International Journal of Aviation, Aeronautics, and Aerospace

Volume 2 | Issue 4 Article 1

10-1-2015

Examining Unmanned Aerial System Threats & Defenses: A Conceptual Analysis

Ryan J. Wallace
Polk State College, ryan.wallace@erau.edu
Jon M. Loffi
Oklahoma State University, jon.loffi@okstate.edu

The expansion of off-the-shelf or civilianized UAS platforms presents unique opportunities for criminal or terrorist exploitation of UAS systems. According to the U.S. Department of State (2006), terrorists are adept at weaponizing technology not originally designed for destructive purposes. Terrorists utilize current technology in both conventional and unconventional means to inflict terror and achieve mass effects (U.S. Department of State, 2006).

Such fears are not merely hypothetical. In December 2013, German Chancellor Angela Merkel attended an outdoor campaign rally in Dresden (Naim, 2013). While on the podium, a small quadcopter crash-landed on the platform next to Merkel and her colleagues (Naim, 2013). Fortunately for Merkel, the UAS stunt was operated by members of the rival Pirate Party and merely flown to make a political statement against the nation's use of unmanned craft for security (Naim, 2013). Not surprisingly, experts were quick to point out the potential security implications of the incident, citing the potential for drones to be outfitted with weapons or explosives. This incident was a wakeup call for global security agencies—civilian use of unmanned vehicles presents new potential threats to public security.

This incident came as no surprise to U.S. law enforcement agencies, as only two years prior, a terrorist plot involving UAS craft was thwarted by the Federal Bureau of Investigation. In 2011, 26-year old Rezwan Ferdaus was arrested for plotting an attack on the Pentagon and Capital buildings using a remotely controlled aircraft containing C-4 explosives ("Feds," 2011; "Model," 2011). Ferdaus planned to fly three miniature, jet-powered models packed with a combined 15 pounds of C-4 and direct the explosive-laden craft at the target buildings ("Model," 2011). A similar plot was foiled in 2015 when El Mehdi Semlali Fahti was caught for plotting to attack a school and federal building using remote-controlled aircraft equipped with improvised explosive devices (Brandon, 2014). Fahti detailed how he would obtain the explosive materials and indicated the plot would be funded through drug profits and money laundering (Brandon, 2014).

Despite its successes in thwarting previous UAS plots, law enforcement efforts continue to show vulnerabilities to potential UAS threats. In January 2015, an allegedly drunken Geospatial Intelligence Agency employee lost control of his friend's small quadcopter UAS in the heart of Washington D.C. (Shear & Schmidt, 2015). Unbeknownst to him, the small craft had overflown the White House perimeter fence and crashed on the presidential residence lawn (Shear & Schmidt, 2015). The drone was reportedly sighted by an on-duty law enforcement officer, but went undetected by the White House's aerial defense radar (Shear & Schmidt,

2015). While this incident was unintentional, it further exemplifies the vulnerabilities against a potential UAS threat.

Drones continue to circumvent traditional security efforts. In yet another incident, a small drone was found on the roof of Japanese Prime Minister Shinzo Abe's office in Tokyo ("Drone," 2015). Initially, Japanese investigators reported not knowing who was responsible for the incident ("Drone," 2015). Most alarming, however, was the discovery that the UAS craft was marked with radioactive symbols, carried a plastic bottle with unidentifiable contents, and registered trace levels of radiation ("Drone," 2015).

Problem

Law enforcement and security agencies have demonstrated they are ill-prepared to combat ever-growing UAS threats. Because of the novelty of UAS systems, potential UAS threats are poorly understood by law enforcement and security personnel. Moreover, there is currently no cohesive defense strategy in which to systematically counter UAS threats.

Purpose

This study sought to identify potential uses and adaptations of UAS systems as weapons of terrorism or crime by establishing a cumulative list of generic, intentional and unlawful uses of UAS systems. The study also sought to propose a recommended model of defenses, countermeasures, and mitigation strategies against illicit UAS employment or attacks.

Definitions

For the purposes of this research study, the following definitions were used:

Political scientist David Rapoport (2008) codifies terrorism as

> Terror is violence with distinctive properties used for political purposes both by private parties and states. That violence is unregulated by publicly accepted norms to contain violence, the rules of war, and the rules of punishment. Private groups using terror most often disregard the rules of war, while state terror generally disregards legally codified rules of punishment, i.e. those enabling us to distinguish guilt from innocence, but both states and non-state groups can ignore either set of rules. (footnote 12).

According to the Merriam-Webster Dictionary (n.d.), crime is defined as

> (1) An act or the commission of an act that is forbidden or the omission of a duty that is commanded by a public law that makes the offender liable to punishment by that law. (p. 1)

Method

This study utilized qualitative, Conceptual Analysis methodology. According to Petocz and Newberry (2010) Conceptual Analysis is "the analysis of concepts, terms, variables, constructs, definitions, assertions, hypotheses, and theories. It involves examining these for clarity and coherence, critically scrutinizing their logical relations, and identifying assumptions and implications" (p. 126).

Academic research articles, unclassified government reports, and open-source news articles were assessed to identify recurring themes related to the targeting, employment, adaptations, and defenses against UAS threats. Thematic trends were categorized and coded to model illicit UAS employment methods and evaluate systematic defense mechanisms.

The study sought to discover answers to the following research questions:

1. How are UAS systems used for illegal purposes or terrorism?
2. What are current defense methods against UAS threats?

Articles were selected using an internet search engine with Boolean search pattern for five preselected search combinations, which included nine unique permutations of terms: UAS/UAV/drone and Terrorism, Threat, and Malicious Use. Articles were assessed for thematic concepts. Researchers established a thematic concepts list for each of the topical areas: illegal/terroristic UAS methodology and UAS defense measures or systems. Articles, which presented unique or original concepts, were added to the respective thematic concept list. Repeating or recurring concepts were annotated according to each concept theme. Some articles contained only a single concept while others contained multiple concepts. Whenever possible, concepts were generalized to fit within the coding system, so long as the generalization did not compromise unique concept findings. Collection of data continued until it was clear that researchers could not derive additional unique concepts from further data analysis—in other words, concept saturation was reached.

Upon completion of data collection, the researchers evaluated each of the thematic concept lists for similar themes and attempted to further generalize

thematic concepts. For each thematic concept list, the researchers evaluated the content area and data to select an appropriate conceptual presentation model.

This research specifically excluded UAS applications by military, state entities, recognized governments, or state-sponsored terrorism. Additionally, articles dated prior to 2005 were withdrawn from the data to ensure study currency and validity.

Results and Discussion

Researchers evaluated 68 academic studies, unclassified government reports, and news articles. An analysis of the recurring conceptual themes yielded the following results.

Terrorism and Criminal Use of UAS Platforms

As the United States moves closer to fully integrating unmanned aerial systems (UAS) into the national airspace the Federal Aviation Administration (FAA) has much work to do in terms of regulations, training, licensing and other related issues for a successful integration of the technology for commercial and societal benefits. The FAA Modernization and Reform Act of 2012, among its many sections, charged the FAA in Subtitle B, Sections 331 through 336 – Unmanned Aircraft Systems, to accomplish a safe integration of UAS into domestic airspace (U.S. Government Publishing Office, 2012). Much controversy over the actual implementation and introduction of UAS into the airspace has the FAA behind the curve in establishing legal and regulatory guidelines. While UAS platforms promise to offer new opportunities, they simultaneously present new security threats.

The nefarious aspects of UAS have moved from concept to reality. Before UAS have been lawfully vetted and licensed for legitimate uses, certain actors have been busying themselves with the criminal aspect and application of UAS. Such incidences present a foreshadowing of possible terrorist scenarios that provide homeland security officials with a glimpse of terror threats looming on the horizon. We must remain vigilant for unexpected methods for the deployment of terror by our adversaries. The National Commission on Terrorist Attacks on the United States (2004) cited four types of failures regarding the protection of the homeland. Chief among the failures was imagination. The report went on to say,

> America stood out as an object for admiration, envy, and blame. This created a kind of cultural asymmetry. To us, Afghanistan seemed very far

> away. To members of al Qaeda, America seemed very close. In a sense, they were more globalized than we were. (p. 340).

As al Qaeda was more globalized then – terrorists remain shrewd with current technology now and UAS is no exception. Some have questioned and even criticized officials for considering UAS as a legitimate method for state and non-state actors to spread terror. In a 2012 article, Wayne Morse, president of American Dynamic Flight Systems alluded that for terrorists to consider the use of UAS as a means for terror was unlikely and they [terrorists] could simply achieve a better result from suicide bombings. The article goes on to call this a myth in the making and politicians will use the concept of UAS as a terror weapon as a political tool (Gosztola, 2012). Could this be further evidence of a lack of imagination if the illicit use of UAS is dismissed as not feasible or practical?

