OFFICE of INTELLIGENCE and ANALYSIS

INTELLIGENCE IN FOCUS

23 AUGUST 2024

DHS-IA-IF-2024-10689

*TERRORISM*

# *(U//FOUO)* Growing Illicit Use of Unmanned Aircraft Systems by Violent Extremists in the Homeland Likely Presents New Security Challenges

*(U//FOUO)* ***Scope Note:*** *This product analyzes small commercial off-the-shelf unmanned aircraft systems – the most prevalent unmanned aircraft system used within the United States. Purchasing, possessing, or flying an unmanned aircraft system is not indicative of criminal or terrorist activity. However, modifying one to create a weapon or flying it in restricted airspace without a permit is illegal per US Code and Federal Aviation Administration regulations.*

*(U//FOUO)* **The threat of unmanned aircraft system (UAS) attacks in the Homeland is rising due to the widespread availability of off-the-shelf technology and violent extremists online increasingly promoting the use of UAS.** Increased online discussions sharing lessons learned from UAS experimentation and weaponization tactics in conflicts abroad have lowered the bar for adoption and illicit use of UAS. Additionally, various state and violent extremist actors worldwide have been enabled by technological advancements to increase their experimentation with UAS, which has resulted in new tactics, techniques, and procedures for downloading software, adding hardware, or modifying systems into weapons—especially to carry and drop dangerous payloads—according to open-source media and academic reporting.[a]

- *(U//FOUO)* US-based individuals adhering to violent ideologies have efficiently adopted commercial off-the-shelf UAS for surveillance, harassment, smuggling, and creating content. According to FBI open-source information, the now-deceased attempted assassin of former President Donald Trump^USPER operated a UAS near the event site for approximately 11 minutes, watching the live feed from the onboard camera, possibly to aid their spatial awareness for the attack.

- *(U//FOUO)* US-based individuals adhering to violent ideologies are beginning to discuss how to modify UAS with explosives, conductive materials, and chemicals for use against various targets, including critical infrastructure, symbolic sites,

[a] *(U)* Over the past five years, we have observed technological advances in UAS navigation systems, range, speed, video quality, data storage capacity, and more efficient payload-carrying capacities—from 1 to 50+ pounds—at accessible price points, starting around $50, decreasing obstacles to their adoption, including cost and expertise.

mass gatherings, and political figures. Violent extremists in the Homeland have the opportunity to use UAS to overcome ground security barriers or large standoff distances and deliver explosive or hazardous payloads on their own or simultaneously with ground attacks.

- *(U//FOUO)* Since 2022, individuals who adhere to violent ideologies have increasingly discussed how to weaponize UAS based on successful examples from foreign conflict zones, according to a body of DHS open-source reporting and a platform that monitors violent extremism online. UAS use in ongoing conflicts has driven an increase in experimentation and has demonstrated that commercial off-the-shelf UAS are effective against various targets at a low cost.

- *(U//FOUO)* Foreign terrorist organizations and US-based individuals adhering to violent ideologies have explicitly highlighted real-world examples as proofs of concept for Homeland attacks and encouraged their replication. Weaponization tactics have proliferated online, including on platforms frequented by US-based individuals who adhere to violent ideologies, and where users share designs for UAS-deployable explosives, discuss store-bought items to increase lethality, and debate how to tailor payloads for specific targets, according to open-source reporting. Criminal incidents in the United States since 2020 have featured weaponized UAS, highlighting their replicability and the limited expertise needed for their adoption.

*(U//FOUO)* **Rapidly advancing and unregulated UAS technology, experimentation with new modifications, and the lack of broad counter-UAS legal authorities outside of certain US government entities will likely hinder DHS partners' abilities to protect against UAS.** However, DHS partners can update security postures and apply other legal means or regulations to mitigate the risk of a lethal UAS attack *(see table in Appendix)*.

- *(U//FOUO)* UAS capabilities are progressing faster than counter-UAS technology and federal prevention frameworks, which could hinder successful law enforcement detection or mitigation, especially as tactics and technology to evade counter-UAS capabilities are circulated and sold online with little to no regulation. Current and expected advances—including autonomous flight, 5G command and control, jamming protection technology, swarming technology, and software that disables geofencing restrictions—could limit UAS tracking and susceptibility to mitigation tools, such as UAS signal jamming.

- *(U//FOUO)* Even when law enforcement partners possess UAS detection tools, they often lack the legal authority to effectively intervene with a nefarious, noncompliant UAS.[b] The Domestic Counter-UAS National Action Plan advocates for expanding law enforcement counter-UAS capabilities for some national security situations, special events, and other mass gatherings, but other potential attractive targets may remain without federal assistance or these expanded authorities.[c] Individuals advocating online for using UAS as weapons have discussed potential targets perceived as having limited-to-no counter-UAS tools, such as substations or public officials without federal protection, as preferred targets for attacks or critical infrastructure disruption, according to DHS reporting.

