INSTITUTE FOR HOMELAND SECURITY

Sam Houston State University

DRONES AND PORT SECURITY

AT THE PORT OF BROWNSVILLE

Institute for Homeland Security

Sam Houston State University

John P. Sullivan

George W. Davis

Tom Adams

Technical Paper: Drones and Port Security at the Port of Brownsville

John P. Sullivan, George W. Davis, and Tom Adams

Keywords: Counter-Unmanned/Uncrewed Aerial Systems (C-UAS), Counter-Swarm, Critical Infrastructure Protection, Drones, Port Security, Unmanned/Uncrewed Ground Vehicles (UGVs), Unmanned/Uncrewed Maritime Vessels (UMVs), Unmanned/Uncrewed Aerial Systems (UAS), Swarms/Swarming

Abstract:

This technical paper recounts a geospatial drone security assessment for the Port of Brownsville, Texas (Brownsville Navigation District). The Port of Brownsville is a major intermodal transportation center and is expanding into a major venue for industrial development. The Port of Brownsville is the only deep-water port directly on the US-Mexico Border. The drone assessment will evaluate the threats posed by aerial drones/unmanned or uncrewed aerial systems (UAS) to the port; assess the potential effects of drones on port operations and port security; suggest potential counter measures (counter-UAS); provide an introduction to emerging drone threats, including unmanned/uncrewed vessels and ground vehicles; and drone swarms (or swarming attacks). The impact of various drone threats with port operations is discussed. Mechanisms for enhancing indications and warning, detection, and response to drone threats on the Port of Brownsville, and potential vehicles for sharing these threat data with other ports, port security personnel, law enforcement, and emergency responders will be discussed.

Introduction

This technical paper provides a drone threat assessment for the Port of Brownsville. The assessment looks at all drone modalities (aerial, ground, and maritime) with special emphasis on aerial drones or unmanned/uncrewed aerial systems (UAS). Figure 1 depicts an aerial drone above the port. The port imports and exports a range of cargoes, including steel slab, hot and cold rolled, steel plate, steel beams (billets), iron ore, pig iron, aluminum T-bars and ingots, grains, sugar, salt, minerals, wax, windmill components, cement, aggregate; and hydrocarbons, including gasoline, diesel, natural gas and several grades of lube oil; as well as containerized cargo. The Port of Brownsville is one of 17 ports in Texas. The Port of Brownsville (UN/Locode: USBRO) is located circa 25° 57′ 0″ N, 97° 24′ 0″ W in Cameron County, Texas. The port is at the southern terminus of the 17 mile-long Gulf Intracoastal Waterway near the mouth of the Rio Grande; it is 8 miles (13km) north of the Mexican border. The port is served by the deep-water Brownsville Ship Channel which accesses the Gulf of Mexico, passing between several barrier islands (North and South Padre Island, and Brazos Island). The Port is governed by the Brownsville Navigation District. The Post of Brownville covers 40,000 acres of land and is served by its own Port of Brownsville Police and Security Department. The United States Coast Guard maintains a Marine Safety Detachment co-located with the Port of Brownsville Police. The port is a Foreign Trade Zone (FTZ No. 62), contributing $ 3 Billion to the Texas economy.

Figure 1. 3D Depiction of Aerial Drone Models at Altitude Above the Port of Brownsville (Authors' Analysis rendered using Geoweb 3d Software)

Situation/Methodology

The Port of Brownsville (POB) is currently operational and has the potential to expand and become a significant regional port on the Gulf of Mexico. Like all ports, it faces a range of threats and risks. Addressing and anticipating these risks is essential to sustaining current operations and anticipating future threats. Drones, specifically UAS have been identified as a potential threat to operations.[1]

In order to assess the scope of current and future drone threat—including the range of drones: UAS, as well as ground and maritime variants to the Port of Brownsville, the threat assessment team conducted a literature review of drone threats. This review built upon review of previous technical papers produced for the Institute of Homeland Security at Sam Houston State University, academic and professional papers on these issues, including contemporary threats faced in Mexico, where criminal armed groups (CAGs) are weaponizing aerial drones, and in Ukraine.

The literature review was augmented by open source, geospatial assessment of the port's terrain features and assessment of drone sensor data available for the port and environs. Figure 2 depicts aerial drones above the port. This baseline data was augmented by video teleconference discussions with the POB Police Executive and Command Staff (chief, lieutenant, and sergeant), a two-day site visit to the port which included three focus group sessions: 1) Port of Brownsville Personnel; 2) Port of Brownsville Tenants; 3) Public Safety Partners; a guided tour of the port; and a private discussion with Chief Dietrich and his command staff. The focus group sessions were augmented with follow on discussions and a survey.

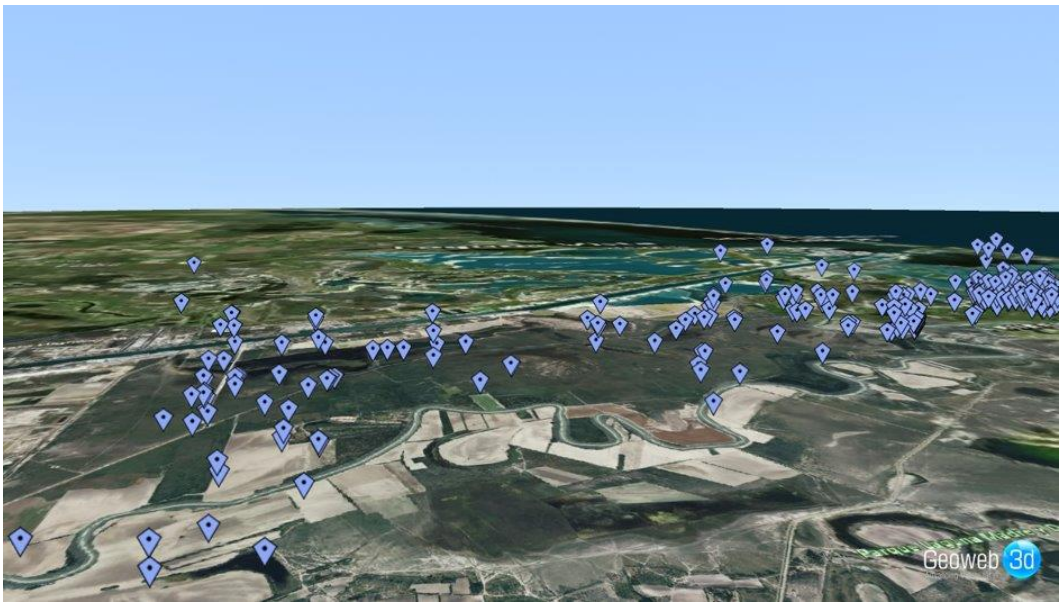

Figure 2. 3D drone data represented as icons clicking on an icon opens the attribute data of the drone. (Authors' Analysis rendered using Geoweb 3d Software)

Overview of Drone Threats (UAS and Emerging Threats)

Drones are both an emerging threat and opportunity. Drones range in size from small consumer vehicles to larger payload specialty vehicles. Drones can be used in the air, on the ground, and on and under the water. This section of the report summarizes the threats that drones of all three general categories can present to a port. Similar threats are faced at other venues and critical infrastructures.[2]

All drone activity can be characterized in one of three ways: 1) it can be an *Irritant*; 2) it can be *Malevolent*, 3) or it can be *Beneficial*. This applies to all three major classes of drone: aerial, waterborne or maritime, and surface or ground. Irritants include unlicensed an unauthorized use, such as hobbyists flying to observe an area out of curiosity, but not observing flight and access restrictions. Malevolent use includes drones used to smuggle illicit goods, surveil an area (this is known as intelligence, surveillance, and reconnaissance or ISR in military settings), or conduct an attack. Drones used for ISR can be casing an area for future attacks (this will be discussed in Section 4: Operational and Legal Issues). Beneficial drone use includes using drones for facility inspections and site security.

Drone Threat Potentials on the Rise

The use of drones—especially aerial drones—has gained increasing notice an interest in recent years. Drones have become a feature of military operations. Drones are also increasingly important in criminal and potential terrorist operations. In Ukraine, battlefield drones have become ubiquitous.[3] Indeed, Ukraine epitomizes the now and future threat posed by the weaponization of commercial drones.[4] Drone threats in Ukraine include a range of aerial drones. This range includes large payload military drones, as well as commercial-off-the-shelf (COTS) and custom-built drones using repurposed military ordnance and homemade

explosives (HME) to accurately target equipment and personnel. The smaller aerial drones are known as small UAS (sUAS) and are able to deploy explosive payloads up to 1.3 kilograms (2.86 pounds),[5] surface or ground vehicles (UGVs),[6] and maritime drones or uncrewed maritime vessels (UMVs); both surface vessels, also known as Uncrewed Surface Vessels (USVs) and subsurface vessels, also known as uncrewed underwater vessels (UUVs). One way attack (OWA) drones that can act as suicide or kamikaze drones, crashing into or detonating above a target, may become another mode of UAS attacks, potentially bringing larger payloads to bear from a greater distance and at a reasonable cost.[7] Finally, the potential for drone swarms is evolving in Ukraine.[8]

Closer to home, criminal drone threats are also evolving. Mexican cartels have weaponized commercial off-the-self drones to conduct attacks against rival cartels and gangs and both police and the military.[9] Mexican cartel drone use is an example of clandestine drone proliferation.[10] The use of aerial drones on the US-Mexico border is a persistent concern.[11] Terrorist use of drones is also an emerging concern.[12] According to Interpol:

> Recent examples include terrorist groups using drones in surveillance activities and delivering chemical, biological, radiological, nuclear and explosive materials in conflict zones, and an environmental group which repurposed a hobby drone to enter the secure airspace of a nuclear site and crash into a building highlighted the current reality of the threat posed by the illicit use of drones.[13]

Drones, specifically sUAS, have also been used to threaten public officials in Mexico[14] and Venezuelan President Nicolás Maduro was subject of a two drone assassination attempt in Caracas in August 2018.[15] These potentials have not yet been fully realized in the United States, but the potential is real.[16] As Dr. Robert J. Bunker has noted:

> A single weaponized drone could engage in ISR and locate a target, engage that target with an IED, and also capture the attack on video.[17]

Potential consequences from sUAS attacks are feasible and their effects may be grave. A recent study of nefarious sUAS use conducted by the Homeland Security Operational Analysis Center, a federally funded research and development center (FFRDC) operated by the RAND Corporation for the US Department of Homeland Security identified four high-risk use cases of nefarious sUAS:

- unauthorized reconnaissance or surveillance
- conveying illicit material [smuggling]
- conducting a kamikaze explosive (i.e., kinetic) attack
- conducting a chemical, biological, or radiological [CBR] attack.[18]

Threats and Opportunities for Ports and Maritime Security

Explosive laden aerial drones have targeted commercial tankers in the Gulf of Oman on both 15 and 18 November 2022.[19] In the five years ending in 2022, 73% of 23 recorded drone attacks on oil and gas targets in the Middle East have been successful.[20] In September 2019, for example, two oil processing facilities in Saudi Arabia were attacked by drones.[21] Another

exemplary oil and gas attack on a port occurred in Yemen at the Al-Mukalla port in October 2022 as an oil tanker was offloading fuel (that is a significant tactic, technique and procedure – TTP for our purposes).[22] Maritime terrorism and attacks on port potential undermine national security and protecting ports is a key critical infrastructure protection need since interruptions of port operations can undermine global logistics and supply chains.[23]

The United States Coast Guard (USCG) has developed a new "Unmanned Systems Strategic Plan" that establishes the future framework for using aerial and waterborne drones for protecting US maritime borders.[24] The USCG envisions using drones of all types, including UAS—and other unmanned systems or UxS—as an enabling capability within its force structure for all Coast Guard mission areas."

> UxS will provide persistent maritime domain awareness; optimize surveillance in order to predict, detect, deter, counter, and mitigate threats to the homeland and the maritime environment; and reduce the dull, dirty, dangerous, and distant demands on personnel, optimizing the employment of limited Coast Guard resources.[25]

The UxS missions for the Coast Guard includes using aerial drones, USVs, and UUVs, both autonomous and semi-autonomous to counter both military threats and threats posed by transnational criminal organizations (TCOs).[26] Indeed, criminal cartels have been adapting semi-autonomous uncrewed semi-submersible vessels (known as narco-submarines) for transporting narcotics across the sea.[27]

As previously mentioned, drones can include aerial systems, such as sUAS, on the ground, including UGVs, and on the water on the surface or underwater, UMVs. It should be noted that these types of drones are based upon the prevailing technology and the distinctions may be blurred in the future (and already are being blurred) as amphibious drones able to operate in multiple settings emerge. One example of this emerging technology is the aerial-submersible combination drone that can fly and swim underwater.[28]

Amphibious drones also highlight another emerging drone threat potential: *Drone Swarms*.[29] Drone swarms involve multiple drones working to achieve a specific goal, such as targeting critical infrastructure like a port or oil refinery or a military or civilian target. Drone swarms can involve a single type of drone massing its effects on a specific target or a range of drones of different types and functions to achieve a collective objective. The first scenario involves "homogeneous" swarms: the second "heterogeneous" swarms. The heterogeneous swarms could involve a mix of aerial, land, and waterborne drones or a mix of weaponized, surveillance, and command and control drones. Smaller swarms can be controlled by human operators using off the shelf devices; larger swarms would require multiple human operators or assistance from artificial intelligence (AI) and are therefore a future threat consideration.[30] Aerial drones—sUAS—are currently the main threat with the greatest disruptive potential.