In August 2015 the Department of Homeland Security (DHS) placed law enforcement officials in America on notice regarding the use of UAS as a means for terror. In their assessment release DHS said, "We cannot rule [out] the ability of future adversaries to acquire and use a commercially available [drone] as part of an attack within the Homeland" ("DHS," 2015, para. 5).

Further evidence exists for the use of UAS as a terror weapon. In October 2014, the New York City Police Department (NYPD) publicly reported concern about an air assault by UAS ("NYPD," 2014). The technology involved in the manufacture of UAS is such that it should be considered as a potential terror threat. The NYPD police commissioner cited examples of videos showing UAS accurately striking targets with a paintball gun. NYPD is especially concerned about the capability of UAS to carry a payload of explosives to a designated target. The commissioner cites the video, which disclosed a UAV hovering and landing in front of the lectern at a public speaking event conducted by Germany's Chancellor Angela Merkel. Had the UAS been carrying a payload of explosives it would have threatened the lives of those in close proximity to the UAS. Such examples reiterate the varied potential for illicit UAS use. To defend against UAS threats, one must first understand the nature of the threat.

Commercial off the Shelf Threat

As in most instances of manufacturing, the technology typically outpaces regulations and laws. This is especially true with the manufacture and use of UAS. The nature of commercial UAS technology makes it exploitable for criminal or terroristic purposes directly out of the box, with little modification.

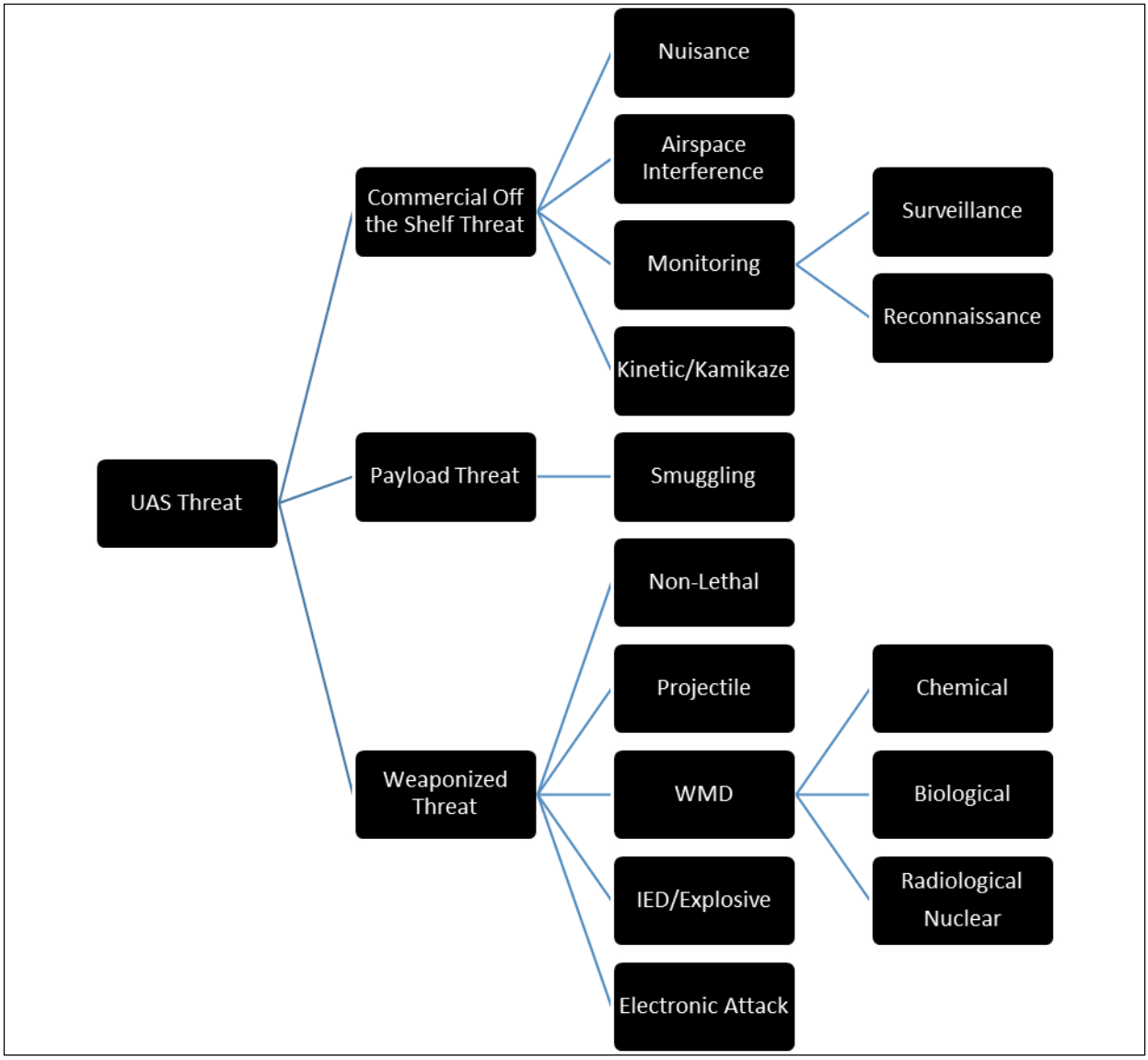

Figure 1. Concepts of Illicit UAS Use.

Nuisance. The most benign illicit use of UAS platforms is the interference they create for the general public. Such actions represent any interference with a property owner's rights to use and enjoy their property without substantial or unreasonable interference (Soloman, 2014). Similarly, UAS platforms may violate an individual's privacy, sometimes referred to as "intentional intrusion upon seclusion," measured by the standard of whether a normal person would be offended by the invasion (Soloman, 2014). The aforementioned behaviors are reflected in civil or tort law. A more serious infraction caused by a drone is

trespassing, or the illegal intrusion onto someone else's property (Soloman, 2014). Trespassing is encompassed in both criminal and civil law. Nuisance threats go well beyond mere irritation. A UAS could potentially upset children or animals on an individual's property.

In a recent wildlife physiology study published in the Journal of Biology, researchers found that large predators, when exposed to drones, can incur cardiovascular stress (Viegas, 2015). In the study, researchers exposed wild bears to short, 5-minute encounters with a flying UAS platform and discovered that the animals' heart rates spiked by up to 400% (Viegas, 2015). Furthermore, drones can elicit fear or adversely affect an individual's perceptions of security or safety. In May 2015, several residents of Del Mar, California, became concerned about a drone that had been spotted numerous times outside the windows of their homes (Chambers, 2015). Despite the fact the drone was not equipped with a camera or monitoring device, it unnerved local residents, as no one knew who was flying the craft and why it was being operated in the middle of the night (Chambers, 2015). The operator, who was later identified, claimed "there's nothing to worry about…I just like flying this [drone]" (Chambers, 2015, p. 1).

Monitoring Threat. One of the most notable concerns about UAS platforms stems from their potential to silently monitor and record their surroundings. Culturally, U.S. citizens tend to be abhorrent to unchecked domestic surveillance, legitimate or otherwise. This attitude is readily apparent, evidenced by the public outcry and subsequent clamor for reform of the recent National Security Agency warrantless wiretapping and similar incidents. One might argue that aerial surveillance is not a new threat – anyone with a pilot certificate and access to an aircraft has the capability of conducting aerial surveillance.

Surveillance. UAS platforms, however, change the dynamic of aerial surveillance, making it accessible and affordable for almost anyone. With the availability of highly automated UAS hobby platforms such as the DJI Phantom, one can purchase a relatively sophisticated aerial monitoring platform with high-resolution capability. Newswire stories of such privacy intrusions by UAS platforms are becoming more commonplace. In August 2015, a Hawaii resident spotted an unmanned rotorcraft hovering outside her bedroom window, yet law enforcement was unable to respond as the action violated no established criminal laws (Kawano, 2015). A similar incident occurred in Kentucky, when a concerned father disabled a drone caught observing his young daughters in their backyard, yet again, police efforts were curtailed since no laws had been broken (Chappell, 2015). Perhaps more frightening is the unknown purpose behind many hobby drone

flights. While many operators are merely enjoying their UAS devices, others may have more sinister observation intentions, such as observing young children.

