Drones and the Future of Security Policy: A Maritime Case Study for Assessing the Risk of Small Unmanned Aircraft Systems

John J. Caton, The Cadmus Group

Given the recent proliferation of affordable and user-friendly small unmanned aircraft systems (sUASs, or "drones") in the commercial marketplace, security professionals around the globe are grappling with how to safely, efficiently, and legally protect critical infrastructure sites from misuse of this emerging technology. While much attention has been afforded to the dangers drones pose to aircraft, most public research has overlooked sensitive facilities such as nuclear power plants, electrical power stations, and major ground transportation hubs. Given the recent use of weaponized sUASs in Syria and Iraq, it is imperative that both military and civilian security professionals have the tools necessary to combat this developing threat. To better illustrate the risks associated with commercially available drones and the danger they pose to infrastructure security, this article uses a major port in the United States (given the pseudonym Port of Opal City to protect existing security policies and procedures) as the case study for a comprehensive severity, probability, and exposure (SPE) risk analysis.

RESEARCH HAS OVER-LOOKED THE DANGERS DRONES POSE TO SENSITIVE FACILITIES.

Under current US law, an aircraft is defined as "any contrivance invented, used, or designed to navigate, or fly in, the air."[1] Building on this definition, an unmanned aircraft (UA) is legally defined as "any aircraft that is operated without the possibility of direct human intervention from within or on the aircraft," while an unmanned aircraft system (UAS) is both a UA and its "associated elements, including communication links and the components that control the unmanned aircraft, that are required for the pilot in command to operate safely and efficiently in the national airspace system."[2] It is important to note that the focus of this article is on small UAs that weigh less than 55 pounds.[3] While there is no globally recognized regulatory definition for the term *drone*, this popular term is commonly used to mean an sUAS, and this article uses both words interchangeably. Although this article uses a US port and the US legal environment for its analysis, its general methodology and findings are widely applicable to similar facilities in other countries. The article's recommendations can likewise be modified to fit other social and legal situations.

Commercially Available Rotary Wing SUASs

Tables 1 through 6 list the current top 10 commercially available rotary wing drones by the following criteria (all prices are in US dollars): (1) lowest cost, (2) highest cost, (3) longest flight time (in minutes), (4) longest operating range (in feet), (5) largest payload capacity (in pounds), and (6) maximum flying speed (in miles per hour).[4] Rotary-wing sUASs exclusively marketed for military use are not included in this list. The Ehang 184, while marketed as a drone, is also not included in this list because it can potentially carry an operator inside the aircraft itself while airborne.[5] Fixed-wing drones are not included in this analysis because of US buyers' strong preference for rotary-wing drones.[6] The purpose of this list is to provide the reader with a sense of the capabilities of commercially available drones. These lists are accurate as of June 2016 and are liable to change.

LOWEST COST

Rank	Name	Company	Number of Rotors	Cost (USD)	Flight Time (Minutes)	Weight (lbs.)	Payload Capacity (lbs.)	Maximum Altitude (ft.)	Maximum Operating Range (ft.)	Maximum Speed (mph)
1	H101	Floureon	4	$15.00	7	0.7	N/A	Unknown	65	Unknown
2	V911S	Wltoys	4	$15.00	6	0.02	N/A	Unknown	98	Unknown
3	FX-10 Mini	Floureon	4	$15.00	6	0.02	N/A	Unknown	82	Unknown
4	W609	HJ	6	$15.00	5	0.03	N/A	Unknown	164	Unknown
5	X165	XinLin	4	$16.00	5	0.03	N/A	Unknown	72	Unknown
6	L6058	Lishtoys	4	$17.00	8	0.01	N/A	Unknown	98	Unknown
7	X165	XinLin	4	$18.00	5	0.03	N/A	Unknown	72	Unknown
8	H8 Mini	JJRC	4	$20.00	5	0.4	N/A	Unknown	492	Unknown
9	Rc Mini	Udi	4	$20.00	5	0.02	N/A	Unknown	98	Unknown
10	H22	JJRC	4	$20.00	7	0.6	N/A	Unknown	98	Unknown

HIGHEST COST

Rank	Name	Company	Number of Rotors	Cost (USD)	Flight Time (Minutes)	Weight (lbs.)	Payload Capacity (lbs.)	Maximum Altitude (ft.)	Maximum Operating Range (ft.)	Maximum Speed (mph)
1	Titan	XactSense	8	$120,000	30	18	50	180	52,805	Unknown
2	MAX 8	XactSense	8	$65,000	25	5	20	397	Unknown	Unknown
3	F100	AEE	4	$58,000	70	13.2	5.51	4,921	32,808	61
4	cyberQuad	Sci.Aero	4	$37,000	25	3.7	1.76	Unknown	1,640	37
5	F50	AEE	4	$37,000	40	4.4	Unknown	2,953	65,617	11
6	G4 Eagle V2 Cargo	Service-Drone	8	$35,360	30	5.5	5.51	Unknown	6,561	37
7	Multirotor Eagle V2 + FREEFLY MoVI M5	Service-Drone	8	$33,940	10	9.9	4.41	Unknown	3,281	36
8	MULTIROTOR G4 Eagle V2	Service-Drone	8	$28,260	30	5.5	5.51	Unknown	6,562	37
9	MULTIROTOR G4 Surveying Robot	Service-Drone	6	$25,420	20	6	5.07	Unknown	9,843	18
10	Martin Indago	Lockheed	4	$25,000	45	4.9	0.44	498	6,562	45

