INSTITUTE FOR HOMELAND SECURITY

Sam Houston State University™

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

TECHNICAL IMPLEMENTATION AND INTEGRATION

Institute for Homeland Security

Sam Houston State University

George W. Davis

John P. Sullivan

Nathan P. Jones

August 2022

Detecting Drone (Unmanned or Uncrewed) Threats at Stadiums (Stadia) and Public Venues: Technical Implementation and Integration

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

Detecting and countering drone threats at public stadiums and large events is a necessary component of modern emergency operations and crisis management. Large event and stadium security regularly deploys drone detection technologies and may soon deploy counter drone technologies. This final technical paper in our series on drones as potential threats to public stadiums will discuss: 1) examples of specific technologies incident commanders will need to integrate drone threat awareness into their planning and operations, 2) provide an overview of drone detection technologies; 3) provide specific examples of drone detection through the lens of the Astroworld event on 5 November 2021, and finally 4) provide policy and operational recommendations for a path forward to secure public stadiums and mass events as drones become an increasingly important part of the threat environment.

Drone Detection Methods

There are four primary detection methods for drones: radio frequency identification (RFID), radar, optical, audio, layered defenses.[1] First, radio frequency (RF) technology is effectively the drone self-reporting data as required by new regulations as it transmits between drone and pilot. RF detection equipment is passive and detects the connection between the drone and its "pilot to determine the location of the drone and in some cases, the pilot's location."[2] The second detection method, radar, which can be both two and three dimensional, detects the physical presence of the drone. The third is optical, which visually detects the drone. This method is difficult because it results in false positives such as a bird or bag in the sky. Research sponsored by Department of Homeland Security, Science and Technology Directorate (S&T) with Sandia National Laboratories is under way to use machine learning and neural networks to differentiate drones. One method is Temporal Frequency Analysis (TFA) which follows the drone over time and identifies its movements as indicative of a drone versus another object.[3] Fourth, there is audio which can hear the drone. Common issues that arise in urban environments is background noise. A fifth lesser discussed detection method is thermal sensors. Thermal sensors can detect the heat signatures of drones, but tests as of 2017 indicated that due to noise, human interpreters were needed for drone detection. Interestingly, "batteries not motors" were the primary source of heat for the drones and the authors who tested the thermal sensors planned future research to mask heat signatures.[4]

Each of these have advantages. Audio may detect the drones despite cloud cover, a situation wherein radar or optical may have difficulty. RFID may gain self-reported data where all other methods fail, yet could ignore the most malicious actor drones with their broadcast intentionally removed for the delivery of bombs or chemical weapons. These detection methods all fit into a layered approach to defense-in-depth wherein security cannot be assured by any single detection method but rather by overlaying multiple methods.[5]

New regulations going into effect in 2022 require drones to electronically identify themselves so that drone detection equipment can have basic information about the drone and its pilot. On the other hand, it is obvious that malicious actors may seek to design drones that do not self-report or strip such mechanisms from existing commercial "off-the-shelf" (COTS) drones. In those cases, layered detection methods that include RFID, optical sensors, radar, laser imaging, detection and ranging (LIDAR), and acoustic sensors can all be used to detect drones.[6] Indeed, one obvious critical infrastructure protection algorithm will be to compare RFID (self-reported drones) to radar detected drones.

A recent US Appeals Court ruling upheld the Federal Aviation Administration's (FAA's) new rules requiring drone manufacturers to produce drones that broadcast their location and that of the pilot while in the air. Congress had directed the FAA to write these rules in 2016 legislation. In 2018 Congress gave authority to the Department of Justice (DOJ) and Department of Homeland Security (DHS) to "disable or destroy threatening drones." Senator Gary Peters (D) and Ron Johnson (R) have introduced (though not yet passed) new legislation to expand that authority to the Transportation Security Administration (TSA) and airports.[7] Others have pointed out that the Department of Energy (DOE) also has counter UAS legal authorization, which is logical given that it is often forgotten that the DOE oversees US nuclear power plants and other critical infrastructure facilities. Researchers seeking to secure Saudi oil and gas are testing artificial intelligence systems to detect and recognize potentially threatening drones.[8]

Adaptation and Evasion

Radar detected drones without RFID signatures will likely pose immediate red flags for further surveillance. On the other hand, depending on government and private sector security responses to such drones, malign actors may engage in what Michael Kenney calls "competitive adaptation."[9] Malicious actors may decide it is better to announce their presence and minimize risk by blending into the sea of legal/licit drones. In effect, terrorists and criminals may let the good guys drown in data. In turn legal actors will need to produce behavioral models and algorithms indicating illicit drone activity to ferret out high probability illicit conduct, etc. This project seeks to add to this literature by exploring the relationship between drones and public stadia as an example of critical infrastructure through geospatial modeling.

Incorporating Drones into the Public Stadium Security: Planning

One advantage to providing security for public stadiums is their location is fixed and thus preplanning allows incident commanders to understand the environment through mapping. Security planners should create detailed maps via drone aerial surveys that consist of a combined sensor package of laser imaging, detection and ranging (LIDAR) and high-definition photographic capability to produce surface and terrain models, orthophotos, and 3D models of the area of interest.[10] Having this done prior to an event allows for the capture of a timely depiction of the scene and provides a foundation to build situation intelligence in response to any emergency that may arise.

Applying a 3D capable Geographic Information System (GIS) with a graphic user interface (GUI) that can ingest the data collected prior to the event and live data and sensor feeds displayed in real time during the event will provide analysts and decision makers a comprehensive situation intelligence capability in the event of a drone or multiple drone incursion into the airspace over the stadium or large-scale outdoor event. Making the detection data available live to first responders and security personnel will decrease the response time needed to act upon drone threats. In the series of photos below examples of drone detection data is integrated into the 3D GIS for a realistic view of the unfolding situation. The deployment of drones with live streaming high-definition video sensors can aid in the discovery of intruder pilots and hasten the disruption of the intrusion.