Reconnaissance. While similar to surveillance, reconnaissance activities take a further step toward illicit behavior. Often confused with surveillance, reconnaissance is an activity derived from military terminology that involves collecting intelligence on a known "enemy" target. To illustrate, consider the example of a criminal seeking to burglarize a house. *Surveillance* would be the actions taken to observe various neighborhood properties; whereas, *reconnaissance* involves scoping out a specific property for exploitable weaknesses, such as security, homeowner arrival and departure times, possible entry locations, and other related "intelligence" information. Unmanned systems have the capability of performing both surveillance and reconnaissance functions. An assessment by the Department of Homeland Security (DHS) indicated drug dealers and drug cartels were already beginning to use UAS platforms to monitor police activities along the U.S. border (Levine, 2015). Moreover, UAS automation allows operators to conduct illicit monitoring activities at a sizable standoff distance, effectively preserving their anonymity from potential criminal investigation. Such illicit monitoring actions allow criminals or terrorists to assess for vulnerabilities in critical infrastructure, government sites, businesses, and private citizens alike.

Airspace Interference. UAS platforms present a genuine threat to safe airspace utilization. The FAA has logged dozens of reports of near-misses between airliners and UAS platforms being improperly operated near airports across the country. In March 2014, a US Airways regional jet nearly collided with a small UAS near Tallahassee, Florida (Whitlock, 2014). September of the same year, Republic Airlines reported nearly striking a small unmanned craft at 4,000 feet. Also in September 2014, three different airlines inbound to LaGuardia reported successive encounters with a UAS operating along the final approach path (Whitlock, 2014). In addition to interfering with normal aviation operations, unmanned aerial vehicles are impeding emergency response functions. In August 2015, a SkyLife helicopter came within 20 feet of being struck by a small-unmanned platform while transporting a patient (Ybarra, 2015). This incident comes just one month after California aerial firefighting teams encountered five hobbyist-operated UAS craft obscured by smoke near a wildfire operation. Fire crews temporarily suspended aerial fire suppression operations for safety while the law enforcement personnel attempted to remove the drones from the area (Martinez, 2015). An airborne UAS creates a collision threat to aircraft and could adversely impact normal and emergency aviation operations. It is conceivable that terrorists or criminals could employ UAS craft to disrupt drug interdiction, law

enforcement, or medical aircraft with the intended purpose of curtailing tracking, emergency response, or disaster mitigation capabilities.

Kinetic/Kamikaze. Even without armaments, a drone is capable of causing damage or injury to people or property on the ground or in the air. While many UAS accidents are likely accidental rather than intentional, the risk is the same. In March 2015, a small UAS hobby platform crashed into a Miami home, breaking a window. Since the drone went unclaimed and police were unable to determine the identity of the operator, the property owner had little recourse to recover damages ("Mystery," 2015). In a more serious event in July 2015, a woman was knocked unconscious by a falling UAS platform after its owner lost control of the device at a Seattle gay pride parade (Rawlinson, 2015). To exemplify the potential kinetic lethality of unmanned vehicles, one can simply turn to a gruesome 2003 event in which 13-year old Tara Lipscombe was struck in the head by an out of control RC aircraft (Allen, 2003). Flying at 50 mph, the 5-foot wide aircraft delivered a lethal blow to the young girl, who died merely three hours after the incident (Allen, 2003). While the aforementioned incidents appear unintentional, they exemplify the lethal potential of UAS systems. Should criminal or terrorist elements wish to carry out an attack, an out-of-the-box UAS platform has the potential to deliver a lethal kinetic blow to soft targets, while having the potential added benefit of appearing as accidental or negligent.

Figure 2. Damage caused by small prototype, fixed-wing UAS against a parked static aircraft. While this accident was inadvertent, the incurred damage demonstrates the kinetic destructive potential of UAS platforms (Used with permission).

Payload Threat/Smuggling. UAS platforms can also be exploited as a transportation mechanism for illegal contraband or cargo. Use of these platforms allow terrorists or criminals to bypass traditional security barriers such as fences, walls, and detection measures. Essentially, drones add a skyward dimension to security considerations. The New York Times reported an incident occurring in Bishopville, South Carolina at the Lee Correctional Institution where a UAS was spotted by prison officials flying from a wooded area near the prison toward the perimeter of the institution (Schmidt, 2015). A guard reported seeing a man running away from the wooded area. Later prison officials found a package left by the UAS, which contained a cellphone, tobacco, and marijuana. The package had become tangled in the power lines near the prison and the crashed remains of a UAS were located nearby. The director of the South Carolina Department of Corrections stated it appeared to be a delivery system (Schmidt, 2015). A similar incident occurred in Tijuana in April 2015. A hexicopter carrying 7 pounds of methamphetamines operating just two miles from the U.S.-Mexico border crashed into a shopping center parking lot (Davis, 2015). The incident marks a novel approach to drug smuggling that law enforcement officials call an emerging threat (Davis, 2015).

Weaponized Threat. Perhaps the most fearsome threat produced by terrorist or criminal entities involve the deliberate construction or modification of UAS systems to carry and employ weapons. This application of UAS platforms has received the bulwark of speculation and even fear mongering among industry experts, but is well-justified considering the relative ease in which a UAS platform can be weaponized to produce devastating results. Wilkinson (2012) explains, "Terrorists have demonstrated repeatedly that their goals and objectives can be accomplished by using the same tactics and 'off-the-shelf' weapons (though cleverly modified or adapted to their needs) that they have traditionally relied upon" (p. 23). Armaments that can be added to UAS platforms vary widely from jury-rigged incendiary or explosive devices to carefully engineered projectile systems.

Non-Lethal Systems. While the use of non-lethal systems are not generally associated with criminal activity, the production of such systems is already underway for law enforcement and security purposes. Mounting a drone with systems capable of firing rubber bullets, tear gas, or taser nodes has several promising applications for law enforcement organizations (Kersey, 2012). In March 2014, the technology company Chaotic Moon successfully armed a UAS with an 80,000-volt Taser and test fired the weapon on a volunteer from the company. Called the Chaotic Unmanned Personal Intercept Drone (CUPID), the experimental device was controlled by a smart phone, with further automated features currently under development (Metro, 2014). It is not unreasonable to

speculate that terrorist or criminal elements could foreseeably gain access to such systems through either proliferation or theft.

Projectile Threats. While the prospect of UAS platforms carrying firearms or other lethal projectile weapons might seem particularly troubling, the likelihood of such a modification is reasonably low compared to other weaponization efforts. The development of an effective projectile weapon system such as a gun or missile requires highly specialized engineering and fabrication expertise. Without engineering expertise, access to these types of UAS systems is generally limited to a select group of special operations or military organizations. Moreover, such technology generally remains tightly guarded against physical theft or proliferation, making the acquisition of such systems by terrorists or criminal elements extremely improbable. Despite the aforementioned complications, some individuals have self-produced UAS projectile systems that show alarming ingenuity. In June 2015 an 18-year old mechanical engineering student equipped his UAS with a semi-automatic pistol and successfully fired the weapon while his UAS was airborne (Kerley, 2015). Local and federal authorities were investigating the incident to determine if any criminal statutes had been violated.

IED/Explosive. The use of drones as a delivery system for improvised explosive devices (IEDs), incendiary devices, or other combustibles remains high. Terrorists in particular have shown great ingenuity in crafting rudimentary explosives. According to Wilkinson (2012), "Relying on unconventional adaptations or modifications to conventional explosive devices, these [terrorist] organizations have been able to develop innovative and devastatingly effective means to conceal, deliver, and detonate all kinds of bombs" (p. 19). Dolnik (2007) further explains that some terrorist groups are already considering the benefits of a UAS delivery system, "Terrorists in Kashmir have experimented with remote-control model planes and Unmanned Aerial Vehicles (UAV) to deliver explosives from the air" (p. 45). The 2011 plot by Rezwan Ferdaus to use remote control aircraft to deliver and detonate explosives against the U.S. Capital building and Pentagon show that terrorists already consider UAS platforms as a viable method of weapon delivery ("Model," 2011).

Weapons of Mass Destruction (WMD). Weapons of mass destruction represent particularly lethal threats stemming from the use of hazardous materials including Chemical, Biological, Radiological, and Nuclear (CBRN) substances. Use of UAS platforms as a delivery system for CBRN substances are particularly troublesome, as such delivery systems could easily bypass traditional security measures. Moreover, such systems can effectively cause mass casualties without the need for precision flying. A drone could merely over-fly the target area where

a CBRN substance could be deployed in aerosol form or a dispensing mechanism dropped from the craft. One such plot by the al-Qaeda terrorist organization was foiled in 2013 by Iraqi military intelligence personnel ("Iraq," 2013). The organization planned to employ remote control aircraft to release chemicals including sarin gas, mustard gas, and chlorine bombs ("Iraq," 2013). According to U.S. officials, these substances were selected to enhance the lethality of the planned attack ("Iraq," 2013).