LONGEST FLIGHT TIME (Minutes)

Rank	Name	Company	Number of Rotors	Cost (USD)	Flight Time (Minutes)	Weight (lbs.)	Payload Capacity (lbs.)	Maximum Altitude (ft.)	Maximum Operating Range (ft.)	Maximum Speed (mph)
1	Pocketflyer	CyPhy Works Inc.	6	Unknown	120	0.20	N/A	Unknown	76	Unknown
2	MD4-1000	Microdrones	4	$2,000	88	5.80	2.65	3,281	1,640	27
3	F100	AEE	4	$58,000	70	13.20	5.51	4,921	32,808	61
4	EF 44 "Atlas"	Allied Drones	4	$15,000	60	Unknown	4.41	Unknown	Unknown	Unknown
5	QR X800	Walkera	4	$2,700	60	8.60	Unknown	Unknown	6,562	Unknown
6	Fotokite Pro	Fotokite	4	$10,000	60	1.30	Unknown	Unknown	65	Unknown
7	Vader X4	SteadiDrone	4	$19,995	50	8.40	9.48	13,123	4,921	44.7
8	Altura Zenith ATX8	Aerialtronics	8	$2,000	45	7.70	6.39	Unknown	3,281	44.7
9	HX3	Yuneec Flying Eyes	6	$3,000	45	3.10	4.4	Unknown	6,562	33
10	HL48 "Chaos"	Allied Drones	8	$20,000	45	15.00	15	Unknown	65,617	30

LONGEST OPERATING DISTANCE (Feet [ft.])

Rank	Name	Company	Number of Rotors	Cost (USD)	Flight Time (Minutes)	Weight (lbs.)	Payload Capacity (lbs.)	Maximum Altitude (ft.)	Maximum Operating Range (ft.)	Maximum Speed (mph)
1	AgBOT	Aerial Technology International	4	$9,750	26	10.4	Unknown	Unknown	87,598	38
2	HL48 "Chaos"	Allied Drones	8	$20,000	45	15	15	Unknown	65,617	30
3	F50	AEE	4	$37,000	40	4.4	Unknown	2,953	65,617	11
4	Titan	XactSense	8	$120,000	30	18	50	180	52,805	Unknown
5	Sky	Flytrex	4	$650	30	2.8	4.41	Unknown	36,089	44.7
6	RC Hexacopter Hawk F700 RTF	Skyhawk	6	$1,600	25	4	2.65	984	32,808	23.4
7	F100	AEE	4	$58,000	70	13.2	5.51	4,921	32,808	61
8	350 QX2 AP Combo	Blade	4	$900	15	2.2	0.55	Unknown	16,404	Unknown
9	Phantom 4	DJI	4	$1,400	28	3	1.02	19,685.04	16,404	44.7
10	Matrice 100	DJI	4	$3,300	40	5.2	2.2	Unknown	16,404	49.2

HEAVIEST PAYLOAD CAPACITY (Pounds [lbs])

Rank	Name	Company	Number of Rotors	Cost (USD)	Flight Time (Minutes)	Weight (lbs.)	Payload Capacity (lbs.)	Maximum Altitude (ft.)	Maximum Operating Range (ft.)	Maximum Speed (mph)
1	Titan	XactSense	8	$120,000	30	18	50	180	52,805	Unknown
2	Transformer UGAV	Advanced Tactics Inc	6	$25,000	25	35.1	22.49	20,013	Unknown	44.7
3	MAX 8	XactSense	8	$65,000	25	5.00	20	396	Unknown	Unknown
4	Infinity 9Pro Octocopter	TurboAce	8	$15,098	15	15.00	20	Unknown	6,335	Unknown
5	QU4D X	SteadiDrone	4	$13,999	20	7.90	17.64	Unknown	Unknown	Unknown
6	AIR8	Airborne Robotics	8	$15,500	15	37.80	15.4	Unknown	6,500	31
7	HL48 "Chaos"	Allied Drones	8	$20,000	45	15.00	15	Unknown	65,617	30
8	SkyJib-8 Ti-QR	Aeronavics	8	$17,945	15	Unknown	11.02	Unknown	9,842	Unknown
9	Thor X4	Aerial Technology International	8	$14,150	15	34.2	10	Unknown	Unknown	66
10	SkyJib-X4 Ti-QR	Aeronavics	8	$15,592	20	Unknown	7.72	Unknown	9,842	49

MAXIMUM SPEED (Miles Per Hour [mph])

Rank	Name	Company	Number of Rotors	Cost (USD)	Flight Time (Minutes)	Weight (lbs.)	Payload Capacity (lbs.)	Maximum Altitude (ft.)	Maximum Operating Range (ft.)	Maximum Speed (mph)
1	F100	AEE	4	$58,000	70	13.2	5.51	4,921	32,808	61
2	Matrice 100	DJI	4	$3,300	40	5.2	2.2	Unknown	16,404	49.2
3	Kasper	North American	4	$720	30	1.4	0.5	Unknown	1,969	48.9
4	Vader X4	SteadiDrone	4	$19,995	50	8.4	9.48	13,123	4,921	45
5	Altura Zenith ATX8	Aerialtronics	8	$2,000	45	7.7	6.39	Unknown	3,281	45
6	Indago	Lockheed Martin	4	$25,000	45	4.9	0.44	499	6,562	45
7	Sky	Flytrex	4	$650	30	2.8	4.41	Unknown	36,089	45
8	Chroma	Blade	4	$1,490	30	2.9	Unknown	Unknown	1,312	40
9	MULTIROTOR G4 Eagle V2	Service-Drone	8	$28,260	30	5.5	5.51	Unknown	6,562	37
10	G4 Eagle V2 Cargo	Service-Drone	8	$35,360	30	5.5	5.51	Unknown	6,561	37