An integrated drone defense strategy should combine the sensor packages described earlier in this paper with the ground truth provided by geospatial data. Security planners should also integrate the locations of the following items into their 3D GIS maps prior to events for integration into their operational graphic user systems: 1) Security stations, 2) Evacuation routes, 3) Staging areas, 4) Emergency medical stations, 5) Counter drone sensor locations, 6) Responder drone launch locations, 7) Fire Department stations, 8) Hospital and first aid stations, 9) Access roads and transportation stops, and 10) Airport flight path proximity information, etc. These site attributes can be documented in pre-incident planning tools such as Response Information Folders (Target Folders) and contingency planning playbooks for a range of threat conditions.[11]

Making this pre-planning information available to emergency responders increases awareness of potential threat situations that could arise at at-risk venues. It also enhances the ability to effectively respond and interdict or mitigate the effects of an incursion.

Mapping the Event Drones: Astroworld as a Notional Case

The images below are examples of GIS mapping of drone activity over the *Astroworld* site during and after the concert. The images are visual representations of increased drone activity during and after the concert and should be viewed as slices in time. It should also be noted that the drone detections happen by the millisecond and thus not every depiction is a unique drone. Indeed, our analysis of the data indicated 25 unique drones and 46 unique flights which increased in frequency during and the day after the concert, likely due to increased media attention.

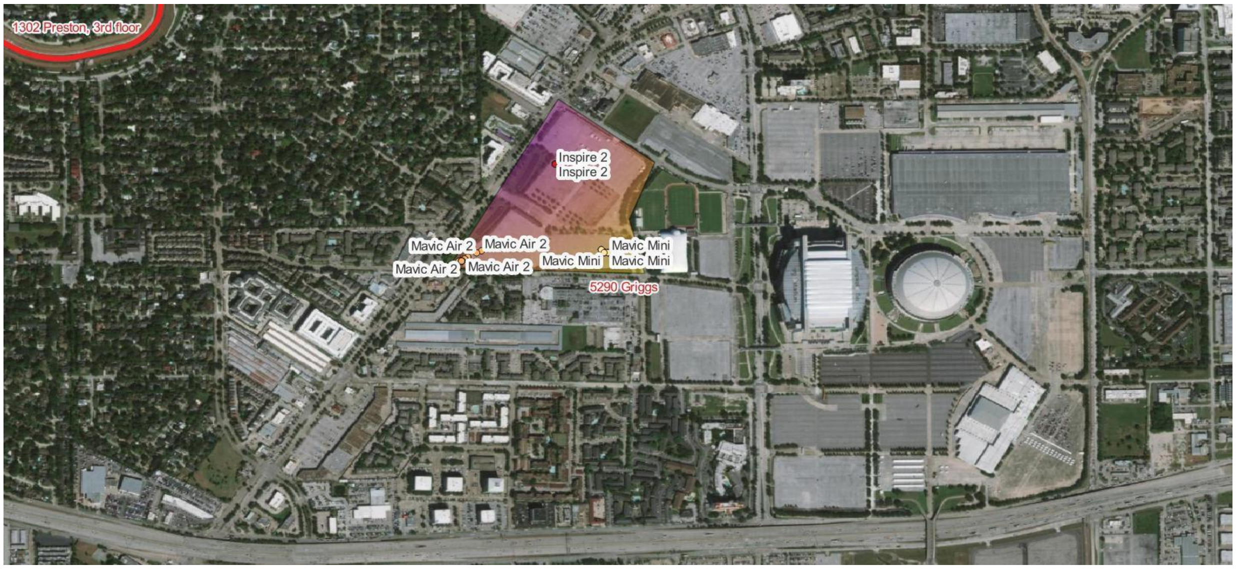


Figure 1. Drones over *Astroworld* (T1) Labels and point data show drone detection in proximity of the area of interest (Authors' Analysis)

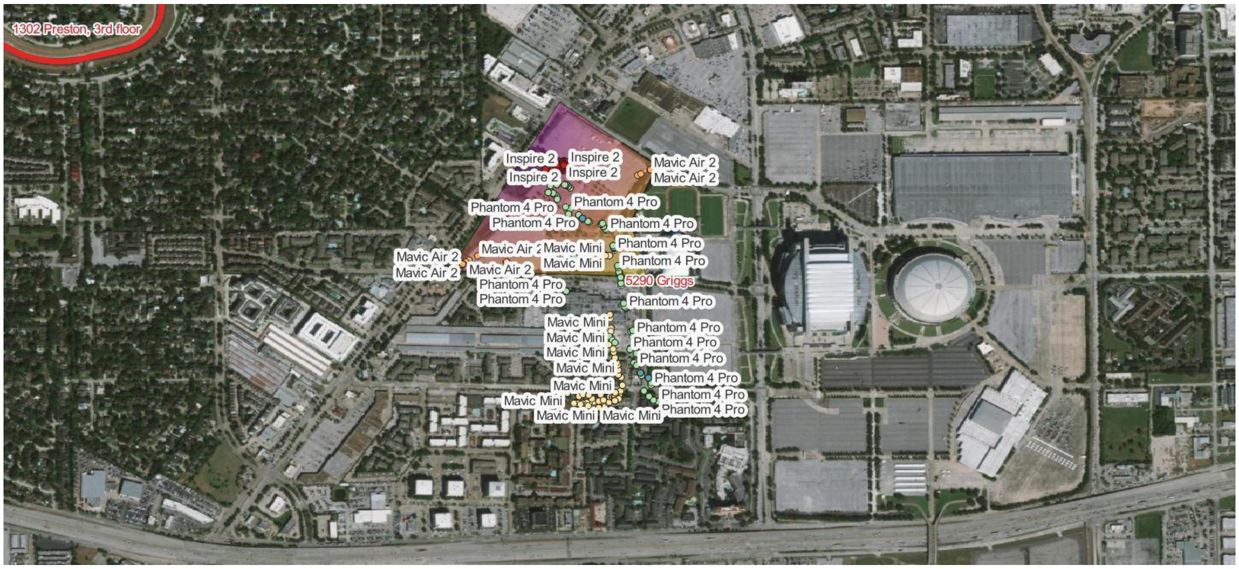


Figure 2. Drones over Astroworld (T2). As more drone detections occur their data is displayed (Authors' Analysis).

