-Sham was controlling territory in northwest Syria for seven years prior to the fall of the regime, it actually took those challenges on, and has continued to do so since it took over most of Syria on December 8, 2024. Of course, dealing with security challenges should not be the only lens through which to view the new rulers in Damascus; it should also take into account the nature of its governance and who is involved in it beyond its core supporters. Yet, if strictly judging the new rulers of Syria by its actions against the Islamic State, Hezbollah, and the captagon trade, they appear to be committed to these tasks, even if continued challenges will likely remain for the foreseeable future.

Ever since Hayat Tahrir al-Sham (HTS) overthrew the Assad regime on December 8, 2024, there have been a number of security concerns related to Syria. In particular, the future of the Islamic State threat, remnants of the Iranian proxy network, especially Hezbollah and weapons smuggling, and what happens to the former regime-linked captagon drug trade now that it is gone. On all fronts, there have been sustained and serious efforts by the new government in Damascus to address all of these challenges. This is a welcome dynamic and one that not only benefits Syria locally, but also the interests of the United States and other Western countries, especially relating to the threat posed by the Islamic State, but also helpful to Israel vis-a-vis Hezbollah, and Syria's neighboring states including Jordan and Saudi Arabia when it comes to the captagon criminal enterprise.

Dr. Aaron Y. Zelin is the Gloria and Ken Levy Fellow at the Washington Institute for Near East Policy, where he also directs the Islamic State Worldwide Activity Map project. He is also a Visiting Research Scholar in the Department of Politics at Brandeis University and founder of Jihadology. Dr. Zelin is the author of the books Your Sons Are At Your Service: Tunisia's Missionaries of Jihad *(Columbia University Press, 2020),* The Age of Political Jihadism: A Study of Hayat Tahrir al-Sham *(Rowman & Littlefield, 2023), and is currently working on another titled* Heartland of the Believers: A History of Syrian Jihadism. *X: @azelin*

While many might not realize it, prior to HTS taking over Syria, the group had already been dealing with these threats when it was a "non-state actor" controlling northwest Syria through its civilian and technocratic Syrian Salvation Government (SSG). Likewise, since 2013, beyond the lawfare approach that came to dominate how it dealt with these issues after late 2017 when the SSG was formed, HTS also previously fought directly on the battlefield against Hezbollah in 2013 and the Islamic State in 2014. HTS has a long track record of confronting these groups, so it is no surprise that since the fall of the Assad regime, those currently in the Syrian government have continued what they had already been doing for years.

After providing some context about the HTS security agency that had been charged with addressing such challenges, this article will outline—in turn—how those now in control in Damascus have confronted the security threats posed by the Islamic State, Hezbollah, and captagon. For each security threat, the article will first provide background on how HTS was dealing with the issue prior to the fall of the regime and then explore the current status over the past three-plus months since the group took over the government.[1]

Broadly speaking, HTS can be described as having taken a lawfare approach to confronting the security threats posed by the Islamic State, Hezbollah, and the captagon trade. This has been done via HTS' General Security Service (GSS). The GSS was HTS' law enforcement/intelligence body and had not officially been a part of the SSG. However, this changed in March 2024 when it was officially folded into the SSG's Ministry of Interior and was renamed the Public Security Department (PSD) after a protest movement began against abuses by HTS in what many locally called the "security cell" issue. This happened in the aftermath of HTS admitting in February 2024 that it had mistakenly arrested many individuals in its own security services in August 2023 for allegedly being in contact with Western intelligence based on poor interrogation tactics (i.e., torture).[2] These individuals were exonerated, and it led to a series of reforms by HTS and the SSG, including the transition from the GSS to the PSD. This came as no surprise to many since in the years prior to the fall of the regime, especially as it related to activists, many residents in HTS territory had criticized the judicial processes for lacking transparency, failing to provide reasons for arrests, holding alleged "kangaroo" trials, and treating prisoners badly (including torture).[3]

The GSS was formally founded in June 2020, though an embryonic version of it had been operating since HTS had begun acting as more of a proto-state under the SSG umbrella in 2017.[4] When the GSS was established in 2020, it released a video providing details on its writ within HTS-controlled areas as well as a breakdown of its structure. The purpose of the GSS, according to the video, was to protect the people of the "liberated" areas (how HTS described its territory) and to prevent any type of crime.[5] To do this, the GSS asserted in the video that it would arrest any person who was "working to destroy life and sow chaos" and then use any intelligence garnered from that arrest to go after others in a broader criminal network.[6]

Five key components of the GSS were the regional information office, the internal security division, the organized crime portfolio, the regime portfolio, and the "Khawarij" ("Kharijites"/"extremists") portfolio.[7] With regard to the extremists' portfolio, the Islamic State is not named specifically, but it is undoubtedly included under this portfolio. Issues such as Hezbollah or captagon would likely have fallen under the regime and organized crime portfolios, respectively. According to the GSS video, the process for the system started with an investigating officer providing detailed reasons for why someone should be arrested.[8] Once the investigation was completed, GSS security officials would arrest the individuals and then that individual would supposedly be brought in front of a public prosecutor to face a trial.[9] Details about the latter aspect within the judicial system have not been shared publicly by HTS, including since it disbanded in forming the new transitional government. To this day, this process seems to be very opaque. Nevertheless, the PSD as a successor institution to the GSS after it was created in March 2024, had the same agenda and writ; however, it reverted back to the GSS after the fall of the regime. It continues to be housed in the new transitional government's Ministry of Interior and acts in the same manner as previously.

The Fight Against the Islamic State

Prior to the fall of the regime, over a seven-and-a-half-year period, HTS publicly claimed 62 discreet operations to arrest members of Islamic State cells in 39 towns and villages throughout the greater Idlib region.[10] Of the 62 discreet raids, five occurred in 2017, 22 in 2018, eight in 2019, eight in 2020, 10 in 2021, six in 2022, zero in 2023, and four in 2024.[11] The data for 2017 only represents the second half of the year when the proto-GSS began publishing information on its operations.

The Islamic State only conducted a single successful attack in HTS territory from July 2018 until the fall of the regime, when HTS senior leader Abu Mariyah al-Qahtani was assassinated in early April 2024.[12] This means that in the years leading up to the fall of the regime, the Islamic State threat had only a very limited effect on daily life in the area that HTS controlled. In other words, HTS was strikingly successful in its counterterrorism fight against the Islamic State.

The uptick in HTS thwarting Islamic State plots in 2024 compared with the previous year is to a significant degree explained by the growth of Islamic State activity in eastern and central parts of Syria in 2024. However, several of the key drivers that led to the Islamic State's bounce-back in 2024 have diminished now that the Assad regime has fallen.[13] A first factor that helped Islamic State activity tick up was the fact that during the summers of 2023 and 2024, the Assad regime and Iran-backed Arab tribal forces in Deir ez-Zor governorate had instigated uprisings against the Syrian Democratic Forces (SDF), in an effort to undermine the SDF and U.S. positions in eastern Syria.[14] This undermined intelligence efforts by the United States and the Global Coalition and SDF in their fight against local Islamic State networks in eastern Syria. These obstacles to confronting the Islamic State were largely removed as a result of the regime falling and the huge weakening of Iran's proxy network in Syria alongside the fact that the new government in Damascus has taken over Deir ez-Zor city and the western part of the governorate. Furthermore, the environment for the Islamic State has also been made less fertile because of the agreement signed on March 11, 2025, between the president of the Syrian transitional government, Ahmad al-Sharaa (previously known as Abu Muhammad al-Julani) and the commander of the SDF, Mazloum Abdi, to integrate the SDF forces into the central government's institutions.[15] Since then, the new government and the SDF have set up a central committee to implement the agreement with specialized military and economic subcommittees.[16] There is also expected to be a prisoner exchange between the government and the SDF after the end of Ramadan in early April.[17] Not only is it hoped the deal between Damascus and the SDF will unify the country, but the hope is that it will also create a more sustainable framework to confront the Islamic State.

A second key factor that had contributed to the Islamic State's bounce-back in 2024 was the decision by Assad and his Russian allies to de-emphasize the fight against the Islamic State. HTS' drone attack against a graduation ceremony for one of the Assad regime's military colleges in Homs in early October 2023[18] led the Assad regime and its Russian allies to draw their forces away from the western side of Deir ez-Zor governorate to focus on attacking HTS' base in Idlib in northwest Syria.[19] This gave the Islamic State more space for attacks and movement of fighters across the frontlines between the Assad regime and SDF-controlled territories. Fast forward to the period after December 8, 2024, and this is no longer a factor.

A third key factor that had helped the Islamic State bounce back was that in the wake of the war in Gaza, U.S. assets and bases in eastern Syria were targeted by Iranian-backed Shi`a proxy groups in Iraq and Syria.[20] These attacks resulted in U.S. forces and the coalition, as a force protection response, limiting their actions against the Islamic State—either independently or alongside the SDF—providing the Islamic State with more breathing room.[21] However, fast forward to the present day and the Iran threat network has been significantly weakened in the region as a result of the serious blows Israel inflicted on Hezbollah in Lebanon in the latter part of 2024.

All in all, the coalition of forces arrayed against the Islamic State, including the new Syrian government, have a much freer hand to combat the Islamic State than they did a year ago. The United States and the Global Coalition alongside the SDF continue to conduct raids against Islamic State cells in northeast and eastern Syria. Based on the author's Islamic State Worldwide Activity map, since the fall of the regime, the SDF has arrested 13 Islamic State cells in al-Raqqah, Hasakah, and Deir ez-Zor governorates as of March 26, 2025.[22] The United States has also conducted two airstrikes and one arrest with the SDF against Islamic State operatives in SDF-controlled territories since the fall of the regime.[23] This continued pace has kept Islamic State operations at a relatively low level in recent months.

To make up for the disappearance of Assad regime forces from central Syria after the collapse of the regime, another U.S. partner force on the ground, the Syrian Free Army (SFA), moved from the Tanf Garrison that hugs the triangle border between Syria, Iraq, and

Jordan into the central city of Palmyra to cover the broader desert terrain in Homs governorate.[24] In the author's assessment, the United States has been able to use intelligence against Islamic State cells and camps in central Syria in a much freer way now since it no longer has to deconflict with Russia. In September and October 2024, before the fall of the regime, the United States carried out three airstrikes against the Islamic State in central Syria.[25] Then, the day the regime fell, the United States struck 75 Islamic State targets in central Syria and carried out another series of airstrikes there eight and 14 days later[26] to try to ensure the Islamic State did not take advantage of any chaos following the fall of the Assad regime. One development that augurs well for the fight against the Islamic State is that the SFA joined the new Syrian Ministry of Defense in late January 2025, creating a potentially useful vehicle for counterterrorism cooperation between Washington and Damascus.[27]

This image released by the new Syrian government's Ministry of Interior shows alleged members of an Islamic State cell who were detained in January 2025 for allegedly trying to blow up the Sayyida Zainab shrine.

In its new guise as the Syrian government, HTS has continued to fight Islamic State cells. So far, they have announced four key actions against the Islamic State. Firstly, on January 11, the new government in Damascus thwarted an Islamic State plot to bomb the Shi`a Sayyida Zainab shrine in the Damascus suburbs designed to incite sectarian tensions.[28] There are media reports that the United States provided the intelligence that led to this plot being broken up.[29] In subsequent interrogation that the Ministry of Interior released from these plotters, those involved in planning this attack also disclosed that they attempted to attack a church in the Christian town of Maaloula on New Year's Day with a car bomb, which was never actualized, and also had a plan to assassinate Ahmad al-Sharaa if he decided to visit the Sayyida Zainab shrine after a successful attack occurred.[30]

Secondly, on February 15, 2025, the GSS arrested Abu al-Harith al-Iraqi, a senior leader in the Islamic State's Iraq Province, who had been involved in the aforementioned assassination of former senior HTS leader Abu Mariyah al-Qahtani in April 2024 and assisting the Sayyida Zainab plot.[31] The arrests relating to the latter plot appear to have led to information that allowed Damascus to find Abu al-Harith, which the Ministry of Interior recently disclosed.[32]

Interestingly, it seems that intelligence garnered from Abu al-Harith then led to the airstrike that killed Abdallah Makki Muslih al-Rufay'i (Abu Khadijah), Abu al-Harith's superior, in Iraq on March 14.[33] Abu Khadijah allegedly was the deputy caliph of the Islamic State, and also served as the *wali* (governor) of Iraq and Syria and head of the Delegated Committee. As part of his remit, he oversaw external operations plots;[34] in 2024, the Islamic State in Iraq was responsible for five failed external operations plots.[35] This all shows that intelligence-sharing between the United States, Syria, and Iraq related to the Islamic State has become mutually beneficial, which led to a state-to-state visit between Damascus and Baghdad on March 14.[36]

Most recently, on February 18 and March 6, the GSS arrested Islamic State cells in the towns of al-Naima and al-Sanamayn, respectively, in Syria's Dara'a governorate.[37]

The Fight Against Hezbollah

Since Hezbollah entered the war in Syria at the behest of Iran to back up the Assad regime, Hezbollah and HTS have been pitted on opposite sides.[38] Due to this factor, it is unsurprising that following the fall of the regime, the new government in Damascus is also interested in taking on remnant Hezbollah networks that are either backing up regime remnant insurgent networks or attempting to continue to smuggle weapons from Iran into Lebanon. Due to the fall of the regime, Iran's position in Syria has been greatly weakened, especially in light of Israel's campaign against Hezbollah in the post-October 7th era.