Responding to Aerial Drones (UAS)

Unmanned or uncrewed aerial systems present a range of concerns and threats in the port environment. At the top of the operational set of issues is determining the nature of the drone

entering the port's airspace. This threat assessment is at the core of counter-drone (C-UAS) response. Are the drones entering the port's airspace an actual threat, a nuisance, or conducting an authorized commercial activity? If a threat what type of threat is involved and what immediate actions are viable to protect the port? As previously mentioned, many sUAS entering the port are irritants or nuisances. They however, congest the airspace, can cause unintentional harm, and can obscure the presence of actual malevolent threats. The volume of UAS incursions is likely to increase as UAS platforms become more common. Developing a C-UAS awareness and sensing capability is therefore an important strategic need. Discerning threats is based upon awareness, recognition, and discrimination.

First, what are the drone's characteristics: size, speed, payload? Is it equipped with specialized capabilities such as cameras, sensors, or weaponized payloads (explosive, chemical/biological or radiological dissemination)? Is there a known operator, can you use technical (sensors, cameras) or human means (patrol cars) to locate the operator? Is the UAS first-person view (FPV) and in line of sight or is it operating across a distance and over the horizon? Is it a single UAS or is it multiple UAS, operating as a swarm? Second, how will a malevolent drone or unintentional drone accident affect the port? Will it diminish perceptions of port security or affect port operations? Will it result in loss of revenue and decreased on time performance. Will it increase liability and insurance coverage? Will it cause injury, death or serious damage to property? Will it disrupt supply chains, etc.?

Addressing these issues relies upon awareness of UAS (and also other drone types such as UGVs and UMVs, surface and subsurface. Awareness requires familiarization and a range of training for different personnel based upon their role (operations personnel, security and law enforcement responders, and fire/rescue/emergency medical service responders. This familiarization and awareness need to be implemented through policies and procedures (*i.e*., standard operating procedures–SOPs and emergency operations procedures–EOPs) with defined role-based TTPs. Intelligence and threat assessment enable these factors to come together for effective incident response and mitigation.

Response and mitigation can be enhanced through inter-agency cooperation and coordination, sharing threat and incident response information, and ensuring effective governance. Effective governance incorporates operationally effective detection capability and articulates clear response roles with established authorities for action. All of these factors must be defined and practiced through exercises and immediate action drills (IADs). These response measures require the establishment of policy and can be augmented by developing specific ordinances for authorized drone use in the port area.

Drones (UAS and other types) can also be used as tools for protecting the port and ensuring effective operations. Drones can be used for inspecting facilities, monitoring hazardous operations (such as various phases of ship operations), responding to and interrogating drone incursions by bringing sensors and visual means (cameras) to assess the incursion or suspect drone(s). Sensors, as discussed in other sections of this report, bring capabilities for protecting the port. These range from threat recognition through response. Various types of sensors can be integrated to detect different components of an overall threat. For example a drone sensor can potentially detect UAS or other drones, multiple detectors can enhance the likelihood of

detection. Drone detectors can be augmented with other tools, including visual sensors, such as video and CCTV, and automated license plate readers (APRs) to monitor approaches to the port where vehicles may be used by the operators of suspect drones. These different sensor types can be located at key approach and perimeter locations and checkpoints in order to triangulate sensor data toward identifying drone operators.

The essential components of a successful counter drone (including C-UAS) capability include defining a counter-drone strategy (including C-UAS), awareness and training, policies and procedures, intelligence and threat assessment for all phases of response (pre-incident, trans-incident, and post-incident. Once a drone is detected (the trans-incident phase), an incident response is required; this includes threat assessment and development of response and mitigation courses of action (COAs). Post-incident actions include incident investigation and attribution, intelligence assessment, information-sharing (within the port and among other ports, local law enforcement agencies, and intelligence fusion centers) to determine baseline threat awareness and identify potential threats or campaigns involving multiple venues. All of these should be followed by and documented in a comprehensive after action review (AAR).

Drones for Incident Response (Drones for Good)

Like all technologies, drones can be used for beneficial purposes, that is they can become "drones for good." The POB Police could potentially use sUAS as part of both a C-UAS program and part of a regular surveillance and incident response capability. Drones used in this fashion could become a force multiplier and extend the Port Police reach and enhance their effectiveness. Of course, this would require additional dedicated resources and personnel. In the interim, the POB Police could potentially build a part-time program and partner with adjacent agencies to start building this capacity. The City of Brownsville Police Department currently operates an "Unmanned Aircraft System (UAS) Program" with FAA-licensed remote pilots.[31]

Site Survey and Port-Specific UAS Issues

This section provides an overview of the terrain and physical infrastructure of the Port of Brownsville and its various components with special attention to UAS threats. The section also provides a discussion of key vulnerabilities for aerial ground, and maritime drone threats.

As this report, and especially the following analysis demonstrates, drones—especially sUAS—need to be recognized as a concern to the Port of Brownsville. This concern is also shared with the wider area as drones are a concern all along the US-Mexico frontier and the border zone in the Rio Grande Valley (RGV). According to the Border patrol Chief for the RGV sector:

> Right now, in the Rio Grande Valley, as beautiful as it is, we have a lot of encounters with drones, you know, coming from across the Mexican side of the border into the United States. And my concern as a chief is mostly for my agents on the border patrolling because they're doing counter surveillance on us, right? And when there's a drone doing counter surveillance on us, especially on the personnel on the ground, and the soldiers, because right now I have about 250 Department of Defense soldiers

> helping us do the mission on the border, they're doing counter surveillance on our operations and where we deploy our border patrol agents…
>
> And fortunately, DoD allowed us… we borrowed some technology for counter drone technology to help us. We only have one unit that we're testing right now. And it's been so successful that we've been able to acquire drones that have come across because we take them over and we bring them down, and we're able to exploit the intelligence out of that, and we're able to find out where it originated from. So we're working very closely with Mexico to be able to make those arrests and be able to prosecute those individuals…
>
> But, we need more of that. We really do. Because as more technology advances, more of the criminal organizations are also purchasing that technology…
>
> But, unfortunately, [there have been] over 24,000 detections of drones in RGV since we started tracking it last year. So that's a lot and it's very conservative. So technology for counter drone technology is what the Border Patrol needs right now in the Rio Grande Valley.[32]

The drone detection sensors described by the Chief of the Border Patrol RGV Sector were used as a foundation of this drone threat assessment. Specific locations of these sensors involved and their specific area of interest surveilled are excluded from this report for operational security reasons. Despite these caveats, there was significant sUAS activity described in relation to the area encompassing the Port of Brownsville. These are discussed in the following sections of the report, but first we will turn to a geospatial assessment of the port terrain using geographic information systems (GIS) or geospatial intelligence (GeoINT) analysis. We will then provide an assessment of the drone sensor data captured toward our overall drone threat assessment and then focus on the aerial environment characteristics underlying that assessment.

Drone Threat Perception Survey

The threat assessment project team administered a "***Stakeholder Survey on Perceptions of Drone Threats to the Port Of Brownsville (POB****)* (See Appendices Three and Four). The survey was disseminated to a total of 31 people and yielded six (6) responses; a 19.35% response rate. The survey was initially offered in print format (which yielded three (3) responses and was then offered in an online format yielding an additional three (3) responses. Three of the respondents were port officials; one was a port tenant; and two were public safety partners. All respondents and their responses were anonymous. The threats were rated on a scale of 1 to 10 with 1 the lowest threat and 10 the highest. Responses in the range of 1 to 3 are considered low threat; responses in the range of 4 to 6 (with 5 being the mid-range) are considered moderate threat; responses from 7 to 10 are considered high threat.

Perceived Threat Level:

- **Uncrewed Aerial Drones (UAS).** The average threat rating for Uncrewed Aerial Drones (UAS) was 7.0 High

- **Uncrewed Ground Vehicles (UGVs).** The average threat rating for Uncrewed Ground Vehicles (UGVs) was 3.67 Low .

- **Uncrewed Maritime Vehicles–Surface (UMVs-Surface).** The average rating for Uncrewed Maritime Vehicles–Surface (UMVs-Surface) was 6.7 Moderate.

- **Uncrewed Maritime Vehicles–Subsurface (UMVs–Subsurface).** The average rating for Uncrewed Maritime Vehicles–Surface (UMVs-Surface) was 6.0 Moderate.

Organizational Plans:

When asked about plans for drone threat awareness and drone threat recognition half the respondents reported the existence of awareness and recognition plans; while half stated the absence of such plans. All respondents reported the existence of drone threat assessment plans. Three respondents stated their organization had operational plans for drone threat response, two stated they did not have such plans, while one respondent did not answer. All six respondents stated that they had plans for drone threat training.

Threat Information Sharing:

All respondents expressed an interest in participating in a threat information-sharing effort at the Port of Brownsville and with other Texas Ports. Similarly, all respondents were interested in participating in threat information efforts with US Gulf Ports. Five of six respondents were interested in national (US) threat information-sharing efforts; while four respondents were interested in international threat information-sharing efforts.

Law Enforcement–Corporate Security Collaboration:

All six respondents stated that they would welcome law enforcement–corporate security collaboration on drone threats.

Drone Response:

The average response for interest in drone detection was 7.83 High. The average response for using drones for counter-threat interrogation was 6.33 Moderate. The respondents were enthusiastic on using drone as a response tool for their own operations (drones for good) with an average response of 8.0 High.
Threat Modeling:

All respondents were interested in threats modeling for various drone threats.

Significance of Drone Threats:

The average rating of the importance of drone threats to port (POB) operations and security was 7.67 High.

Organization/Agency Specific Concerns:

There were four specific responses. One respondent had concerns about regulatory limits placed on UAS response. One respondent indicated a desire for integrating AIS (Automated Identification System) like that used by vessels for aerial UAS. A third respondent emphasized: "Educating stakeholders about identifying and mitigating drone threats." The final comment provided is worth recounting in full:

> The above questions were answered with respect to "capability" vs current known threat of drones. Effort to secure classified information is compromised by the current drone activity over the port, yet no response capability is authorized for local PD or facility to respond. Problem goes all the way to DoD and agency default to "no action is approved" for either kinetic or non-kinetic means of securing the airspace above Critical Infrastructure, or non-critical infrastructure with national security implications. Without approved US policy and resultant TTP then the US will continue to leave their CI [counterintelligence] and national security at risk. After 8 years watching the counter-drone discussion it appears no agency is willing to act until a significant event/incident/catastrophe occurs at the national level. Concern is "when will the critical incident occur?"

It is with this background that we turn to our geospatial and drone sensor analysis.

Geospatial and Drone Sensor Analysis

The threat assessment project team conducted a detailed terrain analysis of the Port of Brownsville. This assessment looked at the POB's physical terrain features and also assessed its vulnerability for UAS incursion. The project team found geospatial data as an important tool for understanding and visualizing risk for both this assessment and potential future application for managing UAS threats. Figure 3 and 4 following provide an illustration of that functionality with the port tenants' parcel boundaries depicted in Figure 3 and the underlying data attributed rendered in Figure 4. This data can be useful in alerting tenants of incursions and during threat assessment and incident response.

