

The Threat of Drones and Police Preparedness: A Mixed-Methods Study

Crime & Delinquency

1–29

© The Author(s) 2026

Article reuse guidelines:

sagepub.com/journals-permissions

DOI: 10.1177/00111287261474835

journals.sagepub.com/home/cad

Andrea Corradi¹ , **Scott Sigmund Gartner²**,
Molly Lynn¹, **M. Hunter Martaindale³**,
and **Logan J. Somers³**

Abstract

Unmanned aerial systems (UAS) present a rapidly evolving challenge with significant implications for law enforcement, such as the use of drones by terrorist and criminal actors. Yet, little empirical work has examined how law enforcement officers perceive or prepare for this threat. Through a nationwide survey of 293 law enforcement officers, this mixed-methods study examines officers' perceptions of drone-related threats, awareness of legal boundaries to response, and organizational preparedness. Qualitatively, approximately two-thirds of respondents characterized the threat to their jurisdiction as moderate or high, highlighting threats to critical infrastructure and potential mass-casualty attacks. Quantitative analyses show the important impact of training, and that officers in local and county agencies report less confidence than federal officers regarding legal authority and responsibility.

¹Georgia Southern University, Statesboro, USA

²Naval Postgraduate School, Monterey, CA, USA

³Texas State University, San Marcos, USA

Corresponding Author:

Andrea Corradi, Georgia Southern University, 1332 Southern Drive, Statesboro, GA 30458, USA.

Email: acorradi@georgiasouthern.edu

Keywords

unmanned aerial systems, drones, police, homeland security, threat

Introduction

Over the last 20 years, drones and unmanned aerial systems (UAS) have reshaped military operations (Agius, 2017; Hutto & Patton Rogers, 2025). However, the shift from the use of large-scale and expensive devices like predator drones in the wars in Afghanistan and Iraq to the recent ubiquity of small and cheap drone warfare in Ukraine has ramifications beyond the battlefield. Drones that cost a few hundred dollars to make can be used to destroy airplanes like in Operation Spiderweb (Kirichenko, 2025), drop explosives (Shuster, 2025), and engage in swarm attacks against critical infrastructure (Pettyjohn & Campbell, 2025). First-person view drones are fast, cheap, small, and effective at navigating traditional defenses, while inflicting costly damage against people, vehicles, and infrastructure (Ito, 2025). Ukraine is clearly showing what has long been known about UAS, that they can be extremely powerful as a feature of asymmetrical warfare (Agwu, 2017), leaving the question as to *when*, not *if*, they will be used against the American homeland. One of the biggest fears for the homeland security community is drones employed as delivery mechanisms for improvised explosive devices (Ilijevski et al., 2021) or chemical, biological, or radiological weapons (Barten et al., 2022; Doctor et al., 2026; Rassler, 2016). It is not just malicious uses of drones that are dangerous, as unwitting drone pilots also pose a threat, where operators are unaware of the problems they are causing, such as accidents, traffic in flight paths, or disrupting response to other incidents (Jones et al., 2025).

The barriers to defending against drone attacks are multi-faceted, but chief among them are the legal and logistical shifts from a national security threat (involving the military) to a civilian threat (involving law enforcement). Only in the last few years have some federal law enforcement agencies gained the legal authority to shoot down or otherwise interdict a drone (S.2836 - 115th Congress (2017-2018): Preventing Emerging Threats Act of 2018, 2018), and state and local law enforcement agencies nationwide still largely lack these authorities and this ability. At the same time, as industry increasingly adopts drones, the chances are growing that a perceived drone threat may actually be legitimately employed in agriculture, real estate, mining, energy development, advertising, or some other commercial activities. All of these concerns put a premium on preparedness and capacity to detect, identify, communicate, analyze, and respond to these emerging threats. In addition to their role in evolving threats, drones also represent rapidly developing tools for law enforcement.

Despite this important and emerging threat, little to no empirical attention has been paid to how law enforcement currently perceives and is preparing to counter the threat posed by drones. It is likely that this is because the current situation is what is referred to as ‘left of boom’; no significant violent incident using drones to target civilians has yet occurred in the U.S. In addition, despite evidence that UAS pose a threat as a tool for terrorist organizations to use for kinetic attacks, surveillance, post-attack interference, and as a force-multiplier (e.g., Doctor et al., 2025b; Dulligan et al., 2025), there is no research on whether law enforcement officers are preparing for this potential. This paper focuses on terrorism and extreme violence, which, while potentially the most deadly and destructive employments of UAS, are also among the least likely to occur. Outside of the risk of significant violent incidents, drones are also becoming a cost-effective way to deliver contraband into correctional settings, with relative safety for pilots who can now be far from the drop point and difficult to identify or pursue. They can be used to drop contraband like drugs and weapons, facilitate escape, conduct surveillance, or attack incarcerated individuals, correctional officers and staff (Russo et al., 2024). Cartels are also increasingly relying on drones for smuggling and surveillance, and outside of the U.S., have used them for attacks on law enforcement (Doctor et al., 2025a).

In light of these concerns, we surveyed law enforcement officers to establish a baseline of their perception of and preparation against the threat of drones within this complicated legal context. Specifically, using a mixed-methods approach employing qualitative and quantitative data we shed light on the following research questions: (1) In what ways do law enforcement officers perceive drones as a threat or public safety concern? (2) How do law enforcement officers perceive the legal and logistical issues of drone interdiction and their own preparedness?

Background

UAS of any kind were first conceptualized in World War I and deployed in World War II (Hummel & Burpo, 2020; Pledger, 2021; Tin et al., 2021). Recreational drones have been used to invade individuals’ privacy, particularly those of females, encouraging potential voyeuristic behaviors (Graham et al., 2021). Fortunately, drones have not yet been used in a successful violent, extremist, or fatal incident within the United States. However, drones have been used to surveil law enforcement agencies (LEAs) near the border, and to smuggle drugs into the country (Jones et al., 2025). In 2024, a man attempted to attack the power grid with a drone carrying explosives in Nashville (Department of Justice, 2024). Rogue drones have been

responsible for interrupting events such as NFL and NCAA games (e.g., Cox, 2023; Farrar, 2022), Green Day Concerts (Buczek & Powers, 2024), and temporarily shutting down air traffic at major airports, including Pittsburgh International Airport (CBS News, 2023) and Ronald Reagan Washington National Airport (Snyder, 2022). Many scholars and homeland security officials believe that it is only a matter of time before drones are used in a lethal manner, to take down commercial aircraft (Hummel & Burpo, 2020), or against other key critical infrastructure (Doctor et al., 2026; Kunstner et al., 2021; Morrow et al., 2021).

In a warfare setting, coordination and cross-level training is necessary to combat threats, particularly against asymmetric threats like those posed by drones (Ito, 2025). Russia's initial inability to coordinate and train forces to combat drones cost them dearly against Ukraine. From a domestic sense, drone use by non-state actors will require the same coordination. While jurisdiction has long posed a barrier to effective response during a crisis for law enforcement (e.g., Corradi et al., 2020; McAuley, 2021; Pickering & Fox, 2022), coordination is even more critical when considering integrating military and law enforcement responses. The need for this integration is especially strong as many LEAs are currently not legally empowered to engage UAS. We seek to examine whether officers are preparing for this threat in any capacity (including by perceiving it as a threat), and how that perception might differ across contexts. Even if not legally able to interdict drones (unless they are certain categories of federal agents), LEA response and coordination to a threat would require awareness, policies, and training at every level. The following sections provide necessary context delineating the previous research asserting the threat posed by drones, the logistical challenges to drone response and law enforcement integration, and the legal boundaries around drone interdiction.