The first indication that Hezbollah entered Syria to assist the Assad regime in its fight against the burgeoning insurgency against its rule was in the summer of 2012.[39] This was through the conduit of an Iranian-created proxy group called Liwa Abu Fadl al-Abbas. It brought together Shi`a foreign fighters from various Iranian proxy groups (Hezbollah, Asa'ib Ahl al- Haq, Kata'ib Hezbollah, and Kata'ib Sayyid al- Shuhada) to obscure their direct involvement in the conflict initially.[40] As early as January 2013, Jabhat al-Nusra was reporting that it was directly fighting Hezbollah in the Damascus region.[41] However, the then Hezbollah leader Hasan Nasrallah only publicly admitted in May 2013 that his group was officially involved in the fighting, stating "this battle is ours, and I promise you victory."[42] Part of this was to legitimize the group's overt involvement in the battle for Qusayr that occurred in May-June 2013 and led effectively to the northern and southern fronts of the anti-regime insurgency being cut off from one another.[43]

The nasty nature of that battle led the late Yusuf al-Qaradawi, a highly influential Egyptian Islamist theologian, to call on Sunni Muslims worldwide to fight against the regime and Hezbollah in Syria: "Anyone who has the ability, who is trained to fight … has to go; I call on Muslims to go and support their brothers in Syria," he stated.[44] And while many attribute the large-scale foreign fighter mobilization in Syria to the Islamic State, in some ways, this helped paved the way for one on a more mainstream level. It also further legitimized the kind of sectarian language that became a key part of the fight between Jabhat al-Nusra and Hezbollah.[45] In particular, al-Qaradawi called Hezbollah "Hizb al-Shaytan" (the party of Satan) in his speech, while Jabhat al-Nusra usually preferred 'Hizb al-Lat' (the party of Lat). The latter is in reference to the pre-Islamic Arabian goddess al-Lat, who was believed to be a daughter of God, thus branding Hezbollah as a group of polytheists and not true believers, who must be smashed similar to the idols during the time of the Prophet Mohammad.

In response to all of this, Jabhat al-Nusra created a Lebanese branch and began to conduct attacks against Hezbollah across the border into Lebanon from December 2013 to as late as July 2015.[46] Many of these were cross-border rocket attacks.[47] However, Jabhat al-Nusra's Lebanon branch also conducted suicide bombings in Hezbollah strongholds in the Hermel region.[48] While the fighting within Lebanon abated, fighting between the two groups would continue for years within Syria itself prior to the fall of the regime. For example, as late as mid-October 2024, six weeks before the offensive to overthrow the Assad regime began, an HTS-run joint operations room called al-Fatah al-Mubin put out a statement condemning Iranian-backed proxies, including Hezbollah, for attacking HTS' positions in northwest Syria.[49]

Prior to HTS' GSS/PSD adoption of a lawfare approach once they had solidified control in northwest Syria in late 2017, HTS' predecessor group Jabhat al-Nusra arrested Hezbollah fighters from the battlefield and held prisoners of war. For example, in late August 2015, Jabhat al-Nusra put out a video highlighting the fourth Hezbollah cell it had arrested in the western Ghouta region outside of Damascus.[50] Likewise, they also promoted imprisoning Hezbollah fighters in mid-November 2015 in the southern Aleppo countryside.[51] During the brutal battle to retake Aleppo in mid-June 2016, Jabhat al-Nusra captured a Hezbollah fighter on the Khalasa front in the southern Aleppo countryside.[52] In July 2017, HTS captured Hezbollah fighters right after they crossed the border from Arsal, Lebanon, into Syrian territory.[53]

In addition to taking Hezbollah fighters off the battlefield, these kind of capture operations were also a way for Jabhat al-Nusra and later HTS to exchange Hezbollah fighters for Nusra/HTS fighters who Hezbollah had previously also taken as prisoners of war. As late as early August 2017, HTS released video appeals from captured Hezbollah fighters to their families to try and pursue an exchange of prisoners.[54] An example of these types of exchanges occurred in late July 2017 in the western Qalamoun region when a Syrian female prisoner from Lebanese prisons and the bodies of eight killed HTS fighters were exchanged for the bodies of five killed Hezbollah fighters.[55] HTS' news agency at the time, called Iba', reported in late April 2018 that an unspecified number of HTS fighters were swapped with an unspecified number of Hezbollah fighters.[56]

جهاز الأمن العام
لحظـة اعتقال أفراد الخلية الأمنية التابعة لميليشـيات حزب الله
@GE_SE_SE
@GE_SE_SE

Image released by HTS' GSS of an HTS takedown of a Hezbollah cell in June 2023 by the GSS in northwest Syria

As the conflict lines began to freeze in Syria, especially in light of the March 2020 Turkey-Russia ceasefire agreement, direct interaction between HTS and Hezbollah became less frequent. While the GSS/SPD would break up a number of cells related to former regime activity in HTS territory in the period prior to the fall of the Assad regime,[57] there is only one known case of the GSS taking down a Hezbollah cell.[58] This occurred in late June 2023 when the GSS claimed that a Hezbollah cell was monitoring locations of HTS fighters, government buildings, and humanitarian organizations as well as allegedly planning assassinations and placing mines in HTS territory.[59]

Now that the regime is gone and the new Syrian government controls most of the country, HTS in its new guise as the government of Syria is confronting remnant Hezbollah cells in Syria. There have been a significant number of clashes with Hezbollah on the border with Lebanon and arrests of Hezbollah cells involved in weapons smuggling.

An image released by the Syrian Ministry of Interior showing the seizure of Hezbollah-bound weapons being smuggled on a truck in mid-January 2025

Thus far, the new government has arrested six Hezbollah cells since the fall of the regime. Most of them were located in the areas around the Syria-Lebanon border in Tartus, Homs, and Rif Dimashq governorates.[60] All of these cells were attempting to illegally smuggle weapons from Syria into Lebanon to provide them to Hezbollah. This has included Kalashnikovs, automatic rifles, rockets, drone parts, and ammunition. The most recent bust happened in Sayyida Zainab, where Hezbollah's network has a long history.[61] Individuals that were part of the affiliated Saudi Hizballah group that used a truck bomb in their 1996 Khobar Towers attack in Saudi Arabia did some of their operational meeting in Sayyida Zainab.[62] In that attack, 19 U.S. service personnel were killed and almost 500 more people from at least seven countries were injured.[63] Interestingly, the new government also arrested in late February 2025 a member of the Iraqi Hashd al-Sha'abi in western Homs for weapons smuggling as well.[64]

Unlike under the Assad regime, there is now a government in charge that is willing to interdict this activity. During a combing campaign to try and stop smuggling operations near the Syria-Lebanon border in early February 2025, Syria's new security forces seized a large number of farms, warehouses, and factories for manufacturing and packaging hashish and captagon pills, in addition to printing presses specializing in printing counterfeit currency, which Hezbollah was also involved in.[65] In response, gangs affiliated with Hezbollah kidnapped two Syrian military members, who Syrian forces later managed to free.[66] The incident generated cross-border clashes that lasted two days,[67] with a Syrian refugee dying and two others injured in the vicinity of Qusayr.[68] Eventually, the new Syrian state and Lebanese army coordinated to calm the situation.[69]

In mid-March 2025, there was another flare-up in fighting between the new Syrian government forces and Hezbollah. This time, Hezbollah members crossed the border, ambushed and kidnapped three Syrian army personnel, brought them back into Lebanon, and executed them, with at least one of them being stoned to death.[70] It is possible this was triggered by Damascus' continued cracking down on smuggling networks or a reprisal for the massacre of Alawites on the Syrian coast on March 6.[71] In response, the forces of the new Syrian government fired rockets into Lebanon from Syrian territory toward Hezbollah. Hezbollah returned fire with anti-tank missiles, injuring a group of journalists, including an al-Arabiya reporter.[72] Similar to the February events, after a couple of days the situation simmered down once the Lebanese Armed Forces arrived, who have since also dismantled three illegal border crossings between Lebanon and Syria.[73] On March 28, 2025, Lebanese and Syrian defense ministers signed an agreement in Jeddah, Saudi Arabia, to demarcate the Lebanese-Syrian border, which will likely further secure both borders.[74]

This all illustrates that Hezbollah poses a challenge to the new Syria not only because of its remnant networks inside Syria that had previously been assisting the Assad regime, but also because of its continued attempts to smuggle weapons via Syria back into Lebanon.

The Campaign Against Captagon

Captagon is an amphetamine-like stimulant in pill form. As far back as 2006, in the aftermath of that year's Israel-Hezbollah war, Hezbollah began to produce, smuggle, and sell counterfeit versions of captagon.[75] This helped supplement Hezbollah's budget from Iran.[76] Due to similar budget shortfalls as a consequence of the Syrian civil war, and the Assad regime's inability to access significant capital outside of help from Russia, Iran, and Hezbollah because of U.S. sanctions, the Assad regime increasingly became a captagon-producing narco-state in the latter part of its rule. In one of many examples, in 2018, the regime took over a factory for potato chips and turned it into a captagon-producing factory.[77]

The Assad regime began to produce the narcotic on an industrial scale to continue to feed its war machine and the corruption in its system. This was primarily the purview of Maher al-Assad and his 4th Division in the Republican Guard. Hezbollah also provided assistance based on its own experience.[78] According to the U.K. government in late March 2023, the former regime's captagon trade was "worth approximately 3 times the combined trade of the Mexican cartels."[79] By the time the regime fell, according to one estimate, the annual global trade of captagon was estimated at $10 billion, while the Assad regime took in around $1.8 billion annually, which was twice the revenue generated from all legal Syrian exports in 2023.[80]

ضبط ما يقارب مليون حبة مخدرة مغلفة ضمن أكياس إثر محاولة إدخالها لمنطقة إدلب
@GE.SE.SE1
@GE_SE_SE

A captagon bust in February 2022 by HTS' GSS that released this image

What can we ascertain about the new government's war on captagon? It is actually a continuation of HTS' policies when it was only in control of northwest Syria. It is worth noting that HTS through the GSS/SPD worked to counter all illegal drugs prior to the fall of the regime, efforts which have continued since.

The first publicized drug bust by the GSS was related to hashish in early 2018.[81] It is also possible that the first captagon-related bust occurred in late May 2019 when HTS security services seized what was referred to as narcotic pills, making it possible this was their first seizure of captagon.[82] Demonstrating its attentiveness to counter-narcotics, in the years prior to the first official captagon-related bust in northwest Syria, HTS bodies carried out briefings and lectures related to the dangers of drugs in general within its territory for the Police Command, the Ministry of Interior, Idlib University, and regional administrations.[83]

The first *publicized* captagon seizure by the GSS was carried out in mid-February 2022.[84] The fact that the baggies the captagon were in had a Lexus logo sticker on them attempted to signify it was related to the regime's industrial manufacturing of it, as that was one of the ways it was promoted to those buying it.[85] Subsequently, the regime began using a Lamborghini sticker to try and obfuscate the captagon's origin. Between that arrest in February 2022 and the collapse of the Assad regime, HTS' GSS conducted six captagon-related drug busts in northwest Syria,[86] including a manufacturing site in mid-January 2023.[87]

An image posted by the Syrian Ministry of Interior showing the discovery by the new Syrian government of captagon hidden in children's toys in mid-January 2025

The biggest busts by the new Syrian government since the fall of the Assad regime have continued to show some of the captagon in bags with the Lexus and Lamborghini stickers, among other variations.[88] This highlights that although remnants of the regime can no longer produce captagon at scale, they are still attempting

"Unlike the Assad regime—which did little to fight the Islamic State, was closely aligned with Hezbollah, and produced captagon on an industrial scale—HTS in its guise as the new government of Syria is taking on these challenges assertively, and has a significant track record in doing so previously. Not only are these efforts a benefit to Syrian society and the security and stability of the country, but they also align with the interests of the United States and U.S. regional allies."

to trade it illicitly.

Over the years in HTS territory, captagon pills have been hidden in piping.[89] Since the fall of the regime, the pills have also been found hidden in industrial equipment, furniture, children's toys, and Styrofoam.[90] In total, the new Syrian government has made 20 seizures of captagon since it took power as of March 27, 2025.[91] These cases have spanned many Syrian governorates including Aleppo, Damascus, Dara'a, Deir ez-Zor, Hama, Homs, Idlib, Latakia, and Rif Dimashq, illustrating both the continued scope of the challenge and the commitment of the new rulers of Damascus to now confront it.[92] Some of these interdictions occurred in border towns close to Lebanon and Jordan, just before the captagon pills were due to enter the illicit market.[93] In carrying out these interdictions, Syria's new authorities discovered manufacturing sites and warehouses that the former regime had used to create and store captagon, in particular ones related to Maher al-Assad's network.[94] On March 21, 2025, the new Syrian government carried out what it said was the largest captagon seizure thus far when it seized three million captagon pills in Aleppo.[95]

Continuing Challenges

Unlike the Assad regime—which did little to fight the Islamic State, was closely aligned with Hezbollah, and produced captagon on an industrial scale—HTS in its guise as the new government of Syria is taking on these challenges assertively, and has a significant track record in doing so previously. Not only are these efforts a benefit to Syrian society and the security and stability of the country, but they also align with the interests of the United States and U.S. regional allies such as Israel, Jordan, Saudi Arabia, and the UAE. In recent years, the captagon trade has been a huge concern to the Sunni Arab states in particular.

