

# **Examining Unmanned Aerial System Threats: A Conceptual Analysis**



**Ryan J. Wallace, Ed.D. & Jon M. Loffi, Ed.D.  
Polk State College & Oklahoma State University**

# Statement of the Problem



Law enforcement, security agencies, and other public service entities have demonstrated they are ill-prepared to combat ever-growing UAS threats. The novelty of UAS systems, potential UAS threats are poorly understood by law enforcement and security personnel. There is currently no cohesive defense strategy in which to systematically counter UAS threats.



# Research Questions



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

- 1.) How are UAS systems used for illegal purposes or terrorism?
- 2.) What current defense methods exist to mitigate UAS Threats?



# Review of Literature



The “review of the literature” included:

- **Academic Research Articles**
- **Unclassified Government Reports**
- **Open-Source News Articles**

# Theoretical Construct



## Constructionism

➔ Symbolic Interactionism

➔ Applied Research

➔ Conceptual Analysis



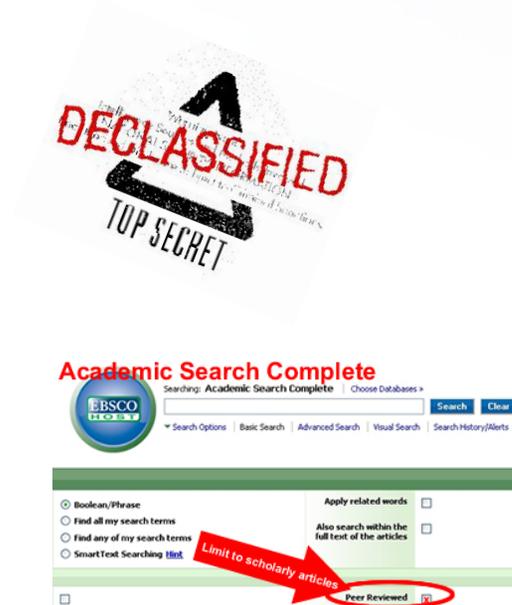
# Examining Unmanned Aerial System Threats

## Findings



Researchers evaluated 68 academic studies, unclassified government reports, and news articles.

An analysis of the recurring conceptual themes yielded the following results:



# Examining Unmanned Aerial System Threats

## Findings



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).

# Examining Unmanned Aerial System Threats

## Findings



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.



# Examining Unmanned Aerial System Threats

## Findings



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” (Homeland Security News Wire, para. 5).



[https://www.youtube.com/watch?v=UujEjjn\\_Kb8](https://www.youtube.com/watch?v=UujEjjn_Kb8)