Drones and Potential for Violence

As (fortunately) no successful terrorist or violent attack using drones has been perpetrated within the U.S., we must look abroad for indicators as to how violent groups may incorporate UAS tactically and strategically. Between 2018 and 2024, Yemen, Syria, Saudi Arabia, and Israel were the most common targets of UAS attacks by terrorist groups, and the Houthis, Hezbollah, and the People's Defense Force of Myanmar were the most common perpetrators (Doctor et al., 2026). The top 10 countries targeted by terrorist drone attacks accounted for 1,267 deaths and 1,491 injuries (Doctor et al., 2026). For attacks in the Middle East and North Africa, the success of a terrorist attack when drones are used ranges from 70% (Barten et al., 2022) to 72.5% (Haugstvedt & Jacobsen, 2020). The drone capabilities of the

terrorist group the Islamic State of Iraq and Syria (ISIS) rapidly progressed between 2014 and 2017, as they developed a formalized structure to their distribution and usage systems that relied upon expertise imported with foreign terrorist fighters who came to join their cause (Almohammad & Speckhard, 2017). Ressler (2016, p. IV) notes that drones:

can be used by terrorist entities in five primary ways: for surveillance; for strategic communications; to smuggle or transport matériel; to disrupt events or complement other activities; and as a weapon. This last category includes instances of a drone being piloted directly to a target, a drone delivering explosives, and a weapon being directly mounted to a drone. . . [to] successfully carry out a targeted assassination; to kill individuals in or gain significant access to a heavily denied area; or to successfully disperse chemical, biological or radiological weapons. (p. IV).

State-sponsored terrorist groups such as the Houthis, Hamas, and Hezbollah appear to have the most advanced techniques, likely due to longer and more sustained access to Iranian UAS programs (Hummel & Burpo, 2020; Sims, 2018). In Mexico, cartels have operationalized drones against law enforcement officers and their critical infrastructure (Doctor et al., 2025a), and there is mixed evidence about the scope of the use of drones at the U.S.-Mexico border, though they are certainly being used for smuggling and trafficking at minimum (Nicas & Villegas, 2026).

While the geographical position of the U.S. has long been seen as a protective advantage against drone warfare, long-range capabilities of drones have surged in the last few years (Ressler, 2024), with drones now being deployed in the Ukraine/Russia conflict that are capable of reaching 1,600 km (The Associated Press., 2025). This has raised the threat profile of a long-range attack against the U.S. (Ressler, 2024), but the most likely attack is still one that originates from a domestic location, though ground and maritime-based drones (rather than only aerial systems) are important to consider as well (Doctor et al., 2025b).

Violent groups are likely to want to employ drones within the U.S. as they allow for a tactical shift away from suicide tactics or car bombs (Sims, 2018). Terrorist groups are specifically likely to use drones in the future, as there is easy access to advanced weapons systems and components through the open supply chain, training and knowledge of drone systems is relatively easy to acquire, and there are no widespread standardized and reliable systems to counter and respond to UAS (Doctor et al., 2025b). The threat of drones is already being experienced in the U.S. in correctional settings, such as the seizure of drones capable of lifting 225 pounds and facilitating an escape in Georgia (Williams, 2025). UAS been discussed as a threat to prisons for more than a decade (e.g., Zapotosky, 2015).

In other contexts, drones used for reconnaissance have contributed to more precise suicide attacks and helped vehicle borne improvised explosive device (VBIED) drivers avoid security measures (Lasconjarias & Maged, 2019), and here in the U.S., Thomas Matthew Crooks reportedly used a drone to pre-surveil the site of his alleged 2024 assassination attempt on President Trump (Doctor et al., 2025b). The intelligence and counterterrorism community will be blindsided if they do not consider that terrorists are able to adapt and aspire to use new technologies before they do (Sim et al., 2024), including the risk to highly vulnerable targets like open areas, high rise buildings with glass siding, rooftop access, and accessible HVAC systems (Doctor et al., 2026).

Logistics and Domestic Drone Response

Principal among the operational challenges to responding to drones is that currently, there is no effective or easily deployable interdiction method that counters all drones. Jamming the signal to the drone causing it to lose contact with the pilot has, when possible, become the standard response. However, jamming can also disrupt wireless network communications nearby, and the proliferation of fiber-optic cable enabled drones has added further complication to this interdiction tactic (Kunstner et al., 2021). There are hopes that artificial intelligence advancements will provide more effective counter drone responses (Pratama, 2025) but generally, threats from the air are difficult to defend against and pose a sophisticated problem (Ilijevski et al., 2021). Attempts to interdict through GPS signal interference (like geo-fencing) can be effective but also can disrupt other activities like air travel (Kunstner et al., 2021) or are easily defeated by wrapping antennae with aluminum foil (Pledger, 2021). Other options for drone interdiction include blinding them with lasers, stopping them with items like nets, spoofing them to gain control, destroying them, or targeting the pilot (Jones et al., 2025). If efforts get around irregular effectiveness and the failure to apply to all (e.g., fiber optic) drones, successful interdiction may create a rogue drone whose destination and actions are unknown—a significant concern with drones with explosive warheads in populated areas.

One of the nightmare scenarios of malicious drone use include the use of drone swarms (Rassler, 2016). Drone swarms are the coordinated attack of multiple drones sharing the same objective (Kallenborn & Bleek, 2018). Due to growth in commercial drone capabilities and affordable pricing, the threat posed by drones has increased as the potential for autonomous swarms with easy payload systems has been amplified (Dulligan et al., 2025). Drones can be coordinated with readily available technologies like Bluetooth (Pledger, 2021). This threat has been on the horizon for at least a decade, as in Bunker,

2015 argued that drone swarms were out of reach for most terror groups but were something that needed preparations for immediately. To this day, effective response to drone swarms is still difficult even on the battlefield, where they are not necessarily a surprise (Rassler & Veilleux-Lepage, 2025), and domestically, they pose just as grave of a threat.

From a policy standpoint, pressure from the commercial use of drones can be a barrier to implementing counterterrorist measures, especially preemptively. Specifically, the proliferation of drones for commercial and individual uses have meant that there are more drones to contend with generally, but also that terrorists can learn from the non-malicious but still dangerous uses that others have employed (Sim et al., 2024). There have been a number of drone detections during NFL games or other events at stadiums that have required the coordination of the FAA and law enforcement to identify the pilot's location and to assess the threat (Jones et al., 2025). There is an urgent need for policies to address regulation of and defense against drones, especially as the use by violent non-state actors has increased dramatically in the last decade (Dulligan et al., 2025).

In addition to the legal difficulties around drone response expanded upon below, it is likely that many targets will include those owned by private entities (such as critical infrastructure or soft-targets). Therefore, as law enforcement is generally responsible for active response to domestic threats, policies that include cooperation between companies/service providers and LEAs are necessary, yet no meaningful framework for this exists (Morrow et al., 2021). Jones et al. (2025) argue that event and facility operators, security staff, crowd management teams, and all first responders (including LEAs, paramedics, and firefighters) should be aware of the threat posed by drones. In addition, they note that these individuals must also be aware of the logistical considerations of how drones could be used against facilities, the types of actions that can be taken with drones, and the interdiction options available to them legally and technically.

Legal Boundaries on Law Enforcement Response

The military has long been considered the main unit for drone defense within the U.S., as most malicious drone incidents have thus far occurred overseas in other conflicts or against U.S. assets abroad. In addition, including law enforcement agencies in a framework designed to counter UAS faces significant legal challenges. However, from a domestic perspective, joint law enforcement and military operations will likely become necessary, and currently, interoperability and a lack of agreed upon procedures are a large barrier to defensive measures (Kunstner et al., 2021). The U.S. federal government is

still the only one that is authorized to use deadly force against drones that pose threats (Federal Aviation Administration, n.d.), and for some time, the federal government has asserted exclusive jurisdiction of aircraft privileges and UAS (Lightfoot, 2018). Even outside of the U.S., calls have been made to increase collaboration between militaries, police forces, and intelligence agencies to counter this significant threat (Pratama, 2025).

Interdiction powers were limited to the military until 2018 when the Department of Homeland Security (DHS) and Department of Justice (DOJ) were given authorization to conduct counterattacks on drone threats. Unlike local or state officers, this empowered federal agents to not only detect or track drones, but they may also seize, disrupt, and destroy drones in coordination with the Secretary of Transportation and the FAA Administrator (S.2836 - 115th Congress (2017-2018): Preventing Emerging Threats Act of 2018, 2018). Yet, the differing legal grounds for the military and law enforcement agencies compound difficulties in coordinating a coherent response to drone threats. Jurisdictional issues between military and police responses are possible, especially if there are incursions near military installations but not actually on a military site (Kunstner et al., 2021).

