INSTITUTE FOR HOMELAND SECURITY

Sam Houston State University

DETECTING DRONE (UNMANNED OR UNCREWED AERIAL SYSTEM) THREATS AT STADIUMS (STADIA) AND PUBLIC VENUES:

OPERATIONAL PERSPECTIVES

Institute for Homeland Security

Sam Houston State University

John P. Sullivan

Nathan P. Jones

George W. Davis

August 2022

Detecting Drone (Unmanned or Uncrewed Aerial System) Threats at Stadium (Stadia) and Public Venues: Operational Perspectives

John P. Sullivan
Nathan P. Jones
George W. Davis

The potential use of aerial drones—or small unmanned or uncrewed aerial systems (sUAS)—to attack or disrupt outdoor public gatherings or sports events at stadiums (stadia), race tracks, or other outdoor venues is a serious public safety concern. It is also a concern to the operators of these facilities since it can have devastating business consequences that amplify the threat to human life. Terrorist threats employing weaponized consumer drones have been a growing concern since the mid-1990s.

Terrorist and Criminal Drone Use

Both terrorist and criminal armed groups (CAGs) have embraced drones to further their goals Indeed, significant terrorist drone incidents include attempts by the Japanese cult Aum Shinrikyo to weaponize a remote control helicopter to deploy the nerve agent sarin in 1994, a thwarted multi-drone assault by al-Qaeda in Pakistan, the continued deployment of commercial off-the-shelf (COTS) and artisanal drones by the Islamic State (IS) in Iraq and Syria.[1] In Northern Iraq and Syria, the IS branch known as the Islamic State of Iraq and the Levant flew modified commercial drones (especially Chinese Da-Jiang Innovations (DJI) Phantom quadcopter), as well as bespoke drones yielding 60 to 100 drone attacks per month during its heyday in 2017.[2]

Drones were also used in an assassination attempt directed against Venezuelan President Nicolás Maduro on 4 August 2018. In that incident, two small explosive-laden DJI M600 drones were detonated during an outdoor speech in Caracas; up to 8 persons were injured.[3] In addition, drones have been used to target military Russian bases in Syria and an Indian Air Force base in Jammu, Kashmir.[4] In Mexico, criminal cartels have used drones to attack the home of the Baja California Public Safety Secretary, attack police and military vehicles, and attack rival cartels and gangs.[5] In Ukraine, Ukrainian forces are using COTS drones to counter the Russian invasion, with modified drones (including DJI Mavic 3 drones) adapted to drop improvised munitions (based on grenades).[6] In addition, Ukraine's *Aerorozvidka* (aerial reconnaissance) volunteers have shown how consumer drones can be adapted into loitering munitions capable of precision strikes, help acquire targets, direct artillery fire, conduct battle damage assessment, and deliver grenades on target.[7]

Weaponized Commercial "Kamikaze" Drone in Ukraine. Ukraine Weapons Tracker, *Twitter*, 29 July 2022, https://twitter.com/UAWeapons/status/1553090460352135169?s=20&t=_fi_lPRrDWkR5N_TsbS9sQ

Drone incidents have also become a concern at sporting events and public gatherings. Recently (30 July 2022), British police seized a drone that had been flown proximate to the Commonwealth Games festival site on Birmingham city center.[8] "Police protecting spectators and ensuring the safe running of the Commonwealth Games in Birmingham […] were quick to seize a drone and its pilots after the unmanned vehicle flew dangerously close to crowds; such incidents at sporting events are not new, […] but do highlight the potential threat posed by drones in crowded public spaces."[9] Anti-drone laser weapons systems are slated to be deployed to defend the 2024 Olympics in Paris.[10]

Protecting Sports Events and Venues from Drone Threats

Major sports events and public gatherings have long-been recognized as potential targets for terrorist attack. The threat against major sporting events (MSEs) has been clear since the 1972 Munich Olympic Attacks when eight Palestinian terrorists representing 'Black September' broke into the Olympic Village killing two members of the Israeli team and taking nine hostages who were ultimately killed.[11] Additional attacks against sports events include armed assault against the Sri Lankan cricket team, and Togo's football team, and the bombing of the Boston Marathon.[12] On 13 November 2015 three Islamic State suicide bombers attacked the Stade de

France (France's National Stadium) during the France vs. Germany game.[13] Threat analysts have been publicly warning about the threat and vulnerability of terrorist drone attacks directed against MSEs. The technology is affordable and accessible.[14]

Drones (sUAS) can be used to collect **intelligence, surveillance, and reconnaissance** (ISR) information for future targeting; to **smuggle contraband** (including drugs and small arms) into a facility (as is often seen at prisons and jails), to **distract and cause a diversion** for another means of attack (such as armed assault), to **deliver explosives** (such as grenades or improvised explosive devices – IEDs) or other threat agents (such as **weaponized chemical, biological or radiological agents or materials**), or to amplify the effects of those other means by filming and disseminating an attack on social media as a form of **propaganda or information operation**.