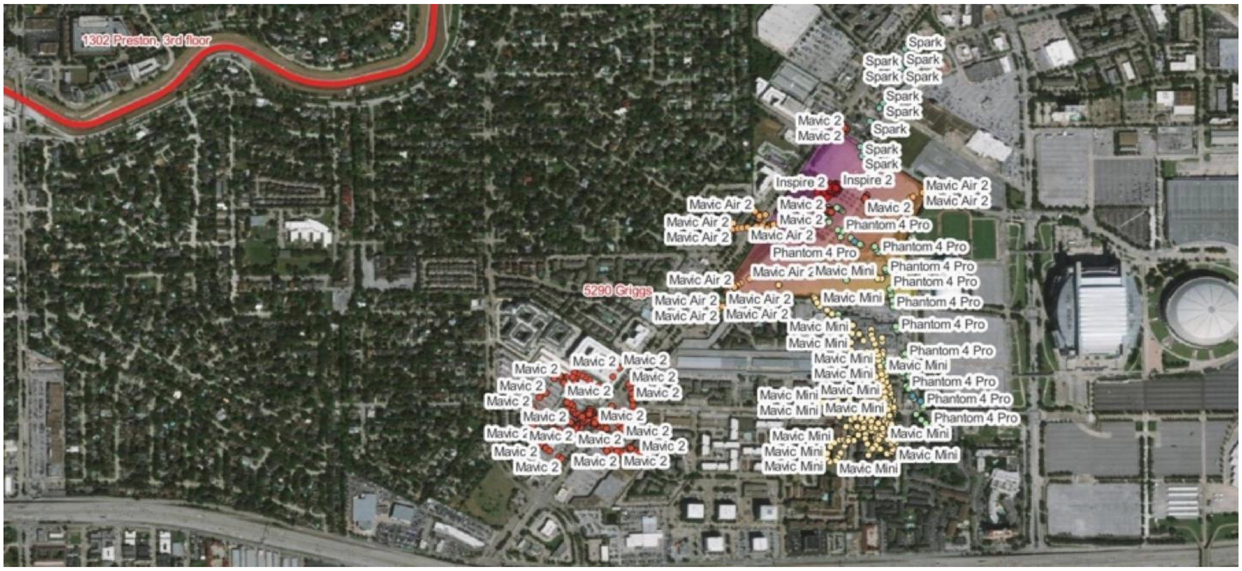
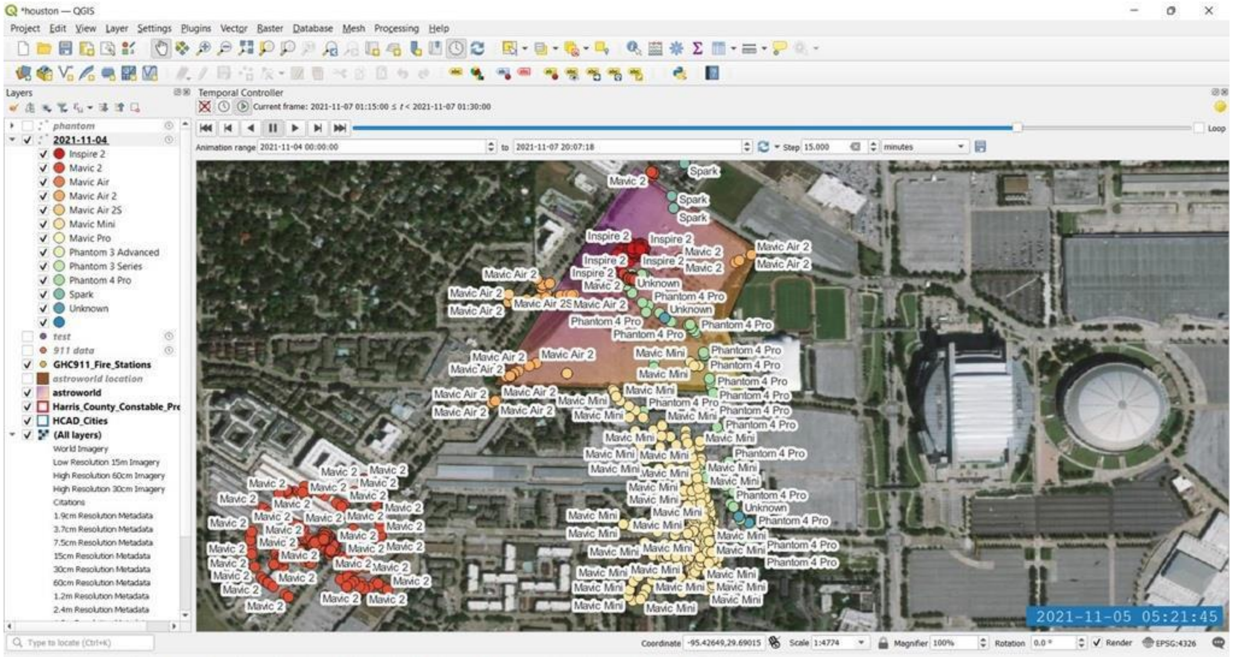


Figure 3. Drones Over Astroworld (T3). This image shows a compilation of the data over the area of interest. (Labels are the drone types detected by the sensors; Authors' Analysis).