Figure 3. Authors' GIS Elaboration of POB Tenant Parcels. (Derived from POB Parcel Data)

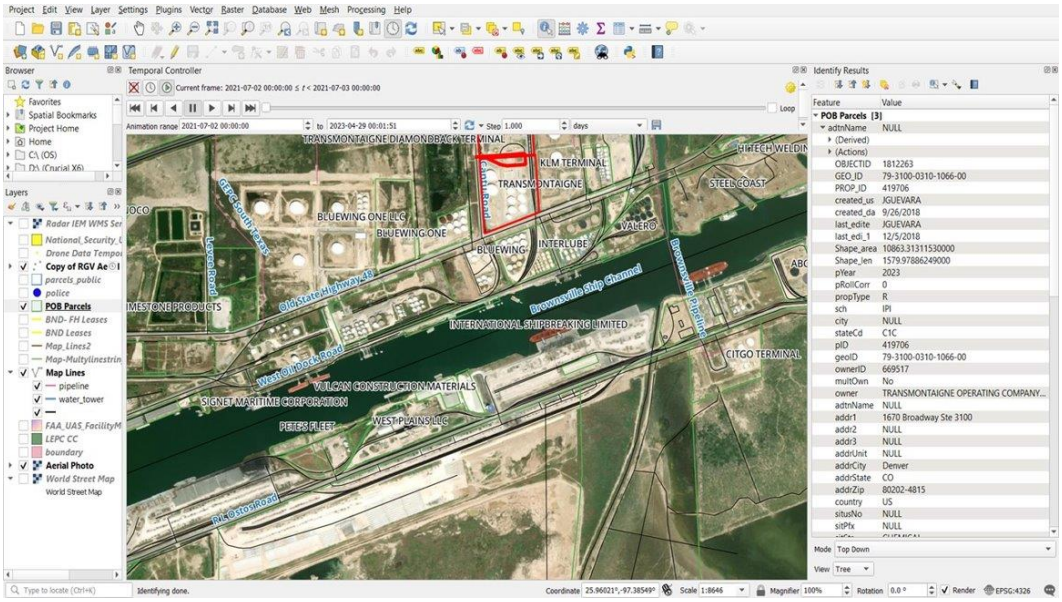

Figure 4. This Image Depicts GIS Functionality for Threat Assessment and Incident Response. (Authors' Elaboration; Derived from POB Parcel Data):

After creating a baseline terrain assessment, the project team conducted an assessment of aerial drone (UAS) incursions in the vicinity of the POB. The following images (Figures 5 and 6) summarize these findings with Figure 5 depicting the location of all aerial drones detected from July 2021 through April 2023. A total of 7,477 UAS were detected.[33] 5 depicts the locations of the drones detected.

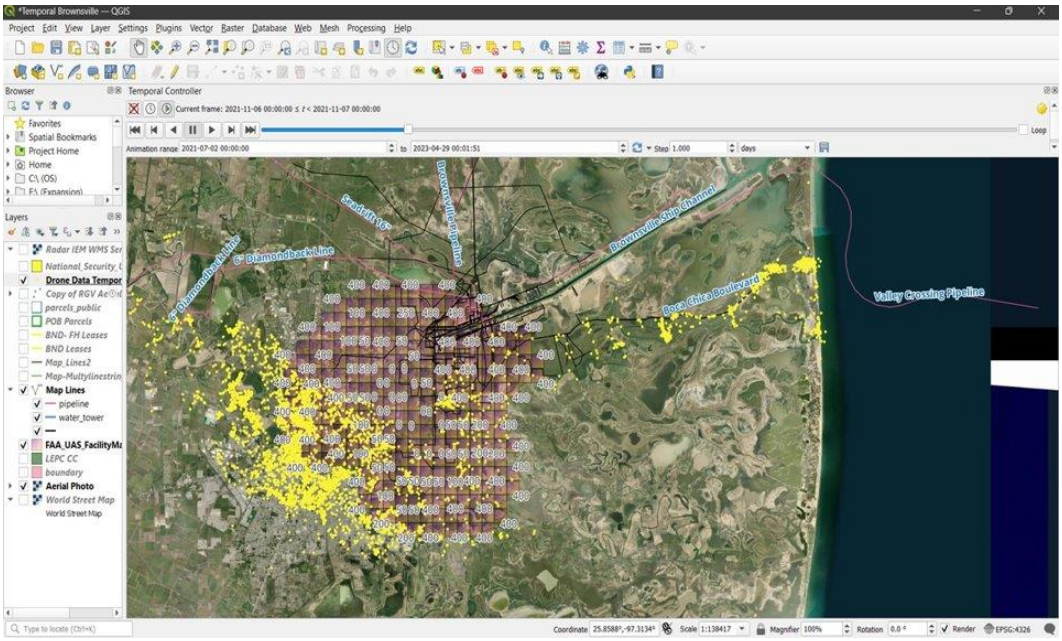

Figure 5. This image shows GIS functionality related to the location of all 7,477 drones detected from 7/21– 4/23. The gridded area in the center shows ceiling height restrictions in vicinity of the Brownsville/South Padre Island International Airport (BRO) airport. (Authors' Elaboration of Aerial Armor, a Dedrone Company Data)

The timeframe for this UAS assessment looks at sensor data from July 2021 through April 2023; it also focuses on an eight (8) mile radius of Brownville. Figure 6 is a Drone Detection Heat Map showing the intensity of drone traffic in that 8-mile radius. Figures 7 and 8 provide detail of the flight paths in the vicinity of the POB along the ship channel and south toward the Rio Grande (Rio Bravo) and US-Mexico border.

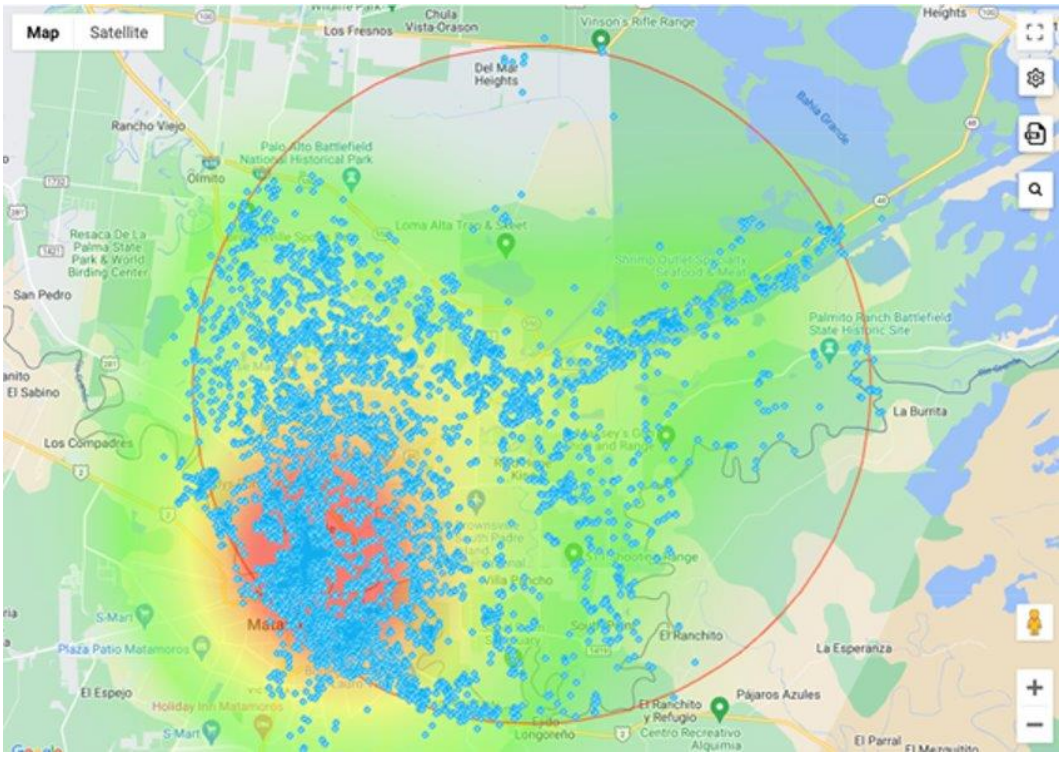

Figure 6. Drone (UAS) Detection Heat Map (Courtesy Aerial Armor, a Dedrone Company)

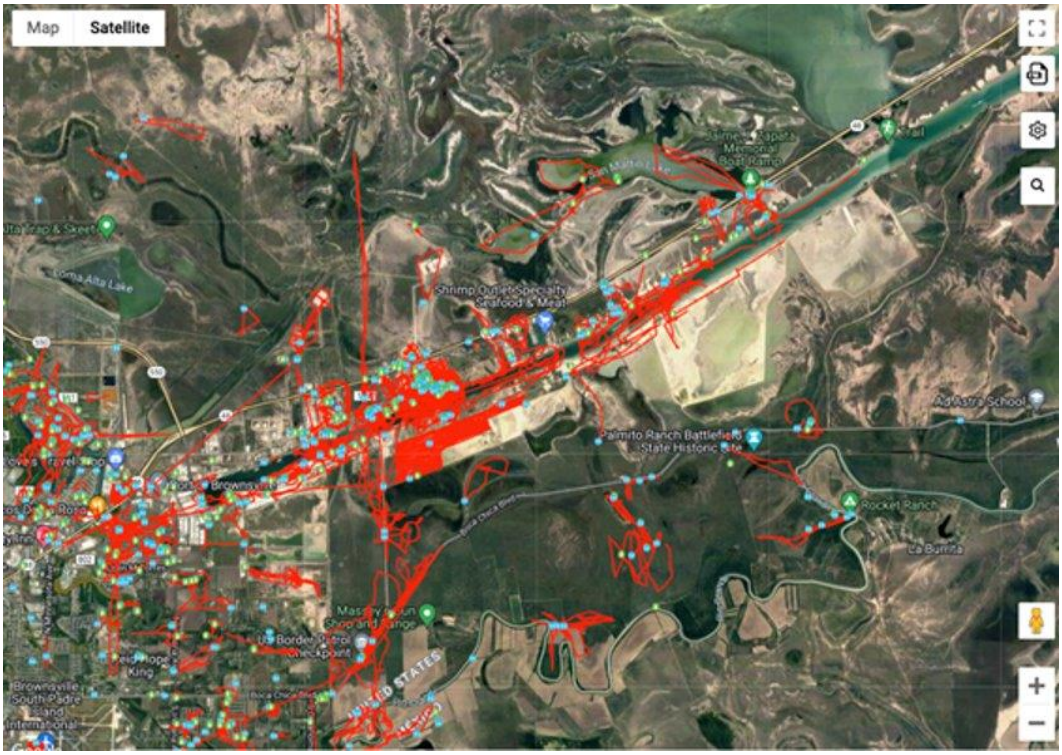

Figure 7. Drone Flight Paths Depicted with Red Lines in Vicinity of the POB (Courtesy Aerial Armor, a Dedrone Company)

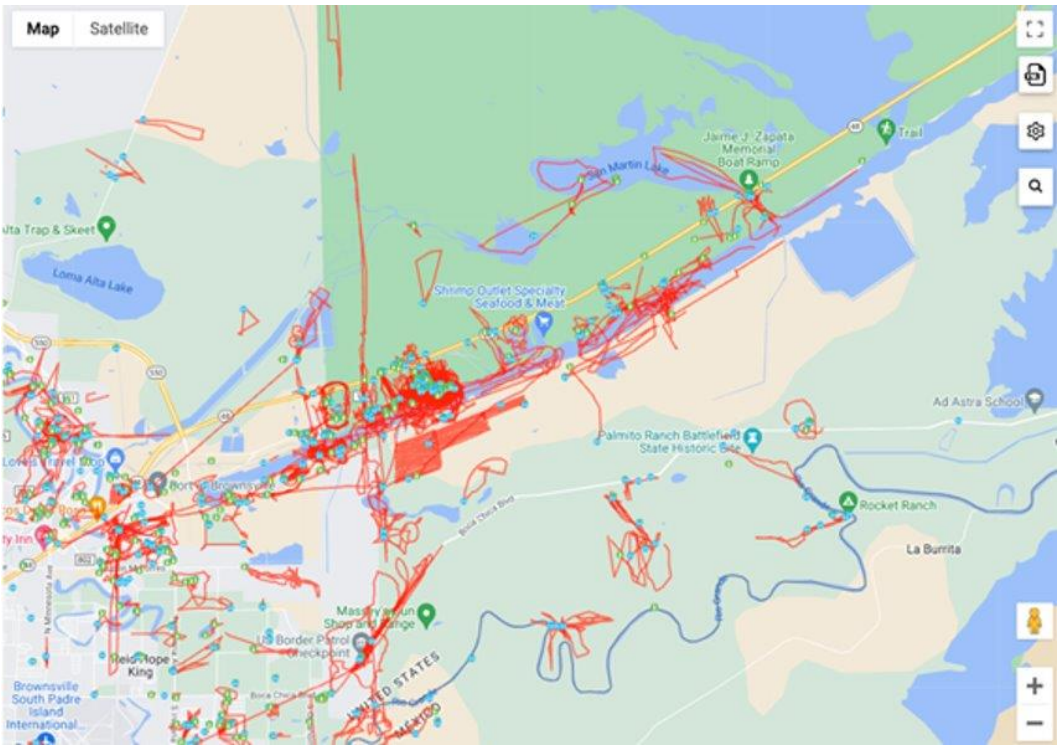

Figure 8. Drone Flight Paths Depicted with Red Lines in Vicinity of the POB (Courtesy Aerial Armor, a Dedrone Company)

A total of 7,948 flights were detected within the area of interest depicted in Figure 6 (an 8-mile radius from the POB). These are attributed to 1,326 unique drones (with a maximum altitude of 6,718 feet. Of the flights detected, 2,259 were found above 400 feet, These flights involved 406 unique drones. Night flights accounted for 1,771 of the drones detected (this data set is slightly larger than that depicted in Figure 5).[34] Figure 9 details the drone activity detected during the 450 days from 1 June 2022 to 11 July 2023. The majority of drone flights were in the 200–400 foot range; followed by drones in the 0–200 foot range; and then the third most common range at 400–600 Feet. Table 1 describes the types of drones and number of flights by each drone type detected during the same 450 days.