The Remote Control Project identified three types of countermeasures that can be used to address threats from non-state actors such as terrorist, insurgents, criminals, and activists deploying aerial drones (sUAS) for attacks and ISR. These are: **Regulatory Countermeasures**, **Passive Countermeasures**, and **Active Countermeasures**:[15]

- *Regulatory countermeasures* include enhanced legislation and regulations restricting drone use, limiting drone capability, establishing no-fly zones (for high risk events such as National Special Security Events), and requiring drone identification signals, and licensing.

- *Passive Countermeasures* involve deploying commercial sensor systems (especially multi-sensor systems) to detect, track, and identify drones within a defensive perimeter or no-fly zone and conceivably the use early warning systems, radio frequency and GPS at special events as allowed by legislation and regulations (in the US this is limited and controlled by the Federal Aviation Administration – FAA); defining the appropriate and lawful use of these technologies requires additional legislative and regulatory action.

- *Active Countermeasures* involves the deployment of less-lethal anti-drone systems, i.e., directional radio frequency jammers, laser, and computer malware, for use in dense urban terrain (in the US this is limited and controlled by the Federal Aviation Administration – FAA). Other active measures deployed outside the US include, the use of directed energy (laser) or kinetic weapons (including shotguns and antiaircraft guns), the use of capture nets, drone-on-drone countermeasures, and the use of predatory birds such as hawks or eagles to take down potential threat drones. Clear guideline on the use of force by the police, military, or other security services against hostile drones as a last resort when human life is threatened are essential; in the US these parameters remain unarticulated and still require legislative and regulatory clarity.

Sports venues are increasingly aware of potential drone threats from hostile actors. This awareness is also increasingly accompanied by police/law enforcement drone (UAS) teams that use UAS to protect the public from illegal or dangerous drone incursions as well as a range of other law enforcement missions (such as search and rescue, reconnaissance during high risk

events). For example, the Arlington, Texas Police use their own drones to augment commercial detection devices at AT&T Stadium during Dallas Cowboy Games—that is they can use their own piloted drone equipped with a camera to visually interrogate an unauthorized drone and its operator.[16] The FAA has authorized a temporary flight restriction (TFR) restricting flights within three nautical miles of a stadium hosting an NFL (National Football League), MLB (Major League Baseball, or NCCA Division A (National Collegiate Athletic Association) game starting one hour before the game starts—at AT&T Stadium that means an average of two unauthorized drones per Cowboys game/TFR.[17] According to the Federal Aviation Administrations (FAA):

> **Stadiums and Sporting Events**
>
> Flying drones in and around stadiums is prohibited starting one hour before and ending one hour after the scheduled time of any of the following events:
>
> - Major League Baseball
> - National Football League
> - NCAA Division One Football
> - NASCAR Sprint Cup, Indy Car, and Champ Series races
>
> Specifically, UAS operations are prohibited within a radius of three nautical miles of the stadium or venue. The FAA and SMA [Stadium Managers Association] have developed a toolbox for stadium management and team representatives to use for media and outreach purposes.[18]

This paper specifically addresses **passive countermeasures**. It does so by looking at a specific case. The case selected involves the presence of consumer drones entering the airspace around the stampede/crushing incident at the Travis Scott Concert at the Houston *Astroworld Festival*. The festival occurred on 5 November 2021 at NRG Park in Houston, Texas. A stampede led to a mass casualty incident (MCI), leaving eight dead on scene and two additional deaths in hospital.[19] This report does not dissect that event on the ground, but rather looks at the increase of drone traffic above and proximate to the incident ground in order to discuss operational issues (including recognizing threats and mitigating incidents) and demonstrate the capabilities and limitations of drone detection technology (which are specifically discussed in greater detail in Part 3 of this series).