However, the security challenges posed by the Islamic State, Hezbollah, and the captagon trade are likely to endure for some time. One concern is the ticking time bomb of the 9,000 male Islamic State prisoners held in northeast Syria and the threat that the Islamic State could break them out.[96]

There also remain lingering questions about how the agreement between al-Sharaa and the SDF leader Abdi plays out and the fact that Turkey's proxies in Syria continue to fight the SDF.[97] These outcomes will shape the degree to which the Syrian state can be effective in combating the Islamic State. Another challenge facing the Syrian government is a lack of financial resources. With Syria in dire economic straits and sectarian tensions recently spiraling in its coastal region, the Islamic State, Hezbollah, and operators in the captagon black market may eye opportunities. It would be foolish to count Iran and Hezbollah out. The Lebanese group is likely to continue to confront the new Syrian government in the border region with Lebanon, especially as Damascus tries to dismantle the infrastructure Hezbollah built up in western Syria when it was backing up the Assad regime.

In addition to the importance of continuing to push Damascus for an inclusive, open, and transparent government, the stakes are also high for the future security of Syria, the region, and far beyond. For these reasons, it would be wise for Washington, London, Paris, Berlin, Brussels, Amman, Ankara, Jerusalem, Riyadh, Abu Dhabi, Baghdad, Beirut, and others to coordinate and support the new rulers in Damascus in their fight against the Islamic State, Hezbollah, and captagon. CTC

Citations

[1] The author explored in extensive detail HTS' counterterrorism fight against the Islamic State in the February 2023 issue of CTC Sentinel. This article updates this assessment but does not include as much detail about the pre-2023 period. For more, see Aaron Y. Zelin, "Jihadi 'Counterterrorism:' Hayat Tahrir al-Sham Versus the Islamic State," *CTC Sentinel* 16:2 (2023).

[2] "The Liberated Leadership Met With Members of the Shūrā Council and the Salvation Government To Talk About the Latest Security Issue," Hayat Tahrir al-Sham, Amjad Media, February 1, 2024, via Aaron Y. Zelin, "New video message from Hay'at Tahrir al-Sham: 'The Liberated Leadership Met With Members of the Shura Council and the Salvation Government To Talk About the Latest Security Issue,'" Jihadology, February 1, 2024.

[3] Khaled al-Khateb, "Jihadi Group in Syria's Idlib Faces Criticism over Unfair Trials, Death Sentences," al-Monitor, August 25, 2021.

[4] GSS releases can be found on GSS' Telegram channel.

[5] "The Security Files," Hayat Tahrir al-Sham, General Security Service (available via Jihadology), June 12, 2020.

[6] Ibid.

[7] Ibid.

[8] Ibid.

[9] Ibid.

[10] "HTS Arrests of IS Database," created by Aaron Y. Zelin, last updated February 18, 2025.

[11] Ibid.

[12] Aaron Y. Zelin, "The Last Days of Abu Mariyah al-Qahtani," Syrian Jihadism, April 20, 2024.

[13] Aaron Y. Zelin, "Remaining, Waiting for Expansion (Again): The Islamic State's Operations in Iraq and Syria," *Current Trends in Islamist Ideology* 35 (2024).

[14] Hassan Hassan and Omar Abu Layla, "Assad's Hidden Hand in the Uprising Against the Kurds in Eastern Syria," New Lines Magazine, September 4, 2023.

[15] "Signing an agreement stipulating the integration of the Syrian Democratic Forces into the institutions of the Syrian Arab Republic, emphasizing the unity of Syrian territory and rejecting division," March 11, 2025, via Aaron Y. Zelin,

"Diary of the Syrian Transition - March 10-11, 2025," Jihadology+, March 11, 2025.

[16] See Aaron Y. Zelin, "Diary of the Syrian Transition - March 13, 2025," Jihadology+, March 13, 2025.

[17] Ibid.

[18] Sarah Dadouch, "At least 80 killed in drone attack on Syrian military academy in Homs," *Washington Post*, October 5, 2023.

[19] Haid Haid, "Smoke and Mirrors: Assad's Exploitation of Israel's War on Gaza to Escalate Atrocities in Idlib," Tahrir Institute for Middle East Policy, February 6, 2024.

[20] Michael Knights, Amir al-Kaabi, and Hamdi Malik, "Tracking Anti-U.S. and Anti-Israel Strikes From Iraq and Syria During the Gaza Crisis," Washington Institute for Near East Policy, October 14, 2024.

[21] "Operation Inherent Resolve Lead Inspector General Quarterly Report to Congress, April 1, 2024—June 30, 2024," Inspector General for Department of Defense, State, and USAID, July 31, 2024.

[22] See "The Islamic State, Select Worldwide Activity," Washington Institute, n.d.

[23] "CENTCOM Forces Kill ISIS Operatives, Destroy Truckload of Weapons in Syria Airstrike," U.S. Central Command, December 23, 2024; "CENTCOM and Partner Forces Conduct Operations in Iraq and Syria to Defeat ISIS," U.S. Central Command, January 6, 2025; "Syrian Democratic Forces, Enabled by CENTCOM Forces, Capture ISIS Cell Leader," U.S. Central Command, March 8, 2025.

[24] "'Syrian Free Army' take control of Palmyra as regime forces fall back," New Arab, December 7, 2024.

[25] "U.S. Central Command Conducts Targeted Strikes Against Terrorist Groups in Syria," U.S. Central Command, September 29, 2024; "U.S. Central Command conducts airstrikes against multiple ISIS camps in Syria," U.S. Central Command, October 12, 2024; "U.S. Central Command Conducts Airstrikes Against Several ISIS Camps in Syria," U.S. Central Command, October 30, 2024.

[26] "U.S. Central Command conducts dozens of airstrikes to eliminate ISIS camps in central Syria," U.S. Central Command, December 8, 2024; "U.S. Central Command Conducts Airstrikes Against ISIS Operatives," U.S. Central Command, December 16, 2024; "CENTCOM Forces Kill ISIS Leader During Precision Strike in Syria," U.S. Central Command, December 20, 2024.

[27] See Aaron Y. Zelin, "Diary of the Syrian Transition - January 29, 2025," Jihadology+, January 29, 2025.

[28] See "The Islamic State, Select Worldwide Activity."

[29] Warren P. Strobel, Ellen Nakashima, and Missy Ryan, "U.S. shared secret intelligence with Syria's new leaders," *Washington Post*, January 24, 2025.

[30] "In the Grip of Security: An Inevitable Fate," Ministry of Interior (Syria), March 18, 2025.

[31] Zelin, "The Last Days of Abu Mariyah al-Qahtani." See also Aaron Y. Zelin, "A History of Hayat Tahrir al-Sham Publicly Announced Counterterrorism Actions Against Islamic State Leaders and Members," Jihadology+, January 11, 2025.

[32] "In the Grip of Security."

[33] See Mohammed Shia Al-Sudani, "[The Iraqis continue their impressive victories over the forces of darkness and terrorism . . .]," X, March 14, 2025. It is likely the case that intelligence garnered from interrogations of Abu al-Harith provided great details on Abu Khadijah's whereabouts since he was working for Abu Khadijah.

[34] Ibid.

[35] "Non-ISKP External Ops Database," created by Aaron Y. Zelin, last updated March 7, 2025.

[36] See "Deputy Prime Minister and Minister of Foreign Affairs receives Syrian Foreign Minister to discuss regional security and joint coordination," Ministry of Foreign Affairs (Iraq), March 14, 2025.

[37] See "The Syrian government announces the arrest of an ISIS cell in a Syrian province," Al-Mubdi'un News Platform, February 19, 2025.

[38] Phillip Smyth, "The Shiite Jihad in Syria and Its Regional Effects," *Policy Focus* 138, Washington Institute for Near East Policy, February 2015.

[39] Phillip Smyth, "Hizballah Cavalcade: What is the Liwa'a Abu Fadl al-Abbas (LAFA)?: Assessing Syria's Shia 'International Brigade' Through Their Social Media Presence," Jihadology, May 15, 2013.

[40] Ibid.

[41] See "Hezbollah fighters withdraw from Damascus after Al-Nusra Front intervenes," Al Rai News, January 14, 2013.

[42] Hassan Nasrallah, "Words on Eid al-Muqawama and the Liberation," al-Manar, May 25, 2013.

[43] Matthew Levitt and Aaron Y. Zelin, "Hizb Allah's Gambit in Syria," *CTC Sentinel* 6:8 (2013).

[44] Thomas Hegghammer and Aaron Y. Zelin, "How Syria's Civil War Became a Holy Crusade," *Foreign Affairs*, July 3, 2013.

[45] Aaron Y. Zelin and Phillip Smyth, "The Vocabulary of Sectarianism," *Foreign Policy*, January 29, 2014.

[46] An archive of the activity of Jabhat al-Nusra's Lebanon branch can be found here: https://jihadology.net/category/jabhat-al-nu%e1%b9%a3rah-in-lebanon.

[47] Ibid.

[48] Ibid.

[49] "Regarding the Escalation By Iranian Militias Against the Liberated Areas," Al-Fatah al-Mubin, October 12, 2024, via Aaron Y. Zelin, "New statement from al-Fatah al-Mubin: 'Regarding the Escalation By Iranian Militias Against the Liberated Areas,'" Jihadology, October 12, 2024.

[50] "Arrest of the Fourth Cell of the Syrian Hizb Allah in Western Ghutah," Jabhat al-Nusrah, al-Manarah al-Bayda Media, August 20, 2015, via Aaron Y. Zelin, "New video message from Jabhat al-Nusrah: 'Arrest of the Fourth Cell of the Syrian Hizb Allah in Western Ghutah,'" Jihadology, August 20, 2015.

[51] "Three Lebanese Hizb Allah Fighters Imprisoned in Rural Southern Aleppo," Jabhat al-Nusrah, al-Manarah al-Bayda Media, November 14, 2015, via Aaron Y. Zelin, "New video message from Jabhat al-Nusrah: 'Three Lebanese Hizb Allah Fighters Imprisoned in Rural Southern Aleppo,'" Jihadology, November 14, 2015.

[52] "A member of Lebanese Hizballah was captured while thwarting an attempt by the rejectionist militias to advance on the town of Khalasa," Jaysh al-Fatah/ Jabhat al-Nusrah, June 17, 2016. Author retains a copy of the photo in his archive.

[53] "3 Hizballah prisoners in the outskirts of Arsal after they attempted to advance towards the mujahidin areas a few days ago," Hayat Tahrir al-Sham, Iba News Agency, July 31, 2017. Author retains a copy of the photo in his archive.

[54] "Appeal of One of the Hizb Allah Prisoners to His Family in Lebanon," Hayat Tahrir al-Sham, July 25, 2017, via Aaron Y. Zelin, "New video message from Hay'at Tahrir al-Sham: "Appeal of One of the Hizb Allah Prisoners to His Family in Lebanon," Jihadology, July 25, 2017; "The Last Moments of the Hizb Allah Prisoners," Hayat Tahrir al-Sham, August 2, 2017.

[55] "Hayat Tahrir al-Sham in Western Qalamoun exchanges a female prisoner from Lebanese prisons and the bodies of 8 martyred rebels, in exchange for 5 bodies of the 'Hezbollah' militia," Hayat Tahrir al-Sham, Iba News Agency, July 31, 2017. The author retains a copy of the photo in his archive.

[56] "The fighters of Hayat Tahrir al-Sham after being freed from the rejectionists in a swap deal with the Lebanese Hizballah," Hayat Tahrir al-Sham, Iba News Agency, April 28, 2018. Author retains a copy of the photo in his archive.

[57] "HTS arrests of regime cells in northwest Syria Database," created by Aaron Y. Zelin, last updated November 27, 2024.

[58] "The General Security Service arrested a security cell affiliated with Hezbollah militias that was active in the liberated areas," Hayat Tahrir al-Sham, June 24, 2023. Author retains a copy of the photo in his archive.

[59] Dhiya' al-'Umar, "Regarding the Arrest of a Security Cell Affiliated With the Lebanese Hizb Allah Militia," June 25, 2023, via Aaron Y. Zelin, "New statement from Hay'at Tahrir al Sham's Diya al-'Umar: 'Regarding the Arrest of a Security Cell Affiliated With the Lebanese Hizb Allah Militia,'" Jihadology, June 25, 2023.

[60] "New Syrian Government versus Hizballah database," created by Aaron Y. Zelin, last updated March 17, 2025.

[61] Syrian Ministry of Inrerior Telegram channel, March 27, 2025.

[62] Matthew Levitt, "Anatomy of a Bombing," *Foreign Affairs*, September 1, 2015,

[63] Ibid.

[64] This can be found on the Homs Governorate Telegram channel.

[65] See Aaron Y. Zelin, "Diary of the Syrian Transition - February 10, 2025," Jihadology+, February 10, 2025.

[66] See Aaron Y. Zelin, "Diary of the Syrian Transition - February 6, 2025," Jihadology+, February 6, 2025.

[67] See Aaron Y. Zelin, "Diary of the Syrian Transition - February 9, 2025," Jihadology+, February 9, 2025.

[68] See Aaron Y. Zelin, "Diary of the Syrian Transition - February 12, 2025," Jihadology+, February 12, 2025.

[69] See Aaron Y. Zelin, "Diary of the Syrian Transition - February 10, 2025," Jihadology+, February 10, 2025.

[70] See Aaron Y. Zelin, "Diary of the Syrian Transition - March 16, 2025," Jihadology+, March 16, 2025.