Figure 9. Flight Range by 200 Foot Increments (Courtesy Aerial Armor, a Dedrone Company)

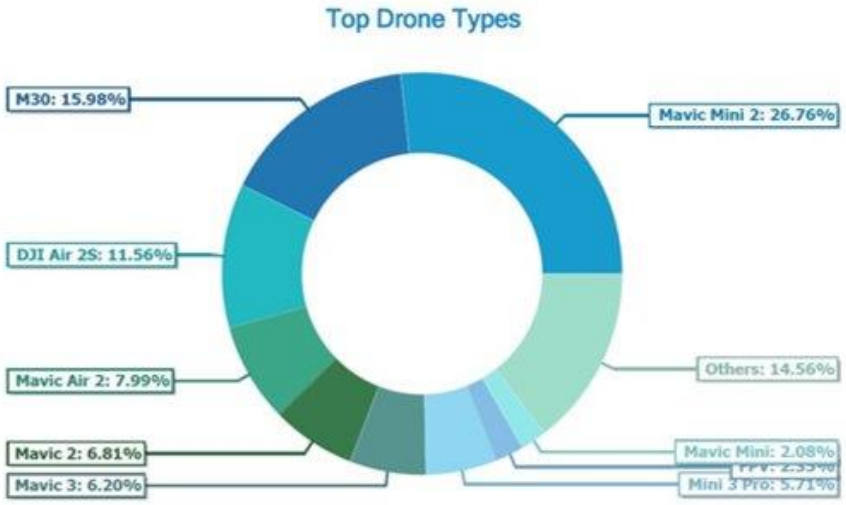

Figure 10. Most Common Drone Types Detected (Courtesy Aerial Armor, a Dedrone Company)

Drone Type	Flight Count
Mavic Mini 2	2,127
M30	1,270
DJI Air 2S	919
Mavic Air 2	635
Mavic 2	541
Mavic 3	493
Mini 3 Pro	454
FPV	187
Mavic Mini	165
Mavic Pro	143
Mini SE	134
Mini 3	80
Unknown	80
Mavic Mini 3 Pro	75
Mavic 2 Enterprise	73
M300	67
M2EA	66
Phantom Pro V2.0	65
Mavic 3C	62
Inspire 2	58
Mavic 3E/3T/3M	44
Phantom 3 Std	22
Mavic 3E/3T	21
Mavic Air	21
Phantom 4 Pro	19
Avata	16
Mini 2 SE	16
Spark	14
P3SE	14
Mavic 3 Pro	12
Phantom 4	12
NewDrone_88	10
NewDrone_87	7
Phantom 4 RTK	7
M200 V2	4
Phantom 4 Adv	3
NewDrone_84	3
NewDrone_73	3
Phantom 3 Series P	2
M600 Pro	1
NewDrone_67	1
M200	1
NewDrone_86	1

Table 1. Drones Type and Corresponding Flight Count (Courtesy Aerial Armor, a Dedrone Company)

Figure 11. Drone Flight Counts by Week and Month (Courtesy Aerial Armor, a Dedrone Company)

Figure 10 describes the most common drones UAS)detected and Figure 11 displays the drone counts by week and month. The drones detected were all COTS UAS produced by DJI (SZ DJI Technology Company, located in Shenzhen, Guangdong, China.) DJI quad-copter drones are the most common commercial sUAS platform. DJI drones come in a variety of models with variable payloads and specialty applications ranging from camera drones that are ideal for ISR operations to agricultural drones used for crop dusting (that can be weaponized to disseminate chemical or biological agents).[35]

While the entire POB is at potential risk from UAS activity, the liquid cargo docks handling petroleum products are at risk due to the volatile and hazardous nature of the products distributed. Tenants handing petroleum and hydrocarbon products deserve special attention. Figure 12 illustrates this risk by displaying UAS flight paths above port petroleum terminals and storage tanks. Another area of concern is the USS Kitty Hawk (CV-63) aircraft carrier being dismantled by International Shipbreaking Limited, LLC. Figure 13 shows drone flight paths above CV-63. Figures 14 and 15 provide 3D models of drones taking photos of the CV-63. While these incursions are most likely hobbyists or irritants, they could also have been commercial Part 107 operations—media photographers operating in unrestricted airspace. It is also possible that they involve malevolent intelligence gathering (ISR) conducted by a foreign power seeking knowledge about the construction of US aircraft carriers, This may therefore involve a counterintelligence threat, warranting enhanced detection and security.

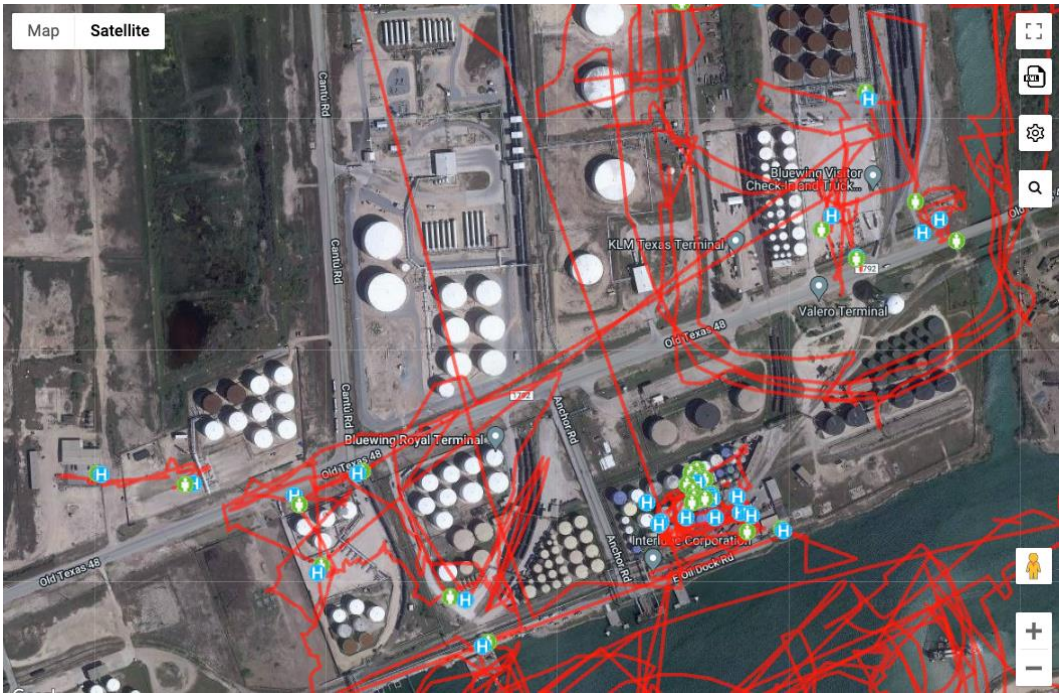

Figure 12. Drone (UAS) Flight Paths Above Oil Terminals and Storage Tanks (Courtesy Aerial Armor, a Dedrone Company)

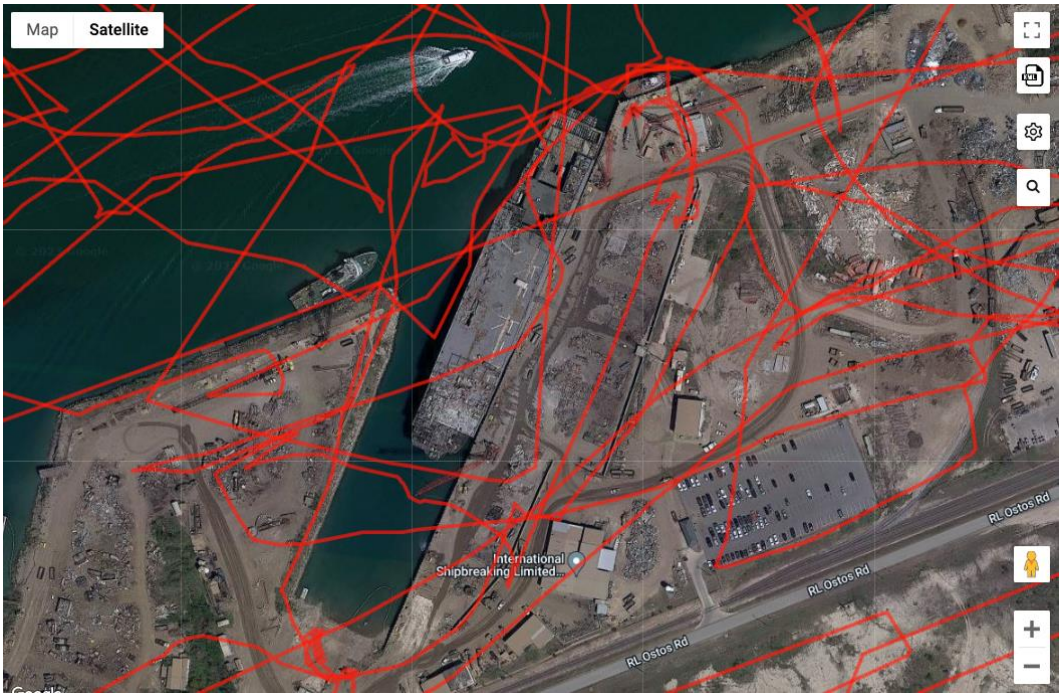

Figure 13. Drone (UAS) Flight Paths Above CV-67(Courtesy Aerial Armor, a Dedrone Company)

Figure 14. 3D Models of (CV-63) and an Aerial Drone Taking Photos (Authors' Elaboration)

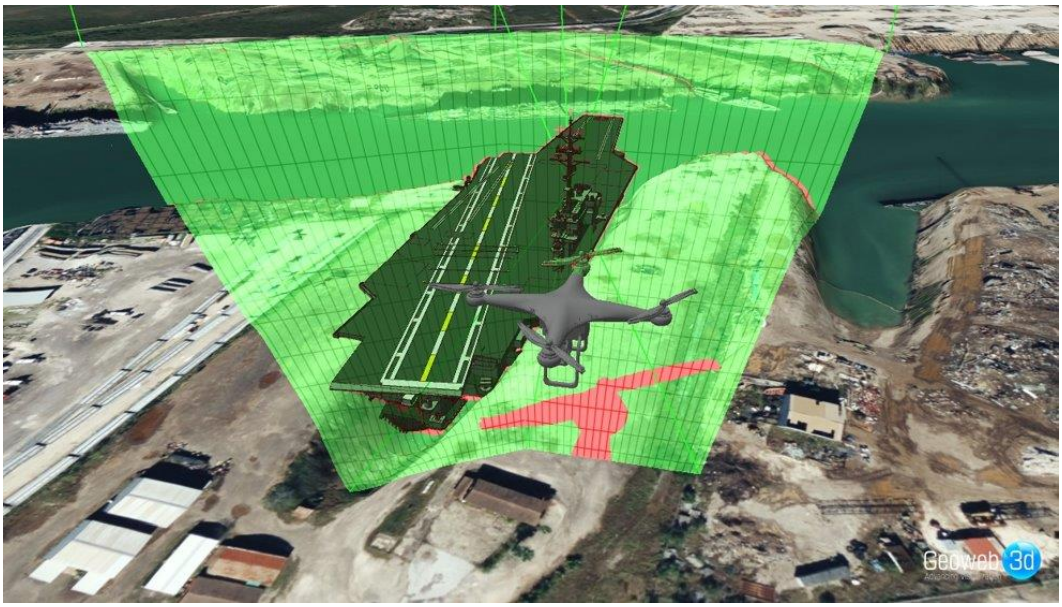

Figure 15. 3D Model of (CV-63) and 3D model of Drone taking Photos with Viewshed Analysis, Depicting in Green what the drone is imaging from that Vantage Point. This is the type of Geospatial Tool that Can be Integrated into a Drone Sensor Command and Control Platform For Threat Assessment and Incident Response. (Authors' Elaboration)

Overall Drone Threat Assessment

The project team recognizes that drone threats are unfamiliar to many port operators, tenants, and public safety personnel. At first glance, these threats appear to be in the realm of science fiction.[36] Yet, contemporary developments in Ukraine have shown that drones of all varieties

are now part of the current and future warfare toolkit. Similar events in Mexico's crime wars show that sub-national groups, drug cartels and gangs, can and do employ drones as part of their repertoire. Terrorists are also embracing drones as part of their TTPs. These various threat vectors are discussed in the preceding Part 2 of this report. Based upon the factors described in that discussion, the project team assesses that drone threats are both a current and emerging threat to US ports in general and the Port of Brownsville (POB) and potentially other Texas ports in specific.

- The *highest level* of current drone threat involves small **Uncrewed Aerial Systems (sUAS)**. That threat is assessed as *Moderate to High*. The level of sUAS threat can be expected to grow as the Port of Brownsville expands and increases it activity.