Crafting an Operational Response to Drone Threats

Anticipating and responding to drone (sUAS) threats at stadia, sports venues, and public gatherings requires a foundation in **awareness**. First, facility and event operators, as well as public safety agencies (police/law enforcement, fire service, emergency medical service), and event crowd management/security staff need to **recognize the threat**, appreciate the **baseline level of threat,** and be aware of the specific **tactics, techniques, and procedures (TTPs**) that can be directed against them by **potential threat actors**. Next, they need to be aware of the **limitations of the drones (sUAS)** that can be directed against their facilities (this includes range,

speed, altitude, payload capacity, and potential weapons effects. Next, they need to recognize the range of **potential threat actions** (described above) and place specific drone actions and signatures into context. Finally, they need to know the **range of countermeasures** available to them (under the law and regulatory framework where they operate) and have an understanding of the technology available to **detect potential drone threats**.[20]

Active drone countermeasures are limited in the US:

> Domestically, counter-UAS activities may be restricted or prohibited by existing federal laws such as the Aircraft Sabotage Act or the Computer Fraud and Abuse Act. However, four federal agencies—the Departments of Defense, Energy, Justice, and Homeland Security—have been authorized to deploy counter-UAS technologies under certain circumstances, such as to protect sensitive government facilities, including domestic military bases and prisons, or to provide security during sports championships.[21]

According to the Government Accountability Office (GAO), counter-UAS technologies fall into two broad categories: **detection** and **mitigation**. Detection technologies include infrared devices to track heat signature, radio frequency (RF) systems to track control systems, acoustic sensors to recognize UAS motors, radar, and of course visual sighting. Mitigation technologies can intercept or repel unauthorized UAS by jamming signals. Using nets, or kinetic means such as lasers or projectiles. Only four federal agencies are authorized to conduct counter-UAS (C-UAS) operations and no state or local agencies have that authority.[22] The Preventing Emerging Threats Act of 2018 gives the DHS statutory authority to counter credible UAS threats (C-UAS).[23]

DHS may employ the following actions: **1) Detect, identify, monitor UAS**, 2) **Warn UAS operator(s)**, 3) **Disrupt control of the UAS**, 4) **Seize or exercise control of the UAS**, 5) **Seize of confiscate the UAS**, and 6) **Use reasonable force to interdict** (*i.e.,* disable, damage, or destroy the UAS).[24]

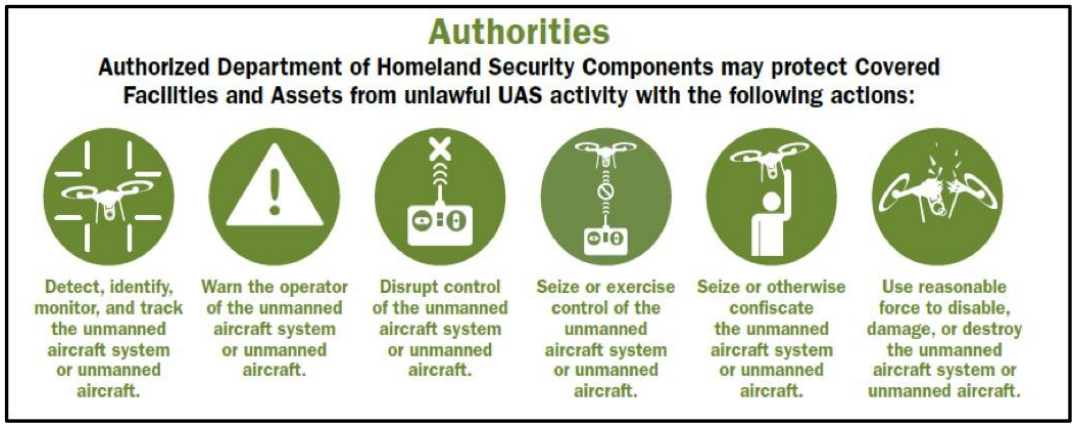

Figure 1: Department of Homeland Security Counter-UAS Authorities; Source DHS

These C-UAS actions can be conducted during certain protection and security missions of the **Coast Guard**, **Customs and Border Protection**, **Secret Service**, and **Federal Protective Service**. They can also be deployed during authorized joint DHS and DOJ missions such as **National Special Security Events (NSSEs**), **Special Event Assessment Rating Events (SEARs)**, state, local, tribal territorial (SLTT) mass gatherings at request of a state's governor, and active federal law enforcement investigations, emergency responses (including disaster response) or security operations.[25]

As consumer-grade UAS proliferate the potential for serious safety and security issues arising from rogue drone use is growing. Many observers believe that local police, sheriff's departments, and law enforcement agencies (LEAs) are not adequately equipped to address the potential threats.[26] LEAs—especially those protecting mass gatherings, special events, and sports venues need additional training and policy to effectively respond. Some recent initiatives, such as the White House "Domestic Counter Unmanned Aircraft Systems National Action Plan" seek to remedy this shortfall.[27] The FAA is also evaluating detection and mitigation systems toward filling the strategic gap in assessing UAS detection and C-UAS programs.[28]