# Examining Unmanned Aerial System Threats



## Findings

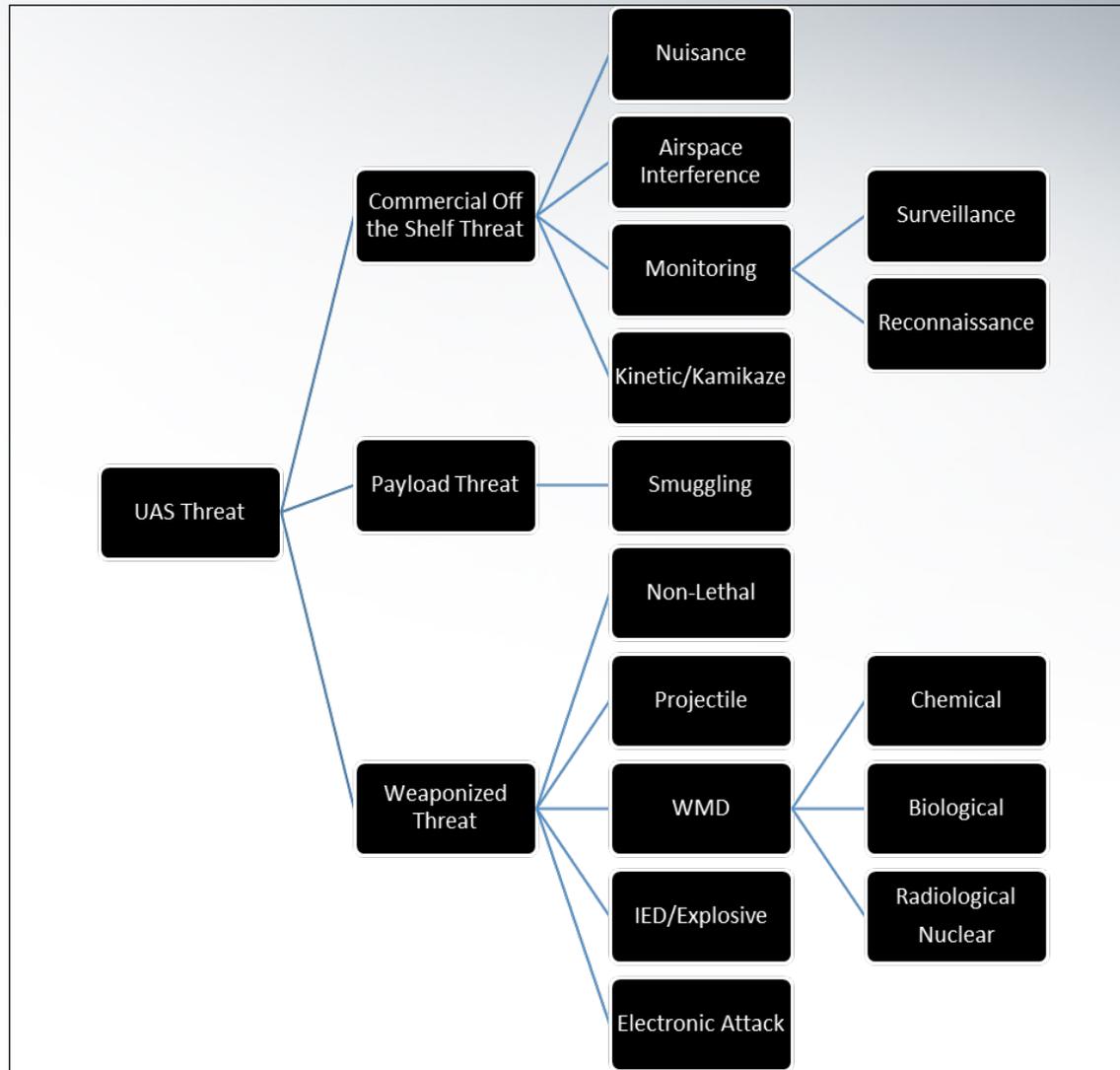


Figure 1. Concepts of Illicit UAS Use.

# Examining Unmanned Aerial System Threats

## Findings



### Commercial off the Shelf Threat

***Nuisance*** - The most benign illicit use of UAS platforms is the interference they create for the general public.

***Monitoring Threat*** - One of the most notable concerns about UAS platforms stems from their potential to silently monitor and record their surroundings.

***Surveillance*** - UAS platforms, however, change the dynamic of aerial surveillance, making it accessible and affordable for almost anyone.

***Reconnaissance*** - While similar to surveillance, reconnaissance activities take a further step toward illicit behavior.

# Examining Unmanned Aerial System Threats

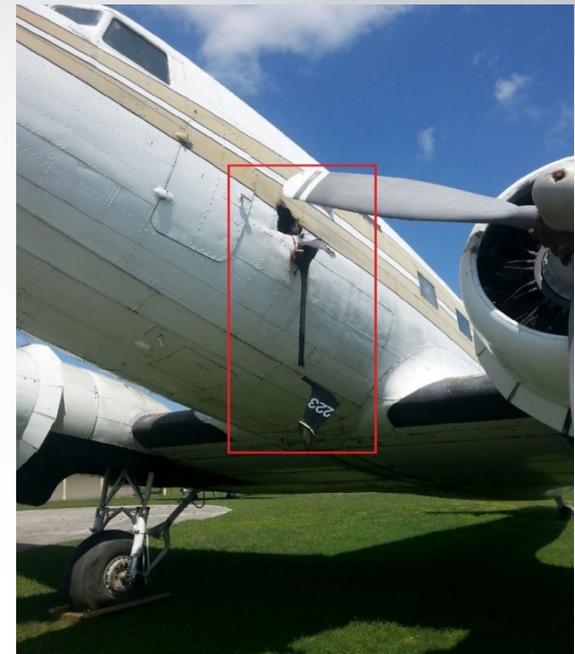
## Findings



### Commercial off the Shelf Threat

*Airspace Interference* - UAS platforms present a genuine threat to safe airspace utilization.

*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.



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

# Examining Unmanned Aerial System Threats

## Findings



### Commercial off the Shelf Threat

***Payload Threat/Smuggling*** - UAS platforms can also be exploited as a transportation mechanism for illegal contraband or cargo.

***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.

***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.

# Examining Unmanned Aerial System Threats

## Findings



### Commercial off the Shelf Threat

***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.

***IED/Explosive*** - The use of drones as a delivery system for improvised explosive devices (IEDs), incendiary devices, or other combustibles remains high.

# Examining Unmanned Aerial System Threats

## Findings



### Commercial off the Shelf Threat

***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.

***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.

# Examining Unmanned Aerial System Threats

## Findings



### 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.

*Broad Defense Strategies* - Prevention, Deterrence, Denial, and Detection. A fifth layer of defense with diverging subcategories of Interruption and Destruction.