Specifically, the agencies under DHS and DOJ that are allowed to participate in counter-drone threat missions include the FBI, U.S. Marshals Service (USMS), Federal Bureau of Prisons, U.S. Coast Guard, U.S. Customs and Border Protection, U.S. Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI), and the U.S. Secret Service. These missions can range from national security to major public events, such as the Super Bowl, state gatherings, and emergency responses to growing crises (S.2836 - 115th Congress (2017-2018): Preventing Emerging Threats Act of 2018, 2018). Alongside the DOJ and DHS, the Department of Defense and the Department of Energy also have permission to prevent drone attacks, and the 2018 act mandated guidelines for departments to use when counter-drone measures are necessary (Ross & Jinks, 2021). Due to stringent civil liberties, privacy concerns, and necessary FAA coordination, the Preventing Emerging Threats Act of 2018 mandated guidelines are based on balancing security and rights, operational requirements, interagency coordination, and data management and transparency (Ross & Jinks, 2021). The Secretary of Homeland Security is also required to evaluate the existing laws and powers of federal, state, local, and tribal governments around preventing malevolent drone usage or threats near any critical infrastructure and major airports. (S.2836 - 115th Congress (2017-2018): Preventing Emerging Threats Act of 2018, 2018). With the passage of the Safer Skies Act, folded into the National Defense Authorization Act for Fiscal Year 2026, non-Federal agencies can use approved means to interdict UAS if they have been trained and certified. Currently,

training takes place at the FBI's National Counter-UAS Training Center (NCUTC), which opened in 2026.

Rather than engage in interdiction, state and local law enforcement agencies without training from the NCUTC are only permitted to collect evidence of illegal drone use, deter drone operations, investigate, and interview and intercept the drone operators (Federal Aviation Administration, n.d.). They also must notify the Regional Operation Center in the event of FAA violations, incidents, and accidents (Federal Aviation Administration, n.d.). The FAA has jurisdiction over the navigable airspace, which preempts any state or local regulations. As of now, it is unattainable for local governments and officers to put restrictions on drones in the air, regardless of how carefully they draft their laws, because the FAA can easily overturn them due to federal jurisdiction (Page, 2018). In addition, newly proposed FAA rules seek to loosen drone restrictions in support of their long-range use in commercial activity (Funk, 2025).

Despite the centralized federal powers over drone interdiction, there is no standardized way to analyze drone incidents or consolidate data to examine patterns, as drone incident reporting is voluntary and most incidents are not reported to national data systems (Tesauro, 2025). In addition, most of the time, state and local law enforcement agencies are the first responders to emergencies, mass casualty events, and terrorist incidents as they are the closest 'boots on the ground'. Yet, when it comes to the immense threat posed by drones, frequently only federal agencies are trained and authorized to counter drone attacks (Snead et al., 2018). The NCUTC is only in its infancy, and it is unclear how widespread the training will be provided. This is a glaring hole in UAS threat prevention and response capabilities that leaves many soft-targets, usually under the purview of non-federal agencies, extremely vulnerable.

Methods

Data for the current study originates from a nationwide Qualtrics survey of law enforcement officers that was administered through the Advanced Law Enforcement Rapid Response Training (ALERRT) Center. Located in central Texas, ALERRT is widely recognized as one of the leading law enforcement training organizations within the U.S. and is responsible for the training of roughly 70,000 officers per year from all 50 states. ALERRT's curriculum is focused on active shooter and related mass casualty response, including integrated response options with Fire/EMS, and does not include any instruction on drone operations, threat assessment, detection, or interdiction.

The survey itself was developed in collaboration with ALERRT and centered around gaining officers' perspectives on drone technologies and their capabilities, information related to drone use within their respective agencies, and demographic characteristics. Due to the rapidly advancing nature of the subject, a convenience sampling frame was chosen. While this has negative implications for full generalizability, this sample acts similarly to a large focus group where the data can be used to explore the topic to inform initial examinations and future analyses (Etikan et al., 2016).

Due to the lack of scholarship surrounding officers' views on drones, the project was designed with a fixed convergent mixed-methods ("QUAL + QUAN") approach in mind (Creswell & Plano Clark, 2007). More specifically, we use "complementarity" rationale (see Greene et al., 1989), which allows for the simultaneous use of quantitative and qualitative data to draw on their respective strengths and provide a more complete understanding of a complex issue (Todak & Somers, 2025). The core research questions are as follows:

Mixed-Methods Question: In what ways do law enforcement officers perceive drones as a threat or public safety concern?

Quantitative Question: How do law enforcement officers perceive the legal and logistical issues of drone interdiction and their own preparedness?

Administration of the survey began in September 2025 when a link was included in ALERRT's quarterly newsletter that is emailed to a listserv of the 400,000 law enforcement officers who have completed one of their training programs. Data collection ran for nearly six weeks and 431 responses were received. After removing participants that did not view the entire survey (136 individuals) or had missing data on the dependent variables (2 individuals), the final sample is 293 officers. Subsequent sections detail the methods for the quantitative and qualitative strands separately. The results are then merged and integrated throughout the discussion section.

Qualitative Methods

To learn more about the way that law enforcement officers (LEOs) perceive drone threats, we asked them the open-ended question: "Please describe your perception of the potential threat drones pose to your jurisdiction," which 265/293 officers responded to. Due to lack of prior research on officer perceptions of drones, a grounded theory approach was taken in the qualitative

analysis, which is appropriate when aiming to generate theory (Charmaz, 2017), and is common in mixed-methods contexts (Lamont & Swidler, 2014). To succinctly capture the types of threats officers are concerned about, and their risk perceptions to their jurisdiction, three members of the research team categorized all 265 responses into the three categories of threat perception listed in Table 3: Low, Moderate, and High. These categories were established collaboratively based on multiple rounds of open and parent coding, with frequent discussions between the coders about patterns and the types of responses provided. Each response was then independently re-coded and a majority rule was used. Ultimately, at least two of the three members agreed on the coding of 97.0% (257 out of 265) of the responses. In the eight cases where coding varied beyond that, the three members met to re-evaluate them and collaboratively coded them together.

Quantitative Methods

Key Variables of Interest. Several dependent variables were created to capture officers' awareness of drone threats, responsibilities and legalities regarding drone interdiction, and any drone related discussions occurring within their agency. More specifically, Likert scales were used to capture their level of agreement (1 = Strongly disagree, 5=Strongly agree) as it relates to *legal awareness* ("If a drone were to pose a threat in my jurisdiction, I am aware of the legal boundaries surrounding my potential actions to prevent it from doing harm"), *discussions* ("Discussions of the threat posed by drones have occurred in my presence or to my knowledge within my agency"), *military responsibility* ("Counter-drone operations should be handled by the military rather than law enforcement"), *extremist threat* ("I view drones as one of the top threats for terrorist or extremist violence"), and *violence* ("I am concerned about the use of drones for violence against individuals or property").

As for independent variables, we created a categorical measure based on each respondent's agency type (federal, state, county, local/municipal, other), and a series of dichotomous measures (1 = Yes) on whether they have *prior military experience*, had responded to a *previous drone call*, had completed any sort of *counter-drone training*, or if their agency had *counter-drone policies*. Moving to control variables, we also included categorical variables for *agency size* (small, medium, large), a continuous measure based on their *length of tenure*, and other binary items indicating whether the respondent was *located in Texas*, if they were *female*, if they were *Nonwhite*, and their highest level of completed *education* (high school, associate's degree, bachelor's, graduate degree).