Severity, Probability, and Exposure Risk Analysis Methodology

Quantifying the risk of an sUAS attack is an especially tedious task, given the variety of harmful ways in which a drone may be deployed. Commercially available sUASs are capable of circumnavigating traditional physical security measures and have the capacity to deliver payloads designed to cause either physical or cybernetic damage. The SPE risk analysis is a method of objectively assessing risk that has been used by the US Coast Guard. The simple methodology involves assigning values to a set of pre-defined criteria. For the purposes of this case study, the first area of focus, *severity*, evaluates the degree to which a successful sUAS attack on the Port of Opal City's infrastructure, personnel, and/or trade-related vehicles and vessels will affect the local, state, and national economies. The *probability* component analyzes drone sales in the United States and reported incidents of drone misuse in other US ports, noting some historical incidents of nefarious drone use worldwide. The final component, *exposure*, classifies targets in the Port of Opal City and discusses pre-existing security policies that the port has in place.

The values allocated to each SPE variable are multiplied together to generate a final risk value, which is then compared against the Coast Guard's pre-determined risk guidance index to determine the port's degree of vulnerability to attack. This study uses objective benchmarks tailored to the Port of Opal City in place of the Coast Guard's original SPE standards, a methodology that may similarly be adapted for use at any major critical infrastructure site, provided enough data is publicly available to establish both comparative and objective benchmarks for a comprehensive review. The language ascribed to each value specifically for the Port of Opal City appears in table 7 below.

Table 7: Criteria and Values for Severity, Probability, Exposure, and Risk of a Drone Attack on a Major Port Facility

Severity Scale	
1	No change in port operations
2	Temporary shutdown of one port pier for less than one hour
3	Shutdown of one port pier for more than one hour but less than 24 hours
4	Shutdown of two or more port piers for more than one hour but less than 24 hours
5	Shutdown of two or more port piers exceeding 24 hours

Probability Scale	
1	0%–20% chance of a drone attack or accidental drone-related incident, which would negatively affect port infrastructure, personnel, and/or trade-related vessels/vehicles
2	21%–40% chance of such a drone-related incident
3	41%–60% chance of such a drone-related incident
4	61%–80% chance of such a drone-related incident
5	81%–100% chance of such a drone-related incident

Exposure Scale	
1	Port security **uses** effective anti-UAS countermeasures. Port precautions **exceed** those implemented at similar US ports.
2	Port security **does not** use anti-UAS countermeasures. Port precautions **exceed** those implemented at similar US ports.
3	Port security **does not** use anti-UAS countermeasures. Port precautions **mirror** those implemented at similar US ports.
4	Port security does not use anti-UAS countermeasures. Port security precautions **fall below** those implemented at similar US ports.

Risk Values*	Degree of Risk	Guidance
80–100	Very High	Discontinue, Stop
60–79	High	Correct Immediately
40–59	Substantial	Correction Required
20–39	Possible	Attention Needed
1–19	Slight	Possibility Acceptable

**Risk value = severity × probability × exposure*

Port of Opal City

As mentioned earlier, the Port of Opal City is a pseudonym for the actual US seaport on which this SPE risk analysis was originally based. While key details have been removed or altered to obscure the port's true identity and uphold the integrity of specific security protocols, the resulting scores of the SPE risk analysis have not been altered in any way. These scores appear at the end of each SPE component evaluation.

> "THE PORT PROCESSES OVER FIVE MILLION 20-FOOT CONTAINER UNITS ANNUALLY."

The Port of Opal City processes over five million 20-foot container units annually and generates billions of dollars in annual trade revenue. Beyond indirectly generating millions of dollars for local businesses that service port customers, the harbor provides well over 200,000 jobs for the region as a whole. The port contracts with the local police department to provide security and also has a separate security patrol dedicated to monitoring port operations. Each of its 12 piers is leased to a private company, which in turn employs its own private facility security. The port authority (the port's management body) actively maintains relationships with both federal law enforcement agencies and regional emergency management agencies. The port has not deployed any sUAS countermeasures and currently does not permit any drone operations within the facility due to security concerns. Both the local police force and the harbor-specific police force currently abide by Federal Aviation Administration (FAA) guidance to not interfere directly with potentially illegal drone operations at the port but instead to report such incidents to the region's FAA office.[7]

Severity

The US Coast Guard defines severity as "an event's potential consequences measured in terms of degree of damage, injury, or impact on a mission."[8] To complement this definition, this section focuses on the likely economic effects that a drone attack on the Port of Opal City would have at the local, state, and

national levels. While there has never been a known drone attack on a US port, the documented effects of national disasters, union strikes, and deliberate or accidental damage to US port infrastructure can serve to illustrate how a kinetic or cybernetic drone assault could have wide-reaching economic ramifications.