- The *next potential level of threat* involves **Uncrewed Maritime Vessels (UMVs), including surface and subsurface vessels**. These are currently evident in military settings or used by criminal cartels to smuggle drugs. These vessels can be weaponized and are likely to become a future factor in port operations. This threat is assessed as *Moderate*, with the potential to grow as the use of these vessels increases and the port grows.

- The *lowest level of threat* is posed by **Uncrewed Ground Vehicles (UGVs)**. This threat is assessed as *Low–Moderate.* While UGVs have been used in combat (specifically in Ukraine), and remotely piloted vehicle borne improvised explosive devices (VBIEDs) have been used by terrorists in the Middle East, these type devices are not currently in wide use in the civil sector. The UGV threat can be detected and mitigated with current defense-in-depth security measures already in place, such as perimeter fencing, cameras, and security patrols.

The threat of multi-modal drone threats, involving drone swarms (of various types) is assessed as a potential future concern. Current efforts to enhance security for drone threats should prioritize sUAS. For UAS threats, awareness of airspace dynamics is essential the following discussion provides an airspace assessment of the port and its environs.

There are five distinct areas where drones are restricted from flying without prior authorization in the vicinity of the Port of Brownsville. In addition to the Class D airspace around the Port of Brownsville, there are flight restrictions at Palo Alto Battlefield National Historic Park, areas along the land and maritime border between the United States and Mexico, and the area around the SpaceX Boca Chica Launch Facility.

Temporary Flight Restrictions over Critical Infrastructure

The Department of Homeland Security Cybersecurity & Infrastructure Agency (DHS CISA) identifies sixteen critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.[37]

One of the sixteen critical infrastructure sectors in the Transportation Systems Sector. One of the seven key subsectors of the Transportation Systems Sector is the Maritime Transportation System which includes 361 ports, and more than 25,000 miles of waterways, including the Port of Brownsville.[38]

Further located within the Port of Brownsville are tenants which may themselves fall within one of the sixteen critical infrastructures, including the chemical sector.

In the 114th Congress (2015-2016), the FAA Extension, Safety, and Security Act of 2016 was passed and signed into law. A crucial provision within this legislation was Section 2209, which mandated the Secretary of Transportation to establish a streamlined procedure enabling applicants to formally request the Administrator of the FAA to impose restrictions or prohibit the operation of unmanned aircraft near fixed site facilities. The implementation of this process was required within 180 days of the bill's enactment. Consequently, on 15 July 2016, President Obama signed the bill into law as Public Law No. 114-190.

The Act established that the following may be considered fixed site facilities: Critical infrastructure, such as energy production, transmission, and distribution facilities and equipment, Oil refineries and chemical facilities, Amusement parks, Other facilities that warrant such restrictions

Operational and Legal Issues

Operational and legal issues related to countering drone threats, especially counter-UAS (C-UAS) are complex and evolving. This section includes a discussion of counter-UAS issues from an operational perspective. First the discussion will address the core components of a counter-UAS framework. Next, the legal issues involved in implementing and sustaining that framework are reviewed.

What is Counter-UAS?

There are varying definitions of Counter-UAS that range from simple descriptions to wordy legal definitions. Although consensus may be lacking on how to specifically define Counter-UAS, a common framework is important that takes into account the varying mission types and legal authorities of organizations or agencies that may perform this mission. Given the current legal and operational Counter-UAS landscape in the United States and other countries around the globe, the following is offered as a universal construct for Counter-UAS operations:

> *"Counter-UAS is the deployment and use of logical, legally authorized technologies, tactics, techniques, and procedures to provide airspace awareness and protection to critical infrastructure, assets, and mass gatherings."*[39]

Current Legal and Legislative Landscape for Counter-UAS in the United States

The following section provides an overview of the current legal and legislative landscape for counter-UAS activities within the United States.[40]

Department of Energy and the Department of Defense

The 2017 National Defense Authorization Act (NDAA) provided legal authority from Congress for both the Department of Energy (DOE) and the Department of Defense (DOD) to protect covered facilities or assets.

The authority for DOD specifically referred to protect covered facilities or assets in the United States, territories, and possessions that meet requirements as determined by legislation. The Army, Navy, Air Force, and Marines are separately responsible for the protection of their own facilities.[41] The status of the protection of DOD facilities covered by the 2017 NDAA is not public knowledge, however, it can be assumed that it is ongoing. Earlier this year, the Marines submitted a Request for Information (RFI) "looking for interested parties to address the United States Marine Corps' (USMC) force protection installation security capability gap for the detection, identification, tracking and defeat of small Unmanned Aircraft Systems (sUAS) operating within the vicinity of specific mission sets associated with 10 U.S. Code Section 130i."[42]

The National Nuclear Security Administration (NNSA), a semi-autonomous agency within the DOE is responsible for maintaining and enhancing the safety, security, and effectiveness of the U.S. nuclear weapons stockpile, among other important functions. NNSA has implemented "No Drone Zones" at restricted sites such as Los Alamos National Laboratory, Nevada National Security Site, Pantex, and Y-12 National Security Complex. NNSA has reported that Counter-UAS systems are protecting sensitive locations such as Y-12 and Pantex.[43]

Department of Justice and the Department of Homeland Security

The FAA Reauthorization Act was signed into law on 5 October 2018. The 2018 Act is a wide-ranging reauthorization measure that provided the Federal Aviation Administration (FAA) with a host of crucial new authorities and responsibilities on an extensive range of aviation issues, including enhancing safety, improving infrastructure, and enabling innovation. The Act also extended the FAA's funding and authorities through Fiscal Year 2023.[44]

The FAA Reauthorization Act included Division H, also known as the "*Preventing Emerging Threats Act of 2018*." This portion of the FAA Reauthorization Act authorized the Department of Justice (DOJ) and Department of Homeland Security (DHS) to engage in Counter-UAS activities that would otherwise violate relevant provisions of federal law.[45]

The Department of Justice (DOJ) or Department of Homeland Security (DHS) authorities have been exercised numerous times since the law was passed in 2018.[46] Although the agencies don't typically publicly disclose their Counter-UAS operations, open-source examples include the United States Secret Service (USSS), DHS Science & Technology Directorate (DHS S&T) and the USCG collaborating on a pilot initiative aimed at testing and evaluating cutting-edge technologies designed to detect, identify, and address the potential risks posed by unmanned aircraft systems; and a DOJ press release in October 2020 addressed the forecast of an increase in the use of Counter-Unmanned Aerial Systems (C-UAS) Protection Activities and

Criminal Enforcement Actions.[47] The release noted that, “From Oct. 1, 2019, to Sept. 30, 2020, the FBI (Federal Bureau of Investigation) has provided counter-UAS support at dozens of events, including national level sporting events such as Super Bowl LIV in Miami, the 2019 World Series, and the 2020 Rose Bowl Game, as well as at other major events that draw large crowds like Washington, DC’s A Capitol Fourth and New York City’s New Year’s celebration.”[48]

Counter-UAS Technologies For Agencies That Are Not DOJ, DHS, DOD, and DOE

The Counter-UAS authorities for state, local, tribal, and territorial (SLTT) public safety and law enforcement agencies, or owners and operators of critical infrastructure who seek to use technologies to counter the threat of careless and clueless, or nefarious drone operators are limited as of 1 August 2023.[49]

SLTT agencies and critical infrastructure owners and operators are limited by federal laws that may prevent, limit, or penalize the sale, possession, or use of UAS detection and mitigation capabilities. The capabilities involved in detecting and mitigating UAS have the potential to raise concerns related to federal criminal laws concerning surveillance, unauthorized access or damage to computers, and aircraft damage.[50]

Technologies that disrupt, disable, or destroy a drone are generally referred to as drone mitigation technologies. Mitigation technologies, with the capability to disrupt, disable, or destroy a drone, are not legally permissible for SLTT and owners and operators of critical infrastructure.[51]

There are some drone detection technologies that are able to be used by SLTT and owners and operators of critical infrastructure. This would include systems such as radars (with the appropriate license from the FCC), electro-optical/infrared (EO/IR) cameras, and acoustic systems. Some radio frequency (RF) detection technologies that monitor the communications passed between the ground control station (remote control) and the drone may implicate federal laws such as The Pen/Trap Statute and Wiretap Act. Recommendations on the testing, acquisition, and purchase of Counter-UAS technology are included later in this paper.[52]

Current Federal Legislative Landscape for the Expansion of the Use of Counter-UAS Technologies

Neither the Department of Justice (DOJ) or Department of Homeland Security (DHS) have the resources to provide airspace awareness and protection to all critical infrastructure, assets, or mass gatherings that warrant or require additional safety and security. The delegation of authorities to our nation's law enforcement agencies and critical infrastructure has sparked significant discussion within the security industry and law enforcement circles, among other sectors. It is widely acknowledged that the implementation of these authorities and technologies at the local level, coupled with appropriate training and oversight, would enhance the security of our local communities and infrastructure.[53]

In April 2022, the Biden Administration released its Domestic Counter-Unmanned Aircraft Systems National Action Plan.[54] The Plan contained eight (8) key recommendations for action:

1. Work with Congress to enact a new legislative proposal to expand the set of tools and actors who can protect against UAS by reauthorizing and expanding existing counter-UAS authorities for the Departments of Homeland Security, Justice, Defense, State, as well as the Central Intelligence Agency and NASA in limited situations. The proposal also seeks to expand UAS detection authorities for state, local, territorial and Tribal (SLTT) law enforcement agencies and critical infrastructure owners and operators. The proposal would also create a Federally-sponsored pilot program for selected SLTT law enforcement agency participants to perform UAS mitigation activities and permit critical infrastructure owners and operators to purchase authorized equipment to be used by appropriate Federal or SLTT law enforcement agencies to protect their facilities;

2. Establish a list of US Government authorized detection equipment, approved by Federal security and regulatory agencies, to guide authorized entities in purchasing UAS detection systems in order to avoid the risks of inadvertent disruption to airspace or the communications spectrum;

3. Establish oversight and enablement mechanisms to support critical infrastructure owners and operators in purchasing counter-UAS equipment for use by authorized Federal entities or SLTT law enforcement agencies;

4. Establish a National Counter-UAS Training Center to increase training accessibility and promote interagency cross-training and collaboration;

5. Create a Federal UAS incident tracking database as a government-wide repository for departments and agencies to have a better understanding of the overall domestic threat;

6. Establish a mechanism to coordinate research, development, testing, and evaluation on UAS detection and mitigation technology across the Federal government;

7. Work with Congress to enact a comprehensive criminal statute that sets clear standards for legal and illegal uses, closes loopholes in existing Federal law, and establishes adequate penalties to deter the most serious UAS-related crimes; and

8. Enhance cooperation with the international community on counter-UAS technologies, as well as the systems designed to defeat them.[55]

Recommendations One, Two, Three, Five and Seven, if enacted, would have a direct positive effect on the safety and security of the protection of critical infrastructure, assets, and mass gatherings throughout the United States.[56]

Texas, Cameron County, and Brownsville UAS Laws and Ordinances

Texas Law[57]

According to the *AUVSI Drone Prepared* website, Texas emerged as the frontrunner in drone policy, displaying remarkable activity with the introduction of twenty bills and the passage of

seven measures that reached the Governor's desk.[58] The significant surge in legislative efforts can be attributed to two key factors. Firstly, in March of 2022, a federal judge declared Texas' drone regulatory code, Chapter 423, as unconstitutional.[59] Secondly, the Texas legislature convenes only during odd-numbered years, placing pressure on lawmakers to swiftly reconstruct their drone regulatory framework within a condensed five-month session.

Senate Bill 947 (2023). This law, signed by the Governor and effective on 1 September 2023, makes it a felony to knowingly damage, destroy, or impair a critical infrastructure or facility using a drone.

House Bill 1833 (2023). This law, signed by the Governor and effective on 1 September 2023, makes it a felony to engage in criminal mischief with a critical infrastructure facility or public power supply through the use of a drone.

No Cameron County or Brownsville UAS-related laws were found during research.

Discussion and Recommendations

The Port of Brownsville is growing and will increase its threat exposure as its operations expand. This growth comes simultaneously with a rise in global tensions, crime, and the implementation of new and emerging technologies. Contemporary military operations, terrorism, and organized crime (including CAGs) are all embracing drones of all types to further their goals. These drone uses in conflict and crime are primarily sUAS but other platforms UMVs and UGVs are also entering the mix. The primary threat faced by the POB involves UAS threats. Therefore counter-UAS measures are the greatest current need. The following section provides and overview of C-UAS technologies and capabilities and provides a set of recommendations to meet current threats and better anticipate future threats (and opportunities).

Overview of Counter-UAS Technologies and Capabilities[60]

The two general categories of counter-UAS technologies previously mentioned are detection systems and mitigation systems. For the purposes of this report, we will further explore detection technologies only as this type of technology is more likely to be utilized by the Port of Brownsville Police Department in the foreseeable future.