Analytical Strategy. Analysis of the quantitative strand begins with a descriptive overview of the dependent, independent, and control variables. Following descriptive analysis, hot deck multiple imputation (Andridge & Little, 2010) was used to retain the sample while addressing small amounts of missingness in the following control variables: agency size (2.4%), tenure (2.0%), located in Texas (0.03%), and race (1.0%).¹ Using the 'how_many_imputations' command in Stata19 to assess adequacy, nine imputations were ultimately used. From there, ordinal logistic regression is used to model each of the five dependent variables, which is appropriate when using Likert-scale based measures (Long & Freese, 2006). In Stata19, we used the "ologit" command to estimate ordinal logistic regression models followed by the command "omodel" to test the proportional odds assumption. A non-significant result indicates that the assumption has not been violated, which holds for all of the models.

Results

Descriptive results pre-imputation (Table 1) demonstrate that the majority of the sample were county (27.0%) and local (43.3%) officers, while state and federal officers made up 16.4% and 4.4% of the sample respectively. The sample was largely White (88.3%), male (95.2%), and from Texas (52.7%). Most relevant to our research questions on preparation for drone interdiction, while 36.9% of individuals reported that they had previously received a call related to illegal drone use, only 19.1% reported having counter-drone policies at their agency. And, related to research showing the importance of training for addressing threats, even less (16.0%) having had any counter-drone training.

Table 2 shows the distribution of responses for all dependent variables. Of note, respondents reported the highest levels of agreement with the perceptions that drone use by extremists posed a significant threat and that drones could be used for violence against individuals or property. The lowest level of agreement was indicated for the statement that drone interdiction should be the responsibility of law enforcement and not the military, showing that more officers believe that LEAs should be part of the counter-drone response as well. We are not claiming that these responses represent a random sample, but rather that they inform a baseline for this and future studies to understand law enforcement perceptions of drones and their initial efforts to prepare for this possible threat.

To learn more about the way that LEOs perceive UAS threats, we asked them the open-ended question: "Please describe your perception of the potential threat drones pose to your jurisdiction." When qualitatively coding these responses, our open and subsequent parent coding identified a number of

Table 1. Descriptive Statistics, Police Drone Survey.

Variable	Obs.	Mean	SD
Dependent variables			
Awareness of Legal Boundaries on Drone Interdiction (<i>Legal Awareness</i>)	293	2.908	1.293
Discussions of Drone Threat Occurring at Agency (<i>Discussions</i>)	293	2.881	1.415
Drone Interdiction Should be Responsibility of Military not LE (<i>Military Responsibility</i>)	293	1.843	1.048
Threat Perception of Drone Use by Extremists (<i>Extremist Threat</i>)	293	3.986	1.134
Concern Over Drone Use for Violence (<i>Violence</i>)	293	3.898	1.175
Independent variables			
Agency Type			
Federal	293	0.044	
State	293	0.164	
County	293	0.270	
Local/Municipal	293	0.433	
Other	293	0.089	
Past Military Experience	293	0.392	
Previous Drone Calls	293	0.369	
Counter-Drone Training	293	0.160	
Counter-Drone Policies	293	0.191	
Control variables			
Agency Size			
Small: 1–49 officers	286	0.402	
Medium: 50–249 officers	286	0.294	
Large: 250+ officers	286	0.304	
Length of Tenure	287	21.836	10.767
Located in Texas	292	0.527	
Female	293	0.048	
Nonwhite	290	0.217	
Education			
High School	293	0.266	
Associates Degree	293	0.215	
Bachelor's Degree	293	0.334	
Graduate Degree	293	0.184	

Note. Due to rounding, variables may not sum exactly to 1.000.

repeated themes that are presented in Table 3. To capture succinctly the types of threats officers are concerned about, and their risk perceptions to their jurisdiction, we categorized responses into the three categories of threat perception listed in Table 3: Low, Moderate, and High. These categories were established collaboratively based on multiple rounds of open and parent coding, and then discussions between coders about patterns and the types of answers provided. When an answer contained references to things that could go in either category, we leaned toward the side of the higher risk assessment.

Table 2. Distributions of the Dependent Variables.

Dependent variable	Strongly disagree (1)	Somewhat disagree (2)	Neither Agree nor disagree (3)	Somewhat agree (4)	Strongly agree (5)	Total
Awareness of Legal Boundaries on Drone Interdiction (<i>Legal Awareness</i>)	54 (18.4%)	62 (21.2%)	69 (23.6%)	73 (24.9%)	35 (12.0%)	293 (100%)
Discussions of Drone Threat Occurring at Agency (<i>Discussions</i>)	75 (25.6%)	42 (14.3%)	64 (21.8%)	67 (22.9%)	45 (15.4%)	293 (100%)
Drone Interdiction Should be Responsibility of Military not LE (<i>Military Responsibility</i>)	146 (49.8%)	79 (27.0%)	45 (15.4%)	14 (4.8%)	9 (3.1%)	293 (100%)
Threat Perception of Drone Use by Extremists (<i>Extremist Threat</i>)	15 (5.1%)	17 (5.8%)	49 (16.7%)	88 (30.0%)	124 (42.3%)	293 (100%)
Concern Over Drone Use for Violence (<i>Violence</i>)	14 (4.8%)	31 (10.6%)	41 (14.0%)	92 (31.4%)	115 (39.3%)	293 (100%)

Note. Rows might not sum to 100% due to rounding.

Table 3. Threat Perceptions of Drones to Officers' Jurisdictions.

Threat category	Examples included in category	Obs.	%
Low	Few, none, low, privacy, accidents, interference, privacy, harassment	77	29.1
Moderate	Possible, growing, counter-surveillance, prison contraband, inability to interdict	92	34.7
High	Mass casualties, terrorism, critical infrastructure, lethal attacks, explosives, CBRN	96	36.2
<i>Total</i>		265	100

In the “low” category, we often received answers such as “We are rural so daily threat is minimal” (Respondent 209) or “Drones are more of a nuisance than a threat in our county” (Respondent 119). They would discuss the potential for invasions of privacy or harassment, which while certainly an issue for the victims, are less of a threat than activities that could cause physical damage. Also in this category were responses describing the risk of drones through their potential for accidents or unintentional interference with investigations or operations.

In the “moderate” category, we included responses that characterized the threat of drones as emerging or growing, or focused on other more serious criminal but not lethal uses of drones, for example: “Counter surveillance trade and illegal goods movement” (Respondent 109). This seemed to be an especially concerning issue for correctional institutions: “I work in a Jail. Personally, I don't see a threat when used by the Department. Outside drones can threaten the safety & security with the ability of drones dropping in weapons / contraband into the outside yards and / or grounds” (Respondent 81). This was a particularly important issue for many respondents, as it continued to be referenced, and was often described alongside the barriers to interdiction:

We operate in an area with 2 state prisons and a mental health hospital that houses the criminally insane. Drones plague these facilities with drops of illegal contraband, and as drone technology has increased, so has the opportunity for the pilot to be located a long distance from the facility they are dropping contraband to. Some years back when drones didn't fly far from the pilot and the controls it was much easier to find the person operating the drone and apprehend them (Respondent 73).

This inability to interdict the threat posed by drones was highlighted in a number of answers. Officers described perceiving that the risk is growing but felt they did not have the power to combat it: “The potential threat is something that needs to be addressed as soon as possible. This is a growing threat

to our communities, and we do not have anything that will stop it at this time” (Respondent 93).

Lastly, in the “high” category, we included answers that detailed any type of lethal threat of drones, which was often described as having a potential for mass casualties at events or on campuses, or being possible due to increased payload capabilities that would make delivering a chemical, biological, radiological, or nuclear (CBRN) weapon or other explosive simple: “It’s the new threat we should all be watching for. Especially in large venues and the weaponization of chemical and bio warfare” (Respondent 102). Or “My mind always goes to terrorism. They are commonplace enough that no one would think twice about seeing one, but the potential payload related to a chemical agent or something to that [e]ffect would be catastrophic” (Respondent 154).

The increased risk for terrorism and other lethal drone threats were frequently linked to the War in Ukraine, and the resultant dramatic changes in the accessibility of drones and information needed to weaponize them:

With ever increasing drone videos from the war in Ukraine, it is just a matter of time before a domestic terrorist is capable of creating and launching their own attack. Drones build instructions using easily accessible parts and 3-D printers are easy to find and watch on YouTube, with descriptions on how to increase battery life, payload, speed, and distance from [the] operator (Respondent 200).