It is important to consider that even temporary disruptions in port operations are likely to cause extensive economic damage to the community, region, and nation. A simulated biological attack or even excessive hindrance by drones could result in a work slowdown or even a strike by port labor. The California longshoremen's strike of 2012, for example, resulted in supply chain disruptions that cost over $1 billion a day.[9] Studies on such a strike occurring at the Ports of New York and New Jersey estimated losses of $110 million per week in economic output.[10]

A RAND report detailing the immediate ramifications of a hypothetical nuclear explosion in the Port of Long Beach stated that such an attack could cost the nation over $1 trillion within 24 hours following the initial detonation.[11] The report furthermore recognized that any chemical, biological, radiological, nuclear, or explosive attack upon a major US port would likely result in the immediate closure of nearby ports as a precautionary measure against any further attacks.[12] The psychological fear of a secondary attack coupled with even a temporary precautionary closure of other major US ports has the high potential to wreak economic havoc exceeding that of the projected $1 trillion loss.[13]

While a drone carrying a full-scale nuclear weapon is highly unlikely for a number of reasons, the potential for a UA to deliver an explosive containing radioactive material is entirely possible. A well-orchestrated attack carried out by multiple sUASs on two or more ports using conventional explosives might result in other precautionary port closures, magnifying the initial economic losses caused by the original attack. Given that a UA's point of origin cannot always be traced, concerns over a follow-up assault by other drones could force port operations adjacent to the initial attack site to cease until local, state, and federal authorities decide that it is safe to resume normal operations. Even unintentional drone mishaps that involve port labor and result in a strike could cause a slowdown of port operations until temporary replacement workers were found. A well-timed, albeit minor, assault by a single drone has the potential to affect the economy not only at the regional level but also at the national level. Given this fact, a deliberate drone assault or even an accidental drone crash that damages critical port infrastructure has the potential to shut down or delay port operations for two port piers for more than one hour but less than 24 hours, at the very least.

Severity Score: 4 (of a possible 5; see table 7)

Probability

Given the relatively recent proliferation of commercial drones in the US marketplace, it is difficult to gauge the probability of a drone attack or accident on any American port. By combining the number of commercial drones presently in circulation in the United States with projected sales figures for the near future to establish a baseline, and comparing this figure with both drone incidents reported by the FAA and a sampling of reported drone incidents at US ports nationwide, it is possible to arrive at some estimates of probability. In addition, a brief overview of some historical nefarious uses of drones provide further context to the probability of an sUAS attack on a major port facility.

At the present time, exact drone sales figures in the United States are not known, because the majority of sUAS manufacturers choose not to disclose them. Despite this lack of precise data, the FAA estimates that there are presently 1.9 million drones currently in circulation, with that number likely to rise to seven million units by the year 2020.[14] The FAA has also noted a sharp increase in the overall number of drone-related incidents or "close calls" in the United States over the past four years. Most of these incidents involve drones flying too close to commercial aircraft. In 2015, over 1,200 of these incident reports were filed, raising concerns among travelers.[15] The Academy of Model Aeronautics has challenged the high number of reported incidents by stating that the FAA's notion of "close calls" lacks any clear regulatory definition, and that many incidents include drones that were conducting legal airborne operations at the time.[16]

Presently, there is no public database listing domestic drone incidents at US ports. In an attempt to shed further light on this issue, the author contacted 59 US port

authorities and asked them to disclose how many or if any drone-related incidents had occurred at their respective facilities between July 2014 and July 2016. Drone-related incidents were defined as unsanctioned drone activity above or on port property or the recovery of a crashed commercial drone on port property. The data compiled from this survey can be found in table 8. At the request of the port security officers contacted for this research, ports have been grouped by annual cargo volume in short tons and are not identified by name. A distinction was made between those ports that had no recorded drone incidents and those that chose not to disclose the number of incidents (only 12 of the 59 port authorities contacted for the study were willing to share that information). There were fewer than five reported drone incidents at nearly all US ports over the past two years.

Table 8. Publicly Disclosed Drone Incidents at US Ports, July 2014–July 2016

Annual Cargo Volume in Short Tons	Number of Ports Contacted in Given Cargo Volume Range	Number of Ports Reporting Zero Drone Incidents	Number of Ports which Reported 1–5 Drone Incidents	Number of Ports which Reported 6 or More Drone Incidents	Number of Ports which chose not to Disclose Number of Drone Incidents
200,000,000+	2	–	–	–	2
199,999,999–100,000,000	1	–	–	–	1
99,999,999–50,000,000	10	–	3	–	7
49,99,999–25,000,000	12	1	–	1	10
25,000,000–1,000,000	34	6	1	–	27

Commercially available drones have been used successfully in a variety of nefarious operations, ranging from surveillance of critical infrastructure sites to actual bomb attacks. The following incidents highlight how commercially available drones have the potential to be used as weapons and for surveillance activities and smuggling operations.

- An online video published by ISIS showed footage captured from a drone over the Baji oil refinery in Iraq.[17] It is believed that the footage was used to assist ISIS commanders in carrying out a later attack on the same facility in April 2015.[18]
- There have been numerous reports of drones being used to smuggle illegal drugs across the US-Mexico border. The first seizure of these drug-carrying drones occurred in August 2015, when US Border Patrol agents seized a drone loaded with 28 pounds of heroin.[19] The US Drug Enforcement Agency estimates that over 150 drone drug trafficking trips were made in 2012 alone.[20]
- In October 2014, during a police interview, El Mehdi Semlali Fathi discussed his plans to carry out attacks on an unnamed US university and federal building by adding an explosive payload to commercially available drones.[21]
- In October 2016, Kurdish fighters shot down an ISIS surveillance drone, which exploded as they were inspecting the wreckage. This was believed to be the first incident of a deliberate bombing mission via a commercial sUAS.[22]

- In April 2015, a rotary wing drone carrying 100 grams of "low-level radioactive sand" landed on the roof of the Japanese prime minister's office in what was later determined to be an act of protest by a private citizen.[23]

Coupling the FAA's estimation of 1.9 million privately owned drones currently in the United States with its 1,200 reported "close calls" involving drones, the current threat of a drone attack on the Port of Opal City would appear to be relatively low. Given the FAA's projection of dramatically increasing drone sales in the next four years, however, the likelihood of either a deliberate or accidental drone incident at the Port of Opal City is bound to increase significantly in the near future.[24] The economic significance of the Port of Opal City and its lack of deployed drone countermeasures (see table 7: Exposure) mean that the probability that the port will be the target of a drone attack or the victim of an accidental drone crash in the near future is relatively high and liable to increase in the coming years.