Current frame: 2021-11-07 01:15:00 ≤ t < 2021-11-07 01:30:00

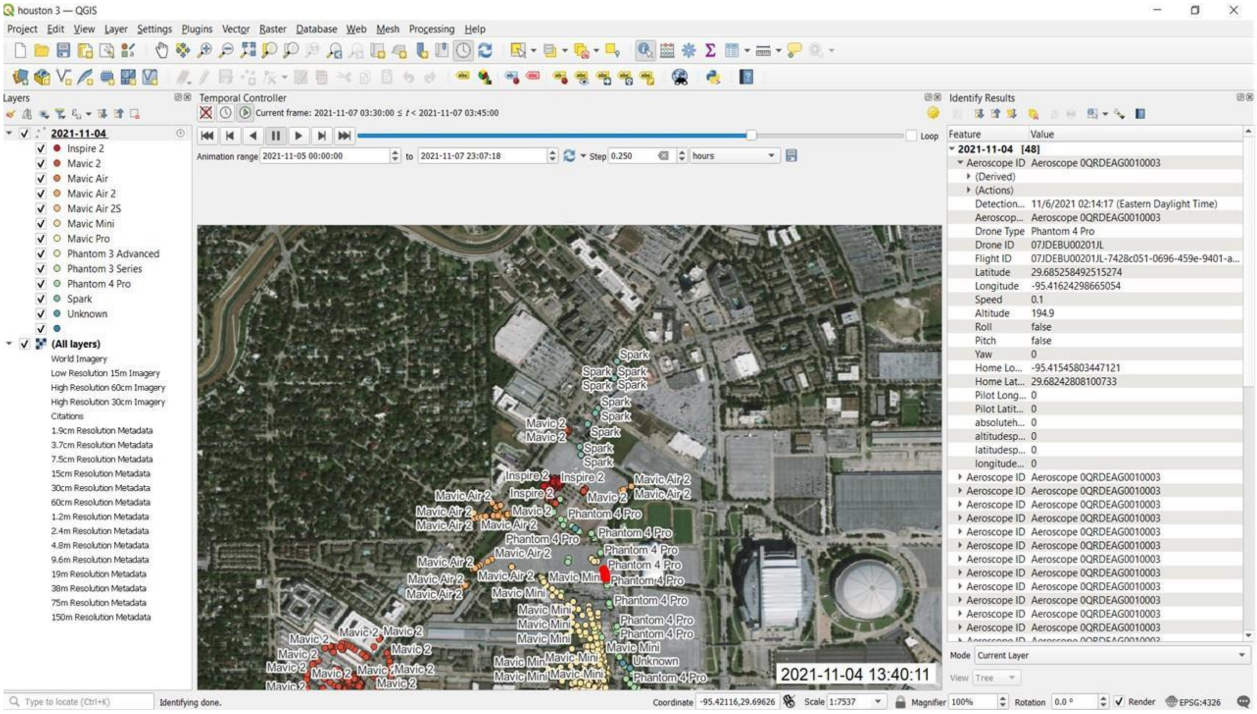
Animation range 2021-11-04 00:00:00 to 2021-11-07 20:07:18 Step 15.000 minutes

- ☐ *phantom*
- ☑ **2021-11-04**
  - ☑ ● Inspire 2
  - ☑ ● Mavic 2
  - ☑ ● Mavic Air
  - ☑ ● Mavic Air 2
  - ☑ ● Mavic Air 2S
  - ☑ ● Mavic Mini
  - ☑ ● Mavic Pro
  - ☑ ● Phantom 3 Advanced
  - ☑ ● Phantom 3 Series
  - ☑ ● Phantom 4 Pro
  - ☑ ● Spark
  - ☑ ● Unknown
  - ☑ ●
- ☐ ● *test*
- ☐ ● *911 data*
- ☑ ● **GHC911_Fire_Stations**
- ☐ *astroworld location*
- ☑ **astroworld**
- ☑ **Harris_County_Constable_Pre**
- ☑ **HCAD_Cities**
- ☑ **(All layers)**
  - World Imagery
  - Low Resolution 15m Imagery
  - High Resolution 60cm Imagery
  - High Resolution 30cm Imagery
  - Citations
  - 1.9cm Resolution Metadata
  - 3.7cm Resolution Metadata
  - 7.5cm Resolution Metadata
  - 15cm Resolution Metadata
  - 30cm Resolution Metadata
  - 60cm Resolution Metadata
  - 1.2m Resolution Metadata
  - 2.4m Resolution Metadata

Type to locate (Ctrl+K)

Coordinate -95.42649,29.69015 Scale 1:4774 Magnifier 100% Rotation 0.0 ° ☑ Render EPSG:4326

Figure 4. Drones Over Astroworld (T4). Image depicting Integrated GIS and Drone Detections over area of interest on Analyst Workstation (Authors' Analysis).



2021-11-04
- ☑ ● Inspire 2
- ☑ ● Mavic 2
- ☑ ● Mavic Air
- ☑ ○ Mavic Air 2
- ☑ ○ Mavic Air 2S
- ☑ ○ Mavic Mini
- ☑ ○ Mavic Pro
- ☑ ○ Phantom 3 Advanced
- ☑ ○ Phantom 3 Series
- ☑ ○ Phantom 4 Pro
- ☑ ● Spark
- ☑ ● Unknown
- ☑ ●

☑ (All layers)
- World Imagery
- Low Resolution 15m Imagery
- High Resolution 60cm Imagery
- High Resolution 30cm Imagery
- Citations
- 1.9cm Resolution Metadata
- 3.7cm Resolution Metadata
- 7.5cm Resolution Metadata
- 15cm Resolution Metadata
- 30cm Resolution Metadata
- 60cm Resolution Metadata
- 1.2m Resolution Metadata
- 2.4m Resolution Metadata
- 4.8m Resolution Metadata
- 9.6m Resolution Metadata
- 19m Resolution Metadata
- 38m Resolution Metadata
- 75m Resolution Metadata
- 150m Resolution Metadata

Current frame: 2021-11-07 03:30:00 ≤ t < 2021-11-07 03:45:00

Animation range 2021-11-05 00:00:00 to 2021-11-07 23:07:18 Step 0.250 hours

Feature	Value
2021-11-04 [48]	
Aeroscope ID	Aeroscope 0QRDEAG0010003
(Derived)	
(Actions)	
Detection...	11/6/2021 02:14:17 (Eastern Daylight Time)
Aeroscop...	Aeroscope 0QRDEAG0010003
Drone Type	Phantom 4 Pro
Drone ID	07JDEBU00201JL
Flight ID	07JDEBU00201JL-7428c051-0696-459e-9401-a...
Latitude	29.685258492515274
Longitude	-95.41624298665054
Speed	0.1
Altitude	194.9
Roll	false
Pitch	false
Yaw	0
Home Lo...	-95.41545803447121
Home Lat...	29.68242808100733
Pilot Long...	0
Pilot Latit...	0
absoluteh...	0
altitudesp...	0
latitudesp...	0
longitude...	0
Aeroscope ID	Aeroscope 0QRDEAG0010003
Aeroscope ID	Aeroscope 0QRDEAG0010003
Aeroscope ID	Aeroscope 0QRDEAG0010003
Aeroscope ID	Aeroscope 0QRDEAG0010003
Aeroscope ID	Aeroscope 0QRDEAG0010003
Aeroscope ID	Aeroscope 0QRDEAG0010003
Aeroscope ID	Aeroscope 0QRDEAG0010003
Aeroscope ID	Aeroscope 0QRDEAG0010003
Aeroscope ID	Aeroscope 0QRDEAG0010003
Aeroscope ID	Aeroscope 0QRDEAG0010003
Aeroscope ID	Aeroscope 0QRDEAG0010003
Aeroscope ID	Aeroscope 0QRDEAG0010003
Aeroscope ID	Aeroscope 0QRDEAG0010003

Mode Current Layer

View Tree

Type to locate (Ctrl+K) Identifying done. Coordinate -95.42116,29.69626 Scale 1:7537 Magnifier 100% Rotation 0.0 ° ☑ Render EPSG:4326

Figure 5. Image displaying the complete attribute table of identified drone detection data on Analyst Workstation (Authors' Analysis).