The speed of the evolution of tactics in Ukraine was frequently highlighted by answers placed in the high category. Many responses described their jurisdictions as having a high number of soft-targets that a drone attack, whether singular or in swarm fashion, could do significant damage against concerts, festivals, political gatherings, and sporting events, especially with the increased potential to weaponize drones. As with answers in the “moderate” category, officers would frequently describe having limited options to prevent this looming threat.

Perception of Boundaries, Responsibility, and Violence

The first presentation of results from the multivariate analysis is displayed in Table 4, which includes models that contribute to findings on officers’ awareness and perceptions of responsibility for drone interdiction. As described in the methodology section, all models are ordinal logistic regression models, reflecting officers’ level of agreement with a statement. Model 1 shows the results for the statement “If a drone were to pose a threat in my jurisdiction, I am aware of the legal boundaries surrounding my potential actions to prevent it from doing harm.” Unsurprisingly, officers who had prior counter-drone training ($p < .001$) were more likely to be in a higher category of agreement

Table 4. Ordinal Logistic Regression Models of Perceptions of Interdiction.

Measures	Model 1		Model 2		Model 3	
	Legal Awareness(N = 293)		Discussions (N = 293)		Military Responsibility (N = 293)	
	OR	(SE)	OR	(SE)	OR	(SE)
Independent variables						
Agency Type						
State	0.961	(0.553)	0.374	(0.216)	2.551	(1.866)
County	0.747	(0.427)	0.234*	(0.133)	2.696	(1.956)
Local/Municipal	0.961	(0.553)	0.287*	(0.160)	3.264	(2.350)
Other	0.715	(0.455)	0.125**	(0.082)	6.509*	(5.207)
Past Military Experience	1.028	(0.233)	1.418	(0.322)	0.513**	(0.124)
Previous Drone Calls	1.186	(0.279)	1.833*	(0.437)	0.686	(0.175)
Counter-Drone Training	6.472***	(2.174)	6.085***	(0.212)	0.640	(0.227)
Counter-Drone Policies	1.661	(0.474)	1.191	(0.335)	0.998	(0.301)
Control variables						
Agency Size						
Small: 1–49 officers	0.824	(0.213)	0.935	(0.254)	0.759	(0.213)
Large: 250+ officers	0.699	(0.215)	0.879	(0.266)	0.682	(0.220)
Located in Texas	1.116	(0.250)	1.204	(0.275)	1.103	(0.269)
Length of Tenure	1.009	(0.011)	1.007	(0.011)	0.985	(0.011)
Female	0.329*	(0.172)	0.183**	(0.114)	1.418	(0.759)
Nonwhite	1.149	(0.316)	0.665	(0.184)	1.181	(0.355)
Education						
Associates Degree	0.782	(0.245)	1.278	(0.402)	1.099	(0.363)
Bachelor's Degree	0.803	(0.234)	1.131	(0.330)	1.495	(0.467)
Graduate Degree	0.911	(0.307)	1.356	(0.456)	1.088	(0.395)

Note. Note that Federal (Agency Type), Medium (Agency Size), and High School (Education) are used as reference categories.
*p < .05, **p < .01, ***p < .001 (two-tailed test).

that they are aware of their legal boundaries. Model 2 regards the statement "Discussions of the threat posed by drones have occurred in my presence or to my knowledge within my department or agency," and there are significant differences at the jurisdiction level. With federal officers as the reference category, county ($p = .011$), local/municipal ($p = .025$), and other officers ($p = .002$) are all significantly less likely than federal officers to be in a higher category of agreement of having experienced such conversations. Those who had received drone calls ($p = .011$) or counter-drone training ($p < .001$) were more likely to be in a higher category of agreement with being aware of these discussions, while those at agencies who simply had counter-drone policies were not ($p = .535$). Although being female is negatively associated with legal awareness and knowledge of discussions of the threat posed by drones ($p = .006$), some of this could be a result of the limited number of females in the sample exerting an inordinate influence.

Model 3 indicates agreement with the statement "Counter-drone operations should be handled by the military rather than law enforcement," and as described in Tables 1 and 2, overwhelmingly officers rejected this notion. Across jurisdictions, only officers in the "other" category were significantly different in their agreement with the perception of this than those at the federal level ($p = .019$), and of interest, those with military experience were more likely to disagree than those without military experience, which appears to indicate that veterans believed law enforcement should play a role in drone interdiction at higher levels than non-veteran officers ($p = .006$).

Table 5 supplements the qualitative results with a quantitative analysis of differences in officers' perception of the risk of drones as an extremist threat ("I view drones as one of the top threats for terrorist or extremist violence"; Model 4) and for potential for violence against individuals or property ("I am concerned about the use of drones for violence against individuals or property"; Model 5). In Model 4, all levels of jurisdiction are significantly less likely to be in a higher level of agreement of the threat posed by extremist drone use than federal agents (state, $p = .032$, county, $p = 0.043$; local/municipal, $p = .015$; other, $p = .002$). Those with counter-drone training ($p = .034$), and officers with longer tenures ($p = .021$) were more likely to be in higher levels of agreement with the extremist drone threat. Lastly, Model 5 shows that unlike with extremist threats, only some jurisdictions differed in their view of the general drone threat for violence, with county officers ($p = .045$) and other officers ($p = .004$) significantly less likely to be in a higher category of agreement than federal. Officers with past military experience ($p = .008$), those who had responded to previous drone calls ($p = .007$), and those with counter-drone training ($p = .023$) were all more likely to be in a higher category of agreement with the violent threat posed by drones.

Table 5. Ordinal Logistic Regression Models of Threat of Drones.

Measures	Model 4		Model 5	
	Extremist Threat (N = 293)		Violence (N = 293)	
	OR	(SE)	OR	(SE)
Independent variables				
<i>Agency Type</i>				
State	0.209*	(0.151)	0.353	(0.223)
County	0.236*	(0.168)	0.285*	(0.179)
Local/Municipal	0.180*	(0.127)	0.310	(0.193)
Other	0.077**	(0.060)	0.128**	(0.092)
Past Military Experience	1.209	(0.283)	1.888**	(0.448)
Previous Drone Calls	1.358	(0.335)	1.953**	(0.484)
Counter-Drone Training	2.076*	(0.717)	2.192*	(0.756)
Counter-Drone Policies	0.695	(0.202)	0.612	(0.179)
Control variables				
<i>Agency Size</i>				
Small: 1–49 officers	0.873	(0.242)	0.780	(0.218)
Large: 250+ officers	0.812	(0.253)	0.801	(0.253)
Located in Texas	1.018	(0.236)	1.126	(0.264)
Length of Tenure	1.026*	(0.011)	1.027*	(0.011)
Female	1.188	(0.644)	0.445	(0.242)
Nonwhite	1.335	0.391	1.027	(0.306)
<i>Education</i>				
Associates Degree	0.985	(0.314)	1.079	(0.348)
Bachelor's Degree	0.999	(0.300)	1.189	(0.359)
Graduate Degree	1.143	(0.402)	0.765	(0.262)

Note. Note that Federal (Agency Type), Medium (Agency Size), and High School (Education) are used as reference categories.

* $p < .05$, ** $p < .01$, *** $p < .001$ (two-tailed test).

Discussion

This mixed-methods study provides one of the first scholarly examinations of how U.S. law enforcement officers perceive the threat posed by drones and how prepared their agencies are to respond to that threat. The findings reveal a consistent pattern across jurisdictions: concern about drone-related risks is widespread, yet preparedness remains limited and is constrained by legal and organizational ambiguity. This disconnect between perceived threat and institutional readiness has important implications for public safety and policy development.

Two-thirds of respondents characterized the drone threat to their jurisdictions as moderate or high. Officers frequently described concerns consistent

with prior research on drone misuse, including counter-surveillance, contra-band delivery, threats to critical infrastructure, and lethal attacks. Importantly, respondents were asked to assess risk to their own jurisdiction rather than abstract national or international threats, suggesting that these concerns are grounded in local operational realities rather than distant or speculative scenarios. Many cited the concerns raised in studies of drones (e.g., Doctor et al., 2026; Jones et al., 2025; Ressler, 2016) and/or cited stories from the Ukrainian War. According to our respondents, drones pose a serious domestic threat.