[71] Aaron Y. Zelin, "Syria's Transitional Honeymoon Is Over After Massacres and Disinformation," Washington Institute for Near East Policy, *Policy Watch* 4012, March 10, 2025.

[72] See Aaron Y. Zelin, "Diary of the Syrian Transition – March 17, 2025," Jihadology+, March 17, 2025.

[73] "Syria and Lebanon reach ceasefire agreement after two days of clashes," Enab Baladi, March 18, 2025.

[74] "Politics / Under the generous directives of the Custodian of the Two Holy

Mosques and His Royal Highness the Crown Prince, the Kingdom hosts a meeting between the Syrian and Lebanese defense ministers to coordinate and enhance cooperation on security and military issues between their two countries," Saudi Press Agency, March 28, 2025.

[75] Boaz Ganor and Miri Halperin Wernli, "The Infiltration of Terrorist Organizations Into the Pharmaceutical Industry: Hezbollah as a Case Study," *Studies in Conflict & Terrorism* 36:9 (2013).

[76] Jon Henley, "Captagon: the amphetamine fuelling Syria's civil war," *Guardian*, January 13, 2014.

[77] Sally Abou AlJoud, "What Assad's fall has revealed about Syria's trade in the stimulant drug Captagon," Associated Press, December 18, 2024.

[78] "Report to Congress on A Written Strategy to Disrupt and Dismantle Narcotics Production and Trafficking and Affiliated Networks Linked to the Regime of Bashar al-Assad in Syria Sec. 1238(c) of the National Defense Authorization Act for Fiscal Year 2023, P.L. 117-263," U.S. Department of State, June 29, 2023.

[79] "Tackling the illicit drug trade fuelling Assad's war machine," Foreign, Commonwealth & Development Office and Lord (Tariq) Ahmad of Wimbledon KCMG, March 28, 2023.

[80] Ibid.; Karam Shaar, Caroline Rose, and Roaa Obaid, "Captagon in 2024: Implications After the Fall of the Syrian Regime," New Lines Institute, February 25, 2025.

[81] "The security office of Hayat Tahrir al-Sham arrests a drug dealer," Hayat Tahrir al-Sham, Iba News Agency, September 4, 2018. Author retains a copy in his archive.

[82] "Police arrest a drug trafficking cell in rural Idlib," Hayat Tahrir al-Sham, Iba News Agency, May 28, 2019. Author retains a copy in his archive.

[83] "Sarmada Region: Police Command 'Your Safety is our Responsibility' Drugs and Their Causes," Sarmada Region Media Office, October 14, 2020; "Minister of Interior, Mr. Ahmed Lattouf, delivers a lecture entitled 'Drugs and Their Danger to Society' in the presence of a number of police officers from the Ministry of Interior," Syrian Salvation Government, December 22, 2020; "Sponsored by Idlib University and in cooperation with the Adwaa team and Sharm Warehouse, we invite you to attend a medical conference entitled: 'The Scourge of Drugs: Between Addiction and Treatment Methods,'" Idlib University, February 2, 2021; "Under the auspices of the Ministry of Interior and the Central Region Administration, a symposium was held in the city of Maarat Misrin on the dangers of drugs and their effects on the liberated areas," al-Sham News Agency, November 7, 2021. Author retains a copy of these in his archive.

[84] "A car attempting to smuggle a shipment of narcotic pills into the Idlib region was seized," Hayat Tahrir al-Sham, General Security Service, February 12, 2022. Author retains a copy in his archive.

[85] Ed Caesar, "How Syria Became the Middle East's Drug Dealer," *New Yorker*, November 4, 2024.

[86] "HTS/New Syrian government Fight Against Captagon Database," created by Aaron Y. Zelin, last updated March 16, 2025.

[87] Ibid.

[88] Caroline Rose, "How Assad's Trade in Captagon Fueled His Downfall," New Lines Magazine, January 23, 2025.

[89] Ibid.

[90] Ibid.

[91] Ibid.

[92] Ibid.

[93] Ibid.

[94] Ibid.

[95] Aaron Y. Zelin, "Diary of the Syrian Transition - March 21, 2025," Jihadology+, March 21, 2025.

[96] Devorah Margolin, "Syria Crisis Leaves Islamic State Prisons and Detention Camps Vulnerable," Washington Institute for Near East Policy, December 9, 2024.

[97] See statements from the SNA and SDF about their continued fighting on the Syrian National Army's official Telegram channel and the Syrian Democratic Forces official website.

The Rising Threat of Non-State Actor Commercial Drone Use: Emerging Capabilities and Threats

By Jake Dulligan, Laura Freeman, Austin Phoenix, and Bradley Davis

Advancements within the commercial drone industry continue to reflect a double-edged sword: one of awe-inspiring innovation coinciding with increased vulnerabilities and threats. While their technology and capabilities offer tremendous advantages to civilians in photography, agriculture, construction, and a plethora of other fields, their weaponization by both state and violent non-state actors highlights the need for comprehensive regulatory frameworks and proper counter-unmanned aerial systems (C-UAS) defense mechanisms. The convergence of cheaper commercial drones, GPS-guided flights, autonomous swarms, and do-it-yourself (DIY) payload capabilities have amplified the asymmetric effects of these systems, with the United States continuing to focus significant resources to defend against such cheap systems. The authors use a quantitative dataset of 22 DJI drones sold from 2013 to 2024 to assess the performance evolution of these commercial drone models. The biggest concern in their view is that drone swarms could dramatically increase the impact of bad actor drone operations, be it kinetic strikes, ISR, or psychological warfare. To effectively mitigate and navigate this evolution, there is an urgent need for policymakers, the military, and the defense industry to prioritize governance and defense against drone threats for the future, investing in research and producing cost-effective C-UAS technologies to outpace the threat going forward. Failure to address these challenges will pose significant security risks, undermining both U.S. national security and public safety.

In recent years, the proliferation of drone technology by violent non-state actors (VNSAs) has revolutionized modern warfare, introducing a new dimension to the security landscape and allowing VNSAs such as the Islamic State, Hamas, and the Houthis to project force in the sky. The accessibility and versatility of commercial-off-the-shelf (COTS) drones have allowed VNSAs to attempt assassinations and carry out bomb-drop attacks, kamikaze strikes, and intelligence, surveillance, and reconnaissance (ISR) missions with drones that cost just a few hundred dollars and can be ordered on consumer sites such as Amazon and eBay. VNSAs modify these drones to suit their operational needs, adding explosive payloads and munitions to carry out attacks using previously advertised 'hobbyist' drones. This threat continues to grow. Nation-states, as seen in Ukraine and Russia, have also replicated VNSAs' drone tactics in armed conflicts. Current counter-unmanned aerial systems (C-UAS) technology is also struggling to combat the threat of commercial drones.[1] These C-UAS systems can be expensive as well as ineffective against the smaller, lower-flying drones, leading to false alarms and missed threats.[2] The proliferation of COTS drone technology has highlighted the importance of an evaluation of the future of C-UAS strategies for the future.

In this article, the authors first provide background on the motivation behind the use of drones by VNSAs. Next, they explore the rapidly expanding capabilities of commercially available drones and then analyze the increased threat space due to use of commercial drones by VNSAs. Lastly, the authors examine emerging technology trends and how they may shape the future use of drones by VNSAs as well as reflect on the need for comprehensive policies and capabilities to counter UAS systems.

VNSAs and the Attractiveness of Drones

Drones provide VNSAs with robust capabilities to conduct operations and advance their agendas. Non-state actor drone use primarily encompasses kinetic strikes on both hard and soft targets, and ISR. VNSAs such as the Islamic State and Hamas have hit targets in the form of "bomb drop" drones, which drop a payload from above onto a target. Typically, payloads include 40mm munitions dropped from a DIY payload release system.[3] VNSAs such as the Houthis and Hezbollah have conducted attacks using kamikaze drones loaded with munitions, flying directly into the specified target.[4] In an open-source study on the use of armed UAVs by non-state actors conducted by Håvard Haugstvedt, 1,122

Jake Dulligan is a Research Assistant at the Virginia Tech National Security Institute, working within the Intelligent Systems Division.

Dr. Laura Freeman serves as the Deputy Director of the Virginia Tech National Security Institute and has a distinguished background, having previously held roles as Assistant Director of the Operational Evaluation Division at the Institute for Defense Analyses and Acting Senior Technical Advisor for the Director of Operational Test and Evaluation (DOT&E).

Dr. Austin Phoenix is the Director of the Mission Systems Division at the Virginia Tech National Security Institute. His prior experience includes supporting the Defense Advanced Research Projects Agency (DARPA) and serving as a Research Scientist at the Naval Research Laboratory.

Dr. Bradley Davis is a Research Associate Professor in the Spectrum Dominance Division at the Virginia Tech National Security Institute.

incidents were recorded from 2006-2023. During this time, 91.3 percent of all attacks occurred in the Middle East and North Africa, with 1,109 out of the 1,122 occurring after 2016. The study highlights a major surge in 2017, with 252 attacks, primarily from the Islamic State's defense of Mosul and Raqqa. The number of attacks then dropped to 35 in 2018, but rose steadily in the following years: 129 in 2019, 105 in 2020, 206 in 2021, 116 in 2022, and peaking at 265 in 2023, the highest amount recorded in the study.[5] As this study demonstrates, VNSA armed drone use has seen a volatile uptick in usage in the last decade, and this trend is likely only to continue to increase as other non-state actors such as the cartels expand their capabilities.

Drone use by VNSAs poses a significant threat as it provides these groups with a versatile platform with capabilities to achieve several operations. Drones provide VNSAs with an additional tool to accomplish their strategic, ideological, and psychological goals. Drones enable VNSAs to gain a presence within the air, granting them a ' miniature' air force, at extremely low costs. Moreover, the cost barrier to entry for recreational 'hobbyist' drones continues to decrease, even as drones continue to see significant performance increases in their capabilities. Commercial and hobbyist drones also require minimum training by operators. COTS drones typically require no training to learn how to fly, and there are numerous instructional videos and forums that operators can learn from online.

Drones enable stand-off operations, with the distance from which attacks can be launched by VNSAs growing.[6] Future advancements in technological capabilities will continue to generate new challenges as well. GPS waypoint missions, multi-sensor control systems, and swarming techniques represent just a few of the developing challenges for the future of C-UAS defense. Drones give VNSAs a symbolic presence within sovereignty. As air power has traditionally been associated with statehood and sovereignty, drone use by VNSAs allows them to enter and in some cases attempt to control sovereign air space.[7] An example of this can be seen with the Islamic State and the battle of Mosul, U.S. General Raymond A. Thomas III recalled: "There was a day [in early 2017] when the Iraqi effort nearly came to screeching halt, where literally over 24 hours there were 70 drones in the air … At one point there were 12 'killer bees,' if you will, right overhead and underneath our air superiority … and our only available response [at the time] was small arms fire."[8]

Drones provide VNSAs with a low-risk, high-reward operation system. If the drone is shot down, the group loses a few hundred dollars and potentially the operator may be exposed. Although C-UAS defense does not typically have a high cost-per-shot ratio, the initial procurement costs of C-UAS defense can be significant, as a majority of systems cost over $100,000 and newer electronic warfare (EW) systems can cost into the hundreds of millions.[9] It is also important to note that in Håvard Haugstvedt's updated 2024 study on non-state actor drone use, there has been a notable shift in targets selected by non-state actors. In the full dataset from 2006 to 2023, 57.8 percent of UAV attacks were directed at hard targets, citing a substantial decrease from the 71.4 percent hard targets reported in the 2020 article.[10] Even with improved C-UAS defense from a military posture, this 13.6 percent decrease over 4 years underscores the shifting tactics on VNSAs, and therefore it is important to highlight the increasing trend of "soft" civilian targets being chosen by VNSAs, presenting new challenges for security and countermeasures in C-UAS defense.

Drone Capabilities

As advancements in the recreational and commercial drone industry are made, VNSAs' drone capabilities will likely continue to improve. DJI is currently the global leader in the commercial drone industry capturing over a 70% share of the total drone market, and DJI's drone models performances have indicated rapid capability advancements.[11] Moreover, DJI drones have also been used by both VNSA and nation-states in weaponized conflicts. DJI Phantoms were the drones of choice for the Islamic State and its 'bomb-drop' drones, as these drones are easily accessible, cheap, modifiable and can perform the needs of most VNSA.[12] DJI had to suspend operations in Ukraine and Russia as their models were being used across the battlefield for both kinetic strikes and ISR.[13] Therefore, the authors use DJI models as a quantitative benchmark dataset to demonstrate the increasing performance capabilities of these drones over the past decade, assessing the improvements in the drones speed, distance, and flight duration.

In the following analysis the authors use 22 models from their dataset of DJI drones sold from 2013 to 2024,[14] as a quantitative evaluation of performance improvements in drones. These models include the DJI Phantom, Mavic, Mini, Avata, Air, Inspire, FPV, Spark, Agras, Matrice and FlyCart 30 models. In this dataset, the authors compiled their quantitative data regarding drone specifications from the manufacturer, DJI's website. All data regarding the models other than payload capacity were collected from each drone model's specification page. DJI does not provide information regarding their drones' model's payload capacity, other than the DJI Agras and Fly Cart 30 as these are payload-specific models. Regarding the payload capacity of each drone model, the authors collected open-source data available online through hobbyists and 3rd parties who have tested each drone's payload capacity. Notably, DJI conducts its performance testing in optimal sites with minimal interference. Therefore, in urban environments, these numbers may vary, but the intent here is to capture trends in performance improvements. To keep a standard across the board for their analysis, the authors used the FCC-compliant capabilities for each drone.