Conversely, some experts argue that CBRN substances are less likely to be used by terrorist organizations. Davis et al. (2014) notes that WMD substances are less than ideal for terrorist use, as they are difficult to weaponize and generally produce fewer casualties than traditional explosives. Davis et al. (2014) further explains that radiological or nuclear substances in particular pose as much threat to terrorists as the general public and that the prolonged exposure required to weaponize a radiological threat would likely be fatal to the instigator. Nevertheless, the 2015 incident in which a drone landed on the roof of the Japanese Prime Minister's office emphasizes the reality of such threats. The canister carried by the drone was believed to contain a radioactive Cesium compound ("Drone laced," 2015).

Electronic Attack. A particularly novel threat presented by drones is the potential to use them as platforms to commit an electronic attack or electronic theft. The SensePost "Snoopy" UAV can be equipped to digitally hijack a smart phone's wireless signal and gain access to personal information contained on the device (Gittleson, 2014). Snoopy developer Glenn Wilkerson alludes that any Wi-Fi-enabled device is vulnerable to the Snoopy system. He further describes how the Snoopy system can impersonate a Wi-Fi trusted network and even exploit the phone's unique MAC address to track its location (Gittleson, 2014). Wilkerson goes on to explain that the mobility of the device allows it to bypass traditional security measures and simultaneously maintain stealth (Gittleson, 2014). The device bears a striking similarity to the Stingray phone tracking system, with substantially enhanced capabilities. It is conceivable that such technology would be highly sought-after by intelligence agencies and law enforcement entities and could be easily adapted by unscrupulous elements to be used for identity theft, blackmail, corporate espionage, or any number of other illicit activities.

UAS Defense Concepts

Analysis of the data revealed 39 unique UAS defense concepts, however, articles only offered a limited array of pragmatic defense options. In no instance was a grand strategy or cumulative protection model presented to cope with UAS

threats. Defense concepts were assessed and organized into a cumulative defense-in-depth model. Viega and McGraw (2002) (as cited in Barnum, Gegick, & Michael, 2005) assert, "The idea behind defense in depth is to manage risk with diverse defensive strategies so that if one layer of defense turns out to be inadequate, another layer of defense will hopefully prevent a full breach" (p. 1). Schneier (2000) (as cited in Barnum et al., 2005) also supports this notion, stating, "Don't rely on single solutions. Use multiple complementary security products so that a failure in one does not mean total insecurity" (p. 1). This concept is used as a staple throughout security industry to protect people and assets.

Organization of the data into a defense in depth model for UAS threats yielded a five-layer, concentric circle of defense which included the following broad defense strategies: Prevention, Deterrence, Denial, and Detection. The fifth and final layer of defense was split into diverging subcategories of Interruption and Destruction.

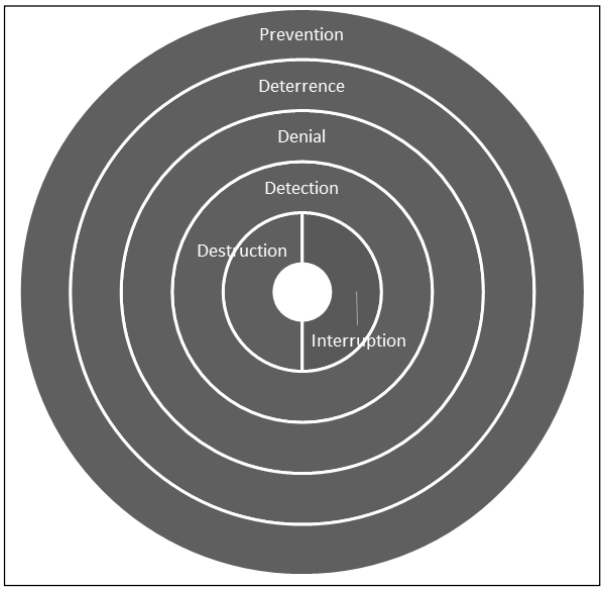

Figure 3. UAS Defense in Depth Model.

Prevention. Perhaps the most important layer of UAS defense lies in preventing a UAS attack. The bulwark of preventing UAS threats is credited to the intelligence community. Preemptive law enforcement investigation and intelligence collection efforts have often been the singular mechanism that interrupts dangerous terrorist and criminal plots. According to Lele and Mishra (2009),

> Existing air defense systems are ineffective against terrorist mini-UAVs…this is where the challenge exists for the state. The main effort of dealing with the threat of terrorist UAVs needs to be on preventative measures. Under such circumstances, the role of *actionable intelligence* [emphasis added] becomes very important. (p. 61).

The unraveling of the 2011 Rezwan Ferdaus plot to fly three remotely-controlled aircraft into the Pentagon and Capital buildings exemplifies the importance of intelligence intervention. After being tipped off by a cooperative witness, undercover FBI agents used traditional surveillance, undercover operations, and other intelligence and investigative methods to discover and thwart Ferdaus' planned drone attack ("Affidavit," 2011; Kimery, 2015).

Supplementing intelligence and preemptive investigative activities, is the establishment of critical component purchase monitoring. Jackson, Frelinger, Lostumbo and Button (2008) suggest the establishment of purchase monitoring and reporting programs for distributors of UAS components or related technologies to report suspicious customer behavior or questionable purchase patterns (Jackson et al., 2008). The authors also call for enhanced counter-proliferation programs to curtail adversary access to heavy payload or long-range UAS platforms (Jackson et al., 2008). The Government Accountability Office (GAO) echoed the call for further proliferation controls, citing an increased U.S. vulnerability to terrorist intelligence gathering or attacks if adversary organizations acquire unmanned systems (U.S. Government Accountability Office, 2012).

Deterrence. The second layer of UAS threat defense lies in the deterrence of UAS attacks. Data overwhelmingly indicated the need for enhanced legislation to curtail illegal or terroristic UAS activities. The legislative remedy to counter UAS threats comes in two basic mechanisms. The first mechanism relies on legislation to create, establish, and most-importantly, fund various formal UAS defense measures by equipping agencies to develop and deploy a concerted UAS defense. The second category of legislative remedy lies in the establishment of civil and criminal penalties to deter illegal UAS use. Wright (2010) suggests that the deterrent effect of legal punishments is based on two distinct factors: the certainty of punishment and the severity of punishment. According to Wright, if people were certain they would be apprehended for committing a crime, most would likely not do so (Wright, 2010). Unfortunately, the deterrent effect is almost negated if the risk of getting arrested, convicted, and punished is negligible (Wright, 2010). Severity of punishment also plays a role in deterrence, if the offending subject is aware of the rules and consequences and subsequently makes a rational cost-benefit analysis of committing the offense (Wright, 2010).

The Federal Aviation Administration (FAA) has done little to capitalize on the deterrent effect of either principle. In fact, even established corporations are breaking the rules. Peter Sosnowski, a preconstruction director for Webcor Builders comments about his company's overt, illegal commercial use of drones stating: "Officially [the FAA's] stance is, You can't do that [fly drones for commercial use]…until someone gets caught and penalized, drone businesses will continue to do business as is" (Nicas, 2015, p. 1). The FAA's use of Cease and Desist letters and civil penalties are proving relatively ineffective in deterring illegal drone use. If the FAA cannot keep seemingly law-abiding businesses in line, it is unlikely established penalties will have any hope of deterring a committed criminal or terrorist.

In addition to legislative deterrence, several articles suggested the implementation of No Fly Zones as an additional deterrent against illegal use of UAS platforms in sensitive areas. In many ways, no fly zones are equally as ineffective as legal deterrent measures, with the exception that such areas are usually manned with other physical or active security measures. While deterrence plays a role in UAS defense, the effectiveness of this security layer relies on the compliance of UAS operators. In the event of terrorism or criminal activity, deterrent measures should be considered relatively ineffective.

Denial. The third layer of UAS threat defense encompasses all passive security measures to thwart the use or effectiveness of drones in conducting illegal activities or terrorism. Passive security measures provide an ideal security mechanism for averting UAS threats, since many such measures are inexpensive and relatively easy to implement with advanced planning. Perhaps the most important denial measure is the protected asset's physical environment. Selection of a location that presents hazards or impediments to UAS operations can dramatically enhance security against UAS threats. Large trees or high structures can make controlling or maneuvering a UAS difficult. Moreover, the presence of such obstacles can also make the likely vector of inbound UAS threats more predictable. In many cases, obstacles can limit the type of UAS platforms that can be employed; confined spaces surrounded by tall obstacles for example denies the ease of approach and maneuverability for fixed wing platforms.

In the event obstacles are not available in the venue area, man-made obstacles such as nets can be deployed to thwart UAS operations (Chuter, 2015). The selection of an indoor venue provides further security from UAS threats, as it provides a physical barrier and obfuscates the exact location of the target from an external UAS attack. Even adverse weather can provide mitigation from a UAS attack, as high winds, limited visibility, precipitation, and other atmospheric factors

can adversely affect UAS controllability or performance, particularly for small platforms.