C-UAS Challenges

The challenges involved in C-UAS action (detection and mitigation) include **effectiveness** (including limited detection capability and false positives or negatives); *unintended effects* (interfering with proximate communications and navigation systems, kinetic unintended consequences from errant projectiles or fallen drones); and limited legal authorities and organizational capacity.[29]

The federal agencies authorized to protect covered facilities and assets from UAS threats are the Departments of Defense (DOD), Energy (DOE), Justice (DOJ), and Homeland Security (DHS).[30] The legal framework covering the technical tools, systems, and capabilities for detecting and mitigating UAS (*i.e.*, C-UAS) are articulated in the United States Code administered by the DOJ and in federal regulations administered by the FAA (Federal Aviation Administration, DHS, and FCC (Federal Communication Commission).[31] Civil liability may also accompany unauthorized counter-UAS (C-UAS) mitigation actions, including unlawful interception of wire, oral, or electronic communications.[32] Additional Federal legislation and regulatory guidance is needed to clarify the scope of potential actions by state, local, territorial, and tribal (SLTT) agencies when addressing hostile drone/UAS threats.[33]

Taking Action

Once a rogue or hostile drone (UAS) enters an area of interest (the designated defensive perimeters for a named area of interest (NAI)), it is imperative to determine the drone's "intent" and threat potential. Threat can be assessed in terms of Path, Pace, Proximity, drone Potential, Payload, and crowd size or People, and Swarm(ing) capacity.[34]

- **Path:** For Path, the drone could be going away or meandering from the NAI, the drone could be tangentially crossing outside the perimeter, tangentially approaching the primary perimeter, or directly, loitering on a potential target.

- **Pace:** Pace could range from hovering to slow, medium, or fast speed (defined in nautical miles).

- **Proximity:** Proximity is defined by position outside the perimeters or within defined tertiary, secondary, and primary perimeters (each acting as tripwires for defensive actions as the drone closes on the area of maximum exposure).

- **Potential:** Drone Potential can be defined as standard COTS drone, Premium COTS drone, slightly modified drone, or a heavily modified drone.

- **Payload:** Payload could be small, medium or large in terms of potential munition capacity, as well as evidence of possible aerosol dispersal capacity for chemical, biological agents, or radiological sources (*i.e*., a radiological dispersal device or RDD).

- **People**: The crowd size or number of people could range from an average or small event to a minor, moderate, or major entertainment, sport or political event.

- **Swarm**(ing): Presence of multiple co-ordinated drones with central control or artificial intelligence (AI) control.

Known threat communications or intelligence, as well as designated high threat time frames, could raise threat potentials for observed drone incursions. The impact or criticality of an incursion could range from a low risk annoyance or distraction (or reconnaissance event), a disruptive event with minor casualty expectations (injuries and deaths), or a major disruption with high casualty expectations. These can be assessed, rated and provided to a designated decision authority to determine scope of action, warning, evacuation, or active countermeasures, ranging from locating, disrupting, or destroying the drone.

In the case of UAS or drone(s) conducting reconnaissance or recce, that is, being utilized for intelligence, surveillance, or reconnaissance (ISR). Terrorist or hostile ISR can be broken down into observable components. These are **casing, reconnaissance, and surveillance**, with casing (which is the term used by police for reconnaissance) including both reconnaissance (observation at a single point in time) and surveillance (an on-going observation/collection effort). Hostile recon or recce occurs during five discrete phases of activity (four pre-attack and one post-attack). These are: Pre-attack recon supporting, 1) **target selection**, 2) **mission planning**, 3) **pre-execution** (confirmation of favorable attack conditions), and 4) **refreshing standing attack plan(s)**. Post-attack recon, 5) is essentially "**battle damage assessment**" (BDA).

Recon discrimination requires the following components:

- Specificity and sensitivity are key elements in signature discrimination. Factors involved are: geospatial intelligence (GEOINT)—activity and target (a baseline is needed)—and actor(s)—which include agents(s), operative(s), and exploited person(s). Discriminating among the various types of actors performing ISR requires social network analysis and/or human intelligence. Together assessment of GEOINT and actor(s) equals "geosocial" intelligence.