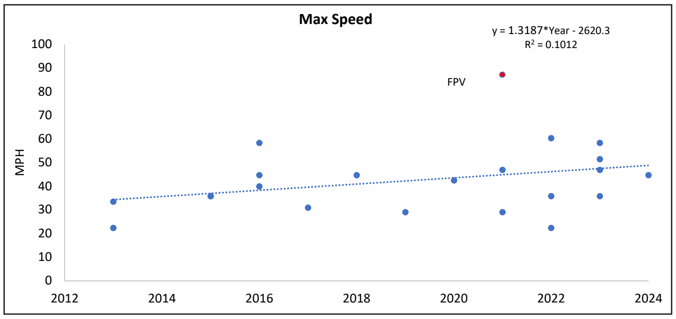

Figure 1: DJI Drone Dataset Max Speed

In the dataset of 22 DJI drone models, the average max speed increase for DJI drones was about 1.32mph per year (Figure 1). The significant outlier in the data is the DJI FPV, plotted in red, which can reach top speeds up to 87 mph. Although this is an outlier for the dataset, it represents the future potential for other models to reach significantly higher speeds. Higher speeds mean shorter reaction times for C-UAS technology and responses. As speeds increase, the threat of bomb-drop and kamikaze drones also dramatically grows as defense systems have smaller windows of time to close the kill chain.

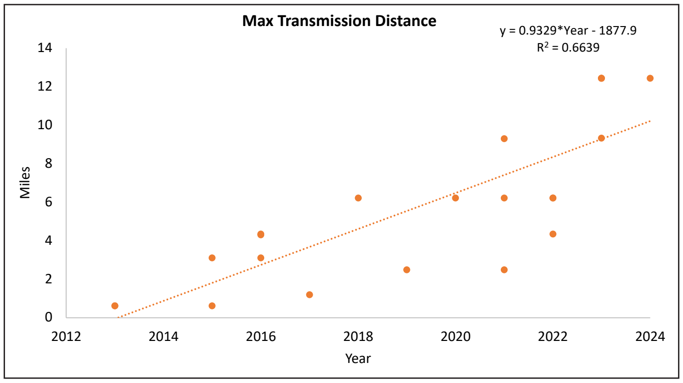

Figure 2: DJI Drone Dataset Max Transmission Distance

Regarding transmission distance, the 22 DJI drones demonstrated a 0.93-mile average increase per year (Figure 2). DJI's Phantom 1 model in 2013 had a transmission distance of 0.62 miles. In 2023, the DJI Air 3 and Mini 4 Pro both had transmission distances of 12.43 miles. In all DJI drones' performance capabilities, transmission distance saw the most operationally significant increase over the span from 2013-2024. This can easily suit the needs of nefarious actors, allowing threats to launch drones from a distance increasingly further away from their target. Although it will give more time for C-UAS detection, it could provide the threat actor with a smaller chance of operator identification.

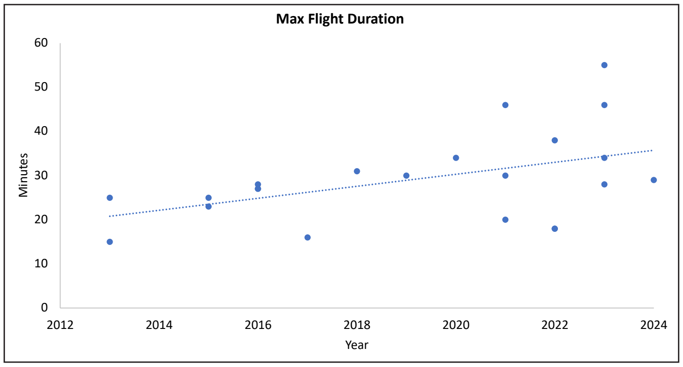

Figure 3: DJI Drone Dataset Max Flight Duration

Max flight duration has also increased by approximately 1.36 minutes per year (Figure 3). The increase in flight times for commercial drones can allow longer ISR missions for threat actors. Longer flight durations coinciding with longer transmissions can provide a significant advantage to VNSAs' ISR missions as they can reach further distances for longer times. The development and evolution of drone technology over the past decade demonstrates the increased threat opportunities VNSAs can pose with these recreational models.

The increasing availability, affordability, and capability of drones have also signaled a new era of potential threats characterized by coordinated drone swarm attacks, a fear that is being heavily researched by governments, militaries, and academia. Current research highlights the growing threat of drone swarms and swarm-like style attacks. In 2018, a group of experts from the National Academies of Sciences, Engineering, and Medicine determined that by 2025, the technologies necessary to deploy collaborative swarms of hundreds of drones will be widely available.[15] Iran demonstrated the impact of coordinated barrage attacks with the use of 170 drones in its April 14, 2024, attack on Israel.[16]

"In the future, VNSAs could use drone swarms to dramatically increase the impact of any of their drone operations, be it kinetic strikes, ISR, or psychological warfare."

Drone swarms, the coordinated use of drones with minimal human intervention through the use of algorithms and sensors, can range from just a few to over thousands.[17] Coordinated drone swarms operate with real-time communication, often employing artificial intelligence for predetermined flight paths and are controlled by a central operator.[18] Swarm-like tactics, on the other hand, are usually used by multiple operators with little automation and communication between the drones, relying on communication amongst the operators. This technology is being widely demonstrated through the use of commercial drones for "drone shows," and in 2024, the company Sky Elements set the world record using 5,000 drones in a single show.[19] Drone swarm technology is researched within academia, government, and the military, with projects analyzing their capabilities to assist in commercial purposes but also in nefarious use. Academic research highlights the nature of drone swarms, including communication methods, the future outlook of commercial drone swarm uses, and analyses of drone swarms being used by states in modern conflicts like Azerbaijan-Armenia and Ukraine-Russia.[20] States have also begun significant testing on drone swarm capabilities, as the U.S. Navy has conducted reconnaissance and bomb-drop tests, China has tested the launch and employment of multiple small UAS (sUAS) in swarm formations from both ground-based and airborne launchers, and Iran has tested the capability to strike 50 targets simultaneously.[21] In an outlook on the future of drone swarms, "a single operator from the ground can control hundreds of drones which can fly hundreds of [kilometers]. They have the capability to carry payloads of 1 [kilogram] each. They can spend about an hour on a target mission."[22]

In the future, VNSAs could use drone swarms to dramatically increase the impact of any of their drone operations, be it kinetic strikes, ISR, or psychological warfare. Hamas used drone swarm tactics to attack Israel in 2023.[23] In 2018, militants in Syria weaponized more than a dozen COTS drones in a swarm-like attack on a Russian airbase.[24] The authors believe this emerging capability represents the greatest potential threat in future VNSA drone operations. Countering drone swarms requires significant defense technology, and as U.S. Colonel Jonathan B. Bell states: "Although DOD's current counter small UAS strategy identifies the threat of drone swarms, it does not adequately address how DOD must overcome the technology risks of high cost and sluggish innovation to counter them."[25] Drone swarms will likely continue to allow VNSAs to portray a significant force within airspace, allowing them to use these swarms against both hard and soft targets to advance their agendas. The future of autonomous drone swarms is one of the most potent C-UAS challenges to be faced within the coming years. The next section examines how the increased capabilities of commercial drones are translating into threats.

Increased Threat Use of Commercial Drones

VNSAs increasingly have the ability and sophistication to strike military and civilian targets with commercial drones. A study by RAND Corporation analyzing small UAS (sUAS) potential nefarious actor capabilities found that of the commercial small UAS (sUAS) market in 2020, 23% (332) of sUAS are capable of conducting ISR missions, 4% (53) conveyance, 5% (72) kamikaze explosive attacks, and 6% (84) chemical, biological, or radiological (CBR) attacks. The study also noted that if speed is less of a concern, the number of drones capable of kamikaze attacks substantially rises.[26] These percentages are only continuing to rise as increased drone technology and performance become widespread within the market.

The authors' dataset indicates that the percentage of drones capable of becoming bomb-drop drones is high. A study analyzing Islamic State bomb-drop drones found that 49.6% out of 121 strikes used 40mm grenades.[27] Bomb drop-drones do not need high speeds or heavy payloads, as a 40mm munition grenade weighs about 225g or .50 lbs.[28] Open sources show Ukrainian soldiers dropping mortar rounds, RGD-5 grenades, and 82mm mines from commercial drones against Russian tanks and manpower.[29] Of the 22 DJI Drone models in the authors' drone dataset, 20 (91%) of the drone models can carry a payload greater than 225g, the weight of a 40mm hand-grenade. These models are extremely accessible in the open market. A quick search online found many of these drones on Amazon, eBay, and DJI's website for less than $1,000. In the dataset of DJI drones, 12 of the 22 (55%) would be capable of carrying a 1.25lb or 575g payload of C-4. It is important for the counterterrorism community to anticipate the threats this could pose. One danger is that it could be used by VNSAs to land on a target for a remote detonation. The proof of concept was demonstrated in 2015 when an anti-nuclear protester landed a drone on the Japanese Prime minister's office roof with trace amounts of radiation in a water bottle payload.[30]

DJI's latest drone delivery model, the DJI FlyCart 30, costs $16,950 and can carry a payload of up to 40,000g or 88lbs. This drone, on dual battery mode, can fly with a 66lb payload up to 9.94 miles.[31] For a relatively small price, this drone can carry a significant payload to be used in either bomb-drop or kamikaze attacks by VNSAs, upgrading them from the previously used 40mm munition and mortar rounds, reaching capabilities similar to military-grade drones. The DJI Agras drone was developed in 2021 and is equipped with spraying and spreading technology for use in agriculture. The drone is equipped with sprinklers and can carry a full operating payload of 40kg.[32] Again, it is important for the counterterrorism community to anticipate risks this could pose. In the hands of a non-state actor, this drone could be used in a chemical attack, utilizing the drone's sprinkler system and payload to disperse chemicals over a target.

Future Challenges

The performance capabilities of commercial drones are only continuing to advance, and the trend in drone weaponization is likely to persist given the recent success of commercial drones being used in warfare. COTS drones have afforded VNSAs with the ability to strike and target increasingly more challenging and secure targets. As a result, it is imperative to develop strategies to mitigate the potential threats posed by VNSAs who operate these drones.

> **"A near-term threat is a single operator who can launch hundreds of autonomous drones onto a target, commanding the drone to hover in place, and then activate a DIY payload system with munitions."**

There is a wide array of countermeasures currently available to combat both commercial and military drone threats. However, new drone technology and threat actor tactics are likely to outpace countermeasure development. It is also important to note that there is no one universal countermeasure that can adequately respond to all drone threats. Current countermeasures typically require a multi-faceted approach comprising various detection and mitigation technologies.[33] Detection technologies focus on the identification and tracking of hostile drone threats, including radar, radiofrequency (RF), infrared, electro-optical, and acoustic sensors. Mitigation technologies focus on the neutralization of a drone once it is identified, targeting the drone itself through kinetic attack, such as Anduril's approach. This includes systems using RF jamming, spoofing, nets, high-powered microwaves, and high-energy lasers. Additionally, integrated detect and defeat combined systems are capable of both identifying and mitigating hostile drones in a given environment.

Proper C-UAS defense requires the successful integration of multiple platforms and systems across the board, as Colonel Michael Parent, Joint Counter-Small Unmanned Systems Office's Acquisition Division Chief, recalled during the JCO's fifth C-UAS demonstration: "So what we saw was that you really do need a full system-of-systems approach, a layered approach, because we're talking about a very large profile, 50 or more [threats] … coming out from different angles, different speeds and different sizes."[34] This requires significant manpower, expertise, and financing, a challenge currently seen by both the United States military and law enforcement.

As commercial drones advance in capability, so too will the threat of their use by nefarious actors. One major concern for the future is autonomous drones guided by GPS waypoint missions. These drones are immune to RF jamming as they operate without an RF link, as well as allow the operator to leave the launch area upon takeoff. Drone flights by GPS waypoints are continuing to develop in efficiency and are already highly accessible at the commercial and hobbyist level. GPS spoofing can also be countered by having a more complex control algorithm that does not simply rely on GPS data.[35] A near-term threat is a single operator who can launch hundreds of autonomous drones onto a target, commanding the drone to hover in place, and then activate a DIY payload system with munitions.

Fixed-wing commercial drones—drones that are manufactured similarly to crewed aircraft with fixed wings and launched via runways, catapults, and vertical take-offs—are also a plausible threat of the future. Fixed-wing commercial drones have not yet been used on a large scale by VNSAs; however, they have been successful in the Ukraine-Russia war with commercial models such as the Skyeye and SupercamS350 being deployed as both one-way attack and multi-use drones.[36] Fixed-wing drones can operate at higher speeds, longer ranges, and longer flight times compared to their quadcopter counterparts. These drones are also widely available at the commercial level and are typically used for land surveying and mapping. They are also highly effective for kamikaze scenarios. As these drones can achieve higher speeds and longer ranges, they offer another accessible threat to the commercial drone market. VNSAs such as the Houthis have extensively used fixed-wing military grade drones, including the Iranian Shahed (Waid), to participate in what Don Rassler has highlighted as "long range stand-off terrorism," enabling VNSAs to conduct attacks on targets hundreds of miles away.[37] A direct example of this form of terrorism can be seen with the Houthis striking Tel Aviv from Yemen with a Iranian-made Samad-3 model on July 19, 2024, killing one and injuring four.[38] VNSAs taking notes from Russia and Ukraine's drone strategies can easily shift these groups toward commercial versions of these fixed-wing drones for kamikaze attacks and should be acknowledged as a future threat area.