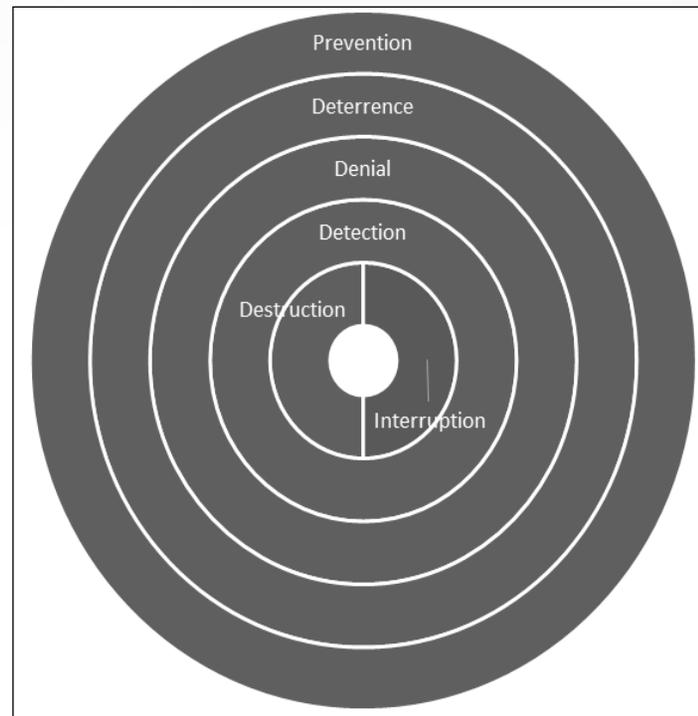
# Examining Unmanned Aerial System Threats

## Findings



### UAS Defense Concepts

***Organizing the Data*** - a conceptual defense in depth model for UAS threats yielded a five-layer, concentric circle of defense.



# Examining Unmanned Aerial System Threats

## Findings



### UAS Defense Concepts

***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.



# Examining Unmanned Aerial System Threats

## Findings



### UAS Defense Concepts

According to Lele & 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).

# Examining Unmanned Aerial System Threats

## Findings



### UAS Defense Concepts

***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. Two basic mechanisms:

- 1) legislation to create, establish, and fund various formal UAS defense measures by equipping agencies to develop and deploy a concerted UAS defense.
- 2) Legislation to establish civil and criminal penalties to deter illegal use of UAS.

# Examining Unmanned Aerial System Threats

## Findings



### UAS Defense Concepts

***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.

***Detection*** - In the event passive defense mechanisms fail to prevent, deter, or deny a UAS threat, active defense mechanisms must be employed.

***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.

***Passive detection.*** Use sensors that sample the electromagnetic spectrum within certain wavelengths to determine the presence of UAS-characteristic signals.

# Examining Unmanned Aerial System Threats

## Findings



### UAS Defense Concepts

***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.

***Interruption*** - Interruption defenses are active measures designed to avert a threat UAS from carrying out an adverse action.

**Three methods** – Operator interruption, jamming, and spoofing

# Examining Unmanned Aerial System Threats

## Findings



### UAS Defense Concepts

***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.

# Examining Unmanned Aerial System Threats



## 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 be utilized for illicit purposes, and be employed as a kinetic weapons.

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.

# Examining Unmanned Aerial System Threats



## Conclusions

### UAS Threats

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.

# Examining Unmanned Aerial System Threats



## Conclusions

### Evaluation of UAS Defenses

An evaluation of the collected data suggest several methods of defending against UAS threats:

- Export Controls
- Critical Component Monitoring
- Intelligence Collection

#### Deterrent Efforts:

- Criminal Penalties
- Civil Torts
- Law Enforcement Presence
- Established no-fly zones

The most efficient and cost-effective means of defense are couched in prevention, deterrence, and denial. 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.

## Examining Unmanned Aerial System Threats



### Final Remarks

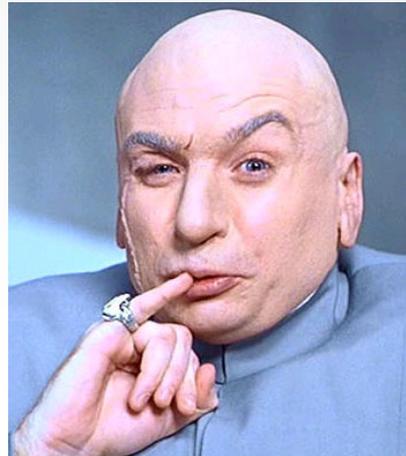
Perhaps the greatest security lesson learned is that UAS technologies must be included in the security assessments. The true threat lies not in what is known about malicious UAS uses, but rather in what is unknown. UAS platforms represent a novel and largely unpredictable threat with many potential asymmetric 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.

## Examining Unmanned Aerial System Threats



### Questions & Discussion



*This paper can be found in the International Journal  
of Aviation, Aeronautics, and Aerospace –  
<http://commons.erau.edu/ijaaa/>*