- Specific factors that aid in discrimination of recon phases include loiter time, persistence/repetition, and specificity. Additional information valuable to assigning a signature include the tools (cameras, video, sensors, etc. used during the recon, as well as the number of persons involved or observed).[35]

Once a potential hostile drone recon is detected and documented, it must be shared with the facility/event manager, its security director, and local LEAs. It must also be shared with the security directors proximate to mass gathering venues, and both DHS and Federal Bureau of Investigation (FBI) threat assessment squads at local field offices and regional fusion centers.[36] Threats must be evaluated according to intent and "communicated threats are normally assessed from three viewpoints: operational practicality, technical feasibility, and the behavioral resolve of the individual(s) communicating the threat."[37] Furthermore threats can be further assessed in terms of risk and criticality or level of impact on people, an agency or venue, and their relative vulnerability. These in turn can be rated high medium or low.[38]

Once a rogue and potentially hostile drone is detected by sensors and signature identification signals, its track must be recognized and visualized on a graphic user interface so a threat analyst and decision authority can determine countermeasures or protective actions (evacuation, in place protection, requesting and staging specialized resources, and emergency medical response, etc. All of these are time critical actions. These can be aided by technical capabilities such as geospatial mapping and evacuation modelling.[39]

A discussion of technical aspects of drone detection counter-drone actions is provided in the next segment, Part 3 of this series.

Author Bios

Nathan P. Jones is an Associate Professor of Security Studies in the college of Criminal Justice at Sam Houston State University. He is the author of Georgetown University Press's peer reviewed book *Mexico's Illicit Drug Networks and the State Reaction (2016)*. His areas of interest include organized crime violence in Mexico, drug trafficking organizations, social network analysis, border security, and the political economy of homeland security. Dr. Jones is also a Senior Fellow with the Small Wars Journal - El Centro, a Rice University Baker Institute Drug Policy and US-Mexico Center non-resident scholar, and the Book Review Editor for the Journal of Strategic Security. Prior to joining the Sam Houston State University Security Studies Department, Dr. Jones was the Alfred C. Glassell III Postdoctoral Fellow in Drug Policy at Rice University's Baker Institute for public policy, where his research focused on drug violence in Mexico.

Dr. John P. Sullivan was a career police officer, now retired. Throughout his career he has specialized in emergency operations, terrorism, and intelligence. He is an Instructor in the Safe Communities Institute (SCI) at the University of Southern California, Senior El Centro Fellow at *Small Wars Journal*, and Contributing Editor at *Homeland Security Today*. He served as a lieutenant with the Los Angeles Sheriff's Department, where he has served as a watch commander, operations lieutenant, headquarters operations lieutenant, service area lieutenant, tactical planning lieutenant, and in command and staff roles for several major national special security events and disasters. Sullivan received a lifetime achievement award from the National Fusion Center Association in November 2018 for his contributions to the national network of intelligence fusion centers. He has a PhD from the Open University of Catalonia, an MA in urban affairs and policy analysis from the New School for Social Research, and a BA in Government from the College of William & Mary.

George W. Davis Jr. specializes in providing technology solutions to the defense and public safety sectors. He is a specialist in geospatial Information Systems and Geospatial Intelligence (GEOINT). After the 9/11 2001 attacks at the World Trade Center he supported the Emergency Mapping and Data Center (EMDC), mapping the area around Ground Zero as well as most of Manhattan south of Canal Street. He served as Geospatial Information Coordinator for the New York Metro Chapter of Infragard. He has worked with the Department of Homeland Security (DHS), New York Police Department (NYPD), FBI, Los Angeles Sheriff's Department (LASD), the Lower Manhattan Security Initiative, and the Business Emergency Operations Center (BEOC) Alliance in New Jersey. Projects included mapping and aerial photography for several national and international disasters (Hurricanes: Charley, Katrina, Rita, Ike and Hugo), the Haiti Earthquake and the Sri Lanka Tsunami, using LIDAR, 3D Modeling software, Unmanned Aerial Systems (Drones), Thermal Imaging, Ground Penetrating Radar (GPR), GPS, and other remote sensing technologies.

Notes

[1] Thomas G. Pledger, "The Role of Drones in Future Terrorist Attacks," Land Warfare paper No. 137. Washington, DC: Association of the United States Army, February 2021; Robert J. Bunker, *Terrorist and Insurgent Unmanned Aerial Vehicles: Use, Potentials, and Military Implications* (Carlisle Barracks: Strategic Studies Institute, U.S. Army War College, August 2015).

[2] T.S. Allen, Kyle Brown, and Jonathan Askonas, "How the Army Out-Innovated the Islamic State's Drones." *War on the Rocks*, 21 December 2020, https://warontherocks.com/2020/12/how-the-army-out-innovated-the-islamic-states-drones/.

[3] "Venezuela President Maduro survives 'drone assassination attempt'," *BBC*, 5 August 2018, https://www.bbc.com/news/world-latin-america-45073385; "Venezuela says it has ID'd mastermind, accomplices in apparent Maduro assassination try." *CNN*, 6 August 2018, https://www.cnn.com/2018/08/06/americas/venezuela-maduro-apparent-assassination-attempt/index.html.