This subsection has depicted *ex post facto* GIS mapping drone data over the Astroworld event. This analysis demonstrated the presence of drones at public events and their potential security implications have been discussed in previous sections. One of the key research findings, discussed previously, is that drone traffic will increase as local and social media raise community awareness of a nearby event. Interviews conducted for this paper with security professionals similarly indicated drone pilots use their drones to surveille and sometimes live broadcast their footage of emergency response personnel, including of special weapons team response to hostage situations. This could result in hostage takers or other nefarious actors accessing tactical information about emergency responders that can endanger the lives of civilians and law enforcement. The next section will discuss the operational real-time integration of 3D mapping, drone detection, and other data streams, into usable interfaces for emergency responders.

Operational Integration

Integrating drone data into the broader stream of multisource streams is a key challenge for incident commanders and emergency responders. Graphic User Interfaces (GUIs) with real time integration make this viable. While this project is agnostic to any brand or software, the following section provides visual examples of software platforms that integrate multiple data streams. The image below notionally (not *Astroworld*) demonstrates the live integration of maps, 3D modeling, closed circuit television (CCTV) and Cell phone footage being integrated in real time for a command center. This modeling includes using friendly or "blue" drones to interrogate/provide data on potential intruder drones. These can also be distributed to users on edge devices such as cell phones and tablets for collaborative threat assessment and response planning.

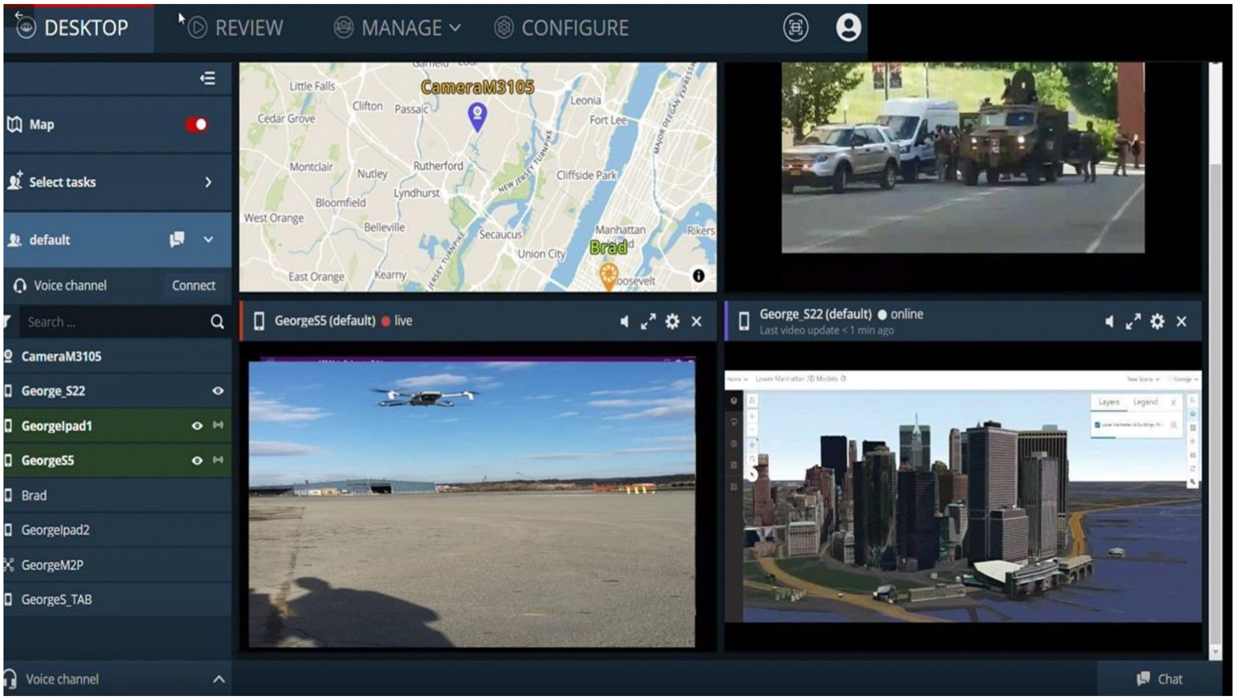
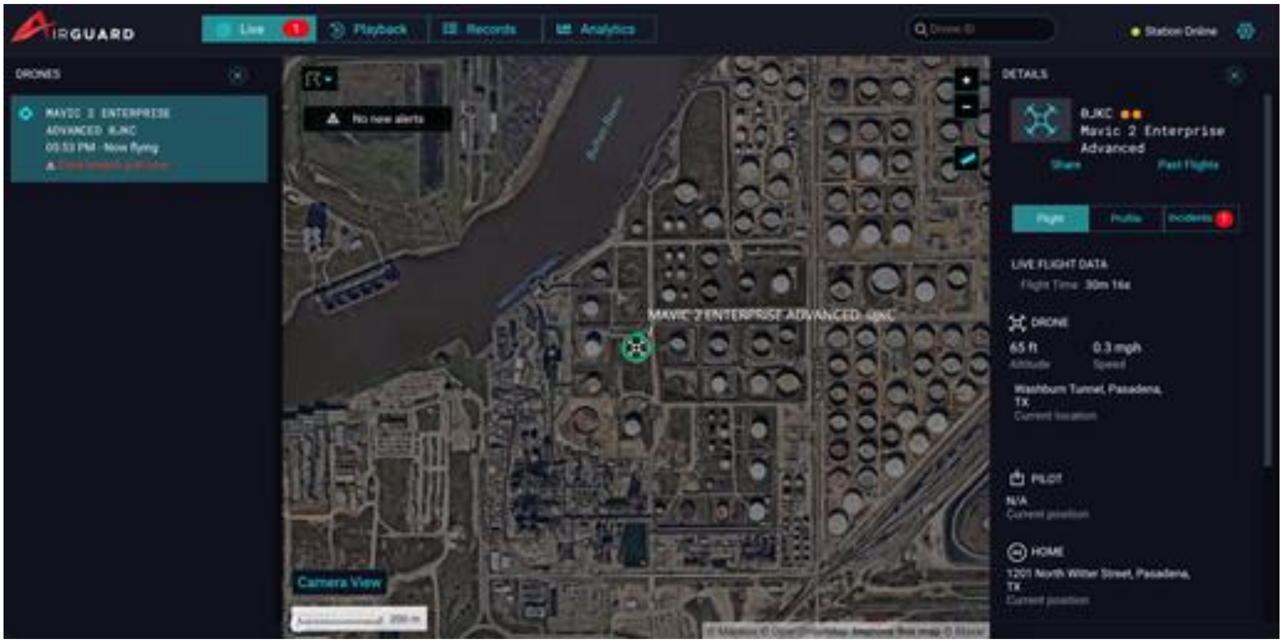