Probability Score: 4 (of a possible 5; see table 7)

Exposure

> "AGENTS SEIZED A DRONE LOADED WITH 28 POUNDS OF HEROIN."

The preceding "Severity" and "Probability" sections respectively addressed the potential economic implications of port supply chain disruptions and the likelihood of drone attacks in the future. This section, "Exposure," evaluates port-specific targets and precautions the Port of Opal City has taken in order to mitigate the risk of a damaging sUAS attack or accident. The Port of Opal City has several types of possible targets, both structural and human, that could attract an assailant. The primary mobile targets of a potential drone assault are ships, trucks, cars, trains, and helicopters. While the type of cargo it carries may play an important role in determining whether a particular mobile target is chosen, officials should consider the target's secondary factors of strategic and social significance when evaluating possible security measures. An assault on a large passenger ship, for instance, could have significant effects on the entire cruise industry by diminishing such economic activity as future cruise sales, ship purchases, port facility usage, and employment.

The infrastructure critical to most port operations, such as cranes, fuel pumping stations, conveyers, rail lines, and buildings where personnel are located, could potentially be immobile targets for a drone attack. While multiple drones may be necessary to severely damage a ship, a single drone with an explosive payload could cause immeasurable harm to less-protected infrastructure sites. Piers that deal with the transportation of corrosive materials and fuel pumping stations that are uncovered and unprotected would be ideal targets for a single drone assault. The deliberate destruction or blocking of rail lines in and around port property could likewise slow the delivery of goods.

It is important to keep in mind that not all drone attacks must be kinetic to cause large-scale damage. Structures that house sensitive information are at risk for remote cyber attacks and surveillance. Commercial drones have demonstrated the ability to carry jamming devices for remote use on a cyber target with no adverse effects to the drone's command and control systems.[25] An sUAS could likewise be outfitted with penetration testing software or unconventional surveillance devices to conduct remote cyber attacks on technological infrastructure. For example, a group of researchers at Ben-Gurion University in

Israel demonstrated that a drone outfitted with a photodiode sensor is capable of receiving proprietary data on compromised air-gapped computers via the system's built-in LED lights.[26]

Both staff and private citizens within the Port of Opal City are potential targets for a drone attack. Unlike mobile and immobile targets, personnel warrant a separate classification because of their unique responsibility in guaranteeing that the port operates efficiently. While direct kinetic attacks on personnel are a possibility, the psychological ramifications of a drone assault may have far more devastating effects on port operations overall. Simulated biological attacks, such as a drone deliberately dropping any kind of white powder, are liable to result in the evacuation of personnel and the disruption of port operations. Even a drone carrying out port-sanctioned operations is liable to accidentally drop objects, which could result in injury or temporary suspension of port operations.

For this study, it is important to note that the port will be graded only on those security measures and procedures that are public knowledge. As mentioned earlier, the port has a vast array of traditional security measures presently at its disposal; one of the unique features of the maritime environment is its overlapping levels of security. Each privately leased pier has its own private security system, which is managed by facility security officers. The Port of Opal City's security sector maintains an active relationship with the state's emergency services department, US Customs and Border Patrol, the Coast Guard, the Navy, Department of Homeland Security investigators, and the FBI. Despite the various security agencies assigned to guard the US maritime economy, however, the Port of Opal City and most other ports in the nation lack the capacity to legally acquire and deploy the technology necessary to defeat a hostile airborne UA. Given the port's numerous targets, lack of sUAS-specific countermeasures, and operational vulnerabilities to cyberattacks, the port has a high degree of exposure to a potential drone attack.

> "THE PSYCHOLOGICAL RAMIFICATIONS OF A DRONE ASSAULT MAY HAVE DEVASTATING EFFECTS ON PORT OPERATIONS."

Exposure Score: 3 (of a possible 4; see table 7)

Risk Assessment

Risk Value = Severity × Probability × Exposure
Risk Value = 4 × 4 × 3
Risk Value = 48 (of a possible 100; see table 7)

Utilizing the SPE formula, the Port of Opal City is assigned a risk value of 48. According to the Coast Guard's Risk Value chart, this number shows that the port is at a "substantial" degree of risk of a drone attack and that the port authority should take measures to improve security (see table 7: Guidance).

Policy Solutions and Available Countermeasures

The FAA's definition of navigable airspace as "airspace at and above the minimum flight altitudes … including airspace needed for safe takeoff and landing" has generated much controversy in the wake of commercial drone use, given the lack of clear legal guidance on what constitutes "minimum flight altitudes."[27] Presently, the FAA categorizes drones as aircraft, which makes it the only US government body with jurisdiction over sUAS use or misuse.[28] The FAA has

released preliminary guidance for local law enforcement officers to follow, should they witness a possible violation of any sUAS regulations, but local police do not have any authority to stop airborne drone operations at this time. Their role is limited to interviewing witnesses, identifying any sUAS operator(s), recording the location of the alleged sUAS incident, and identifying nearby sensitive locations, events, and/or activities.