A critical sub-component of denial lies in the use of unpredictability, often called random security measures. Terrorists usually prepare attacks according to a carefully executed planning cycle that includes: broad target selection, intelligence gathering and surveillance, specific target selection, pre-attack surveillance and planning, rehearsals, actions on the objective [attack], and culminates with escape and exploitation (U.S. Army Training & Doctrine Command, 2003). Ensuring unpredictability in security through the use of random security measures interrupts the terrorism planning cycle by denying the adversary critical intelligence and surveillance information. According to Card (2014), unpredictable security measures such as varying transport routes and schedules "make it harder for all terrorists to target high-risk personnel, not just against possible UAV attacks, and it is recommended these measures continue to be used" (Card, 2014, p. 26). The importance of unpredictability and random security measures cannot be understated when defending against UAS threats.

Another proposed mechanism of UAS threat denial is the encoding of UAS navigation software to prevent UAS use in certain designated areas. Called "geo-fencing," this approach is coded in the hardware by the UAS manufacturers to prevent the craft from operating within the confines of pre-established virtual boundaries. Drone producer DJI currently uses geo-fencing to prevent its drones from operating in the Washington D.C. area and around airports (Gettinger, 2015).

Detection. In the event passive defense mechanisms fail to prevent, deter, or deny a UAS threat, active defense mechanisms must be employed. The employment of weapons or other active defense means requires rapid detection or early warning of the UAS, identification of the threat, and subsequent telemetry tracking to perform an engagement. Several varieties of emerging technologies have been developed to fulfill this security requirement.

Active detection. Active detection mechanisms involve the use of radar signals produced by a transmitting device to reflect off a UAS and be detected by the radar receiver. Conventional radar has significant difficulty detecting and tracking small UAS craft. First, small UAS craft have very small cross-sections—the surface area that reflects radar signals. This small surface area results in a smaller reflectivity of the radar signal, which reduces the probability that the radar return signal strength will exceed the radar's detection threshold. Secondly, most radar systems are equipped with computer or operator-assigned detection thresholds that further filter out spurious radar returns such as wildlife,

precipitation, or other non-relevant information. Without such radar filtering systems, operators would have difficulty determining the difference between an aerial contact and clutter. Despite these operational challenges, some radar experts have achieved success in overcoming UAS detection difficulties. Thales Nederland has configured its Squire multipurpose radar system to detect UAS systems (Chuter, 2015). In Chuter (2015), Thales sensor development expert Wilm Shuttert highlighted the capabilities of the new system,

> Detection is not the issue. Everybody can detect an object. The big trick is discriminating small UAVs from birds. We have invested a lot in developing the algorithms to detect and discriminate a UAV from birds smaller than a blackbird (p. 1).

Thales' success reveals that with modification, radar systems can be configured to detect and track UAS systems. Further study of radar modifications is recommended to determine their false alarm rate to wildlife.

Passive detection. Passive detection systems use sensors that sample the electromagnetic spectrum within certain wavelengths to determine the presence of UAS-characteristic signals. Passive UAS detection systems currently include visual, acoustic, thermal/infrared, and UAS communications/control frequencies (Beaudoin, Gademer, Avanthey, Germain, & Vittori, 2015).

Visual detection of UAS platforms is perhaps the simplest method of detection. Several factors can affect the visual detection of UAS platforms including: distance of the UAS, the ambient illumination of the UAS, atmospheric clarity, color and contrast of the UAS, position of the UAS within the field of view, focus of the eye, and visual fatigue ("Aviation," n.d.). Visual detection is further complicated by individual physiological limitations or visual degradation caused by drugs, alcohol or other vision-degrading substances ("Aviation," n.d.). Finally, visual detection can also be adversely affected by a number of visual illusions ("Aviation," n.d.).

UAS platforms can also be detected by evaluating ambient sound for characteristic engine noises. This technology generally focuses on detecting the acoustic wave frequencies formed by commonly-used UAS engines (Quantum Technology Sciences, 2015). Quantum Technology acoustic detection systems use advanced acoustic processing, allowing an operator to determine both the bearing and the type of UAS threat, based on its unique signature (Quantum Technology Sciences, 2015). Quantum Technology Sciences (2015) report the ability to acoustically detect and track a UAS platform at up to 350 meters. A competing

company, Drone Labs, claims their systems can detect a drone up to 100 feet away in normal environments, and up to 300 feet away in quiet conditions ("It's a bird," 2015). While these systems show great promise, their application is likely to be limited based on the ambient noises of the environment and may not be appropriate for all security situations.

Thermal or infrared detection systems make use of the infrared radiation spectrum, which utilizes slightly longer wavelengths then visible light. While both systems use the infrared spectrum, what they detect is quite different. The near wavelength infrared spectrum lies just beyond the visual EM spectrum, functions characteristically similar to visible light, and is what some people would call night vision (B. Lincoln, 2013). These systems are ideal for detecting UAS platforms in low-light conditions. Conversely, long wavelength infrared utilizes lower infrared frequencies that can differentiate thermal variances and is more commonly known as thermal imaging (Light, n.d.). These systems detect the difference between the ambient environmental temperature and the heat-producing parts of an unmanned system, such as the engines ("UAVs," 2015). Thermal infrared systems benefit from high sensor contrast between a heat-producing target and relatively homogeneous background (Koretsky, Nicoll, & Taylor, 2013).

The final method of passive detection of UAS craft involves the monitoring of the EM spectrum typically associated with UAS control or communications (Beaudoin et al, 2015). This form of signal detection provides an alert to UAS control signal presence after which triangulation can be used to obtain signal bearing information. Signal identification can be derived from comparing received signals to a database of known UAS platform control signals that takes into account signal frequency, modulation, and other factors to uniquely identify an electronic fingerprint for the signal source—in this case, a UAS transmitter. This method of UAS detection should be employed in concert with complementary active defenses such as control interruption, spoofing, or jamming.

Rapid detection, identification, and tracking of UAS threats are critical to establishing an effective threat response. Timely detection will allow maximum opportunity to employ active defense measures against a threat UAS, permit rapid evacuation, and execute pre-established emergency response plans.

Active defenses. Active defenses represent the final, layer of security against UAS threats. It is important to note that not all UAS threats require an active response. A risk management evaluation should be performed to assess the potential UAS threat's capabilities, available response time, mitigation alternatives, and the potential for collateral damage caused by implementing an active defense

measure. Active UAS defense measures come in two basic varieties: UAS *interruption* or UAS *destruction*.

Interruption. Interruption defenses are active measures designed to avert a threat UAS from carrying out an adverse action. Interruption can be carried out in one of three ways: operator interruption, jamming, and spoofing. The most obvious method of UAS interruption is to locate and identify the UAS operator and either forcibly compel the operator's compliance in removing the UAS threat or assuming direct control of the UAS. Park rangers in Hawaii recently confronted a tourist illegally operating a UAS near the Hawaii Volcanoes National Park caldera where a large crowd had gathered (M. Lincoln, 2015). When confronted by the ranger, the operator refused to provide identification and attempted to flee the scene, resulting in the suspect being "tasered" by the ranger and subsequently arrested (M. Lincoln, 2015). This method of UAS interruption is highly unpredictable due to a number of factors.

First, the operator may be uncooperative in complying with security instructions in removing the UAS threat, such as a terroristic or criminal use of a UAS. Secondly, detaining the operator may not prevent the threat UAS from completing its assigned activity, as certain automated UAS systems can be programmed to perform functions with little operator input. In the event the UAS operators is uncooperative in redirecting, landing or removing the UAS threat, security personnel may be required to take direct control of the UAS to avoid a disaster. The lack of UAS control standardization, required specialized flying experience, and other unpredictable complicating factors may make assuming direct control of the threat UAS just as dangerous as allowing the operator to continue the adverse action. It is difficult to provide recommendations in such a circumstance, as an appropriate response would be dictated based on a multitude of situational factors.

The second method of interrupting a threat UAS platform involves jamming its control or navigation system. Jamming is the electronic bombardment of frequency interference designed to drown out the UAS control system from receiving transmitted control instructions or navigation information. With many UAS platforms reliant on external navigation inputs from Global Positioning System (GPS) satellites, jamming these frequencies may prevent the threat UAS from precisely carrying out its operator-assigned task. This response method presents its own unique risks and requires knowledge of the UAS type and specific system capabilities to determine effectiveness. Some UAS platforms have inertial navigation systems that supplement GPS navigation; these UAS systems would be relatively unaffected and incur only degraded precision navigation performance.

Other systems will merely perform a static hover until navigation connectivity is restored or until the UAS power is depleted. Perhaps more importantly, the jamming of navigation signals, particularly GPS, can adversely affect other legitimate GPS systems within the jamming transmitter's field of influence. Succinctly, jamming operators must be cautious against inadvertently causing collateral interference by interrupting other GPS-reliant systems in its proximity.