[4] David Reid, "A Swarm of Armed Drones Attacked a Russian Military Base in Syria," CNBC, 11 January 2018, https://www.cnbc.com/2018/01/11/swarm-of-armed-diy-drones-attacks-russian-military-base-in-syria.html; Aijaz Hussain, "Drone Attacks on Indian Air Force Base in Jammu Underscore New Threat," 28 June 2021, https://thediplomat.com/2021/06/drone-attacks-on-indian-air-force-base-in-jammu-underscore-new-threat/.

[5] Robert J. Bunker and John P. Sullivan, "Mexican Cartels are Embracing Aerial Drones and They're Spreading," War on the Rocks, 11 November 2021; Robert J. Bunker and John P. Sullivan, eds, *Criminal Drones Evolution: Cartel Weaponization of Aerial IEDs* (Bloomington: Xlibris, 2021).

[6] Pierre Ayad and Pariesa Young, "Ukrainian soldiers are turning consumer drones into formidable weapons of war," *The Observers* (France 24), 8 August 2022, https://observers.france24.com/en/europe/20220808-ukraine-russia-modified-commercial-drones-battlefield-donations-weapons?ref=tw_i.

[7] David Hambling. "Ukraine Racing Drone Converted Into Loitering Munition Makes Precision Strike Through Doorway." *Forbes*, 1 August 2022, https://www.forbes.com/sites/davidhambling/2022/08/01/ukraine-racing-drone-converted-into-loitering-munition-makes-precision-strike-through-doorway/amp/.

[8] Nick Horner, "Drone seized in Birmingham after being flown 'dangerously' over Commonwealth Games crowds." Birmingham Live, 30 July 2022, https://www.birminghammail.co.uk/news/midlands-news/drone-seized-birmingham-after-being-24630389.

[9] Andrew Stanniforth, "Commonwealth Games drone incursion highlights the threat from rogue operators," *Policing Insight*, 4 August 2022, https://policinginsight.com/features/commonwealth-games-drone-incursion-highlights-the-threat-from-rogue-operators/.

[10] Eliott Brennan, "Anti-drone laser weapon system to be used to defend Paris 2024." *Inside the Games*, 4 August 2022, https://www.insidethegames.biz/articles/1126595/anti-drone-laser-system#.YvEkaevRC9E.twitter.

[11] Andrew Silke and Anastasia Filippidou, "What drives terrorist innovation? Lessons from Black September and Munich 1972." *Security Journal* 33, 210–227, 210-227, 2020, https://doi.org/10.1057/s41284-019-00181-x.

[12] Yair Gailily, Morgan Yarchi, Ilan Tamir, and Tal Samuel-Azran, "Terrorism and Sport: A Global Perspective," *American Behavioral Scientist* 60, no. 9, https://doi.org/10.1177/0002764216632839.

[13] This attack at the Football (soccer) ga=me was part of a broader swarming attack involving three co-ordinated teams. A concert hall, restaurants and bars were attacked near simultaneously leaving 130 persons dead and hundreds wounded. "Paris attacks: What happened on the night." BBC, 9 December 2015, https://www.bbc.com/news/world-europe-34818994.

[14] "Press release: Civilian drones at risk of being used by terrorist and other hostile groups. Stricter regulation and countermeasures needed, new report finds," Remote Control Project via *Open Briefing*, 11 January 2015, https://www.openbriefing.org/uncategorized/press-release-civilian-drones-at-risk-of-being-used-by-terrorist-and-other-hostile-groups-stricter-regulation-and-countermeasures-needed-new-report-finds/; "Hostile drones: The hostile use of drones by non-state actors against British targets," Remote Control Project via *Open Briefing*, 11 January 2015, https://www.openbriefing.org/publications/report-and-articles/hostile-drones-the-hostile-use-of-drones-by-non-state-actors-against-british-targets/; Chris Abbott, Matthew Clarke, Steve Hathorn, and Scott Hickie, *Hostile drones: The use of civilian drones by non-state actors against British targets*. (London: Remote Control Project, via Open Briefing, January 2015), https://www.openbriefing.org/docs/Hostile-use-of-drones-report_open-briefing.pdf.