Despite this elevated perception of risk, respondents repeatedly indicated that their agencies are not adequately prepared to address drone-related threats. Only a small proportion reported receiving counter-drone training or working with agencies with similar training. This lack of preparedness is particularly striking given that more than one-third of respondents had already responded to calls involving illegal drone use, indicating that drone-related incidents are no longer hypothetical. The gap between exposure to drone activity and institutional readiness suggests agencies are operating reactively to this emerging threat. We note three policy-relevant central themes related to the lack of preparedness:

Lack of Training

Training emerged as a central dividing line in respondents' perceptions and confidence. Specifically, only 16% of the respondents claim to have had training to address the drone threat. Given the threat's newness, its rapid evolution, and the impact of the speed of drone action, which places a premium on rapid decision making, it is not surprising that most of our respondents, who are untrained in how to deal with drones, are concerned about their lack of preparation. Many respondents viewed their and their organization's lack of training as a concern, citing similar views seen in analyses (e.g., Doctor et al., 2025b; Dulligan et al., 2025).

Jurisdiction Confusion

Jurisdictional confusion further compounds preparedness challenges. Results show that officers in local and county agencies are significantly less confident than federal officers regarding legal authority. As drones move across municipal, state, and federal boundaries, traditional jurisdictional frameworks become increasingly misaligned with operational realities, as seen in other challenging jurisdictional contexts (e.g., Corradi et al., 2020). Given the rapid advancement of drones as weapons, greatly accelerated by the Ukrainian War, drones also blend the military/civilian divide. To add to the confusion, drones have legal protections, and the technology to interdict is

often in an legally ambiguous arena. Specifically, “if you bought and deployed all the emerging counter-drone technology available today inside America’s borders, you’d be breaking up to two dozen U.S. laws, dealing with everything from privacy to communications channels to aircraft interdiction” (Watson, n.d.). Related to jurisdiction is the need for collaboration. In many cases, effective response requires multiple organizations to work together, rapidly in real time (Pratama, 2025).

Weak Interdiction Methods

Respondents’ qualitative comments reflect tension present when considering interdiction methods, with many acknowledging the seriousness of the threat while expressing uncertainty about who is authorized to act, when, and how. Non-federal LEOs generally lack the tools to detect, identify, decide, and interdict UAS. However, respondents overwhelmingly rejected the idea that counter-drone operations should be handled exclusively by the military. This finding highlights a normative expectation among practitioners that domestic drone threats fall, at least in part, within the law enforcement mission, even when formal legal authority is limited.

Taken together, these findings suggest that the primary challenge facing law enforcement is not a lack of awareness about the drone threat, but rather a lack of clarity, capacity, and coordination to address it. Officers recognize drones as an emerging and potentially severe risk, yet many operate within environments that provide little in the way of guidance and training. This misalignment creates conditions under which response may be delayed or inconsistent, potentially increasing harm during critical incidents. These patterns directly motivate the policy recommendations that follow. Addressing the gap between threat perception and preparedness will require investments in training, clearer jurisdictional frameworks, and mechanisms to interdict that reflect the unique characteristics of the UAS threat. Without such reforms, LEOs are likely to remain aware of the problem while structurally constrained from addressing it effectively.

Policy Recommendations

The findings from this study point to a clear policy problem rather than a simple operational failure. Law enforcement officers widely perceive drones as a growing threat to public safety, yet most agencies lack the training and authority needed to respond effectively. This gap between perceived risk and response capacity suggests that policy interventions should focus on building foundational preparedness rather than assuming interdiction capability already exists. In light of these findings, we offer three policy recommendations.

More Training

Expanded and standardized counter-drone training is needed across LEAs. Only a small fraction of respondents (16%) reported receiving any counter-drone training, yet training was consistently associated with greater legal awareness, higher perceived threat, and greater engagement in departmental discussions. These findings suggest that training does not simply convey technical skills, but also shapes how officers recognize, interpret, and communicate about emerging threats. We therefore recommend the development of scalable counter-drone training modules that can be adapted to local, county, state, and federal agencies. Importantly, such training should emphasize detection, threat assessment, legal constraints, and interagency coordination rather than focusing narrowly on interdiction tactics that many agencies are not currently authorized to use. The NCUTC is expected to make strides in this area, but more research is needed on how this is rolling out.

More Collaboration

Policies should prioritize interagency collaboration rather than agency-specific solutions. Respondents repeatedly highlighted uncertainty surrounding responsibility, authority, and coordination when drone threats cross jurisdictional boundaries. This is not surprising given that drones routinely move across jurisdictional airspace that requires collaboration to counter. Our findings indicate that officers expect law enforcement to play a role in drone response, even if federal agencies retain primary interdiction authority. Policy efforts should therefore formalize communication pathways, joint training exercises, shared protocols, and common language beforehand rather than relying on ad hoc coordination during incidents. Collaborative frameworks may also reduce redundancy and allow agencies with limited resources to benefit from shared expertise.

Clarify Jurisdiction

Clearer articulation of jurisdictional authority and responsibility *prior* to an active event is necessary to reduce uncertainty and hesitation during potential drone-related incidents. Most respondents found the jurisdictional environment to be unclear, and that is in part due to opaque UAS jurisdictional responsibilities. The observed jurisdictional ambiguity creates the risk of delayed response or inaction during these time-sensitive incidents. Policymakers should seek to clarify not only who has authority to interdict drones, but also what actions are permissible short of interdiction, including detection, evidence collection,

communication with partners, and coordination with aviation authorities. Clarifying these roles does not require expanding interdiction powers to all agencies, rather, it ensures that officers understand their lawful options and obligations within the existing legal framework.

Taken together, these recommendations emphasize preparedness over reaction. The absence of fatal drone attacks in the United States should not be interpreted as evidence that existing policies are sufficient, particularly given respondents' widespread belief that the threat is growing. Proactive investments in training, coordination, and legal clarity may reduce the likelihood that law enforcement agencies are forced to develop policy in the aftermath of a catastrophic event. By addressing these issues now, policymakers can better align law enforcement capacity with the emerging risks posed by unmanned aerial systems.

Limitations and Future Work. This study seeks to contribute to a clearer understanding of law enforcement perceptions of the threat posed by UAS and agencies' preparedness to address it. Because it is based on a survey of law enforcement practitioners rather than solely the authors' interpretations, it offers direct insight into how the threat is viewed by those at the forefront of this issue. At the same time, the study is not based on a random or comprehensive sample of law enforcement personnel and the generalizability of the findings should be interpreted with caution. The sample has a notable Texas focus, which may limit generalizability to agencies in other states with different legal, organizational, or threat environments. Participation was voluntary, raising the possibility of selection bias if respondents differ systematically from non-respondents. Additionally, the anonymous design prevented us from linking responses to specific agency or jurisdictional characteristics (e.g., federal agency type, rural vs. urban context). This is particularly important for the findings around training, agencies who view the threat as higher might invest more in counter-drone training, potentially contributing to the significant association. Future research should address these limitations through broader sampling strategies and more detailed organizational data to further advance understanding of law enforcement perspectives on UAS threats.

Bottom line: Overall, law enforcement officers are identifying the growing threat posed by drones, and express concern about the lack of capabilities and options available to them for response. This threat represents an urgent matter that requires policy intervention prior to an active attack. History has demonstrated the dramatic policy shifts (and possible over-reactions) that a new type of terrorist attack can produce (e.g., 9/11). There is still time to calmly and deliberately address the UAS issue prior to a tragic, mass casualty event. LEOs are raising the alarm, and it is imperative that we listen to them.

Authors' Note

The views presented are those of the authors and do not necessarily represent the views of the US Department of Defense, the Department of the Navy, or the Naval Postgraduate School.

ORCID iD

Andrea Corradi  <https://orcid.org/0000-0003-4612-2292>

Funding

The authors received no financial support for the research, authorship, and/or publication of this article.