UAS detection systems refer to technology that can detect, locate/track, and/or classify/identify drones. The four common categories of UAS detection technologies are:

- Radar
- Passive RF
- Electro-Optical and Infrared (IR) cameras
- Acoustic sensors

Radars function by emitting a focused radio signal with a known frequency and power in a specific direction. They subsequently detect the return signal that is reflected back from the

target. Radars come in two variants: two-dimensional (2D) and three-dimensional (3D). The primary function of 2D radars is to determine the direction and distance to a target. On the other hand, 3D radars go beyond that by additionally providing information about the target's altitude.

From an operational perspective, a counter-UAS radar by itself is generally an ineffective tool. Operators would be required to interpret the suspected drone detections from the radar without any method to verify the information with other sensors. This task is made even more difficult as motions such as hubcaps on a vehicle, flags waving in the wind, rotating sprinkler systems, and air conditioning fans are examples of everyday activities that can result in false positive radar detections. Radar is a more effective tool when, at minimum, it is integrated with an EO/IR camera where the camera can “slew to cue” to suspected targets from a radar, RF detection sensor, or an acoustic sensor.

Passive RF sensors depend on antennas to receive RF signals, which are then analyzed by computers. These signals are specifically associated with the communication between the Ground Control Station (GCS) and the Unmanned Aerial Vehicle (UAV). Passive RF sensors conduct analysis of radio signatures and modulations unique to UAS. These sensors possess the ability to identify specific UAS models and manufacturers, while also determining the origin of the signal transmission, which could be the UAV itself or the GCS.

Many passive RF sensors employ databases containing established radio signatures of known unmanned aerial systems. These systems compare the detected signals with those stored in the database to classify or identify the UAS. Periodic updates to the signature libraries are carried out to incorporate new UAS signatures and revise existing ones. Some Passive RF sensors, based on their functionality, may violate Federal law, such as the Wiretap Act and the Pen/Trap Statute. Because of this, it is strongly recommended that prior to the testing, acquisition, installation, or use of Counter-UAS systems, including “passive” or “detection only” systems, that entities fully understand how the system functions and seek the advice of counsel experienced with both federal and state criminal, surveillance, and communications laws.

EO/IR sensors, also known as electro-optical/infrared sensors, are advanced digital video cameras specifically designed to gather environmental data across both the visible and infrared light ranges. These sensors are capable of capturing electromagnetic radiation encompassing wavelengths spanning from 400 nanometers to 1 millimeter. Similar to the previous statement regarding the radar, an EO/IR camera with no advanced artificial intelligence/machine learning (AI/ML) capabilities, or that is not integrated with other detection sensors, such as a radar, RF sensor, or acoustic sensor is generally ineffective. Without those capabilities, an operator is generally left to manually search for drones in the sky. Some EO/IR camera systems have AI/ML capabilities where objects in the airspace are identified, and in some cases classified. Many of these systems are built to specifically to identify and classify drones or drone-like objects transiting through the airspace.

Acoustic sensors operate in a passive manner by utilizing microphone arrays with exceptional sensitivity, combined with audio analysis applications. Their purpose is to detect, track, and

identify sounds generated by the motors and propellers of UAVs. Each type of UAV propeller produces distinct acoustic patterns, enabling the creation of a comprehensive library of these sound signatures. This library facilitates the identification of various UAV types and provides a means to ascertain the approximate direction of the sound source.

Each of the different types of Counter-UAS detection systems can be operated separately, using their own separate graphical user interface, or GUI. When two or more UAS detection systems are being used, it is more efficient to have the sensors integrated into a common operating picture (COP) for efficiency and effective operational decision making.

Remote Identification for Drones

Beginning 16 September 2023, the FAA's Remote ID (RID) rule will become effective. All commercially flown UAS, regardless of weight, are required to broadcast RID message elements. All recreational UAS that weigh 250g (.55 lbs.) or higher are also required to broadcast Remote ID message elements.[61]

Remote ID is akin to a "digital license plate" in the sky. To comply with RID regulations, an operator has a few options. They can either use a Standard RID UAS equipped with built-in RID broadcast capabilities or attach a Broadcast RID Module to the drone. Otherwise, the drone must either operate in Federally Recognized Identification Areas (FRIA), which are specially approved non-RID areas, or remain grounded.[62]

Counter-UAS Considerations

Counter-UAS or airspace awareness and protection is not just the application of technology to counter the threat of UAS. A solid foundation for a department program begins with policies and procedures, training, developing technology user requirements, and then, if authorized, integrate logical technology to enhance existing security measures.

Policies and Procedures

Policies and procedures are the first step in establishing a Counter-UAS program. Developing a Counter-UAS policy will provide general guidelines that outline the organization's plan for tackling the airspace awareness and security issue. The policies can provide a bridge between the organization's security vision and its day-to-day operations. Counter-UAS procedures explain specific actions for carrying out the Counter-UAS policy. Procedures provide a blueprint for how to deal with specific solutions. Examples include:

- What happens when a suspected drone is visually detected flying over the port?
- What are the procedures to respond to a suspected drone threat?
- What happens if a drone crashes within the Port of Brownsville?

C-UAS Training

Training provides an opportunity to learn new skills and grow, not only as an individual, but as an organization. Recommended training for the Port of Brownsville Police Department includes:

- UAS Fundamentals and Threats. Understanding UAS capabilities, threats, and fundamentals.
- Basic Airspace Fundamentals. This training would focus on understanding the basics of airspace rules for drones, and Texas drone laws related to critical infrastructure
- Basic Counter-UAS Principles. Responding to suspected drone threats, pilot interviews, safety and threat considerations, and other related topics.

Develop Technology User Requirements

The integration of Counter-UAS technology into the existing physical security infrastructure of the Port of Brownsville should be a carefully crafted strategy that includes legally authorized and logical equipment solutions.

Traditionally, some companies in the security industry will often tell critical infrastructure or public safety entities, what is needed. In fact, it should be just the opposite. The Port of Brownsville Police Department, should work with experienced professionals to understand the Counter-UAS landscape, and develop user requirements for drone detection equipment based on their department's unique needs, then find and test system that meet their pre-determined criteria.

Information-Sharing and Threat Warning and Analysis

Developing an information sharing and analysis program for drone threats at the Port of Brownsville and beyond can help establish appreciation of threat potentials and trends. It can also help build a baseline of current threats and intrusions that can inform threat assessment and incident response. Such an effort can start internally, sharing information among the POB and its tenant and public safety partners. The effort could be then expanded to link Texas Ports, then US Gulf Ports, nationally, and then internationally. This effort could be linked to the Texas Fusion Center and its Infrastructure Liaison Officer (ILO) Program.[63] Broader efforts throughout Texas Ports, at Gulf Ports, nationally, and internationally could also become valuable.[64]

Recommended Courses of Action

The drone assessment team recommends the following courses of action for the Port of Brownsville. It is recommended that the Port of Brownsville develop and implement a comprehensive counter-drone framework. This framework should prioritize measures to mitigate and counter threats from Unmanned/uncrewed Aerial Systems—especially small UAS (sUAS) platforms. That is the first step is developing and implementing a Counter-UAS (C-UAS) Program. Next measures to address emerging drone threats, such as uncrewed ground vehicles (UGVs) and uncrewed maritime vessels (UMVs) can be tackled.

C-UAS/C-UMV Efforts

Training. Counter-UAS efforts should start with building awareness of the UAS threat to the port through awareness training. The POB and POB Police should sponsor a basic *UAS awareness training* session for port personnel, including all port police and security officers, pilots port tenants (especially their security managers), and cooperating public safety agencies (law enforcement and fire) that operate at or proximate to the port. This training could include a one-day orientation for all participants and potentially a two-day specialist course for public safety personnel (including POB Police, Cameron County Sheriff's, Constables, Texas Department of Public Safety (DPS), Brownsville Fire, and Texas Parks and Wildlife Game Wardens. US Coast Guard, Border Patrol, and Customs and Border Protection officials should be invited as observers.

Policies and Procedures. The Port of Brownsville should develop a comprehensive set of policies and procedures defining the POB posture on UAS. This policy and procedures should include SOPs for day-to-day operations and EOPs for emergencies involving UAS incursions resulting in injury, death, or property damage. These documents should set the basic framework of the port's efforts, mandate training for port personnel, and define the need for on-going assessment of the UAS threat in specific and related drone threat in the future. Cooperative arrangements, such as mutual aid for UAS response, joint training, and joint operations should be specified. In addition information sharing, alerts and warning for drone threats should be articulated.

Geospatial Information Systems (GIS) and Geospatial Intelligence (GeoINT). The POB should consider development of a comprehensive geospatial analysis capability including development of GIS tools and data sets for use in routine and emergency purposes (including crisis and disaster management). These tools can be integrated into command and control/dispatch systems and linked with airspace awareness tools to guide response.

C-UAS/C-UMV Drone Detection. The POB should consider implementing systems and applications, such a drone sensor platform, to detect and track UAS incursions into the port's operational area that may interfere with port operations. The POB should commission a *sensor engineering study* to assess the best option for C-UAS detection, including the potential of multiple systems to maximize detection. An engineering study to asses similar drone detection capabilities for UMVs in the ship channel and approaches should also be considered. Optimally, the command and control/sensor display system should be able to display all modes of drone incursion and then integrate that data into a comprehensive geospatial display (using a common GIS platform). The resulting sensor network could be designed to build a basic (foundational) system operated by the POB that can be expanded to integrate addition tenant-specific feeds or surge detection capability during designated maritime security (MARSEC) levels, specifically MARSEC Level 2 or 3.[65]

Drone (UAS) Response Capacity. The POB Police should consider developing a long-range drone response capability (Drones for Good) where sUAS can be used by Port Police to evaluate and assess the threat of drone incursions over Port of Brownsville airspace, as well as monitor and prepare response for critical incidents and emergencies. This capacity could be

an organic port-specific program or a cooperative venture with adjacent law enforcement agencies such as the Cameron County Sheriff and the City of Brownsville Police.

Drone Threat Information-Sharing. The Port of Brownsville Police should consider developing or collaborating in the development of a port threat information and analysis/warning system for drone threats (specifically UAS and UMV) threats to ports. This initiative could start at the POB and share information with port tenants and plots servicing the port. It could then be expanded to include all Texas Ports, US Gulf Ports, Nationally, and then Internationally.

Advocacy and Development of Counter Drone (C-UAS/C-UMV) Legislation and Ordinances. The Port of Brownsville, through the Brownsville Navigation District Board of Commissioners should advocate for the development of enhanced Texas State laws and County Ordinances to enhance the level of legislation necessary to protect the port and provide effective enforcement options for the Port Police and cooperating law enforcement agencies in Cameron County. This effort could build on the prohibitions on unmanned aircraft at the Port of Corpus Christi Authority (Item 614(I) 12-25-15) pursuant to Texas Government Code, Section 423.0045 et. seq. described in note 1 of this report. This should focus on clarifying the vagueness in the statute's definitions. This effort could be conducted in concert with the Texas Ports Association.[66]

Building this level of response will take time and an investment in financial and human resources. Optimally, the POB will start developing policy and procedures and then the training needed to sustain effective C-UAS and C-UMV capabilities. This will require further analysis and engineering studies for full implementation.

Author Biographies

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.

Tom Adams is CEO of AeroVigilance and Co-Founder of C-UAS Hub. Tom retired from the Federal Bureau of Investigation (FBI) after 20 years of service in October 2022. He spent the early part of his federal law enforcement career investigating white-collar crime matters in Florida and Texas. In 2008, Tom completed the FBI's Hazardous Devices School and became a Special Agent Bomb Technician (SABT), a role in which he served for over 11 years. During his time as a SABT, he deployed to Africa, the Middle East, Europe, and Southern Asia in support of US counter-terrorism efforts. Tom's last three years in the FBI were spent as a Supervisory Special Agent in the Counter-UAS Program. In this role, he led the evolution of the team, including developing a training program, policies and procedures, and operational standards. Tom has a bachelor's degree from Montana State University in Biomechanics, and a master's degree from Embry-Riddle Aeronautical University in Unmanned Systems. Prior to serving in the FBI, Tom was a Medical Service Corps Officer in the US Army. Tom currently serves as the Co-Chair of the Operating

Requirements Working Group of the FAA UAS Detection and Mitigation Aviation Rulemaking Committee.

Senior Reviewer Biography

Dr. Richard Rotanz has over 50 years of experience in the fire service, emergency management, research and academia. His eclectic career has had him functioned as program manager in New York City's Department of Health and Mental Hygiene; co-developed and perform as the Executive Director of the Applied Science Foundation for Homeland Security; co-developed Adelphi University's graduate degree in Emergency Management; created and performed as the first Commissioner for the Office of Emergency Management of Nassau County, New York. He also served in the New York City Fire Department, working through the ranks and special divisions such as the Safety Command and with Special Operations Command. After such assignments he was detailed by the mayor's office as Deputy Commissioner of New York City's Office of Emergency Management, located in World Trade Center 7. In this detail, he was responsible for research & planning, and to organize and manage the emergency operations center during major events. During the September 11th attacks upon New York City, he re-instituted and relocated the destroyed emergency operation center to Pier 92 and managed the multi-organization response of over 120 agencies, organizations, and businesses, to the 9-11 tragedy.