Nefarious sUAS activities are bound to occur in restricted airspace regardless of any federal laws. For this reason, both military and civilian facility security officers must be aware of all viable countermeasures at their disposal if they wish to mitigate the dangers of this emerging threat. In the United States, however, many of these countermeasures remain illegal and would require prior federal approval.

Drone countermeasures tend to fall into one of two major categories: kinetic or cybernetic. A kinetic countermeasure involves disabling a targeted drone by physically damaging or immobilizing one or more components necessary to keep the drone aloft. Cybernetic countermeasures encompass a variety of tactics involving electronic manipulation of a drone's communication/guidance system. The legal parameters surrounding kinetic and cybernetic countermeasures present their own unique challenges.

> IN THE UNITED STATES, MANY DRONE COUNTERMEASURES REMAIN ILLEGAL AND WOULD REQUIRE PRIOR FEDERAL APPROVAL.

Kinetic Countermeasures

Falconry abatement is the use of specific kinds of birds of prey (e.g., falcons and buteos) to scare small migratory birds away from airports in order to prevent the smaller birds from being sucked into airplane engines.[29] The Dutch National Police Force and French Air Force have been experimenting with using birds of prey to attack airborne drones, but this strategy has never been implemented in the United States.[30] While the US federal government now allows states to issue falconry licenses in accordance with state laws as of 2014, some states still reserve the right to issue specialty licenses regarding the use of non-domestic animals and birds (species that are not traditionally raised for companionship or food) for commercial services.[31] A drone abatement license could hypothetically be issued as long as a master falconer, in compliance with local, state, and federal animal welfare laws, took the necessary precautions to protect his or her birds from any damage that might be caused by sUAS rotors. If these conditions could be normalized, falconry drone abatement could become a reality not only for airports but also for major centers of economic commerce and critical infrastructure sites.

Another kinetic drone countermeasure that is slowly making its way into the global marketplace is the launching of a projectile at a drone with the goal of either trapping it or knocking it out of the sky. Physically discharging a metal or rubber bullet or shell at a drone is not a legally valid option in the United States at this time.[32] While shooting pressurized water from a fire hose may be another option for physically knocking a drone out of the sky, the time necessary to set up a pump and hose is not practical, given how quickly a drone incident may occur. Companies such as SkyWall have developed a shoulder-fired canister that traps a drone with a net and then deploys a parachute to slowly lower the ensnared drone to the ground.[33] While SkyWall has not yet set a release date for this countermeasure, it has great potential for use in the United States because it minimizes the risk of injuring bystanders with falling debris.

The most widely practiced drone countermeasure has been the use of "anti-drone" drones. These drones are manually operated and typically sport a large net below the drone's airframe. If flown properly, these drones can be used to chase down and catch a targeted sUAS. This countermeasure has seen especially wide use in Tokyo, Japan, where the local government has established an anti-drone squad within the Tokyo police force.[34] Other models of anti-drone drones include net-firing drones, but this technology is still in the experimental stage.

Cybernetic Countermeasures

Cybernetic countermeasures can remove a drone from the sky while minimizing any potentially damaging physical fallout. Three primary cybernetic solutions are spoofing, hacking, and jamming. Spoofing deceives a drone's control system into accepting commands from a communication signal that was not generated by the true pilot's base station. The operator spoofing the targeted sUAS must have either prior knowledge of the exact wireless channel the drone is functioning on or the technological ability to independently determine that information.[35] Hacking a drone is, as the name implies, sending invasive computer code to the drone's onboard flight controller or base station transponder and changing the guidance

programming to accept a different command signal or operate on a different set of flight protocols.[36] To jam a drone, the countermeasure operator spams the drone's radio frequency with incoherent "noise" that prevents the drone from communicating with the true operator's base station. Most commercial drones have a built-in "safe mode," which is designed to either keep the sUAS stationary in the air or fly it back to the site where it made its initial takeoff, should it lose contact with its base station.

While all three cybernetic options have been proven to be among the safest solutions to mitigating unwarranted drone activity, some countries, including the United States, have cyber security laws that impose regulatory hurdles to such technology. Hacking, for instance, is generally illegal, although it is unclear whether using such technology as a drone deterrent would be unlawful.[37] Spoofing, while not explicitly illegal, may fall under the definition of hacking in certain instances. Furthermore, spoofing depends heavily on external factors such as the target drone pilot's signal strength and the lack of any anti-spoofing hardware on the targeted drone.[38] Jamming has been the most widely advertised solution to unwanted drones, but given its potential for abuse, the US Federal Communications Commission has prohibited the use of jamming technology by any non-federal agency.[39]

Presently, the FAA is field-testing the British-made Anti-UAV (unmanned aerial vehicle) Defense System (AUDS).[40] A ground-based system designed to detect, identify, and if necessary, jam a drone's communication signals, AUDS shows the greatest potential to secure large areas from unwarranted drone activity.[41] Until US laws regarding jamming technology are changed, however, AUDS will not be an option for facilities such as the Port of Opal City.[42]

> "THREE PRIMARY CYBERNETIC SOLUTIONS ARE SPOOFING, HACKING, AND JAMMING."