Declaration of Conflicting Interests

The authors declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Note

1. Sensitivity analyses demonstrate that pre-imputation and post-imputation results are substantively identical with the exception of gender in Model 1, due to the already small number of females, and county jurisdiction in Models 4 and 5 when hovering around the level of significance. Pre-imputation models are available upon request.

References

- Agius, C. (2017). Ordering without bordering: Drones, the unbordering of late modern warfare and ontological insecurity. *Postcolonial Studies*, 20(3), 370–386. <https://doi.org/10.1080/13688790.2017.1378084>
- Agwu, F. A. (2017). *Armed drones and globalization in the asymmetric war on terror: Challenges for the law of armed conflict and global political economy*. Routledge.
- Almohammad, A., & Speckhard, A. (2017). ISIS drones: Evolution, leadership, bases, operations and logistics. *International Center for the Study of Violent Extremism*, 1–17.
- Andridge, R. R., & Little, R. J. A. (2010). A review of hot deck imputation for survey non-response. *International Statistical Review = Revue Internationale de Statistique*, 78(1), 40–64. [10.1111/j.1751-5823.2010.00103.x](https://doi.org/10.1111/j.1751-5823.2010.00103.x)
- Barten, D. G., Tin, D., De Cauwer, H., Ciottone, R. G., & Ciottone, G. R. (2022). A counter-terrorism medicine analysis of drone attacks. *Prehospital and Disaster Medicine*, 37(2), 192–196. <https://doi.org/10.1017/s1049023x22000139>
- Buczek, J., & Powers, S. (2024, September 6). Green Day rushed off the stage at Detroit concert after drone flies over show. *CBS News*. <https://www.cbsnews.com/detroit/news/green-day-rushed-off-the-stage-at-detroit-concert/>

- Bunker, R. J. (2015). *Terrorist and insurgent unmanned aerial vehicles: Use, potentials, and military implications* (pp. 13–27). Strategic Studies Institute, US Army War College.
- CBS News. (2023, June 5). Unauthorized drone causes temporary ground stoppage at Pittsburgh International Airport. *CBS News*. <https://www.cbsnews.com/pittsburgh/news/pittsburgh-international-airport-ground-stoppage-drone/>
- Charmaz, K. (2017). The power of constructivist grounded theory for critical inquiry. *Qualitative Inquiry*, 23(1), 34–45. <https://doi.org/10.1177/1077800416657105>
- Corradi, A., Sanders, C. B., & Popham, J. (2020). “But I’m standing inside right now and i need help”: Security projects and the perceptions of campus security. *Journal of Qualitative Criminal Justice & Criminology*, 9, 8. <https://doi.org/10.21428/88de04a1.0a0f9aa6>
- Cox, T. E. (2023). Man who flew drone over Ohio State–Maryland game facing charges. *KIRO 7*. <https://www.kiro7.com/news/trending/man-who-flew-drone-over-ohio-state-maryland-game-facing-charges/Z4PKB63L6RFX3BVDHLTRYIPXIA/>
- Creswell, J. W., & Plano Clark, V. L. (2007). *Designing and conducting mixed methods research*. Sage.
- Department of Justice. (2024). *Man arrested and charged with attempting to use a weapon of mass destruction and to destroy an energy facility in Nashville*. U.S. Department of Justice Archives. <https://www.justice.gov/archives/opa/pr/man-arrested-and-charged-attempting-use-weapon-mass-destruction-and-destroy-energy-facility>
- Doctor, A. C., Cubukcu, S., Elson, J., Grispos, G., & Harms, M. (2026). *Mapping weaponized drone attacks attributed to Mexican drug cartels 2021-2025*. NCITE.
- Doctor, A. C., Cubukcu, S., Elson, J., Grispos, G., & McCoid, T. (2025a). *Rapid review A: The logic of terrorist use of unmanned aerial systems, enabling factors, and barriers to exploitation*. NCITE.
- Doctor, A. C., Cubukcu, S., Elson, J., Grispos, G., & McCoid, T. (2025b). *Rapid review B: Risk factors in terrorist use of unmanned aerial systems*. NCITE.
- Dulligan, J., Freeman, L., Phoenix, A., & Davis, B. (2025). The rising threat of non-state actor commercial drone use: Emerging capabilities and threats. *CTC Sentinel*, 18(3), 39–45.
- Etikan, I., Musa, S. A., & Alkassim, R. S. (2016). Comparison of convenience sampling and purposive sampling. *American Journal of Theoretical and Applied Statistics*, 5(1), 1–4. <https://doi.org/10.11648/j.ajtas.20160501.11>
- Farrar, D. (2022, September 25). Atlanta Falcons–Seattle Seahawks game at Lumen Field stopped due to unlicensed drone. *USA Today*. <https://www.usatoday.com/story/sports/nfl/2022/09/25/seahawks-falcons-game-delayed-drone-over-lumen-field/8116976001/>
- Federal Aviation Administration. (n.d.). *Law enforcement guidance for suspected unauthorized UAS operations*. U.S. Department of Transportation. https://www.faa.gov/sites/faa.gov/files/uas/resources/policy_library/FAA_UAS-PO_LEA_Guidance.pdf
- Funk, J. (2025). *U.S. Government proposes easing some restrictions on drones traveling long distances*. Associate Press.

- Graham, A., Kutzli, H., Kulig, T. C., & Cullen, F. T. (2021). Invasion of the drones: A new frontier for victimization. *Deviant Behavior*, 42(3), 386–403. <https://doi.org/10.1080/01639625.2019.1678973>
- Greene, J. C., Caracelli, V. J., & Graham, W. F. (1989). Toward a conceptual framework for mixed-method evaluation designs. *Educational Evaluation and Policy Analysis*, 11(3), 255–274. <https://doi.org/10.3102/01623737011003255>
- Haugstvedt, H., & Jacobsen, J. O. (2020). Taking fourth-generation warfare to the skies? An empirical exploration of non-state actors' use of weaponized unmanned aerial vehicles (UAVs—'drones'). *Perspectives on Terrorism*, 14(5), 26–40.
- Hummel, S., & Burpo, F. J. (2020). *Small groups, big weapons: The nexus of emerging technologies and weapons of mass destruction terrorism*. Combating Terrorism Center. <https://apps.dtic.mil/sti/html/trecms/AD1100991/>
- Hutto, J. W., & Patton Rogers, J. (2025). The drone revolution: Towards a synthesis in the drone debate. *European Journal of International Security*, 11(2), 1–21. <https://doi.org/10.1017/eis.2025.10005>
- Ilijevski, I., Dimovski, Z., & Babanoski, K. (2021). The weaponisation of drones—a threat from above used for terrorist purposes. *Journal of Criminal Justice and Security*, 3, 336–349.
- Ito, T. (2025). Intelligence failures in the asymmetric war between Ukraine and Russia: A literature review of Ukraine's drone attacks on Russian military infrastructure. *Security Intelligence Terrorism Journal (SITJ)*, 2(3), 262–273. <https://doi.org/10.70710/sitj.v2i3.63>
- Jones, N. P., Sullivan, J. P., & Davis, G. W. (2025). Detecting drone threats at stadiums and public venues. *Journal of Strategic Security*, 18(3), 372–414.
- Kallenborn, Z., & Bleek, P. C. (2018). Swarming destruction: Drone swarms and chemical, biological, radiological, and nuclear weapons. *The Nonproliferation Review*, 25(5–6), 523–543. <https://doi.org/10.1080/10736700.2018.1546902>
- Kirichenko, D. (2025, June 5). Ukraine's cheap robot drones extract a heavy price from Russia. *The Interpreter*. <https://www.lowyinstitute.org/the-interpreter/ukraine-s-cheap-robot-drones-extract-heavy-price-russia>
- Kunstner, J., Berndsen, S., & Haider, A. (2021). Law enforcement. In *A comprehensive approach to countering unmanned aircraft systems* (pp. 319–336). The Joint Air Power Competence Centre.
- Lamont, M., & Swidler, A. (2014). Methodological pluralism and the possibilities and limits of interviewing. *Qualitative Sociology*, 37(2), 153–171. <https://doi.org/10.1007/s11133-014-9274-z>
- Lasconjarias, G., & Maged, H. (2019). Fear the drones: Remotely piloted systems and non-state actors in Syria and Iraq. *IRSEM, École Militaire, Place Joffre 75700 PARIS SP*, 07, 1–20.
- Lightfoot, T. R. (2018). Bring on the drones. *Natural Resources & Environment*, 32(4), 41–45.
- Long, J. S., & Freese, J. (2006). *Regression models for categorical dependent variables using Stata* (2nd ed.). Stata Press.