Acknowledgements

The research/assessment team led Dr. John P. Sullivan and Mr. George Davis was assisted by Mr. Tom Adams who provided technical advice and subject matter expertise. Mr. Adams also participated in the team's site visit to the Port of Brownsville and reviewed and contributed to the report. In addition, Dr. Richard Rotanz provided senior technical advice and senior review for the report. The team would also like to acknowledge the support of Chief William Dietrich, Lieutenant Julio Romo, and Sergeant Edgar Garcia of the Port of Brownsville Police Department, as well as the port officials, tenants, and public safety partners that participated in our focus group sessions. The team also acknowledges the support of Aerial Armor, a Dedrone Company (Drone Detection Systems), especially Josh Strange and Travis Scott, for sharing and assisting in the interpretation of their drone sensor data. Finally, we would like to thank Mr. Grant Threatt and Mr. Heberto Villareal of the Sam Houston State University, Institute of Homeland Security for their support throughout the project.

Endnotes

[1] A Security Vulnerability Assessment (SVA) of the Port of Brownsville was recently performed for the Institute of Homeland Security at Sam Houston State University. That Report identified concerns about aerial drones (UAS) and recommended the following: "**Recommendation: Commission UAV Assessment:** Several tenants raised concerns about drones flying in and around the port. At the time of this assessment, there was no clear consensus on whether the drones were being operated by ship enthusiasts capturing photos of a decommissioned aircraft carrier, nature lovers, or more nefarious groups. The pending UAV assessment and drone mitigation plan will address the concerns expressed and should consider implementing policies prohibiting drones similar to what other ports in Texas have enacted." See "Security Vulnerability Assessment: Port of Brownsville, May 2023" (Huntsville: Sam Houston State University, Institute of Homeland Security, May 2023), at page 25. That recommendation referred to prohibitions unmanned aircraft at the Port of Corpus Christi Authority (Item 614(I) 12-25-15 pursuant to Texas Government Code, Section 423.0045 et. seq. See https://portofcc.com/wp-content/uploads/TARIFF_ITEM_614.pdf and https://texas.public.law/statutes/tex._gov%27t_code_title_4_subtitle_b_chapter_423. In addition, see Note 90 of this report for a discussion of the issues of that led to major portions of the current legislation to be struck down.

[2] Examples of aerial, or Uncrewed Aerial Systems (UAS), risks include threats to public venues such as stadia (stadiums). For an overview of that risk and associated responses issues (many of which are also applicable in other settings, see the series referenced in the series of papers: *Detecting Drone threats at Stadiums*, https://ihsonline.org/Research/Technical-Papers/Detecting-Drone-Threats-at-Stadiums: Nathan P. Jones, John P. Sullivan, and George W. Davis, "Detecting Drone (Unmanned or Uncrewed Aerial System) Threats to Stadiums (Stadia) and Public Venues: Framing the Issue: (Report No. IHS/CR-2022-2023). The Sam Houston State University Institute for Homeland Security. August 2022; John P., Sullivan, Nathan P. Jones, and George W. Davis, "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. August 2022; George W. Davis, John P. Sullivan, and Nathan P. Jones, "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. August 2022. Unmanned aerial vehicle (UAV) threats against nuclear facilities are also a concern, see Jae San Kim, "A Study on the Possibility of Unmanned Aerial Vehicles (UAV)' Threat in Nuclear Facilities," *Transactions of the Korean Nuclear Society Autumn Meeting Goyang, Korea,* 24-25 October 2019, https://www.kns.org/files/pre_paper/42/19A-202-김재산.pdf. Electric power distribution is also at risk, see Kevin Killough, "Drones A Very Real Threat To Power Substations And Other Critical Infrastructure," Cowboy State Daily, 8 February 2023, https://cowboystatedaily.com/2023/02/08/drones-a-very-real-threat-to-power-substations-and-other-critical-infrastructure/.

[3] See Alan Taylor, "Photos: Ukraine's Battlefield Drones," *The Atlantic*, 24 May 2023, https://www.theatlantic.com/photo/2023/05/photos-ukraine-war-drones/674160/; "How Ukrainians modify civilian drones for military use," *The Economist*, 8 May 2023, https://www.economist.com/science-and-technology/2023/05/08/how-ukrainians-modify-civilian-drones-for-military-use: John Amble, "MWI Podcast: Who Innovates Wins? Drones and Adaptation in the Ukraine War," *Modern War Institute*, 15 January 2023, https://mwi.westpoint.edu/mwi-podcast-who-innovates-wins-drones-and-adaptation-in-the-ukraine-war/.

[4] Benjamin Fogel and Andro Mathewson, "Will the Drone War Come Home? Ukraine and the Weaponization of Commercial Drones, *Modern War Institute*, 22 August 2022, https://mwi.westpoint.edu/will-the-drone-war-come-home-ukraine-and-the-weaponization-of-commercial-drones/.

[5] Elias Yousif, "Drone Warfare in Ukraine: Understanding the Landscape," *Stimson*, 30 June 2022, https://www.stimson.org/2022/drone-warfare-in-ukraine-understanding-the-landscape/; The Explosive payload figure is attributed to Eric Schmidt, "The Future of War Has Come in Ukraine: Drone Swarms," *Wall Street Journal*, 7 July 2023, https://www.wsj.com/articles/the-future-of-war-has-come-in-ukraine-drone-swarms-kamikaze-kyiv-31dd19d7.

[6] Remotely piloted car bombs (vehicle borne improvised explosive devices or VBIEDs) have been technically feasible for years and some violent non-state groups have been manufacturing them for years. Yet, despite this remote control capability, these RC-VBIEDs have not been widely used. See Hugo Kaaman, "The Myth of the Remote-Controlled Car Bomb," Report n.15, European Eye on Radicalization, September 2019, https://eeradicalization.com/wp-content/uploads/2019/09/Hugo-Report-Remote-VBIEDs-Final.pdf. Battlefield use in Ukraine, coupled with the potential rise in autonomous vehicles (both cars and trucks), may change the equation in the future. See Max Hunder, "Ground vehicles are the new frontier in Ukraine's drone war," *Reuters*, 13 July 2023, https://www.reuters.com/world/europe/ground-vehicles-are-new-frontier-ukraines-drone-war-2023-07-13/; John P. Sullivan, "Robotics in Urban Conflict and Megacities," in *Batmobiles in Gotham City: Unmanned Ground Vehicles & Manoeuvre in the Future Urban Environment*, Hannah Croft, Ed., *Defence iQ*, 15 November 2019, https://www.academia.edu/40940306/Robotics_in_Urban_Conflict_and_Megacities

[7] Marcel Plichta, "Beyond Reapers and DJI Mavics: Are Scholars and Policymakers Ready for One-Way Attack Drones?" *Irregular Warfare Initiative*, 6 April 2023, https://irregularwarfare.org/articles/beyond-reapers-and-dji-mavics-are-scholars-and-policymakers-ready-for-one-way-attack-drones/.

[8] Eric Schmidt, "The Future of War Has Come in Ukraine: Drone Swarms," *Wall Street Journal*, 7 July 2023, https://www.wsj.com/articles/the-future-of-war-has-come-in-ukraine-drone-swarms-kamikaze-kyiv-31dd19d7.

[9] Robert J. Bunker and John P. Sullivan," Mexican cartels are embracing Aerial Drones and They're Spreading, " *War on the Rocks*, 11 November 2021, https://warontherocks.com/2021/11/mexican-cartels-are-embracing-aerial-drones-and-theyre-spreading/.

[10] For a detailed survey, see Robert J. Bunker and John P. Sullivan, Eds. *Criminal Drone Evolution: Cartel Weaponization of Aerial IEDs*, Bloomington: Xlibris, October 2021.

[11] John P. Sullivan and Robert J. Bunker, "Mexican Cartel Strategic Note No. 18: Narcodrones on the Border and Beyond," *Small Wars Journal*, 28 March 2016, https://smallwarsjournal.com/jrnl/art/mexican-cartel-strategic-note-no-18-narcodrones-border-and-beyond; Aaron R. Schmershal, "Fifty Feet Above the Wall: Cartel Drones in The U.S.–Mexico Border Zone Airspace, And What To Do About Them," Unpublished Master's Thesis. Monterey: Naval Post Graduate School, March 2018, https://apps.dtic.mil/sti/citations/AD1052881.

[12] Alyssa Sims, ""The Rising Drone Threat from Terrorists." *Georgetown Journal of International Affair*s. Vol. 19 , 2018: pp. 97–107, http://www.jstor.org/stable/26567532; Thomas G. Pledger, "The Role of Drones in Future Terrorist Attacks," *Land Warfare Paper* No. 137, Association of the United States Army, February 2021, https://www.ausa.org/sites/default/files/publications/LWP-137-The-Role-of-Drones-in-Future-Terrorist-Attacks_0.pdf.

[13] "Drone technology: security threats and benefits for police focus of INTERPOL forum," *INTERPOL*, 1 January 2018, https://www.interpol.int/ar/1/1/2018/Drone-technology-security-threats-and-benefits-for-police-focus-of-INTERPOL-forum#:~:text=Recent%20examples%20include%20terrorist%20groups,and%20crash%20into%20a%20building.

[14] An armed drone was used to threaten Baja Public safety secretary, Gerardo Sosa Olachea, at his residence on Tecate in July 2018. See John P. Sullivan, Robert J. Bunker and David A. Kuhn, "Mexican

Cartel Tactical Note #38: Armed Drone Targets the Baja California Public Safety Secretary's Residence in Tecate, Mexico," *Small Wars Journal*, 6 August 2023, https://smallwarsjournal.com/jrnl/art/mexican-cartel-tactical-note-38-armed-drone-targets-baja-california-public-safety.

[15] Two explosive-laden drones were detonated above Maduro while he made a speech. See Joe Parkin Daniels and Mariana Zúñiga, "Venezuela's Nicolás Maduro survives apparent assassination attempt," *The Guardian*, 4 August 2018, https://www.theguardian.com/world/2018/aug/04/nicolas-maduros-speech-cut-short-while-soldiers-scatter.

[16] Robert J. Bunker, *Terrorist and Insurgent Unmanned Aerial Vehicles: Use, Potentials, and Military Implications,* Carlisle Barracks; Strategic Studies Institute, US Army War College, August 2015, https://scholarship.claremont.edu/cgi/viewcontent.cgi?article=1050&context=cgu_facbooks.

[17] Robert J. Bunker, "Weaponized Aerial Drones and the Homeland: Increasing Domestic Terrorism Concerns," *Homeland Security Today*, 29 December 2022, https://www.hstoday.us/featured/weaponized-aerial-drones-and-the-homeland-increasing-domestic-terrorism-concerns/.

[18] Bradley Wilson, Shane Tierney, Brendan Toland, Rachel M. Burns, Colby Peyton Steiner, Christopher Scott Adams, Michael Nixon, Raza Khan, Michelle D. Ziegler, Jan Osburg, Ike Chang, *Small Unmanned Aerial System Adversary Capabilities,* Homeland Security Operational Analysis Center, Santa Monica; RAND, 2020, p. xii, https://www.rand.org/pubs/research_reports/RR3023.html.

[19] These attacks targeted the M/T *Pacific Zircon*, which was struck by a Shahad-136 drone causing damage to its outer hull on 15 November 2022, according to a US Navy analysis, "U.S. Navy Analysis Confirms Iranian Link to Drone Attack," U*.S. Central Command News*, 22 November 2022, https://www.centcom.mil/MEDIA/NEWS-ARTICLES/News-Article-View/Article/3225713/us-navy-analysis-confirms-iranian-link-to-drone-attack/ and the VLCC *Pratika* on 18 November 2022. The *Pratika* was moving crude oil between the Ports of Al Ruwais (UAE) and Ash Shihr (Yeman), see "Drone strikes: new challenges for maritime security," *MariTrace*, 13 December 2022, https://www.ww3.maritrace.com/post/drone-strikes-new-challenges-for-maritime-security.

[20] Ibid.

[21] Ben Hubbard, Palko Karasz, and Stanley Reed, "Two Major Saudi Oil Installations Hit by Drone Strike, and U.S. Blames Iran," *New York Times*, 14 September 2019, https://www.nytimes.com/2019/09/14/world/middleeast/saudi-arabia-refineries-drone-attack.html.

[22] This was not the first attack on Yemeni port infrastructure. See, Saeed Al-Batati, "Houthis launch fresh drone attack on Yemeni port," *Arab News*, 9 November 2022, https://www.arabnews.com/node/2196786/middle-east.