Figure 6. Integrated Analyst Workstation for Assessing Drone Incursion (Authors' Analysis).

Integrating Drone Detection Layers

The next set of images are examples of drone detection images in 3 detection layers as provided by Airsight via their Airguard software platform.[12] The first layer of detection is an Aeroscope (RFID) which detects all Da-Jiang Innovations (DJI) drones with accurate GPS information. According to their website it is a DJI Aeroscope sensor, and gathers information on 80% of drones.[13] The image below represents the type of visual interface generated.



MAVIC 2 ENTERPRISE ADVANCED 8JKC
05:53 PM · Now flying

MAVIC 2 ENTERPRISE ADVANCED 8JKC

8JKC
Mavic 2 Enterprise Advanced

LIVE FLIGHT DATA
Flight Time 30m 16s

DRONE
65 ft Altitude
0.3 mph Speed
Washburn Tunnel, Pasadena, TX
Current location

PILOT
N/A
Current position

HOME
1201 North Witter Street, Pasadena, TX
Current position

Figure 7. Depiction of Airsight Layer 1 Drone Detection.[14]

Airsight then uses a second layer of detection in the form of a directional finding sensor to detect non DJI drones though only in specific direction and without accurate GPS information. This is a DJI Aeroscope with a passive sensor and multiple radios; gathering information on 95% of drones.[15]

In a third layer of detection, Airsight uses radars that can track objects in the air for an accurate depiction of non DJI drones. This layer also includes cameras and can detect 99% of drones.[16] Their system then can integrate the three layers of detection visually. The picture below demonstrates the visual representation of Layer 1 (Aeroscope detection), Layer 2 (directional detections from 3 sensors in yellow cones), and Layer 3 (adds cameras) detection.

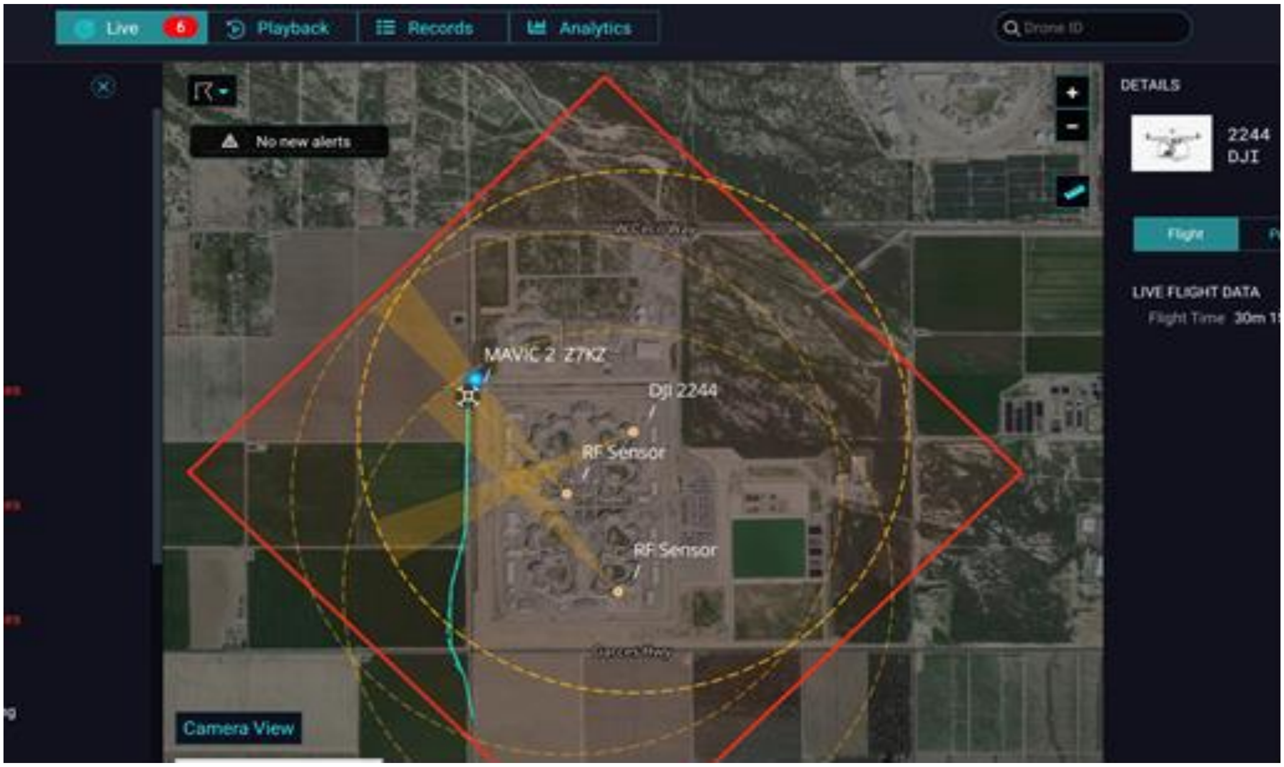


Figure 8. Image Depicting Airsight Layer 1, 2 and 3 Detection.