[b] *(U)* Only DHS, DOD, DOE, and DOJ are authorized to use counter-UAS technologies within US airspace to down a UAS, which would otherwise be illegal under US code.

[c] *(U)* More information on the Domestic Counter-UAS National Action Plan can be found at: https://www.whitehouse.gov/briefing-room/statements-releases/2022/04/25/fact-sheet-the-domestic-counter-unmanned-aircraft-systems-national-action-plan/%20.

## *(U)* Appendix

OVERALL TABLE CLASSIFICATION: UNCLASSIFIED

| *(U)* UAS Threat Best Practices & Resources |
|---|
| *(U)* Incorporate UAS into risk assessments. Assess critical assets and areas that may be most vulnerable to UAS. Identify and monitor possible launch and landing zones on or near your facility. |
| *(U)* Establish procedures for safely handling downed UAS. Ensure that any downed UAS are rendered safe and properly handled to prevent potential harm to personnel, disruption of operations, or destruction of evidence. |
| *(U)* Reevaluate security postures and CCTV cameras and camera views to consider airborne threats. |
| *(U)* Train employees on recognizing and reporting suspicious UAS activity.[d] |
| *(U)* Place "No Drone Zone" signs in areas where UAS takeoff or landing is restricted by state or local laws.[e] |
| *(U)* Conduct exercises to test and prepare response capabilities should a UAS incident occur. |
| *(U)* Update emergency action plans to include UAS incidents and responses. These might address evacuation protocols, depending on the model; visible hazardous attachments; or UAS payload size. |
| *(U)* Consider using UAS detection technology and Remote ID receivers to enhance situational awareness of UAS activity. Consult legal counsel before employing detection technology, as certain systems may violate federal statutes and regulations.[f] |

[d] *(U)* For UAS risk information and resiliency exercises, please refer to CISA resource: https://www.cisa.gov/resources-tools/resources/responding-drone-calls-guidance-emergency-communications-centers.

[e] *(U)* Federal Aviation Administration resources on "No Drone Zones" can be found at: https://www.faa.gov/uas/resources/community_engagement/no_drone_zone.

[f] *(U)* For more information, refer to the "Advisory on the Application of Federal Laws to the Acquisition and Use of Technology to Detect and Mitigate Unmanned Aircraft Systems" at: https://www.dhs.gov/publication/interagency-legal-advisory-uas-detection-and-mitigation-technologies.

## Source, Reference, and Dissemination Information

**Definitions**

*(U)* **Autonomous UAS Flight:** A UAS operated using artificial intelligence-powered navigation and operation software, which does not require human intervention to fly**.**

*(U)* **Commercial Off-the-Shelf UAS:** A UAS commercially ready-made and available for sale to the general public in a kit or ready to fly configuration.

*(U)* **Counter-Unmanned Aircraft System:** A system or device capable of lawfully and safely disabling, disrupting, or seizing control of an unmanned aircraft or unmanned aircraft system. Only DHS, DOD, DOE, and DOJ are authorized to use these kinds of technologies within US airspace to down a UAS, which would otherwise be illegal under US code.

*(U)* **Geofencing**: The use of GPS or radio frequency identification technology to create a virtual geographic boundary, enabling software to trigger a response when a mobile device enters or leaves a particular area, often applied to the settings of a UAS by the manufacturer.

*(U)* **National Defense Airspace:** Any airspace of the contiguous United States that is an Air Defense Identification Zone, in which the ready identification, location, and control of all aircraft (except DOD and law enforcement aircraft) is required in the interest of national security, or non-Air Defense Identification Zone airspace in which the control of aircraft is required for reasons of national security.

*(U)* **Swarming Technology:** The Federal Aviation Administration defines a swarm as an operation of more than one UAS in which all operate in unison based on commands from one pilot, who commands them all through a common link.

*(U)* **Unmanned Aircraft Systems (UAS):** An unmanned aircraft and associated elements (including communication links and the components that control the unmanned aircraft) that are required for the operator to operate safely and efficiently in the national airspace system.

**Privacy and Civil Liberties Considerations**

*(U//FOUO)* US persons linking, citing, quoting, or voicing the same arguments or symbols are likely engaging in First Amendment-protected activity, unless they are acting at the direction or control of a domestic violent extremist group or actor. Furthermore, variants of the topics covered in this product, even those that include divisive terms, should not be assumed to reflect violent extremism absent information specifically attributing the content to domestic violent extremists. This information should be considered in the context of all applicable legal and policy authorities to use open-source information while protecting privacy, civil rights, and civil liberties.

**Reporting Suspicious Activity**

*(U)* **To report suspicious activity, law enforcement, Fire-EMS, private security personnel, and emergency managers should follow established protocols; all other personnel should call 911 or contact local law enforcement.** Suspicious activity reports (SARs) will be forwarded to the appropriate fusion center and FBI Joint Terrorism Task Force for further action. For more information on the Nationwide SAR Initiative, visit www.dhs.gov/nsi.