The jamming operator must also understand how the threat UAS will respond to control frequency jamming. Some UAS aircraft will automatically return to the launch point if the UAS loses control connectivity, whereas others will carry out the last operator instructions. UAS response to jamming is highly variable based on the UAS manufacturer and designed system capabilities.

The final method of UAS interruption is a form of deceptive jamming known as spoofing. Defensive spoofing involves an operator sending falsified navigation or control data to a threat UAS that mimics legitimate data. Spoofing systems can divert a UAS threat away from the target area by feeding it false coordinates or control instructions (Gettinger, 2015). Unencrypted control or navigation systems are vulnerable to spoofing, since the UAS system has no way to differentiate between authentic control signals verses the "spoofed" signals.

While system interruption provides an active defense against UAS threats, these defense mechanisms are wrought with unknown risks. Jamming defense measures should not be employed without a clear identification of the UAS platform and a knowledge of expected system responses to lost navigation or control links.

Destruction. Destructive defense measures are employed with the sole purpose of eradicating a threat UAS platform. This defense mechanism can be implemented using a wide variety of means including projectile weapons, directed energy weapons, guided munitions, and interception. Destructive weapons should be used as a last resort, as the airborne destruction of a UAS threat can potentially cause collateral damage. In the event a threat UAS platform is damaged or destroyed, collateral damage can be incurred by falling debris, falling weapon projectiles, field of fire obstructions, scattered NBC elements (if equipped) and other related factors. Gallagher (2013) agrees, citing, "Just shooting drones in a crowded environment could cause more damage than the drones themselves" (p. 1).

Projectile weapons are perhaps the most obvious form of destructive defense. Firearms can certainly damage or destroy a small UAS platform. Turkish

police used firearms to destroy a small quadcopter overviewing protests in Istanbul in 2013; and, in a posted video, the drone can be seen being struck by bullet and falling to the ground (Estes, 2013). It is notable that during this shooting, the UAS could be seen operating at low altitude. Furthermore, the video revealed tall obstacles and buildings present in near proximity to the UAS, however, it is unknown if the engagement caused any collateral damage.

In September 2014, a New Jersey man discharged a shotgun at an airborne drone, which caused the operator to lose control (Back, 2014). A similar incident occurred in Kentucky in July 2015, in which a homeowner used a shotgun to down a drone flying at 250' over his home (Chappell, 2015). In Gallagher (2015) Klaas Jan de Kraker and Rob van de Wiel suggest, "Rapid fire guns with suitable ammunition and machine guns are considered as very effective means for neutralizing mini UAVs," but add "hard kill systems could generate collateral damage." (p. 1). A possible projectile variant in lieu of firearms is the use of anti-helicopter weapons that spread shrapnel or pointed projectiles such as flechettes (Chuter, 2015).

Projectile weapons can increase lethality against small UAS systems when a guidance system is added. So-called smart weapons allow for tracking systems to provide updated telemetry, course correction, and detonation commands to the projectile warhead (Prigg, 2015). The U.S. Army is currently testing a new system dubbed the Extended Area Protection and Survivability Integrated Demonstration, where a truck-mounted 50mm cannon fires a smart projectile carrying a directional fragmentary-explosive (Prigg, 2015). The projectile would receive in-flight course updates and detonation commands from mobile fire control computer (Prigg, 2015). While guided surface-to-air weapons such as Patriot missiles, MANPADS, other similar systems can theoretically be used against UAS systems, such systems are largely impractical in urban environments (Gettinger, 2015).

De Kraker and van de Weil advocate directed energy weapons such as lasers or microwave systems to destroy UAS threats, citing such systems yield a lower risk to people and property than projectile weapons (Gallagher, 2013). Some experts disagree, however, Chuter (2015) states, "Lasers are an expensive way of solving the problem…part of the problem is that blowing up, or in the case of a laser, burning, even a small UAV in urban areas or over critical infrastructure may be unacceptable" (p. 1). According to Popular Mechanics (2009), lasers have limited application against UAS threats, because lasers are susceptible to atmospheric refraction, cloud cover, and must maintain contact with the platform to overheat the targeted flight component. While this developmental technology

minimizes the collateral damage caused by an errant projectile weapon, it fails to eliminate the hazards caused by falling debris.

The final proposal in UAS threat destruction lies in the employment of unmanned counter-UAS platforms. This methodology of UAS defense is still largely speculative (Gettinger, 2015). Some suggested implementations of this approach involve defending UAS platforms capturing threat UAS craft with nets or other impediments (Gettinger, 2015). While this suggested defense is intriguing, the development necessary to make it a reliable and pragmatic defense measure make this little more than a hypothetical possibility at this point.

Conclusions

UAS Threats

UAS platforms can be used by terrorist or criminal elements for several purposes. In their unmodified state, UAS platforms can create a public nuisance, interfere with aircraft or airspace operations, collect information that can be utilized for illicit purposes, and be employed as a kinetic weapons. As a transportation device, a UAS device can be used to smuggle illegal substances into forbidden areas by bypassing traditional security measures. Finally, UAS platforms can be weaponized with non-lethal, projectile, improvised explosives, weapons of mass destruction, or even commit digital attacks.

UAS technology represents a new tool that can be used for either good or ill. While it is likely that most UAS platforms will be employed for legitimate and productive purposes, one cannot ignore the potential for illicit exploitation of such capabilities. The wide availability and low cost of UAS platforms make them an attractive purchase for terrorists or criminals to add aerial capability to illicit activities. Moreover, the use of unmanned systems adds a new layer of complication in the investigative process, as automation and increased standoff distances provide perpetrators a shield of anonymity. In the event of a plot failure, this anonymity reduces the risk of capture, leaving terrorists or criminals "free to strike another day."

The threat is real. Terrorists are adept at using new technology to their advantage and purpose. UAS have been modified to carry explosives, automatic weapons, and non-lethal weapons. Criminals have used UAS to further their enterprises. The threat is not exaggerated or hyped. Homeland security and law enforcement officials have taken notice of the real threats posed by UAS platforms. The potential malicious uses of UAS platforms are limited only by the imagination

of the user. The many documented incidents of terrorist and criminal uses of UAS both domestically and abroad should be a red flag to officials to act and employ mitigation strategies against this evolving threat.

Evaluation of UAS Defenses

An evaluation of the collected data suggest several methods of defending against UAS threats. Measures such as export controls, critical component monitoring, and intelligence collection efforts can preempt a UAS threat before it can be employed. Similarly, deterrent efforts such as criminal penalties, civil torts, law enforcement presence, or established no-fly zones can potentially dissuade perpetrators from illicitly using UAS platforms. The use of random security measures and careful selection of locations that includes natural or man-made obstructions, can effectively deny UAS threat operations. The inclusion of geo-fencing protections in commercially-sold UAS platforms can also deny UAS platforms from performing illicit operations in certain geographical areas. If unimpeded by previous defense measures, rapid detection, identification and tracking of the UAS threat is required to effectively employ active, counter-UAS defenses. With modification, active sensor systems have shown promise in detecting UAS threats. With additional development and testing, it is highly likely that passive sensors will also become viable detectors for UAS threats. The final defense against UAS threats include interruption or destruction of the UAS craft. Interruption activities such as jamming, spoofing, or operator intervention are possible, but increase the risk of creating unintentional or unanticipated side effects. Alternatively, UAS threat destruction methods appear to be effective, however, are likely to cause collateral damage, particularly in urban environments.

While it may be tempting to focus UAS defense efforts on the establishment of new interruption or destructive systems, the most efficient and cost-effective means of defense lie in prevention, deterrence, and denial. While entrepreneurial efforts are currently underway to develop new technologies to detect, interrupt, or destroy UAS platforms, the industry should not be so quick to dismiss existing resources. A repurposing of existing technology such as radar and select passive detection technology shows great promise in addressing the challenges of UAS detection, identification, and tracking.

Similarly, a shotgun seems equally up to the task of engaging certain threat UAS platforms as more expensive developmental weapon systems. The selection and employment of defensive systems should be based on the threat UAS capabilities, coupled with an evaluation of the risk, including risks to non-participating groups. While the myriad of traditional and novel UAS defenses have

demonstrated the ability to negate an airborne UAS threat, aerial engagement may not always be the most appropriate response. While the initial temptation may be to immediately destroy a potential UAS threat, careful consideration must be given to the potential for collateral damage caused both by the engaging weapon system and falling UAS debris. In such cases, the consequences of an in appropriate defensive response could create a more severe catastrophe than the offending UAS platform.