Proposed Solutions and Conclusion

The Port of Opal City is currently pursuing legal options designed to restrict drone takeoffs and landings on port property. Because the FAA regulates the entirety of the US national airspace system, this may be the best regulatory option for the Port of Opal City to pursue at this time. A secondary policy option would be for the port to take advantage of existing FAA guidance, which mandates that drone operators receive permission from all nearby heliport operators prior to operating their craft on or near the port facility.[43] While there are numerous qualifying heliports within the designated two-nautical-mile radius of the Port of Opal City, there are currently no sUAS regulations mandating such permission, contrary to the guidance provided on the FAA's website.

At the present time, the largest regulatory hurdle the port must overcome prior to using any of the countermeasures described earlier are the legal protections given to drones by the FAA. Because all drones are classified as aircraft, they are protected from "sabotage" in any form, and knocking a drone out of the sky via projectile, net, or bird of prey qualifies as sabotage under existing law.[44] Given that AUDS uses a combination of proprietary cybernetic countermeasures and is designed to be used at airports in the near future, such facilities will need to receive special legal permission prior to deploying the AUDS's jamming technology. An argument can therefore be made that, due to the economic importance of the port, it should receive similar legal protection and the right to strategically deploy the AUDS technology for its own protection. It is highly recommended

that the Port of Opal City pursue legislation at the federal level that would give it and all other critical infrastructure facilities the right to use either cybernetic countermeasures or the AUDS.

As with any developing technology, drones can be used as either a benefit or a detriment to society. Drones empower the private citizen to reach areas that were previously inaccessible and to deliver goods in highly unconventional ways. The SPE Risk Assessment of the Port of Opal City reveals that critical infrastructure sites are strikingly vulnerable to both deliberate and accidental drone incidents and that such exposure will only increase over time. It is imperative that both civilian and military security officials are aware of and have access to the tools necessary to safely and legally combat this developing threat. On the ever-changing battlefield against modern terrorism, attacks that are prevented due to strategic forethought and the implementation of proper security countermeasures are rarely accounted as victories. Taking proactive steps to mitigate the quickly emerging threat of drones will help to ensure the security of critical infrastructure sites and the vital services that such assets provide to society. ❖

ABOUT THE AUTHOR

John J. Caton works in the Homeland Security sector of the Cadmus Group.

NOTES

1 "49 U.S. Code § 40102—Definitions," Cornell University Law School, n.d.: https://www.law.cornell.edu/uscode/text/49/40102

2 H.R. 95, 112 Cong. (2012) (enacted). Section 331.

3 H.R. 95, 112 Cong. (2012) (enacted). Section 331(6).

4 All data was gathered from "Drones," Specout, n.d.: http://drones.specout.com/ , and it is accurate as of July 2016. All figures and rankings are liable to change with manufacturer changes and further consumer testing.

5 "Autonomous Aerial Vehicle," Ehang 184, 2016: http://www.ehang.com/ehang184

6 DroneDeploy, *Commercial Drone Industry Trends* (August 2016): http://cdn2.hubspot.net/hubfs/530284/White_Papers/Commercial_Drone_Industry_Trends_Report_Aug_16.pdf

7 The Federal Aviation Administration (FAA) is an agency under the US Department of Transportation and is responsible for regulating the use of US airspace.

8 "SPE Risk Assessment Model Work Sheet," US Coast Guard, n.d.: https://www.uscg.mil/hq/nsfweb/foscr/ASTFOSCRSeminar/Presentations/Safety/SPERISKASSESSMENTMODEL.pdf

9 Mamta Badkar, "Strikers Have Shut Down Two of the Most Important Economic Gateways in the World—And It's Costing the US Billions," Business Insider, 3 December 2012: http://www.businessinsider.com/economic-impact-of-la-and-long-beach-port-strikes-2012-12

10 Mike Obel, "Longshoremen's Strike at Port of NY and NJ Could Devastate US Economy; But Can Labor and the ILA Finally Win One?" *International Business Times*, 5 December 2015: http://www.ibtimes.com/longshoremens-strike-port-ny-nj-could-devastate-us-economy-can-labor-ila-finally-win-1040290

11 Charles Meade and Roger C. Molander, *Considering the Effects of a Catastrophic Terrorist Attack* (Santa Monica, Calif.: RAND, 2006): http://www.rand.org/content/dam/rand/pubs/technical_reports/2006/RAND_TR391.pdf

12 Ibid.

13 Ibid.

14 Roger Schaufele, *FAA Aerospace Forecast: Fiscal Years 2016–2036* (Washington, D.C.: Federal Aviation Administration, 2016): http://www.faa.gov/data_research/aviation/aerospace_forecasts/media/FY2016-36_FAA_Aerospace_Forecast.pdf

15 "Drone Close Calls with Airliners Surged in 2015," Newsmax, 29 March 2016: http://www.newsmax.com/Newsfront/drones-airlines-close-calls-FAA/2016/03/29/id/721290/

16 Keith Laing, "Drone Operators Bristle at Feds' Tracking of 'Close Calls' with Planes," *The Hill*, 31 August 2015: http://thehill.com/policy/transportation/252358-drone-users-bristle-at-federal-close-call-tracking

17 Ralph Avellino and Gilad Shiloach, "Video: ISIS Uses Drones in Oil Refinery Assault," Vocativ, 17 April 2015: http://www.vocativ.com/world/isis-2/isis-using-drones-in-iraq/

18 Caleb Weiss, "Islamic State Releases New Video from the Baiji Oil Refinery," *Long War Journal*, 30 April 2015: http://www.longwarjournal.org/archives/2015/04/islamic-state-releases-new-video-from-the-baiji-oil-refinery.php . Note that the video itself has been removed from the article.