*(U)* **To report a computer security incident, please contact CISA at 888-282-0870; or go to https://www.cisa.gov/forms/report. Please contact CISA for all network defense needs and complete the CISA Incident Reporting System form.** The CISA Incident Reporting System provides a secure, web-enabled means of reporting computer security incidents to CISA. An incident is defined as a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices. In general, types of activity commonly recognized as violating typical security policies include attempts (either failed or successful) to gain

unauthorized access to a system or its data, including personally identifiable information; unwanted disruption or denial of service; the unauthorized use of a system for processing or storing data; and changes to system hardware, firmware, or software without the owner's knowledge, instruction, or consent.

*(U)* **To report an incident to the Intelligence Community, please contact your DHS I&A Field Operations officer at your state or major urban area fusion center, or e-mail DHS.INTEL.FOD.HQ@hq.dhs.gov.** DHS I&A Field Operations officers are forward deployed to every US state and territory and support state, local, tribal, territorial, and private sector partners in their intelligence needs; they ensure any threats, incidents, or suspicious activity is reported to the Intelligence Community for operational awareness and analytic consumption.

**Warning Notices & Handling Caveats**

*(U)* **Warning:** This information is provided only for intelligence purposes in an effort to develop potential investigative leads. It cannot be used in connection with any foreign or domestic court proceedings or for any other legal, judicial, or administrative purposes.

*(U)* **Warning:** This document is UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public, the media, or other personnel who do not have a valid need to know without prior approval of an authorized DHS official. State and local homeland security officials may share this document with authorized critical infrastructure and key resource personnel and private sector security officials without further approval from DHS.

*(U)* This product contains US person information that has been deemed necessary for the intended recipient to understand, assess, or act on the information provided. It has been highlighted in this document with the label USPER and should be handled in accordance with the recipient's intelligence oversight and/or information handling procedures. Other US person information has been minimized. Should you require the minimized US person information, please contact the Homeland Security Single Point of Service, Request for Information Office at DHS-SPS-RFI@hq.dhs.gov, DHS-SPS-RFI@dhs.sgov.gov, DHS-SPS-RFI@dhs.ic.gov.

CLASSIFICATION: UNCLASSIFIED//FOR OFFICIAL USE ONLY

Homeland Security

Office of Intelligence and Analysis

# Customer Feedback Form

Product Title: (U//FOUO) Growing Illicit Use of Unmanned Aircraft Systems by Violent Extremists in the Homeland Likely I

All survey responses are completely anonymous. No personally identifiable information is captured unless you voluntarily offer personal or contact information in any of the comment fields. Additionally, your responses are combined with those of many others and summarized in a report to further protect your anonymity.

**1. Please select partner type:** Select One **and function:** Select One

**2. What is the highest level of intelligence information that you receive?** Select One

**3. Please complete the following sentence: "I focus most of my time on:"** Select One

**4. Please rate your satisfaction with each of the following:**

| | Very Satisfied | Somewhat Satisfied | Neither Satisfied nor Dissatisfied | Somewhat Dissatisfied | Very Dissatisfied | N/A |
|---|---|---|---|---|---|---|
| Product's overall usefulness | ○ | ○ | ○ | ○ | ○ | ○ |
| Product's relevance to your mission | ○ | ○ | ○ | ○ | ○ | ○ |
| Product's timeliness | ○ | ○ | ○ | ○ | ○ | ○ |
| Product's responsiveness to your intelligence needs | ○ | ○ | ○ | ○ | ○ | ○ |

**5. How do you plan to use this product in support of your mission?** ***(Check all that apply.)***

□ Drive planning and preparedness efforts, training, and/or emergency response operations
□ Observe, identify, and/or disrupt threats
□ Share with partners
□ Allocate resources (e.g. equipment and personnel)
□ Reprioritize organizational focus
□ Author or adjust policies and guidelines
□ Initiate a law enforcement investigation
□ Intiate your own regional-specific analysis
□ Intiate your own topic-specific analysis
□ Develop long-term homeland security strategies
□ Do not plan to use
□ Other:

**6. To further understand your response to question #5, please provide specific details about situations in which you might use this product.**

**7. What did this product *not* address that you anticipated it would?**

**8. To what extent do you agree with the following two statements?**

| | Strongly Agree | Agree | Neither Agree nor Disagree | Disagree | Strongly Disagree | N/A |
|---|---|---|---|---|---|---|
| This product will enable me to make better decisions regarding this topic. | ○ | ○ | ○ | ○ | ○ | ○ |
| This product provided me with intelligence information I did not find elsewhere. | ○ | ○ | ○ | ○ | ○ | ○ |

**9. How did you obtain this product?** Select One

**10. Would you be willing to participate in a follow-up conversation about your feedback?** Yes

***To help us understand more about your organization so we can better tailor future products, please provide:***

*Name:*
*Organization:*
*Contact Number:*
*Position:*
*State:*
*Email:*

Submit Feedback

Privacy Act Statement

CLASSIFICATION: UNCLASSIFIED//FOR OFFICIAL USE ONLY

Product Serial Number: DHS-IA-IF-2024-10689