Perhaps the greatest security lesson learned is that UAS technologies must be included in the security assessments. The true threat lies not in what is known about malicious UAS uses, but rather in what is unknown. UAS platforms represent a novel and largely unpredictable threat with many potential asymmetric terroristic and criminal applications. In the same manner that the 9/11 changed attitudes about the potential threats of civil aviation, the misuse of unmanned systems has the potential to cause similar catastrophic results. Until now, the security community has been fortunate that recent newsworthy events caused by UAS platforms at the Merkel campaign fundraiser, White House, and Japanese Prime Minister's office have all had relatively benign impact. Such situations must serve as a clear wakeup call for the industry to acknowledge the security risks presented by UAS technology and prepare defenses against illicit UAS applications. Security personnel must now remain vigilant to the skies and keep UAS threats in their cross-check.

References

Affidavit of Special Agent Gary S. Cacace (2011). *Homeland Security Today U.S.* Retrieved from http://hstoday.us/fileadmin/PDFs/11-4270-aff.pdf

Allen, P. (2003). Teenager is killed after she is hit by model plane. *Daily Mail*. Retrieved from http://www.dailymail.co.uk/news/article-177139/Teenager-killed-hit-model-plane.html

Aviation medicine: Principles & problems of vision. (n.d.) *Pilotfriend.* Retrieved from http://www.pilotfriend.com/aeromed/medical/vision_and_flying.htm

Back, S. (2014). New Jersey man accused of shooting down neighbor's remote control drone. *CBC Philly.* Retrieved from http://philadelphia.cbslocal.com/2014/09/30/new-jersey-man-accused-of-shooting-down-neighbors-remote-control-drone/

Barnum, S. Gegick, M., & Michael, CC. (2005). *Defense in depth.* Retrieved from https://buildsecurityin.uscert.gov/articles/knowledge/principles/defense-in-depth

Beaudoin, L., Gademer, A., Avanthey, L., Germain, V., & Vittori, V. (2015). Potential threats of UAS swarms and the countermeasure's need. *European Conference on Information Warfare and Security (ECIW), 2011*, Tallinn, Estonia. Retrieved from https://hal.archives-ouvertes.fr/hal 01132236/document

Brandon, A. (2014). FBI: Man plotted to fly drone-like toy planes with bombs into school. *CBS News.* Retrieved from http://www.cbsnews.com/news/fbi-man-in-connecticut-plotted-to-fly-drone-like-toy-planes-with-bombs-into-school/

Card, B. (2014). *The commercialization of UAVs: How terrorists will be able to utilize UAVs to attack the United States* (unpublished thesis). The University of Texas at El Paso, El Paso, TX. Retrieved from http://academics.utep.edu/Portals/4302/Student%20research/Capstone%20projects/Card_Commercialization%20of%20UAVs.pdf

Central Intelligence Agency (n.d.). *Terrorist CBRN: Materials and effects.* Retrieved from https://www.cia.gov/library/reports/general-reports-1/terrorist_cbrn/terrorist_CBRN.htm

Chambers, J. (2015). *Midnight drone worries Del Mar residents*. Retrieved from http://fox5sandiego.com/2015/05/20/midnight-drone-worries-del-mar-residents/

Chappell, B. (2015). *Dispute emerges over drone shot down by Kentucky man*. Retrieved from http://www.npr.org/sections/thetwo-way/2015/07/31/428156902/dispute-emerges-over-drone-shot-down-by-kentucky-man

Chiaet, J. (2013). Drone pilot challenges FAA on commercial flying ban. *Scientific American.* Retrieved from http://www.scientificamerican.com/article/drone-pilot-challenges-faa-commercial-flying-ban/

Chuter, A. (2015). Mini drones spark heightened interest in countering threat. *Defense News.* Retrieved from http://www.defensenews.com/story/defense/air-space/strike/2015/06/20/small-drones-raise-interest-in-combating-threat/28977373/

Crime. (n.d.) In *Merriam-Webster Online.* Retrieved from http://www.merriam-webster.com/dictionary/crime

Davis, K. (2015). Two plead guilty in border drug smuggling by drone. *Los Angeles Times.* Retrieved from http://www.latimes.com/local/california/la-me-drone-drugs-20150813-story.html

Davis, L.E., McNerney, M.J., Chow, J., Hamilton, T., Harting, S., & Byman, D. (2014). *Armed and dangerous: UAVs and U.S. security.* Santa Monica, CA: Rand Publishing.

DHS warns local law enforcement to watch for drones used by terrorists, criminals. (2015). *Homeland Security News Wire.* Retrieved from http://www.homelandsecuritynewswire.com/dr20150803-dhs-warns-local-law-enforcement-to-watch-for-drones-used-by-terrorists-criminals

Dolnik, A. (2007). *Understanding terrorist innovation: Technology, tactics and global trends.* New York: Routledge Press.

Drone 'containing radiation' lands on roof of Japanese PM's office. (2015). *The Guardian.* Retrieved from http://www.theguardian.com/world/2015/apr/22/drone-with-radiation-sign-lands-on-roof-of-japanese-prime-ministers-office

Drone laced with radiation lands on Japan PM's office. (2015, April 22). *Aljazeera.* Retrieved from http://www.aljazeera.com/news/2015/04/drone-laced-radiation-lands-japan-pm-office-150422185726666.html

FBI: Man plotted to fly drone-like toy planes with bombs into school. (2014). *CBS News.* Retrieved from http://www.cbsnews.com/news/fbi-man-in-connecticut-plotted-to-fly-drone-like-toy-planes-with-bombs-into-school/

Estes, A.C. (2013). Watch police shoot down a drone flying over Istanbul. *Gizmodo.* Retrieved from http://gizmodo.com/watch-police-shoot-down-a-drone-flying-over-istanbul-513228306

Federal Aviation Administration. (2015). Overview of small UAS notice of proposed rulemaking. Washington D.C: U.S. Government Press. Retrieved from https://www.faa.gov/regulations_policies/rulemaking/media/021515_sUAS_Summary.pdf

Feds: Massachusetts man planned to blow up Pentagon. (2011). *CBS News.* Retrieved from http://www.cbsnews.com/news/feds-mass-man-planned-to-blow-up-pentagon/

Gallagher, S. (2013). German chancellor's drone "attack" shows the threat of weaponized UAVs. *ARS Technica.* Retrieved from http://arstechnica.com/information-technology/2013/09/german-chancellors-drone-attack-shows-the-threat-of-weaponized-uavs/

Gettinger, D. (2015). Domestic drone threats. *Bard College Center for the Study of the Drone.* Bard College: Annandale-On-Hudson, NY. Retrieved from http://dronecenter.bard.edu/what-you-need-to-know-about-domestic-drone-threats/

Gittleson, K. (2014). Data-stealing snoopy drone unveiled at black hat. *BBC News.* Retrieved from http://www.bbc.com/news/technology-26762198

Gosztola, K. (2012). And the 'terrorists might use drones' myth was born. *Shadowproof.* Retrieved from http://shadowproof.com/2012/03/27/and-the-terrorists-might-use-drones-myth-was-born/

Hoenig, M. (2014). Hezbollah and the use of drones as a weapon of terrorism. *Federation of American Scientists.* Retrieved from http://fas.org/pir-pubs/hezbollah-use-drones-weapon-terrorism/

Homeland Security News Wire. (2015). *DHS warns local law enforcement to watch for drones used by terrorists, criminals.* Retrieved from http://www.homelandsecuritynewswire.com/dr20150803-dhs-warns-local-law-enforcement-to-watch-for-drones-used-by-terrorists-criminals

Iraq uncovers al-Qaeda 'chemical weapons plot'. (2013). *BBC News.* Retrieved from http://www.bbc.com/news/world-middle-east-22742201

It's a bird, it's a plane, no…it's a drone. (2015). *Security Info Watch.* Retrieved from http://www.securityinfowatch.com/article/12081056/drone-labs-technology-helps-users-mitigate-security-threats-posed-by-uavs

Jackson, B.A., Frelinger, D.R., Lostumbo, M.J., & Button, R.W. (2008). *Evaluating novel threats to the homeland.* Santa Monica, CA: Rand National Defense Research Institute. Retrieved from http://www.rand.org/content/dam/rand/pubs/monographs/2008/RAND_MG626.pdf

Kawano, L. (2015). Drone hovers outside Hawaii Kai woman's bedroom, but no crime was committed. *Hawaii News Now.* Retrieved from http://www.hawaiinewsnow.com/story/29765309/drone-hovers-outside-hawaii-kai-womans-bedroom-but-no-crime-was-committed

Kerley, D. (2015). Gun firing drone subject of federal investigation. *ABC News.* Retrieved from http://abcnews.go.com/US/gun-firing-drone-subject-federal-investigation/story?id=32585072

Kersey, B. (2012). New police drones could be equipped with non-lethal weapons. *Slash Gear.* Retrieved from http://www.slashgear.com/new-police-drones-could-be-equipped-with-non-lethal-weapons-12217918/