Another concern for the future is the hardening of drones by threat actors against electronic warfare C-UAS technologies. Currently, it is simply more cost-efficient to purchase more COTS drones rather than harden them. Stronger transmitters may require more battery power to operate. Improved antennas can also weigh more, resulting in the drones' performance capabilities experiencing a notable decrease. This reality has been widely demonstrated in Ukraine-Russia, where both sides have opted to continue purchasing cheap, commercial-off-the-shelf drones versus hardening existing supplies. These drones, on average, last approximately three missions before being destroyed.[39] This trend is likely to continue in the coming years; however, as with all technologies this can be subject to change with reduced costs and improved capabilities. The hardening of commercial drones against C-UAS technologies can pose a significant challenge for C-UAS defense in the future if the technology and capability become widespread and affordable.

Another concern is the potential for threat actors to build their own drones. This capability would allow VNSAs to build these drones specifically to meet their own needs, be it heavier payloads, longer transmission ranges, faster speeds, etc. An example of this can be seen through the transmission range. The commercial drone industry keeps its transmission range standards compliant with both the FCC (United States) and CE (Europe) in their drones. However, by building their own drones, threat actors could purchase their own transmitters and receivers to achieve this goal of maximizing the drones' transmission range past compliance standards.

Conclusion

As seen over the last decade, drones are a new phenomenon of modern warfare. Drones have been widely deployed in the Middle East, by VNSAs such as the Islamic State, Hamas, and the Houthis, but also by nation-states like Ukraine and Russia, which have demonstrated the potential impact drones will continue to have on modern warfare. Drones have been used in a variety of operations, ranging from bomb-drop strikes, ISR missions, artillery guidance, and kamikaze attacks. This is likely just the tip of the iceberg. As drone swarms and artificial intelligence technologies increase and continue to develop in tandem with one another, both state militaries and VNSAs will likely develop new capabilities and tactics.

As demonstrated by Figures 1-3, the advance of commercial drone technology is offering bad actors ever greater threat opportunities. As these commercial models continually see improvements in speed, flight duration, and transmission distance one can confidently assume that VNSAs will take advantage. The 22 DJI drones selected represented these frightening opportunities, as VNSAs can easily tailor specific models to achieve kamikaze attacks, coordinated swarms, and significant ISR missions. VNSAs have recognized the success and potential of future capabilities in drone operations, and it is crucial to acknowledge the advancements that are being made in the drone industry that can assist these operations, and the challenges in addressing them.

In 2021, the Department of Defense released its initial Counter-Small Unmanned Aircraft Systems Strategy, focusing on enhancing the joint force through innovation and risk-based investments, material and non-material solutions, and international partnerships.[40] This strategy provides a crucial foundation for the future of C-sUAS defense for the U.S. military; however, as advancements in the drone industry continue, it is imperative that this strategy remains fluid and adaptive. The DoD has already proven this to be the case, as in 2024 then Secretary of Defense Lloyd Austin signed a classified Strategy for Countering Unmanned Systems that "unifies the Department's approach to countering these systems that looks across domains, characteristics, and timeframes."[41] As previously noted, VNSAs have increasingly targeted soft targets within the last four years, and if this trend continues, the Defense Department must successfully continue to adapt this strategy to meet the needs of its federal, state, and local public safety counterparts. CTC

Citations

[1] Vikram Mittal, "The Challenges of Counter-Drone Technology as Seen in Recent Conflicts," *Forbes*, October 19, 2023.

[2] Audelia Boker, "Counter-Uas Technology: Misconceptions & Reality," Sentrycs Counter Drone Solutions, November 6, 2024; Bruno Oliveira Martins, Arthur Holland Michel, and Andrea Silkoset, "Countering the Drone Threat: Implications of C-Uas Technology for Norway in an EU and NATO Context," Peace Research Institute Oslo, 2020.

[3] Seth Frantzman, "Why 2024 is the 'Year of the Drone' After Iran's Attack on Israel," MSN, June 1, 2024.

[4] Ibid.

[5] Håvard Haugstvedt, "Still Aiming at the Harder Targets: An Update on Violent Non-State Actors' Use of Armed UAVs," *Perspectives on Terrorism* XVIII:1 (2024).

[6] Don Rassler, *Going the Distance: The Emergence of Long-Range Stand-off Terrorism* (West Point, NY: Combating Terrorism Center, 2024).

[7] Elise Archambault and Yannick Veilleux-Lepage, "Drone Imagery in Islamic State Propaganda: Flying Like a State," *International Affairs* 96:4 (2020): pp. 955-973.

[8] David Larter, "SOCOM Commander: Armed ISIS Drones Were 2016's 'Most Daunting Problem,'" Defense News, August 18, 2022.

[9] Kelley M. Sayler, Andrew Feickert, and Ronald O'Rourke, "Department of Defense Directed Energy Weapons," August 22, 2023; Martins, Michel, and Silkoset.

[10] Haugstvedt.

[11] Neil Anwar, "World's Largest Drone Maker is Unfazed - Even if it's Blacklisted by the U.S.," CNBC, February 8, 2023.

[12] Samuel Bendett, "Mass-Market Military Drones Have Changed the Way Wars Are Fought," Center for a New American Security, accessed July 9, 2024.

[13] Ulrike Franke, "Drones in Ukraine and Beyond: Everything You Need to Know," European Council on Foreign Relations, August 11, 2023.

[14] "DJI - Official Website," DJI Official, August 2024.

[15] "Counter-Unmanned Aircraft System (CUAS) Capability for Battalion-and-Below Operations (Abbreviated Version of a Restricted Report)," Board on Army Science and Technology, Division on Engineering and Physical Sciences, National Academies of Sciences, Engineering, and Medicine, 2018.

[16] Joshua A. Schwartz, "What Iran's Drone Attack Portends for the Future of Warfare," Modern War Institute, West Point, April 30, 2024.

[17] "Science & Tech Spotlight: Drone Swarm Technologies," U.S. Government Accountability Office, September 14, 2023.

[18] Ibid.

[19] "Sky Elements Flies 5,000 Drone Show with Uvify in Mansfield," Sky Elements, November 30, 2024.

[20] Jonathan B. Bell, "Countering Swarms: Strategic Considerations and Opportunities in Drone Warfare," National Defense University Press, October 24, 2022.

[21] Ibid.

[22] "How Drone Swarm System Works: What Is Drone Swarm?" RF Wireless World, n.d.

[23] Kenia Chávez and Ori Swed, "How Hamas Innovated with Drones to Operate Like an Army," Bulletin of the Atomic Scientists, November 1, 2023.

[24] Jeff Daniels, "Russia Says It Killed Rebels Behind Swarm Drone Attack in Syria, but Experts See More Such Strikes Ahead," CNBC, January 13, 2018.

[25] Bell.

[26] Brian Wilson, Scott Tierney, Brian Toland, Rachel M. Burns, Jan Osburg, Michael D. Ziegler, Rasool Khan, Michael Nixon, Christopher S. Adams, and Christian Steiner, "Small Unmanned Aerial System Adversary Capabilities," Rand Corporation, March 12, 2020.

[27] Nick Waters, "Types of Islamic State Drone Bombs and Where to Find Them," Bellingcat, May 24, 2017.

[28] "40mm Low-Velocity Grenades," Gary's U.S. Infantry Weapons Reference Guide, n.d.

[29] Pariesa Brody and Pierre Ayad, "Ukrainian Soldiers Are Turning Consumer Drones into Formidable Weapons of War," France 24, August 8, 2022.

[30] "Update 3-Drone with Minuscule Quantity of Radiation Found on Japan PM's Office Roof – Media," Reuters, April 22, 2015.

[31] "DJI FlyCart 30," DJI Official, n.d.

[32] "DJI Agras T40," DJI Official, n.d.

[33] "10 Types of Counter-Drone Technology to Detect and Stop Drones Today," Robin Radar Systems, n.d.

[34] Joe Lacdan, "Joint Counter-Small UAS Office Conducts Successful Counter Drone-Swarm Demonstration," U.S. Army, July 27, 2024.

[35] Princess Chimmy Joeaneke, Onyinye Obioha Val, Oluwaseun Oladeji Olaniyi, Olumide Samuel Ogungbemi, Anthony Obulor Olisa, and Oluwaseun Ibrahim Akinola, "Protecting Autonomous UAVs from GPS Spoofing and Jamming: A Comparative Analysis of Detection and Mitigation Techniques," *Journal of Engineering Research and Reports* 26:10 (2024).

[36] Stacie Pettyjohn, "Evolution Not Revolution," Center for a New American Security, February 8, 2024.

[37] Rassler.

[38] Rami Amichay, "Tel Aviv hit by drone attack claimed by Iranian-backed Houthis," Reuters, July 19, 2024.

[39] Ibid.

[40] "Counter-small Unmanned Aircraft Systems Strategy," U.S. Department of Defense, 2021.

[41] "DoD Announces Strategy for Countering Unmanned Systems," U.S. Department of Defense, December 5, 2024.

Into the Crowd: The Evolution of Vehicular Attacks and Prevention Efforts

By Alexandre Rodde and Justin Olmstead

In recent months, there have been a series of vehicular attacks in Germany, the United States, and Israel targeting civilians during celebrations and public gatherings. This is representative of an increase in the use of the tactic. Following the Nice and Berlin attacks in 2016, vehicular ramming terrorist attacks in North America and Europe reached a peak in 2017, before subsiding with the waning of the international terror threat posed by the Islamic State and its supporters. Of the 18 terrorist vehicular ramming attacks between 2014 and March 2025, 15 (83%) were carried out by jihadis and three (17%) by right-wing extremists. Since 2016, governments and security practitioners have focused significant attention on protecting against the vehicle-ramming threat to pedestrianized areas, bringing in new technologies. Yet, the relative ease of launching a vehicle attack and the very large number of soft targets available means it is a tactic that is very difficult to defend against. When it comes to indicators and warnings of future attacks, the demonstration effect created by high-casualty vehicle-ramming attacks has in the past seemingly produced a surge in copycat attacks, which means the security agencies should be particularly vigilant given the recent uptick in high-profile attacks, including the New Orleans attack.

Five recent mass-casualty attacks underline the continued threat posed by the vehicle-ramming terrorist tactic. On December 20, 2024, Taleb Jawad Al-Abdulmohsen, a 50-year-old Saudi psychiatrist and self-professed atheist and anti-Islamist,[1] drove his rented BMW X3 around the Magdeburg Christmas Market in northeast Germany. Using an emergency escape road set up by local law enforcement,[2] the perpetrator was able to drive into the crowd for 400 meters, killing six and injuring 299.[3]

Eleven days later, Shamsud-Din Jabbar, a U.S. veteran from Texas, drove a Ford F-150 Lightning pickup truck flying an Islamic State flag into pedestrians celebrating New Year's Eve on Bourbon Street in New Orleans, Louisiana.[4] Crashing his vehicle after 400 meters, he opened fire on the crowd before being neutralized by law enforcement officers. Fourteen people were killed and 35 were injured during the attack.[5]

A few weeks later, on February 13, 2025, Farhad Noori, a 24-year-old Afghan national, rammed his Mini Cooper into a union demonstration close the Munich train station. Two people—a mother and her two-year-old daughter—were killed and 37 others were injured before the suspect was arrested by German law enforcement. Noori was known to share Islamist content online; he screamed "Allah Akbar" multiples times as he was arrested.[6]

A further two weeks later, in a terrorist attack on February 27, 2025, a 53-year-old Palestinian driver injured 13 people at a bus stop in Israel before being neutralized by Israeli law enforcement.[7]

Most recently, on March 3, 2025, in Mannheim, Germany, a 40-year-old German national with mental health challenges drove his car into a crowd, before fleeing. The attack killed two people and injured 11 others. The driver then attempted suicide using an alarm pistol in his car, before being detained.[8]

This article explores the characteristics of vehicular attacks, with part one discussing the tactical advantages they offer to the assailants both during the preparation of attacks and in their execution. The second part of the article discusses the evolution of the threat, and the third part examines the evolution of prevention efforts.