[15] Remote Control Project, Note 13.
[16] "Illegal Drones at Sporting Events: Hidden Level Combines Rooftop Sensors and Sophisticated Software," *Drone Life*, 7 February 2022, https://dronelife.com/2022/02/07/illegal-drones-at-sporting-events-hidden-level-combines-rooftop-sensors-and-sophisticated-software/.
[17] "Illegal Drones," Note 15.
[18] "Stadiums and Sporting Events Washington, DC: : Federal Aviation Administration, 2 October 2021, https://www.faa.gov/uas/getting_started/where_can_i_fly/airspace_restrictions/sports_stadiums. The FAA/SMA Toolbox, "Drones Are Prohibited In and Around Stadiums" is available at https://www.faa.gov/uas/resources/community_engagement/no_drone_zone/stadiums.
[19] Taylor Mims and Bill Donahue, "Astroworld Report Leads to Finger-Pointing Over Jurisdiction and Blame for Tragedy." Billboard, 21 April 2022, https://www.billboard.com/business/touring/astroworld-texas-concert-task-force-report-1235061643/; "Governor Greg Abbott's Task Force on Concert Safety - April 2022 Report," *Texas Music Office*, https://gov.texas.gov/music/page/governor-abbotts-texas-task-force-on-concert-safety-april-2022-report; "Event Production Guide," *Texas Music Office*, https://gov.texas.gov/music/page/tx-event-production-guide.
[20] While this report addresses UAS, similar drone threats can involve unmanned ground vehicle (UGY) such as remotely piloted vehicles and unmanned surface vessels (USVs) or unmanned marine vehicles (UMVs) including subsurface drones.

[21] GAO Summary of "Counter Drone Technologies," Government Accountability Office (GAO), 15 March 2022 at *USNI News*, 24 March 2022, https://news.usni.org/2022/03/24/gao-report-on-counter-drone-technologies.
[22] GAO, "Counter Drone Technologies," Note 20.
[23] S.2836 - *Preventing Emerging Threats Act of 2018,* codified at 6 U.S. Code § 124n - Protection of certain facilities and assets from unmanned aircraft, https://www.law.cornell.edu/uscode/text/6/124n.
[24] "Counter Unmanned Aircraft Systems Legal Authorities," Washington, DC: Department of Homeland Security, https://www.cisa.gov/sites/default/files/publications/19_0502_cisa_dhs-cuas-legal-authorities-factsheet.pdf.
[25] A SEAR is an special event that SLTT authorities voluntarily submit for DHS risk assessment. These include the Super Bowl, Indianapolis 500, and Kentucky Derby. These are rated as "Level 1: Significant events with national and/or international importance that require extensive federal interagency support; Level 2: Significant events with national and/or international importance that may require some level of federal interagency support; Level 3: Events of national and/or international importance that require only limited federal support; Level 4: Events with limited national importance that are managed at the state and local levels; Level 5: Events that may be nationally recognized but generally have local or state importance." Level 1 and 2 events are supported by a Federal coordination Team that acquires capabilities that exceed the local jurisdictions capacity.
"Fact Sheet: What are Special Event Assessment Rating (SEAR) Events?" Washington, DC: US Department of Homeland Security, 25 July 2022, https://www.dhs.gov/sites/default/files/publications/19_0905_ops_sear-fact-sheet.pdf.
[26] J. "Matt" Rowland and Chris Fleischer, "Why state and local law enforcement needs legal authority from Congress to counteract dangerous drones." *Police1*, 10 October 2021, https://www.police1.com/police-products/police-drones/articles/why-state-and-local-law-enforcement-needs-legal-authority-from-congress-to-counteract-dangerous-drones-Cer6e9HCGbfZvDRr/,
[27] "White House Takes Dramatic Step to Secure Airspace from Drone Threats," *Commercial UAV News*, 2 August 2022, https://www.commercialuavnews.com/regulations/white-house-takes-dramatic-step-to-secure-airspace-from-drone-threats, "FACT SHEET: The Domestic Counter-Unmanned Aircraft Systems National Action Plan." Washington, DC: The White House, 25 April 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/04/25/fact-sheet-the-domestic-counter-unmanned-aircraft-systems-national-action-plan/.
[28] "While FAA Is Coordinating With Other Agencies on Counter-UAS, Delays in Testing Detection and Mitigation Systems Could Impact Aviation Safety," Office of the Inspector General, Federal Aviation Administration (FAA). Washington, DC: Department of Transportation, Report AV2022026, 30 March 2022, https://www.oig.dot.gov/sites/default/files/FAA%20C-UAS%20Final%20Report_3.30.2022.pdf.
[29] GAO, "Counter Drone Technologies," Note 20.

[30] Joint Advisory, "Advisory on the Application of Federal Laws to the Acquisition and Use of Technology to Detect and Mitigate Unmanned Aircraft Systems," Washington, DC: US Department of Justice, US Department of Transportation, Federal Communications Commission, and US Department of Homeland Security. August 2020, https://www.faa.gov/sites/faa.gov/files/uas/resources/c_uas/Interagency_Legal_Advisory_on_UAS_Detection_and_Mitigation_Technologies.pdf.