- McAuley, W. (2021). Jurisdictional challenges in the 21st century security environment: Subnational design-basis threats. *The Journal of Intelligence, Conflict, and Warfare*, 4(1), 7–25.
- Morrow, A., Pitsky, P., & Samani, A. (2021). Protection of critical infrastructure. In Col Matthew Willis (US AF), Lt Col André Haider (GE A), Lt Col Daniel C. Teletin (RO AF), Lt Col Daniel Wagner (GE AF) (Eds.), *A comprehensive approach to countering unmanned aircraft systems* (pp. 303–318). The Joint Air Power Competence Centre.
- National Defense Authorization Act for Fiscal Year 2026, S. 1071, 119th Cong. (2025) (enacted as Pub. L. No. 119–60).
- Nicas, J., & Villegas, P. (2026, February 12). Do drug cartels actually use drones at the border? *The New York Times*. <https://www.nytimes.com/2026/02/12/world/americas/mexico-drone-border-cartels.html>
- Page, L. (2018). Drone trespass and the line separating the national airspace and private property note. *George Washington Law Review*, 86(4), 1152–1180.
- Pettyjohn, S., & Campbell, M. (2025, September 10). *Countering the swarm: Protecting the Joint Force in the drone age*. Center for a New American Security. <https://www.cnas.org/publications/reports/countering-the-swarm>
- Pickering, J. C., & Fox, A. M. (2022). Enabling collaboration and communication across law enforcement jurisdictions: Data sharing in a multiagency partnership. *Criminal Justice Policy Review*, 33(7), 732–755. <https://doi.org/10.1177/08874034211066756>
- Pledger, T. (2021). The role of drones in future terrorist attacks. *Association of the United States Army*, 26.
- Pratama, S. Y. (2025). Collaborative state apparatus strategy in countering autonomous drone threats to the president and vice president of the Republic of Indonesia. *Security Intelligence Terrorism Journal (SITJ)*, 2(2), 129–138.
- Rassler, D. (2016). *Remotely piloted innovation: Terrorism, drones and supportive technology*. Combating Terrorism Center.
- Rassler, D. (2024). Going the distance: The emergence of long-range stand-off terrorism. *CTC Sentinel*, 17(2), 1–10.
- Rassler, D., & Veilleux-Lepage, Y. (2025). On the horizon: The Ukraine war and the evolving threat of drone terrorism. *CTC Sentinel*, 18(3), 1–24.
- Ross, C. T., & Jinks, K. M. (2021). Doj and drones: Protection: Policy, and enforcement. *Department of Justice Journal of Federal Law and Practice*, 69(3), 275–288.
- Russo, J., Woods, D., Peterson, S., Vermeer, M. J., & Jackson, B. A. (2024). *Countering the emerging drone threat to correctional security*. RAND.
- S.2836 - 115th Congress (2017–2018): Preventing Emerging Threats Act of 2018. (2018). <https://www.congress.gov/bill/115th-congress/senate-bill/2836>
- Shuster, S. (2025, September 24). *How Ukraine gamified drone warfare*. Time. <https://time.com/7319847/>
- Sim, S., Hartunian, E., & Milas, P. J. (Eds.). (2024). *Emerging technologies and terrorism: An American perspective*. Strategic Studies Institute; NATO COE-DAT; U.S. Army War College.

- Sims, A. (2018). The Rising Drone Threat from Terrorists. *Georgetown Journal of International Affairs*, 19(1), 97–107. <https://doi.org/10.1353/gia.2018.0012>
- Snead, J., Seibler, J. M., & Inserra, D. (2018). *Establishing a legal framework for counter-drone technologies*. Heritage Foundation.
- Snyder, T. (2022, July 21). *Errant drone briefly shuts down D.C. airport*. Politico. https://www.politico.com/news/2022/07/21/drone-dc-airport-shutdown-00047213?utm_campaign=Bundle&utm_medium=referral&utm_source=Bundle
- Tesauro, L. L. (2025). *Drone incident reporting in the United States: The impact it has on the overall domestic drone threat* [Doctoral dissertation, Saint Leo University].
- The Associated Press. (2025). *A Ukrainain startup develops long-range drones and missiles to take the battle to Russia*. The Associated Press. <https://www.ap.org/news-highlights/spotlights/2025/a-ukrainian-startup-develops-long-range-drones-and-missiles-to-take-the-battle-to-russia/>
- Tin, D., Kallenborn, Z., Hart, A., Hertelendy, A. J., & Ciottone, G. R. (2021). Rise of the unmanned aerial vehicles: An imminent public health threat mandating counter-terrorism medicine preparedness for potential mass-casualty attacks. *Prehospital and Disaster Medicine*, 36(5), 636–638. <https://doi.org/10.1017/s1049023x21000765>
- Todak, N., & Somers, L. J. (2025). A tutorial on mixed methods research for policing scholars. *The Police Journal: Theory, Practice and Principles*, 98(2), 426–441. <https://doi.org/10.1177/0032258x241299749>
- Watson, B. (n.d.). Against the drones. *Defense One*. <https://www.defenseone.com/feature/against-the-drones/>
- Williams, R. (2025, December 1). Contraband is entering Georgia prisons from the sky as drone drops rise again, state agency says). *Georgia Recorder*. <https://georgiarecorder.com/briefs/contraband-is-entering-georgia-prisons-from-the-sky-as-drone-drops-rise-again-state-agency-says/>
- Zapotosky, M. (2015, September 22). Three indicted in attempt to smuggle contraband by drone into Maryland prison. *The Washington Post*. <https://go.gale.com/ps/i.do?id=GALE%7CA429510849&sid=googleScholar&v=2.1&it=r&linkaccess=abs&issn=01908286&p=AONE&sw=w&userGroupName=anon%7Ef17ce2b6&aty=open-web-entry>

Author Biographies

Dr. Andrea Corradi is an Assistant Professor in the Department of Criminal Justice and Criminology at Georgia Southern University, and Director of the Extremism Research Lab. Her research areas include the use of mechanisms of social control, extremism, security, and the use of innovative research methods including social network analysis and mixed-methods.

Dr. Scott Sigmund Gartner is a Professor of Defense Analysis and past Provost at the Naval Postgraduate School. Gartner was previously Director of the Penn State School of International Affairs (and remains affiliated). His over fifty publications

include *Costly Calculations: A Theory of War, Casualties and Politics* and *The Historical Statistics of the United States*. His honors include the Jefferson award for best government resource and the APSA's best policy thesis award.

Molly Lynn is a Biostatistics graduate student in the Masters of Public Health program at Georgia Southern University. She works in Extremism Research Lab as a Graduate Research Assistant. With a B.S. in Psychology from East Tennessee State University, her research topics include extremism and behavior, diagnostic accuracy, and data analytics.

Dr. M. Hunter Martaindal is Director of Research at the ALERRT Center and Associate Research Professor in the School of Criminal Justice and Criminology at Texas State University. His work focuses on police decision making, officer performance under stress, and evidence-based training. He leads multidisciplinary projects on active attack response, physiological stress, and virtual reality-based training evaluation. He has published widely in CJ outlets and collaborates with agencies nationwide to advance research driven approaches to police training and public safety.

Dr. Logan J. Somers is an Assistant Professor in the School of Criminal Justice and Criminology at Texas State University. His research focuses largely on officer work experiences, police use of force, police culture, and policy. He has published in leading journals such as *Justice Quarterly*, *Criminal Justice & Behavior*, and *Criminology and Public Policy*