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

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

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

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

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

VNSAs and the Attractiveness of Drones

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

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

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

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

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

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

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

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

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

Drone Capabilities

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

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

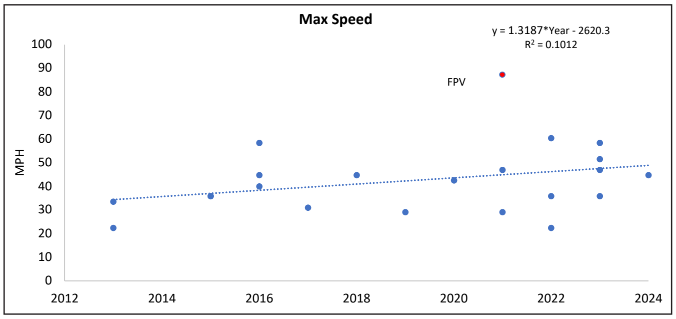

Figure 1: DJI Drone Dataset Max Speed

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

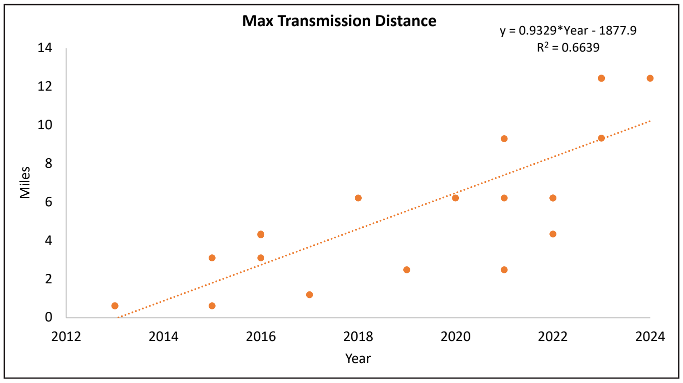

Figure 2: DJI Drone Dataset Max Transmission Distance

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

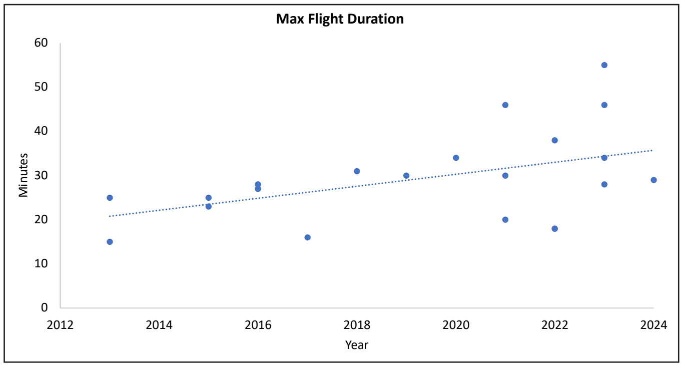

Figure 3: DJI Drone Dataset Max Flight Duration

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

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

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

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

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

Increased Threat Use of Commercial Drones

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

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

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

Future Challenges

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

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

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

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

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

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

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

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

Conclusion

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

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

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

Citations

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

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

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

[4] Ibid.

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

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

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

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

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

[10] Haugstvedt.

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

12 Samuel Bendett, "Mass-Market Military Drones Have Changed the Way Wars Are Fought," Center for a New American Security, accessed July 9, 2024.
13 Ulrike Franke, "Drones in Ukraine and Beyond: Everything You Need to Know," European Council on Foreign Relations, August 11, 2023.
14 "DJI - Official Website," DJI Official, August 2024.
15 "Counter-Unmanned Aircraft System (CUAS) Capability for Battalion-and-Below Operations (Abbreviated Version of a Restricted Report)," Board on Army Science and Technology, Division on Engineering and Physical Sciences, National Academies of Sciences, Engineering, and Medicine, 2018.
16 Joshua A. Schwartz, "What Iran's Drone Attack Portends for the Future of Warfare," Modern War Institute, West Point, April 30, 2024.
17 "Science & Tech Spotlight: Drone Swarm Technologies," U.S. Government Accountability Office, September 14, 2023.
18 Ibid.
19 "Sky Elements Flies 5,000 Drone Show with Uvify in Mansfield," Sky Elements, November 30, 2024.
20 Jonathan B. Bell, "Countering Swarms: Strategic Considerations and Opportunities in Drone Warfare," National Defense University Press, October 24, 2022.
21 Ibid.
22 "How Drone Swarm System Works: What Is Drone Swarm?" RF Wireless World, n.d.
23 Kenia Chávez and Ori Swed, "How Hamas Innovated with Drones to Operate Like an Army," Bulletin of the Atomic Scientists, November 1, 2023.
24 Jeff Daniels, "Russia Says It Killed Rebels Behind Swarm Drone Attack in Syria, but Experts See More Such Strikes Ahead," CNBC, January 13, 2018.
25 Bell.
26 Brian Wilson, Scott Tierney, Brian Toland, Rachel M. Burns, Jan Osburg, Michael D. Ziegler, Rasool Khan, Michael Nixon, Christopher S. Adams, and Christian Steiner, "Small Unmanned Aerial System Adversary Capabilities," Rand Corporation, March 12, 2020.
27 Nick Waters, "Types of Islamic State Drone Bombs and Where to Find Them," Bellingcat, May 24, 2017.
28 "40mm Low-Velocity Grenades," Gary's U.S. Infantry Weapons Reference Guide, n.d.
29 Pariesa Brody and Pierre Ayad, "Ukrainian Soldiers Are Turning Consumer Drones into Formidable Weapons of War," France 24, August 8, 2022.
30 "Update 3-Drone with Minuscule Quantity of Radiation Found on Japan PM's Office Roof – Media," Reuters, April 22, 2015.
31 "DJI FlyCart 30," DJI Official, n.d.
32 "DJI Agras T40," DJI Official, n.d.
33 "10 Types of Counter-Drone Technology to Detect and Stop Drones Today," Robin Radar Systems, n.d.
34 Joe Lacdan, "Joint Counter-Small UAS Office Conducts Successful Counter Drone-Swarm Demonstration," U.S. Army, July 27, 2024.
35 Princess Chimmy Joeaneke, Onyinye Obioha Val, Oluwaseun Oladeji Olaniyi, Olumide Samuel Ogungbemi, Anthony Obulor Olisa, and Oluwaseun Ibrahim Akinola, "Protecting Autonomous UAVs from GPS Spoofing and Jamming: A Comparative Analysis of Detection and Mitigation Techniques," *Journal of Engineering Research and Reports* 26:10 (2024).
36 Stacie Pettyjohn, "Evolution Not Revolution," Center for a New American Security, February 8, 2024.
37 Rassler.
38 Rami Amichay, "Tel Aviv hit by drone attack claimed by Iranian-backed Houthis," Reuters, July 19, 2024.
39 Ibid.
40 "Counter-small Unmanned Aircraft Systems Strategy," U.S. Department of Defense, 2021.
41 "DoD Announces Strategy for Countering Unmanned Systems," U.S. Department of Defense, December 5, 2024.