[23] Mikhail Zelenkov, Yuliya Laamarti, Marina Charaeva, Tatyana Rogova, Olga Novoselova, Aehlita Mongush, "Maritime terrorism as a threat to confidence in water transport and logistics systems," *Transportation Research Procedia*, Vol. 63, 2022, pp. 2259-2267, https://doi.org/10.1016/j.trpro.2022.06.256.

[24] Deputy Commandant for Operations, "Unmanned Systems Strategic Plan," Washington, DC: United States Coast Guard, March 2023, https://www.dco.uscg.mil/Portals/9/DCO%20Documents/2023%20Unmanned%20Systems%20Strategic%20Plan.pdf?ver=5EALzxVMXI1TAe_FVn_zvQ%3d%3d.

[25] USCG Unmanned Systems Cross-Functional Team Lead, Captain Thom Remmers in Bridget Johnson, "New Strategy Details Coast Guard Plans to Use Unmanned Systems to Protect Maritime Borders, Enhance Missions," *Homeland Security Today*, 17 May 2023, https://www.hstoday.us/featured/new-strategy-details-coast-guard-plans-to-use-unmanned-systems-to-protect-maritime-borders-enhance-missions/.

[26] Jasper Campbell and James Martin, "The War on Drugs on Autopilot," *Proceedings*, U.S. Naval Institute, Vol. 147/1/1,415, January 2021, https://www.usni.org/magazines/proceedings/2021/january/war-drugs-autopilot.

[27] 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, 27 July 2022,* https://www.cofutures.net/post/narco-drone-submarines-seized-and-workshop-raided-in-14-month-long-operation-kraken.

[28] Harry Guiness, "Watch a 'flying fish' drone hover in the air and then swim underwater," *Popular Science*, 8 June 2023, https://www.popsci.com/technology/amphibious-quadcopter-drone/; Holly Chik, "Could this flying, diving drone one day help with ocean rescues? Its Hong Kong and mainland China developers say it's possible," *South China Morning Post*, 20 May 2023, https://www.scmp.com/news/china/science/article/3220967/could-flying-diving-drone-one-day-help-ocean-rescues-its-hong-kong-and-mainland-china-developers-say.

[29] Zachary Kallenborn, "Drone Swarms and Amphibious Operation," *Small Wars Journal*, 30 May 2023, https://smallwarsjournal.com/jrnl/art/drone-swarms-and-amphibious-operations; Jarred Samuelson, "Sea Control 445 – Drone Swarms in Amphibious Operations with Zachary Kallenborn," *CIMSEC* (Center for International Maritime Security), 16 July 2023, https://cimsec.org/sea-control-445-drone-swarms-in-amphibious-operations-with-zachary-kallenborn/; "Zachary Kallenborn, Gary Ackerman, and Philipp C. Bleek, "Swarming Terror," *Small Wars Journal*, 30 June 2022, https://smallwarsjournal.com/jrnl/art/swarming-terror; Zachary Kallenborn, "InfoSwarms: Drone Swarms and Information Warfare," *Parameters*, Vol. 52, no. 2, 202, pp. 87-102, https://press.armywarcollege.edu/parameters/vol52/iss2/13/.

[30] David Hambling, "A fleet of drones can be controlled by one person with a smartphone," *New Scientist*, 30 September 2020, https://www.newscientist.com/article/2255997-a-fleet-of-drones-can-be-controlled-by-one-person-with-a-smartphone/; Bruce Crumley, "New Raytheon tech lets a single operator control 130 drones," *Drone DJ*, 13 January 2022, https://dronedj.com/2022/01/13/new-raytheon-tech-lets-a-single-operator-control-130-drones/.

[31] "Brownsville Police Unmanned Aircraft System," Brownsville Police Department, https://www.brownsvillepd.com/bpd-uas; Brownsville Fire Department also uses drones; see 'Fire department finding multiple practical uses for drones," *my RGV*, 17 October 2017, https://myrgv.com/uncategorized/2017/10/17/fire-department-finding-multiple-practical-uses-for-drones/. Also see, Maria Valdovinos Olson, James Specht, and Jennifer Zeunik, *Law enforcement & unmanned aircraft systems (UAS): Guidelines to enhance community trust*. Washington, DC: Office of Community Oriented Policing Services and National Policing Institute, 2016, https://www.policinginstitute.org/publication/community-policing-unmanned-aircraft-systems-uas-guidelines-to-enhance-community-trust/; Scott Ladd, "Port Authority's Drone Program Takes Off," Port *Authority NY NJ*, 31 October 2022, https://www.panynj.gov/port-authority/en/blogs/security/port-authority-s-drone-program-takes-off.html; Patrick Sisson, "Welcome to Chula Vista, where police drones respond to 911 calls," MIT Technology Review, 27 February 2023, https://www.technologyreview.com/2023/02/27/1069141/welcome-to-chula-vista-where-police-drones-respond-to-911-calls/.

[32] Comments of Gloria Chavez, Chief of RGV Sector, US Border patrol in Steve Taylor, "Video: Chavez: Border Patrol has a problem with drones in the RGV," Rio Grande Quarterly, 12 February 2023, https://riograndeguardian.com/video-chavez-border-patrol-has-a-problem-with-drones-in-the-rgv/.

[33] This drone sensor data was provided to the drone threat assessment team for assessing the drone threat potentials to the Port of Brownsville (POB). The data was collected by Aerial Armor a Dedrone Company as part of a pilot project looking at the POB. This data was used with the permission of Aerial

Armor, a Dedrone Company. This data set is the basis of all POB-specific UAS sensor data in this report. "405 Day Drone Activity Report, 06/01/22 to 07/11/23," Aerial Armor, a Dedrone Company, 2023.

[34] Additional analysis is required to establish the specific cause of the difference (likely slightly different detection/reporting windows), but since the variance does not alter the overall assessment was it was not performed.

[35] the DJI website provides specific details of each of their drone product lines: https://www.dji.com.

[36] An excellent primer in future drone warfare in the maritime setting is found in P.W. Singer and August Cole, *Ghost Fleet: A Novel of the Next World War*, New York: William Morrow, 2016.

[37] "Critical Infrastructure Sectors," *Cybersecurity & Infrastructure Security Agency*," https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors.

[38] "Transportation Systems Sector," *Cybersecurity & Infrastructure Security Agency*," https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/transportation-systems-sector.

[39] "What is Counter-UAS?" *C-UAS Hub*, 2 February 2023, https://cuashub.com/content/what-is-counter-uas/.

[40] See [40] "New Counter-UAS Legislation Text," *C-UAS Hub*, 27 May 2023, https://cuashub.com/content/new-counter-uas-legislation-introduced/.

[41] "Title 10 U.S. Code Section 130i- Department of Defense," *Cr-UAS Hub*, 29 October 2022, https://cuashub.com/content/title-10-us-code-section-130i/.

[42] "USMC Installation Counter-UAS RFI Updated Response Date," *C-UAS Hub*, 15 January 2023, https://cuashub.com/content/usmc-installation-counter-uas-rfi-updated-response-date/.

[43] "NNSA 'No Drone Zones,'" *C-UAS Hub*, 24 November 2022, https://cuashub.com/content/nnsa-no-drone-zones/.

[44] Op. cit., "New Counter-UAS Legislation Text" at note 40.

[45] Ibid.

[46] Ibid.

[47] Ibid.

[48] Ibid.

[49] "Advisory on the Application of Federal Laws to the Acquisition and Use of Technology to Detect and Mitigate Unmanned Aircraft Systems," *C-UAS Hub*, 30 October 2022, https://cuashub.com/content/advisory-application-federal-laws/.

[50] Ibid.

[51] Ibid.

[52] Ibid.

[53] Op. Cit., "New Counter-UAS Legislation Text" at note 40.

[54] "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/.

[55] Op. Cit., "New Counter-UAS Legislation Text" at note 40.

[56] Ibid.

[57] Texas drone laws are codified at Chapter 423 (use of Unmanned Aircraft) of the Texas Government Code. See Chapter 423: Use of Unmanned Aircraft, *Texas.Public.Law*, https://texas.public.law/statutes/tex._gov%27t_code_title_4_subtitle_b_chapter_423.

[58] AUVSI Advocacy, "2023 End Of State Sessions Report: Texas," *AUVSI: Assuring Autonomy Blog*. 1 June 2023, https://www.auvsi.org/industry-news/blog/2023-end-state-sessions-report-texas.

[59] The United States District Court for the Western District of Texas struck down the majority of the Texas drone statute at Chapter 423. In his ruling on 28 March 2022, Judge Pitman found that parts of the statute violated the First Amendment with some of the language contained in the statue as vague and not sufficiently defined. As a consequence, Sections 423.002, .003, .004, .005 .0045, and .0046 are now stricken and inapplicable. The ruling could be appealed to the United States Court of Appeals for the Fifth Circuit or the Texas Legislature could pursue an amended version of the statute to remediate the issues identified in the current statute. See Tiffany Lashmet (tiffany.dowell), "Federal Court Strikes Down Texas Drone Law," *Texas Agricultural Law Blog*, 11 April 2022, https://agrilife.org/texasaglaw/2022/04/11/federal-court-strikes-down-texas-drone-law/ and *National Press Photographers Association, Texas Press Association, and Joseph Pappalardo v. Steven McCraw, Dwight Mathis, and Wes Mau*, United States District Court for the Western District of Texas, Case 1:19-CV-946-RP, 28 March 2022, https://agrilife.org/texasaglaw/files/2022/04/Order-here.pdf.

[60] See 'Counter-UAS Technology Guide," *C-UAS Hub*, 19 October 2022, https://cuashub.com/content/counter-uas-technology-guide/. The technologies described here are derived from the "Counter-Unmanned Aircraft Systems: Technology Guide," New York: National Urban Security Technology Laboratory (NUSTL), Department of Homeland Security, Science and Technology Directorate, (CUAS-T-G-1), September 2019, https://cuashub.com/wp-content/uploads/2022/10/c-uas-tech-guide_final_28feb2020.pdf.

[61] "Remote Identification: A Primer for Security Professionals," *C-UAS Hub*, 5 may 2023, https://cuashub.com/content/remote-identification-a-primer-for-security-professionals/.

[62] Ibid.

[63] See Texas Fusion Center," *Texas Department of Public Safety*, https://www.dps.texas.gov/section/intelligence-counterterrorism/texas-fusion-center; and "Infrastructure Liaison Officer (ILO) Program," *Texas Department of Public Safety*, https://www.dps.texas.gov/section/intelligence-counterterrorism/infrastructure-liaison-officer-ilo-program.

[64] The Port Police and their partners may benefit from reviewing this following historical reference on building threat information-sharing networks: 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: Transportation Research Board, national Research Council, National Academy Press, 2022, https://nap.nationalacademies.org/catalog/24722/communication-of-threats-a-guide. Also see, Deon Canyon, Wade Turvold, and Jim McMullin. "A Network of Maritime Fusion Centers throughout the Indo-Pacific," *Daniel K. Inouye Asia-Pacific Center for Security Studies*, February 2021, https://dkiapcss.edu/nexus_articles/a-network-of-maritime-fusion-centers-throughout-the-indo-pacific/; and Hal Kempfer and John P. Sullivan, "Connecting Partnerships for fhe Co-Production Of Full-Spectrum

Threat Intelligence," Naval Intelligence Week at CIMSEC (Center for International Maritime Security), 2 April 2021, https://cimsec.org/connecting-partnerships-for-the-co-production-of-full-spectrum-threat-intelligence/.

[65] MARSEC levels are set by the Secretary of Homeland Security or the Commandant of the Coast Guard. MARSEC Level 1 is the level of minimum appropriate security measures that shall be maintained at all times. MARSEC Level 2 is the level of appropriate additional protective security measures that shall be maintained for a specified period of time as a result of heightened risk of a transportation security incident. MARSEC Level 3 is the level for which further specific protective security measures shall be maintained for a specific limited period of time when a transportation security incident is probable, imminent, or has occurred, although it may not be possible to identify the specific target.

[66] The Texas Ports Association represents the ports of Bay City, Beaumont, Brownsville, Calhoun Port Authority, Corpus Christi, Freeport, Galveston, Harlingen, Houston, Orange, Palacios, Port Author, Port Isabel, Port Mansfield, Sabine Neches, Texas City, and Victoria. Collectively, these port handle 66.2 million tons of foreign and domestic cargo and are ranked second among the US states in waterborne commerce. See *Texas Ports Association*, https://www.texasports.org. The ports in Cameron County are the Port of Brownsville, Port of Harlingen Authority, and Port Isabel-San Benito Navigation District. The SpaceX South Texas Launch Site (Starbase) is an FAA approved private spaceport east of Brownsville. All of these entities share an interest in effective C-UAS/C0UMV ordinances.

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, J. P., Davis, G. W., & Adams, T. (2023). Drones and Port Security at the Port of Brownsville. Sam Houston State Institute for Homeland Security, (Report No. IHS/CR-2023-1001).