Due to the potential for false positives in radar detection, *e.g.*, birds, layer 3 also includes a camera to eliminate these false positives. The image below is an example of a camera cued by the radar to get visual confirmation/make a determination on the drone.

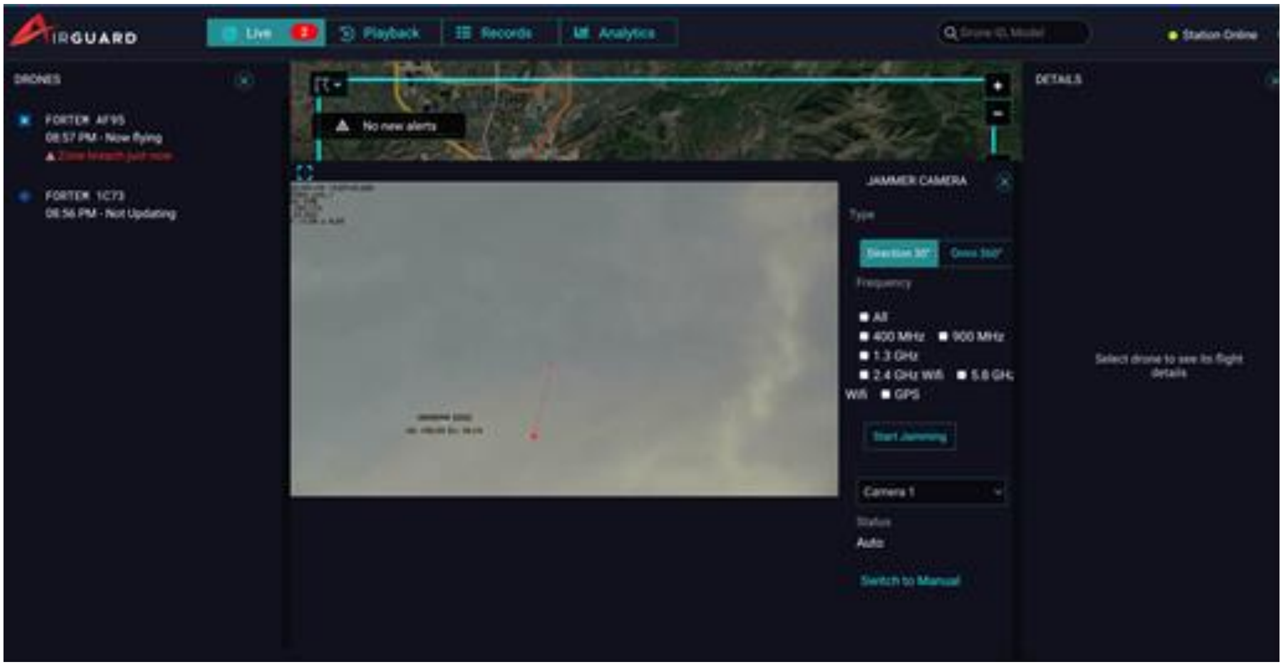


Figure 9. Airsight Layer 3 Detection with Camera Interrogation.

This section provided a discussion and visual representation of the technologies needed to operationally secure public stadiums and mass events in the context of potential drone threats. It has demonstrated the complexity and varied nature of the data streams which include drone multiple layers of drone detection data, CCTV, first responder body cameras, GIS mapping, etc. This complexity must be visually represented and integrated to incident commanders in real time to be able to respond to drone threats which require rapid response. Future operational integration systems will no doubt incorporate artificial intelligence to assist incident commanders in synthesizing and rapidly reacting to drone threats to public stadiums. This will be especially important in the context of drone swarms and future threats. The next section concludes with policy recommendations based on this 3-part technical paper series.

Summation: Innovation and Algorithms

GUI visualization systems which can integrate multiple data streams in real time are critical for emergency managers. Many technologies exist that can be integrated into data streams such as real time monitoring of Open Source Intelligence (OSINT) and social media intelligence (SOCMINT), as well as integrating cell phone footage from emergency management and security personnel team members on the ground assessing a potential threat drone. The future lies in the ability to integrate all of these data streams into something security personnel can use and react to quickly enough for drone threats. To this end, algorithms that can determine likely threat drones, blacklists (threat drones), whitelists (authorized drones), geofencing areas, are all incumbent on systems that will be able to integrate large quantities of data into usable forms for the human mind to process. [17] No doubt artificial intelligence will become an increasingly important part of processing these data streams.

Policy Recommendations

1. Develop and improve information sharing via Cloud based graphic user interface (GUI) drone detection analytical systems. These can integrate drone detection, commercial flight, geospatial intelligence, and critical infrastructure location information. They will be critical to the operational success of onsite incident command for public stadia and large public events. Early examples of such platforms include *Cirrus* a GUI system developed at the Texas A&M Corpus Christi Lone Star UAS Center (LSUASC) of Excellence and Innovation which integrates commercial flight data, and drone detection data based on local fixed and mobile antennas, into a real time geospatial representation. Another example of a real time GUI style system is the URSA analytical drone detection platform.[18]

2. These platforms could integrate data on potential blind spots in counter drone technologies such as power lines generating electromagnetic interference for radar systems.[19]

3. We recommend creating an aerial survey and producing a digital twin of the location in the hours prior to pre-planning the event. This allows incident commanders and their staff to more effectively and rapidly respond to drone threats.

4. Develop behavioral and movement profiles for potential malicious drone use including illicit intelligence, surveillance, and reconnaissance (ISR) for terrorist activity. Where possible develop these into automated algorithms that can alert humans to potential problematic activity for further sifting. The future of drones will require separating much wheat from chaff. Useful algorithms identified in interviews for this project included flagging drones that exceeded their max commercially viable flight time/altitude/or other capability.

5. Consider statutorily expanding counter drone measures to local, state, and more federal agencies. One possible model might be to create taskforces wherein agencies with counter drone technology authorization, work with local and state agencies to effectively expand the implementation of counter-drone technologies at public stadia and airports.

6. Legislators should consider further regulations which could require manufacturers to build programmable no fly zones or "geofencing" capabilities (the capacity of government officials to automatically prevent flights into restricted airspace).[20] This capacity could also be built into drones at the manufacturing stage for the US market.