Kimery, A. (2015). The threat of small, manned, unmanned aircraft in Washington airspace has long been known. *Homeland Security Today U.S.* Retrieved from http://www.hstoday.us/columns/the-kimery-report/blog/the-threat-of-small-manned-unmanned-aircraft-in-washington-airspace-has-long-been-known/9c6177043dadfc7a5f064f89a435fc93.html

Koretsky, G.M., Nicoll, J.F., & Taylor, M.S. (2013). A tutorial on electro-optical/infrared (EO/IR) theory and systems (IDA Doc D-4642). Alexandria, VA: Institute for Defense Analysis. Retrieved from https://www.ida.org/~/media/Corporate/Files/Publications/IDA_Documents/SED/ida-document-d-4642.pdf

Lele, A., & Mishra, A. (2009). Aerial terrorism and the threat from unmanned aerial vehicles. *Journal of Defense Studies, 3(3), 54-65.* Retrieved from http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=8&ved=0CFMQFjAHahUKEwij7Jep34LHAhVH2B4KHa4hB1Y&url=http%3A%2F%2Fwww.idsa.in%2Fsystem%2Ffiles%2Fjds_3_3_alele_amishra.pdf&ei=nAm6VaOuFcewe67DnLAF&usg=AFQjCNFpQ4PxTxWEose6HM3K8smgDq80_w&bvm=bv.99028883,d.dmo

Levine, M. (2015). Sensitive U.S. sites vulnerable to drone attach, DHS assessment says. *ABC News.* Retrieved from http://abcnews.go.com/US/sensitive-us-sites-vulnerable-drone-attack-dhs-assessment/story?id=32825708&cid=skygrid

Light. (n.d.). *Sparkfun.* Retrieved from https://learn.sparkfun.com/tutorials/light/infrared-light

Lincoln, B. (2013). Thermal vs near infrared. *Beneath the Waves.* Retrieved From http://www.beneaththewaves.net/Photography/Thermal_versus_Near_Infrared.html

Lincoln, M. (2015). Drone operator chased, tased by ranger at Hawaii Volcanoes National Park. *Hawaii News Now.* Retrieved from http://www.hawaiinewsnow.com/story/28914009/drone-operator-chased-tased-by-ranger-at-hawaii-volcanoes-national-park

Martinez, M. (2015). Above spectacular wildfire on freeway rises new scourge: Drones. *CNN.* Retrieved from http://www.cnn.com/2015/07/18/us/california-freeway-fire/

Model airplanes a new terrorist weapon: Experts say they pose little threat. (2011). *Fox News.* Retrieved from http://www.foxnews.com/us/2011/09/29/could-model-airplanes-be-next-terrorist-weapon/

Mystery drone damages Hialeah home. (2015). *CBS Miami.* Retrieved from http://miami.cbslocal.com/2015/03/01/mystery-drone-damages-hialeah-home/

Naim, M. (2013). The next global security threat: Explosive devices on small drones. *The Atlantic.* Retrieved from http://www.theatlantic.com/international/archive/2013/10/the-next-global-security-threat-explosive-devices-on-small-drones/280953/

National Commission on Terrorists Attacks upon the United States., Kean, T.H., & Hamilton, L. (2004). *The 9/11 Commission report: Final report of the national commission on terrorist attacks upon the United States.* Washington D.C.: National Commission on Terrorist Attacks upon the United States. Retrieved from http://www.9-11commission.gov/

Nicas, J. (2015). Drone ban: corporations skirt rules. *The Wall Street Journal.* Retrieved from http://www.wsj.com/articles/drone-ban-corporations-skirt-rules-1424373939

NYPD scanning the sky for new terrorism threat. (2014). *CBS News.* Retrieved from http://www.cbsnews.com/news/drone-terrorism-threat-is-serious-concern-for-nypd/

Petocz, A., & Newbery, G. (2010). On conceptual analysis as the primary qualitative approach to statistics education research in psychology. *Statistics Education Research Journal, 9(2), 123-145.* Retrieved from http://iase-web.org/documents/SERJ/SERJ9(2)_Petocz_Newbery.pdf

Prigg, M. (2015). The anti-DRONE missile: US Army fires steerable smart shells that can bring down UAVs from miles away. *Daily Mail.* Retrieved from http://www.dailymail.co.uk/sciencetech/article-3176712/The-anti-DRONE-missile-Army-firessmart-shells-bring-UAVS.html

Quan, D. (2014). RCMP dears terrorists could use off-the-shelf drones to attack VIPs, internal documents reveal. *National Post.* Retrieved from http://news.nationalpost.com/news/canada/rcmp-fears-terrorists-could-use-off-the-shelf-drones-to-attack-vips-2

Quantum Technology Sciences. (2015). Detecting & tracking drones. Cocoa Beach, FL: Author. Retrieved from http://www.qtsi.com/wp-content/uploads/2015/07/Quantum_AppNotes_Drones.pdf

Rapoport, D.C. (2008). Before the bombs there were mobs: American experiences with terror. *Terrorism & Political Violence,* 20(2) 167-194. doi: 10.1080/09546550701856045

Rawlinson, K. (2015). Man comes forward after woman knocked out by drone. *BBC News.* Retrieved from http://www.bbc.com/news/technology-33345417

Schmidt, M.S. (2015). Airmail via drone is vexing for prisons. *New York Times.* Retrieved from http://www.nytimes.com/2015/04/23/us/drones-smuggle-contraband-over-prison-walls.html?_r=0

Shear, M., & Schmidt, M. (2015). White House drone crash described as a U.S. worker's drunken lark. *NY Times.* Retrieved from http://www.nytimes.com/2015/01/28/us/white-house-drone.html?_r=0

Sofge, E. (2009). Killer lasers work, but are they the best defense against UAVs. *Popular Mechanics.* Retrieved from http://www.popularmechanics.com/military/a12250/4302301/

Soloman, E.D. (2014). Part two: Unmanned aircraft systems ("UAS") – aka drones legal issues: Where are we headed. *Blank & Rome*. Retrieved from http://www.blankrome.com/index.cfm?contentID=37&itemID=3338

UAVs at the White House: An Infrared solution to detect potentially dangerous drones. (2015). *PRWEB.* Retrieved from http://www.prweb.com/releases/2015/02/prweb12484325.htm

U.S. Army Training & Doctrine Command. (2003). *A military guide to terrorism in the twenty-first century (TRADOC DSCINT Handbook).* Leavenworth, KS: U.S. Army HQ TRADOC. Retrieved from http://smallwarsjournal.com/documents/terrorismhandbook.pdf

U.S. Department of State (2006). *National strategy for combating terrorism.* Retrieved from http://2001-2009.state.gov/s/ct/rls/wh/71803.htm

U.S. Government Accountability Office. (2012). Nonproliferation: Agencies could improve information sharing and end-use monitoring on unmanned aerial vehicle exports (GAO-12-536). Washington, DC: U.S. Government Printing Office. Retrieved from http://www.gao.gov/assets/600/593131.pdf

U.S. Government Publishing Office. (2012). FAA modernization and reform act of 2012: Conference report to accompany H.R. 658. Washington D.C.: U.S. Government Publishing Office. Retrieved from http://www.gpo.gov/fdsys/pkg/CRPT-112hrpt381/pdf/CRPT-112hrpt381.pdf

Versprille, A. (2015). Small off-the-shelf drones causing alarm in security circles. *National Defense.* Retrieved from http://www.nationaldefensemagazine.org/archive/2015/May/pages/SmallOfftheShelfDronesCausingAlarmInSecurityCircles.aspx

Viegas, J. (2015). Drones bothers bears, nearly triggering heart attacks. *Discovery.* Retrieved from http://www.discovery.com/dscovrd/tech/drones-bother-bears-nearly-triggering-heart-attacks/

Whitlock, C. (2014). Near collisions between drones, airliners surge, new FAA reports show. *Washington Post.* Retrieved from https://www.washingtonpost.com/world/national-security/near-collisions-between-drones-airliners-surge-new-faa-reports-show/2014/11/26/9a8c1716-758c-11e4-bd1b-03009bd3e984_story.html

Wilkinson, P. (2012). *Technology and terrorism.* New York: Routledge Publishing.

Wright, V. (2010). *Deterrence in criminal justice: Evaluating certainty vs. severity of punishment.* Washington DC: The Sentencing Project. Retrieved from http://www.sentencingproject.org/doc/Deterrence%20Briefing%20.pdf

Ybarra, J. (2015). Drone almost hits Skylife helicopter in Fresno. *ABC Action News.* Retrieved from http://abc30.com/news/officials-drone-almost-hits-skylife-helicopter-in-fresno/925394/