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.

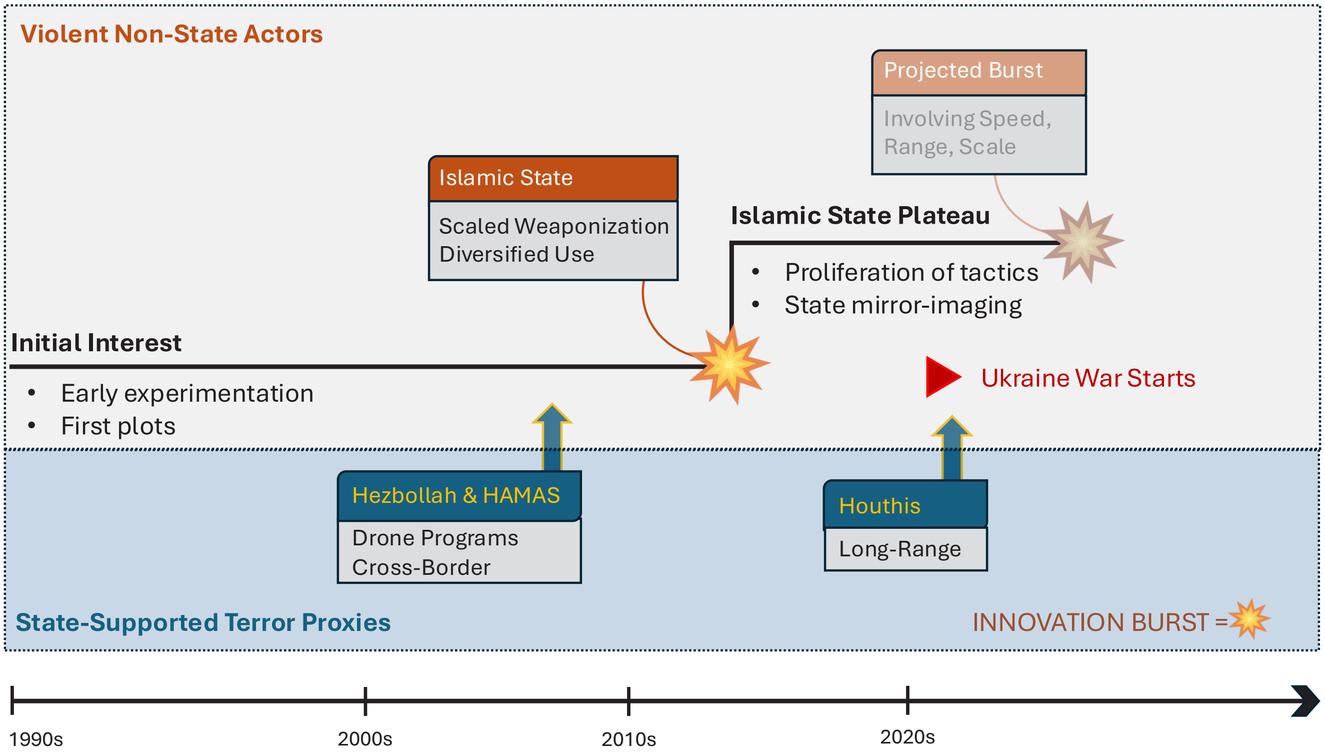

Figure 1: The Punctuated Evolution of Drone Terrorism[11]

> **"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).

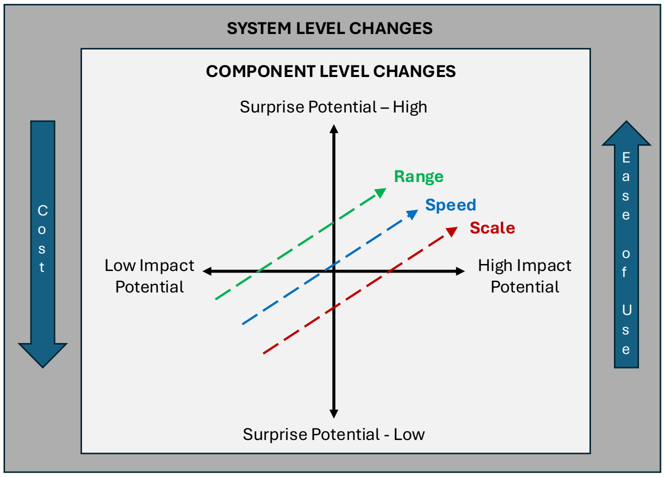

Figure 2: VEO Drone Capability-Impact Framework

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.

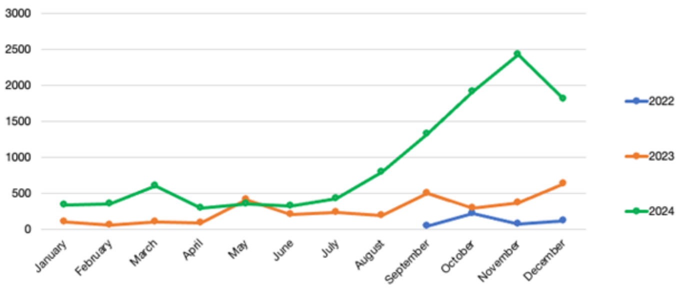

Figure 3: Number of Russian Shahed or Shahed-type drone attacks on Ukraine, by year and month[100]

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.

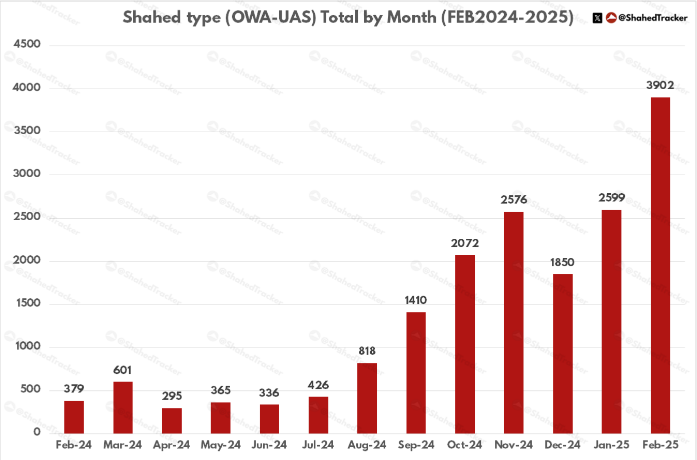

Figure 4: Data on Russian Shahed drones used in Ukraine, compiled by @ShahedTracker[104]

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.