Characteristics of Vehicular Attacks

Vehicle-ramming tactics, and efforts to stop them, are far from a new phenomenon and were first observed in Israel in the early 1970s and have more recently been a regular feature of Islamic State terrorism in the West.[9] Vehicular attacks are, by definition, a low-skill and low-tech *modus operandi*. Most individuals are familiar with the use of a motor vehicle, and no technical knowledge is required outside of the target selection phase of the attack. Access to a vehicle can be gained through various means such as theft (as seen in Berlin in 2016 where Anis Amri stole the truck he used to target the Breitscheidplatz Christmas Market)[10] or taken from work (as seen in an attack in Jerusalem in 2008 involving a bulldozer).[11]

In other cases, assailants have used their personal vehicles during

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

Justin Quinn Olmstead, Ph.D., is a historian for Sandia National Laboratories in Albuquerque, New Mexico. Prior to that, he was Associate Professor of History at the University of Central Oklahoma. His most recent book is From Nuclear Weapons to Global Security: 75 Years of Research and Development at Sandia National Laboratories. He is a Resident Fellow at the CMC, a Senior Research Fellow at the Armed Services Institute in the Center for Military Life, Thomas University, Visiting Fellow at the Center for Peace & Security, Coventry University, U.K., and an Associate Editor for the Journal of the Society for Terrorism Research.

attacks, as seen as in a car-ramming attack in Munster, Germany, in 2018[12] and Waukesha, Wisconsin, in December 2021.[13] In numerous cases, perpetrators rented—at no significant cost—the vehicles they used in attacks. For example, Mohamed Lahouaiej-Bouhlel, who carried out what remains the deadliest vehicular attack in history in 2016 in Nice, France, rented a truck for a few thousand euros.[14] The rise of vehicle-sharing apps, similar to the one used by the New Orleans attacker, can reduce the cost of obtaining a vehicle while at the same time allow perpetrators to avoid whatever scrutiny they might face from commercial car renting companies.[a]

Perpetrators of vehicular attacks also have access to a vast number of potential targets given the growth of pedestrianized areas in urban centers and of open-air gatherings following the COVID-19 pandemic. Despite attempts by authorities to protect certain zones where there is high foot traffic, it remains all too easy for perpetrators to find targets. According to an examination by the authors of mass casualty attacks in the West between January 2012 and December 2022—defined as attacks in which four or more victims were killed—vehicular ramming was the second most common method used after mass shootings.[15]

Vehicular attacks also have a particularly shocking component, due to their speed and kinetic force and the fact that they occur in highly vulnerable pedestrian spaces. This facilitates an important aspect of terrorism: media coverage, especially if images or videos of the attack are posted online or broadcast. In the case of the Magdeburg attack, CCTV images immediately spread on social media in the minutes following the attack, before being broadcast on traditional channels. Some assailants seek to maximize the media impact, with one example being the New Orleans attacker flying an Islamic State flag at the back of his attack vehicle.[16]

Countering vehicular attacks is hugely challenging. Potential targets are numerous, changing in number according to seasonal activities, events, or time of day. The type of vehicle used by attackers will also impact the type of protection that needs to be set up, according to speed, weight, size, and special capacity in the case of a weaponized excavator or bulldozer. Detection of potential attackers is also made difficult because of the number of vehicles in urban areas and because of the usual absence of criminal acts in the preparation of attacks. In the Magdeburg, New Orleans, and Munich attacks, the intention of the perpetrators was only clear to law enforcement personnel at the moment the vehicle entered the restricted zones, just seconds before the attacks began.

On the response side, vehicular attacks are extremely fast-paced events with the immediate potential for a large number of casualties, including numerous polytraumatized victims who need immediate medical attention. The speed and impact of vehicular attacks sometimes resemble more of a large bomb attack than a mass shooting. The complexity of the victims' injuries presents challenges that go beyond the medical capacities of first responders.

The Evolution of the Threat

According to the University of Maryland's Global Terrorism Database, there were 288 incidents of vehicular terrorism from 1970 to 2020.[17] This number is focused on vehicles used as blunt-force weapons to attack civilians and does not include vehicle-borne explosives, or, in the case of Israel, against soldiers.

In 1973, Olga Hepnarová killed eight people in Prague when she drove her Praga RN truck into a group of pedestrians. Four years later, a man in his early 30s rammed his car into the stage during a Ku Klux Klan rally in Plains, Georgia, injuring some 30 people.[18] Seven years later, in 1984, an individual looking to "get even with the police" drove his car into a crowd in Los Angeles, killing one person and injuring 54 injured.[19] Similar attacks took place elsewhere in the world, including in Australia and Brazil.[20] From 1990 to early 2000, there were regular vehicular attacks in Israel and the West Bank, frequently targeting IDF soldiers at bus stops.[21] This method of attack continued and expanded in the 2010s, mostly used by lone operators organizing attacks without the support of a group. In a 2010 edition of the al-Qa`ida magazine Inspire, jihadi groups promoted such tactics due to their efficiency, calling followers to "mow down the enemies of Allah."[22] In the mid-2010s, there was an increase in Palestinian vehicular attacks in Israel and the West Bank,[23] at the same time a wave of Islamic State-organized and -inspired attacks started in Western Europe.[24]

In September 2014, Islamic State spokesman Abu Muhammad al-Adnani called for supporters to use vehicles as weapons, saying that if they were "not able to find an IED or a bullet," then they should "single out the disbelieving American, Frenchman, or any of their allies, smash his head with a rock, or slaughter him with a knife, or run him over with your car."[25] Just weeks later, on October 20, 2014, one of the group's supporters, Martin Couture-Rouleau, heeded the call in a vehicle attack that killed a member of the Canadian armed forces.[26] There were, however, no further terrorist vehicular ramming attacks in the West until a January 2016 attack on the French military in the town of Valence. (See Table 1 in the appendix.)

The watershed moment for the threat came on France's national day in 2016. At 10:32 PM on July 14, a 19-ton Renaud Midlum truck, driven by 31-year-old Tunisian jihadi named Mohamed Lahouaiej-Bouhlel, plowed into the crowd on the Promenade des Anglais in Nice, France, for more than a kilometer. Eighty-six people were killed and 458 were injured in the span of four minutes and 17 seconds, before the terrorist was shot dead by law enforcement. He had carefully organized his attack, using his job as a delivery man to rent the truck in advance, and practicing reconnaissance and driving in the area 11 times in the days preceding the attack.[27] In the years that followed the Nice attack, there was an increase in mass-casualty vehicular attacks in the West. (See Table 1.) Just five months after the Nice attack, in December 2016, another jihadi attack using a semi-trailer truck killed 12 people at a Christmas market in Berlin. As noted by Vincent Miller and Keith Hayward, "the VRA [vehicle ramming attack] has transitioned from being a relatively rare occurrence, to become, by 2016, the most lethal form of terror attack in Western countries, claiming just over half of all terrorism-related deaths in the West that year."[28]

The following year saw a surge in vehicular terrorist attacks in the West (defined for the purpose of this study as North America, Europe, Australia, and New Zealand), with seven attacks, the most seen in any year. (See Table 1.) These included mass-casualty attacks by jihadis in London in March 2017 (five killed, including four with a vehicle),[29] in Stockholm in April (five killed),[30] Barcelona in August (13 killed),[31] and New York in October (eight killed).[32]

[a] According to reports, the vehicle used by Shamsud-Din Jabbar in the New Orleans attack was rented via the car-sharing app Turo. Natalie Neysa Alund, "What is Turo? Car rental app was used in both New Orleans attack and Las Vegas explosion," USA Today, January 2, 2025.

It is noteworthy that there was a surge in vehicular terrorist attacks following the two deadliest attacks (Nice and Berlin). The authors assess that this created a demonstration effect in which the high casualties and significant media coverage of those attacks showed the effectiveness of this terror tactic and in turn produced a copycat effect. This suggests that the demonstration effect is a more powerful indicator of future attacks than calls by terrorist leaders such as the late Abu Muhammad al-Adnani for the tactic to be used.

The surge in vehicular attacks during this period was also seen in the developed world as a whole, to include Palestinian terrorism targeting Israel. Writing in 2019, Brian Michael Jenkins stated, "because there are relatively few events over a long period of time (more than 45 years), the trend lines can be misleading. However, the recent increase is obvious. There were 16 attacks between 1973 and 2007 and 62 attacks between 2008 and the end of April 2018. Thirty of these occurred in 2017 and the first four months of 2018 alone."[33] According to Brian Michael Jenkins and Bruce Butterworth, the use of vehicles as weapons of terror in developed countries increased from two in the years 1994-1997 to 68 in the period from 2014-2019.[34 b]

These tactics soon extended beyond the jihadi ecosystem to include attacks perpetrated by non-ideological attackers in Melbourne, Australia, in 2017 (six killed, 27 injured);[35] Munster, Germany, in 2018 (four killed, 20 injured);[36] Trier, Germany, in 2020 (five killed, 23 injured);[37] and Waukesha, Wisconsin, in 2021 (six killed, 62 injured). Far-right terrorists also applied the same tactics, in London, United Kingdom, in front of the Finsbury Park Mosque where one person was killed and 12 others were injured by Darren Osborne in 2017[38] and London, Canada, where a 20-year-old killed four members of a Pakistani family with his car in 2021.[39]

According to the authors' database, there were 18 terrorist vehicular ramming attacks between January 2014 and March 2025 in the West. The large majority of attacks were carried out by jihadis, many of whom were inspired by the Islamic State. Fifteen (83%) of the terrorist attacks were carried out by jihadis and three (17%) by right-wing extremists. Five of the attacks (28%) targeted the military, police, and security services.

Cars were most often used in the attacks. Thirteen of the attacks (72%) were carried out by cars, three of the attacks (17%) were carried out by trucks and two (11%) by vans. It is notable that the two highest casualty attacks were carried out by trucks—the Nice attack (86 killed and 458 injured) and the Berlin attack (12 killed, 56 injured)—underlining that this form of vehicular attack poses the greatest threat. Nine of the attacks (50%) were carried out by vehicles owned by the perpetrators, seven of the attacks (39%) were carried out in rented vehicles, and two (11%) were carried out in stolen vehicles, in both cases trucks.

A total of 152 people died in the 18 attacks. Demonstrating that attacks are highly likely to produce casualties after being launched, 12 (67%) of the attacks produced fatalities and only one attack resulted in no injuries.

As can be seen Table 1, with the waning of the Islamic State international terror threat, terrorist use of vehicular attacks dropped in the West from 2018 onward, before ticking up in 2025 with the attacks in New Orleans and Munich. Both these attacks, especially the New Orleans attack, received significant media coverage or, in other words, created a new demonstration effect that could lead to a surge in copycat attacks in the months ahead.

The Evolution of Prevention Measures

Beginning in the 1990s, there have been efforts in the United States to harden buildings and other critical infrastructure from vehicle-borne improvised explosive devices (VBIEDs).[40] In many cases, this had the added benefit of protecting pedestrians who use the sidewalks separating the street from commercial or government buildings. Security practitioners saw bollards as one means of hardening the landscape while not limiting the aesthetic value of the area. From the1990s, the use of bollards has been the preferred choice of protecting campuses and buildings in the United States. In the United States alone, 90,000 sites have added concrete bollards since the 1995 Oklahoma City bombing.[41]

Attempts to prevent any type of vehicular collision with pedestrians began as early as the 18th century with the use of wood and iron structures to direct pedestrians away from horse-drawn vehicles.[42] Preventative measures continued to be adopted in the form of streets and highways being designed around neighborhoods well into the 20th century.[43] As Paul Hess and Sneda Mandhan point out, in New York, prior to the 2017 vehicle-ramming attacks in Nice and Berlin, physical security of public spaces was focused on VBIEDs.[44] The U.S. Federal Emergency Management Agency did not provide any guidance on how to protect against vehicle ramming that was not delivered via VBIED.[45] Protection rested on diversion of vehicles from high pedestrian zones with the use of bollards and other physical barriers, or limiting access of vehicles and pedestrians to areas deemed critical.[46] According to the Mineta Transportation Institute, since 2012, preventative measures have evolved to include more technology, such as cameras, fencing, and effective intelligence gathering, to disrupt potential attacks.[47]

It was after the Nice and Berlin attacks of 2016 that governments and security practitioners in the West focused significant attention on protecting against the vehicle-ramming threat to pedestrianized areas. Governments and security practitioners began working on new prevention techniques. Traditional retractable traffic bollards were deemed no longer sufficient because they cannot withstand the impact of large trucks. Stronger protective measures were put in place, with, for example, the French company La Barrière Automatique (LBA) developing a retractable bollard capable of withstanding the impact of a 7.5-ton truck going 80 kilometers per hour (approximately 50 miles per hour).[48] The LBA model is deployed one meter above ground and another 1.70 meters below, providing an 'iceberg' protection effect. While traditionally delivering products for the French Vigipirate national security plan, LBA is seeing its customer base expand from embassies, industrial sites, and stadiums to communities and businesses such as shopping centers and supermarkets. Much like the LBA model, Intertex Barriers of Valencia, California, has developed a retractable barrier that can be manually operated or function autonomously.[49]

In recent years, the use of active, passive, deployable, or improvised vehicle-ramming mitigation tools became common practice.[50] Vehicle inspections and security checks at entry points, remote parking, and shuttle services have also helped in mitigating the risk as once an attack is underway, it is extremely difficult to stop because of the speed of the attack and the difficulty in bringing a moving vehicle to a stop. During the Nice attack, for example,

[b] The data includes all cases, including non-ideological ones, in OECD-signatory countries.

the killing was only stopped by the action of a civilian was able to throw his scooter in front of the 19-ton truck, slowing it down so that law enforcement officers were able to shoot and neutralize the terrorist.[51] The use of hollow point bullets by a majority of law enforcement agencies[52] is another impediment to stopping attacks in their tracks due to the deflection caused by the windshield.[53] The difficulty of responding to an active vehicular ramming attack underlines the importance of preventing attacks.

Conclusion

Vehicular attacks committed by terrorists are not a new phenomenon. As described in this article, this *modus operandi* has been used by lone actors and groups for decades around the world. The recent cases in Germany and the United States are not a return of the vehicular attacks in the West but rather an evolution of the *modus operandi*, using new technical tools such as the use of electric cars and peer-to-peer apps.[54]

The recent attacks do represent an uptick in the use of the tactic, however. Following the Nice and Berlin attacks in 2016, vehicular ramming terrorist attacks in North America and Europe reached a peak in 2017, before subsiding with the waning of the international terror threat posed by the Islamic State and its supporters. Of the 18 terrorist vehicular ramming attacks between 2014 and March 2025, 15 (83%) were carried out by jihadis and three (17%) by right-wing extremists. Most of the attacks involved cars but the two of the highest casualty attacks (Nice and Berlin) involved trucks, underlining that these forms of vehicular attacks pose the greatest threat. Most of the attacks produced fatalities and only one resulted in no injuries, demonstrating the high likelihood that vehicular ramming attacks will produce casualties once launched.