[31] See "Protecting Against Rogue Drones," *In Focus*, Washington: DC, Congressional Research Service, 3 September 2020, https://apps.dtic.mil/sti/pdfs/AD1110853.pdf.

[32] See 18 U.S.C. § 2520. In addition, it is important to note that "Because no other entities have been granted that authority, it is important that state, local, tribal and territorial (SLTT) and private sector entities without such statutory authority (including SLTT law enforcement organizations, SLTT governments, and owners and operators of critical infrastructure, stadiums, outdoor entertainment venues, airports, and other key sites) understand that federal laws may prevent, limit, or penalize the sale, possession, or use of UAS detection and mitigation capabilities." The advisory also notes that it "does not address the general authorities of public safety agencies, or specific actions they might take consistent with governing law, to protect the public in exigent circumstances." Joint Advisory (at p. 2). Note 22.

[33] See for example, "US Senate outlines proposals to give local law enforcement agencies more C-UAS powers," Unmanned Airspace, 1 August 2022, https://www.unmannedairspace.info/latest-news-and-information/us-senate-outlines-proposals-to-give-local-law-enforcement-agencies-more-c-uas-powers/, which discusses the introduction of Senate Bill 4687. S, 4687: *Safeguarding the Homeland from the Threats Posed by Unmanned Aircraft Systems Act* (available at https://www.congress.gov/bill/117th-congress/senate- bill/4687?s=1&r=3) would clarify C-UAS authorities.

[34] This schema is modified by the authors from earlier operational research conducted on "Unmanned Aircraft Systems Futures" during the *2017 Public-Private Analytic Exchange Program*, Concluding Summit, September 2017.

[35] This recon/recce discrimination model was developed by Sullivan. See John P. Sullivan, "Red Teaming and Detecting Terrorist ISR." *Red Team Journal (RTJ),* 19 February 2018, https://www.academia.edu/35989297/Red_Teaming_and_Detecting_Terrorist_ISR.

[36] A model of critical infrastructure threat sharing can be found in John N. Balog, Matthew G. Devost, and John P. Sullivan, *Public Transportation Security: Volume 1 Communication of Threats: A Guide. TCRP Report 86.* Washington, DC: National Academy Press, 2002, https://nap.nationalacademies.org/catalog/24722/communication-of-threats-a-guide.

[37] See, for example, Testimony of Ronald L. Dick, Deputy Assistant Director, Counterterrorism Division, and Director, National Infrastructure Protection Center, Federal Bureau of Investigation (FBI) , Before the House Committee on Transportation and Infrastructure, Subcommittee on Water Resources and Environment. Washington, DC, 10 October 2001, https://archives.fbi.gov/archives/news/testimony/terrorism-are-americas-water-resources-and-environment-at-risk.

[38] This framework is adapted from *Domestic Antiterrorism Efforts at Selected Sites*, GAO/PEMD-88-22 (13) as described and expanded in Annabelle Boyd and John P. Sullivan, *Emergency Preparedness for Transit Terrorism. Synthesis of Transit Practice 27*. Washington, DC: National Academy press, 1997, https://onlinepubs.trb.org/onlinepubs/tcrp/tsyn27.pdf.

[39] On an example of a potential evacuation modelling initiative, see "SportEvac: Choreographing a Stadium Stampede. Archived Content, *Department of Homeland Security, Science and Technology*, Updated 27 January 2022, https://www.dhs.gov/sportevac-choreographing-stadium-stampede.

INSTITUTE FOR HOMELAND SECURITY

Sam Houston State University

The Institute for Homeland Security at Sam Houston State University is focused on building strategic partnerships between public and private organizations through education and applied research ventures in the critical infrastructure sectors of Transportation, Energy, Chemical, Healthcare, and Public Health.

The Institute is a center for strategic thought with the goal of contributing to the security, resilience, and business continuity of these sectors from a Texas Homeland Security perspective. This is accomplished by facilitating collaboration activities, offering education programs, and conducting research to enhance the skills of practitioners specific to natural and human caused Homeland Security events.

Institute for Homeland Security
Sam Houston State University

Sullivan, John P., Jones, Nathan P., & Davis, George W. (2022). Detecting Drone (Unmanned or Uncrewed Aerial System) Threats to Stadiums (Stadia) and Public Venues: Operational Perspectives (Report No. IHS/CR-2022-2024). The Sam Houston State University Institute for Homeland Security. https://ihsonline.org/Research/Technical-Papers/Detecting-Drone-Threats-at-Stadiums