19 Sarah Berger, "Mexico Drug Trafficking: Drone Carries 28 Pounds of Heroin across Border to US," *International Business Times*, 13 August 2015: http://www.ibtimes.com/mexico-drug-trafficking-drone-carries-28-pounds-heroin-across-border-us-2051941

20 Oscar Lopez, "Mexican Drug War News: DEA Reveals Cartels Use Drones to Transport Drugs from Mexico into US," *Latin Times,* 10 July 2014: http://www.latintimes.com/mexican-drug-war-news-dea-reveals-cartels-use-drones-transport-drugs-mexico-us-190217

21 Scott Malone, "Moroccan Man Arrested in Connecticut after School Bomb Plot: Officials," Reuters, 8 April 2014: http://www.reuters.com/article/us-usa-connecticut-drones-idUSBREA371B220140408

22 Michael S. Schmidt and Eric Schmitt, "Pentagon Confronts a New Threat from ISIS: Exploding Drones," *New York Times*, 12 October 2016: http://www.nytimes.com/2016/10/12/world/middleeast/iraq-drones-isis.html?_r=0

23 "Japan Radioactive Drone: Tokyo Police Arrest Man," BBC, 25 April 2015: http://www.bbc.com/news/world-asia-32465624

24 Schaufele, *FAA Aerospace Forecast*.

25 "Drones Hacking Drones (Part 1), Hak5 1518.1," YouTube video, posted by Hak5, 18 December 2013: https://www.youtube.com/watch?v=Fk1Bpy5ccPU

26 Andy Greenberg, "Malware Lets a Drone Steal Data by Watching a Computer's Blinking LED," *Wired*, 22 February 2017: https://www.wired.com/2017/02/malware-sends-stolen-data-drone-just-pcs-blinking-led/

27 Aeronautics and Space, 14 C.F.R. § 1.1 (2017): https://www.ecfr.gov/cgi-bin/text-idx?rgn=div8&node=14:1.0.1.1.1.0.1.1

28 Federal Aviation Administration, *Law Enforcement Guidance for Suspected Unauthorized UAS Operations* (Washington, D.C.: Federal Aviation Administration, 11 August 2016): https://www.faa.gov/uas/resources/law_enforcement/media/FAA_UAS-PO_LEA_Guidance.pdf

29 "Falconry License," California Department of Fish and Wildlife, n.d.: https://www.wildlife.ca.gov/Licensing/Falconry

30 Mindy Weisberger, "Drone-Hunting Eagles Can Snatch Devices Out of the Sky," CBSNews, 8 February 2016: http://www.cbsnews.com/news/drone-hunting-eagles-can-snatch-the-devices-out-of-the-sky/

31 See, for example, "Evaluation Process of California Falconry Regulations," California Department of Fish and Wildlife, n.d.: http://www.dfg.ca.gov/wildlife/falconry/

32 "Negligent Discharge of a Firearm, [California] Penal Code 246.3 PC," Shouse California Law Group, n.d.: http://www.shouselaw.com/pc246-3.html

33 Kelsey D. Atherton, "SkyWall Is a New Anti-Drone Net Bazooka for Police," *Popular Science,* 7 March 2016: http://www.popsci.com/skywall-is-an-anti-drone-net-bazooka

34 Martyn Williams, "This Japanese Security Drone Will Chase Down Intruders," *PCWorld*, 11 December 2015: http://www.pcworld.com/article/3013810/security/this-japanese-security-drone-will-chase-intruders.html

35 Sean Kilcarr, "Telematics Hacking: Three Things You Need to Know," 3 September 2015: http://fleetowner.com/technology/telematics-hacking-three-things-you-need-know

36 Chris Opfer, "Can You Hack a Drone?" How Stuff Works, n.d.: http://computer.howstuffworks.com/hack-drone.htm

37 "US Hacking Laws," Hacker Law, 15 February 2015: http://www.hackerlaw.org/?page_id=55

38 Keith Wagstaff, "Can Police Protect Their Drones from Hackers?" NBC News, 13 April 2016: http://www.nbcnews.com/tech/security/can-police-protect-their-drones-hackers-n553026 ; Daniel Shepard, Jahshan A. Bhatti, and Todd E. Humphreys, "Drone Hack: Spoofing Attack Demonstration on a Civilian Unmanned Aerial Vehicle," GPS World, 1 August 2012: http://gpsworld.com/drone-hack/

39 "Jammer Enforcement," Federal Communications Commission, n.d.: https://www.fcc.gov/general/jammer-enforcement

40 "FAA Expands Drone Detection Pathfinder Initiative," Federal Aviation Administration, 1 July 2016: https://www.faa.gov/news/updates/?newsId=85532

41 Ibid.

42 "Jammer Enforcement," Federal Communications Commission.

43 "Unmanned Aircraft Systems (UAS) Frequently Asked Questions," Federal Aviation Administration, 15 March 2017: https://www.faa.gov/uas/faqs/

44 "2. Aircraft Sabotage (18 U.S.C. 32)," Department of Justice, n.d.: https://www.justice.gov/usam/criminal-resource-manual-2-aircraft-sabotage-18-usc-32 ; "18 U.S. Code § 32—Destruction of Aircraft or Aircraft Facilities," Cornell University Law School, n.d.: https://www.law.cornell.edu/uscode/text/18/32