Since 2016, governments and security practitioners have focused significant attention on protecting against the vehicle-ramming threat to pedestrianized areas, bringing in new technologies. Protective measures such as using fixed or mobile bollards are key because once an attack is underway, it is very difficult to stop. But the facility of launching a vehicle attack and the very large number of soft targets means it is a tactic that is very difficult to defend against. Therefore, preventing attacks from being carried out in the first place through intelligence and law enforcement efforts is key but nonetheless challenging because an attack involving a vehicle can be planned and prepared with little risk of arousing suspicion.

When it comes to indicators and warnings of future attacks, the demonstration effect created by high-casualty attacks has, in the past, seemingly produced a surge in copycat attacks, which means that security agencies should be particularly vigilant in the months ahead given the recent uptick of high-profile attacks, including in New Orleans. CTC

Appendix: Table 1 - Terrorist Vehicular Attacks in the West since 2014

Date	Location	Perpetrator	Target	Ideology	Vehicle	Casualties
October 20, 2014[55]	Saint Jean sur Richelieu (Canada)	Martin Couture-Rouleau	Two Canadian Forces members	Islamic State inspired	Car (Nissan Altima, owned)	1 killed, 1 injured
January 1, 2016[56]	Valence (France)	Raouf El Ayed	French military members in front of a mosque	Islamic State inspired	Car (Peugeot 307, owned)	4 injured
July 14, 2016[57]	Nice (France)	Mohamed Lahouaiej-Bouhel	Bastille Day celebrations	Islamic State inspired	Truck (Renault Midlum, rented)	86 killed, 458 injured
November 8, 2016[58]	Columbus, Ohio (United States)	Abdul Razak Ali Artan	Students on a campus	Islamic State inspired	Car (Honda Civic, owned)	11 injured, including some stabbed
December 19, 2016[59]	Berlin (Germany)	Anis Amri	Christmas market	Islamic State inspired	Truck (Scana R 450, stolen)	12 killed, 56 injured
March 22, 2017[60]	London (United Kingdom)	Khalid Mansoor	People on Wesminster Bridge and in front of Westminster Palace	Islamic State inspired	Car (Hyundai Tucson, rented)	4 killed using the car, 1 killed by stabbing, 48 injured
April 7, 2017[61]	Stockholm (Sweden)	Rakhmat Akilov	Pedestrians on the Drottninggatan Street	Islamic State inspired	Truck (Mercedes Benz Actros, stolen)	5 killed, 15 injured
June 19, 2017[62]	Paris (France)	Adam Lotfi Djaziri	Gendarmes in a vehicle on the Champs Elysées	Islamic State inspired	Car (Renault Megane, owned)	None
June 19, 2017[63]	London (United Kingdom)	Darren Osborne	Muslims close to the Finnsbury Mosque	Right-wing extremism	Van (Luton Box, rented)	1 killed, 11 injured
August 9, 2017[64]	Levallois-Perret (France)	Hamou Benlatrèche	French military members	Islamic State inspired	Car (BMW Serie II, rented)	Six injured
August 12, 2017[65]	Charlottesville, Virginia (United States)	James Alex Fields Jr.	Protesters during a counter demonstration	Right-wing extremism	Car (Dodge Challenger, owned)	1 killed, 35 injured
August 17, 2017[66]	Barcelona (Spain)	Younes Abouyaaqoub	Pedestrians on the Ramblas	Islamic State inspired	Van (Fiat Talento, rented)	13 killed, around 130 injured
October 31, 2017[67]	New York, New York (United States)	Sayfullo Saipov	People on a bike path in Manhattan	Islamic State inspired	Car (Ford Super Duty, rented)	8 killed, 13 injured
August 14, 2018[68]	London (United Kingdom)	Salih Khater	People close to Westminster Palace	Global jihad	Car (Ford Fiesta, owned)	3 injured
April 27, 2020[69]	Colombes (France)	Youssef Thilah	French police officers	Islamic State inspired	Car (BWM Serie 1, owned)	3 injured
June 6, 2021[70]	London (Canada)	Nathaniel Veltman	Member of a Canadian-Pakistani family	Right-wing extremism	Car (Dodge Ram, owned)	4 killed
January 1, 2025[71]	New Orleans, Louisiana (United States)	Shamsud-Din Jabbar	People on Bourbon Street	Islamic State inspired	Car (Ford F150 Lightning, rented)	14 killed, 54 injured using the car, 3 shot
February 13, 2025[72]	Munich (Germany)	Farhad Noori	Demonstrators	Global jihad	Car (Mini Cooper, owned)	2 killed, 37 injured

Citations

[1] "The 'atheist' Saudi refugee suspected of Germany attack," Agence France-Presse, December 21, 2024.

[2] "Täter nutzte Fluchtweg – hat Sicherheitskonzept versagt?" T-Online, December 21, 2024.

[3] "Magdeburg Christmas market attack deaths rise to six," BBC, January 6, 2025.

[4] Brian Thevenot and Chris Kirkham, "Exclusive: New Orleans' planned new Bourbon Street barriers only crash-rated to 10 mph," Reuters, January 4, 2025.

[5] Tucker Reels and Kerry Breen, "At least 14 killed, dozens hurt on Bourbon Street in New Orleans as driver intentionally slams truck into crowd; attacker dead," CBS News, January 2, 2025.

[6] Alex Therrien, "Mother and child die from injuries after Munich car attack," BBC, February 15, 2025.

[7] Nadine El Bawab and Jordana Miller, "At least 13 injured after car rams into bus stop in Israel," ABC News, February 27, 2025.

[8] "Two dead, several injured in Germany as car rams into crowd," *Monde*, March 3, 2025; Orestes Georgiou Daniel, "Mannheim car ramming attack suspect a German with history of mental illness, say investigators," Euronews, March 3, 2025.

[9] Brian Michael Jenkins and Bruce R. Butterworth, "An Analysis of Vehicle Ramming as a Terrorist Tactic," Security Perspective, Mineta Transportation Institute, San Jose State University, May 2018.

[10] "Berlin truck attacker Anis Amri killed in Milan," BBC, December 23, 2016.

[11] "At least four dead in Jerusalem bulldozer attack," France 24, July 2, 2008.

[12] "Münster victim dies weeks after car rampage," Deutsche Welle, April 26, 2018.

[13] "Judge sentences man to life in prison for Waukesha Christmas parade attack," NPR, November 16, 2022.

[14] Alexandre Rodde, *Le Jihad en France 2012-2022* (Paris: Editions du Cerf, 2022), pp. 215-216.

[15] Based on the author's (Rodde) database, unpublished.

[16] "FBI Statement on the Attack in New Orleans," FBI National Press Office, January 1, 2025.

[17] "Global Terrorism Database 1970 - 2020 [data file]," START, National Consortium for the Study of Terrorism and Responses to Terrorism, 2022.

[18] "Car Crashes Klan Rally in Plains, 30 injured," *Eugene Registe Guard*, July 3, 1977.

[19] "Driver Booked in Fatality Close to Olympic Village," *Blade Toledo*, July 29, 1984.

[20] "Man who drove road train into pub denied parole," ABC News (Australia), September 5, 2013; "Estudante Joga Caro Na Mltidao e Fere 15," *Jornal do Brasil*, April 20, 1993.

[21] Deborah Sontag, "Palestinian's Hit-and-Run Bus Kills 8 Israelis and Injures 20," *New York Times*, February 14, 2001.

[22] Eve Sampson, "Vehicle Ramming Attacks: Using Cars and Trucks as Weapons Has Become Common," *New York Times*, January 1, 2025.

[23] Brian Michael Jenkins and Bruce R. Butterworth, "'Smashing Into Crowds' -- An Analysis of Vehicle Ramming Attacks," San José State University, Mineta Transportation Institute, November 2019.

[24] Ibid.

[25] Duncan Gardham, "ISIL issued warning to 'filthy French,'" Politico, November 15, 2015.

[26] "Canadian soldier killed by convert to Islam in hit and run," *Guardian*, October 21, 2014.

[27] Rodde, pp. 215-216.

[28] Ryan Scott Houser, "Democratization of terrorism: an analysis of vehicle-based terrorist events," Trauma Surgery & Acute Care Open, September 8, 2022; Vincent Miller and Keith J. Hayward, "'I Did My Bit': Terrorism, Tarde and the Vehicle Ramming Attack as An Imitative Event," *British Journal of Criminology* 59:1 (2019): p. 4.

[29] "Westminster attack: What happened," BBC, April 7, 2017.

[30] "Stockholm truck attack: Who is Rakhmat Akilov?" BBC, June 7, 2019.

[31] "Barcelona attack: 13 killed as van rams crowds in Las Ramblas," BBC, August 17, 2017.

[32] "Sayfullo Saipov Indicted on Terrorism and Murder In Aid Of Racketeering Charges In Connection With Lower Manhattan Truck Attack," U.S. Attorney's Office, Southern District of New York, November 21, 2017.

[33] Jenkins and Butterworth.

[34] Ibid.;

[35] Karen Percy, "Bourke St murderer James Gargasoulas given life jail sentence but could get parole in 46 years," ABC News, February 21, 2019.

[36] "German police see mental illness behind Muenster van attack," France 24, April 8, 2018.

[37] "Trier: Five die as car ploughs through Germany pedestrian zone," BBC, December 1, 2020.

[38] Kevin Rawlinson, "Darren Osborne jailed for life for Finsbury Park terrorist attack," *Guardian*, February 2, 2018.

[39] Kate Dubinski, "Judge rules killer of London, Ont., Muslim family committed terrorism, calling it a textbook example," CBC, February 22, 2024.

[40] Paul Hess and Sneha Mandhan, "Ramming Attacks, Pedestrians, and the Securitization of Streets and Urban Public Space: A Case Study of New York City," *Urban Design Institute* 28:1 (2022).

[41] Gerald Dlubala, "Concrete Bollards Are Crucial To Separating Cars From Pedestrians and Buildings," Park and Facilities Catalog, May 17, 2017.

[42] Mark Jenner, "Circulation and Disorder: London Streets and Hackney Coaches, 1640-1740" in Tim Hitchcock and Robert Shoemaker eds., *The Streets of London: From the Great Fire to the Great Stink* (London: Rivers Oran Press, 2008), p. 43.

[43] Hess and Mandhan.

[44] Ibid.

[45] "Incremental Protection for Existing Commercial Buildings from Terrorist Attack: Providing Protection to People and Buildings," Risk Management Series, FEMA 459, April 2008.

[46] Nicole Gelinas, "Vehicular Terrorism in the Age of Vision Zero," Bloomberg, October 17, 2018; "Incremental Protection for Existing Commercial Buildings from Terrorist Attack;" Hess and Mandhan.

[47] Daniel C. Goodrich and Frances L. Edwards, "Transportation, Terrorism and Crime: Deterrence, Disruption and Resilience," Mineta Transportation Institute, Project 1896, January 2020.

[48] Anastassia Gliadkovskaya, "Watch: This destructive barrier was created to stop lorry attacks," Euronews, June 26, 2018.

[49] Jeff Anderson, "Anti-Terrorist Barriers Help Protect Facilities," Library AutomationDirect.com, June 1, 2007.

[50] "Vehicle Incident Prevention and Mitigation Security Guide," Cybersecurity and Infrastructure Security Agency, April 2024.

[51] Rodde, p. 213.

[52] "U.S. Social Security orders 174,000 hollow-point bullets," CBC, September 4, 2012.

[53] Chris Butler, "Implications of shooting through a windshield," Blue Line, June 25, 2022.

[54] Yannick Veilleux-Lepage and Marc-André Argentino, "2025 New Orleans Truck Attack: The Role of Electric Vehicles and Peer-to-Peer Platforms,"ICCT, January 2025.

[55] "Canadian soldier killed by convert to Islam in hit and run."

[56] Rodde, *Le Jihad en France 2012-2022*.

[57] Ibid.

[58] Mitch Smith, Richard Pérez-Peña, and Adam Goldman, "Suspect Is Killed in Attack at Ohio State University That Injured 11," *New York Times*, November 28, 2016.

[59] "Berlin Christmas market attack," Deutsche Welle, December 17, 2021.

[60] "London attack: Khalid Masood identified as killer," BBC, March 23, 2017.

[61] "Stockholm truck attack."

[62] Rodde, *Le Jihad en France 2012-2022*.

[63] "Darren Osborne guilty of Finsbury Park mosque murder," BBC, February 1, 2018.

[64] Rodde, *Le Jihad en France 2012-2022*.

[65] "A woman recalls the deadly car attack at the Charlottesville rally organizers' trial," NPR, November 8, 2021.

[66] "Barcelona attack."

[67] Benjamin Mueller, William K. Rashbaum, and Al Baker, "Terror Attack Kills 8 and Injures 11 in Manhattan," *New York Times*, October 31, 2017.

[68] "Westminster car crash driver Salih Khater jailed for life," BBC, October 14, 2019.

[69] Rodde, *Le Jihad en France 2012-2022*.

[70] Dubinski.

[71] Reels and Breen.

[72] Therrien.