7. Separately, Congress should consider the role of for-profit and nonprofit organizations in the implementation of counter drone (C-UAS) measures. As is oft quoted, 85% of US critical infrastructure is private,[21] and thus the role of non-profit and for-profit entities which may be the first line of detection, should be considered in future deliberations on counter-drone authorization.

8. Future research should assess drone threats involving UAS, surface and subsurface vessels, and unmanned ground vehicles at ports, railways, and other transportation critical infrastructures. In particular future research should assess the threats of drone swarm attacks on these infrastructures.[22]

Acknowledgements

The authors would like to thank the Texas A&M Corpus Christi Lone Star Unmanned Aircraft System (UAS) Center of Excellence & Innovation Center (LSUASC) Director Michael J. Sanders and staff including Matthew Wesson, Tom Frierson, and others for providing a tour of facilities and follow up interviews. The authors would like to thank *Airsight* for the provision of sample data related to the *Astroworld* event, which the authors used as a notional case study of potential threats posed by drones to public stadiums.

DISCLAIMER

The technologies and platforms discussed here are only *examples* of the types of drone detection, counter-drone and real time data integration tools useful for securing US critical infrastructure related to stadiums and mass gatherings. Nothing in this three-part technical paper series should construed as an endorsement of a particular brand or firm.

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] Bill Edwards and Chuck Harold, “June 2022: Commercial Drones in Combat, Plus Exploiting Risk for Organizational Success,” *Security Management*, 6 June 2022, https://soundcloud.com/security-management/june-2022-commercial-drones-in-combat-plus-exploiting-risk-for-organizational-success.

[2] “Drone Detection | Everything You Need to Know| Can Drones Be Detected?,” *Airsight*, 20 May 2022, https://www.911security.com/en-us/knowledg-hub/drone-detection.

[3] “Snapshot: Detecting Drones Through Machine Learning, Cameras,” *Homeland Security: Science and Technology*, 2 November 2018, https://www.dhs.gov/science-and-technology/news/2018/11/02/snapshot-detecting-drones-through-machine-learning-cameras.

[4] Petar Andraši et al., “Night-Time Detection of UAVs Using Thermal Infrared Camera,” *Transportation Research Procedia*, INAIR 2017, 28 (1 January 2017): 183–90, https://doi.org/10.1016/j.trpro.2017.12.184.

[5] Edwards and Harold, “June 2022.”

[6] Edwards and Harold; “Drone Detection | Everything You Need to Know| Can Drones Be Detected?”

[7] David Shepardson, “U.S. Appeals Court Upholds FAA Rules on Drone Identification,” Reuters, 29 July 2022, https://www.reuters.com/business/aerospace-defense/us-appeals-court-upholds-faa-drone-identification-rules-2022-07-29/.

[8] For a survey on counter drone systems see Park Et Al below. Mohammad Hijji, “Using Artificial Intelligence to Protect, Detect and Mitigate Oil and Gas Sectors of KSA from Drones and Missiles Assaults,” in *2022 2nd International Conference on Computing and Information Technology (ICCIT)*, 2022, 335–39, https://doi.org/10.1109/ICCIT52419.2022.9711599; Seongjoon Park et al., “Survey on Anti-Drone Systems: Components, Designs, and Challenges,” *IEEE Access* 9 (2021): 42635–59, https://doi.org/10.1109/ACCESS.2021.3065926.

[9] Michael Kenney, *From Pablo to Osama: Trafficking and Terrorist Networks, Government Bureaucracies, and Competitive Adaptation* (University Park, PA.: Pennsylvania State University Press, 2007).

[10] NOAA, “What Is LIDAR,” *National Oceanic and Atmospheric Administration*, 26 February 2021, https://oceanservice.noaa.gov/facts/lidar.html.

[11] InterAgency Board (IAB), “Annual Report” (The InterAgency Board for Equipment Standardization and InterOperability, 2002), https://interagencyboard.org/sites/default/files/publications/FY02%20IAB%20Annual%20Report.pdf.

[12] 911 Security went through a rebranding to *Airsight* during this project.

[13] “Drone Detection & Tracking Software | AirGuard by Airsight,” *Airsight*, 2022, https://www.911security.com/airguard-drone-detection/software-platform.

[14] Layer 1 - Aeroscope - Detects all DJI drones with accurate GPS information. These are notional pictures (Not *Astroworld*) using the technology used to look at *Astroworld*.

[15] “Drone Detection & Tracking Software | AirGuard by Airsight.”

[16] “Drone Detection & Tracking Software | AirGuard by Airsight.”

[17] Ibid.

[18] “URSA Inc. | One Intuitive Platform for Comprehensive UAS Analysis,” URSA Inc., 20 June 2022, https://ursainc.com/.

[19] “Science, Technology Assessment, and Analytics: Counter-Drone Technologies.”

[20] “Geofencing on Drones (All You Need to Know),” *Drone Blog*, 2022, https://www.droneblog.com/geofencing-on-drones/

[21] Ted G. Lewis, *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation* (Hoboken: John Wiley & Sons, 2006).

[22] On maritime drones see, Robert J. Bunker and John P. Sullivan, “Narco Drone Submarines Seized and Workshop Raided in 14 Month Long Operation Kraken in the Provinces of Cádiz, Málaga, and Barcelona, Spain*,” C/O Futures Cartel Research Note Series*. Claremont, CA: 27 July 2022: 1-15, https://www.cofutures.net/post/narco-drone-submarines-seized-and-workshop-raided-in-14-month-long-operation-kraken. On unmanned ground vehicles see John P. Sullivan. “Robotics in Urban Conflict and Megacities,” in Batmobiles in Gotham City: Unmanned Ground Vehicles & Future Manoeuvre in the Future Urban Environment. *Defence iQ*, 2019, https://www.academia.edu/40940306/Robotics_in_Urban_Conflict_and_Megacities.

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

Detecting Drone Threats at Stadiums

Davis, George W., Sullivan, John P., & Jones, Nathan P. (2022). Detecting Drone (Unmanned or Uncrewed Aerial System) Threats to Stadiums (Stadia) and Public Venues: Technical Implementation and Integration (Report No. IHS/CR-2022-2025). The Sam Houston State University Institute for Homeland Security. https://ihsonline.org/Research/Technical-Papers/Detecting-Drone-Threats-at-Stadiums