NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

COUNTERING UNMANNED AIRCRAFT SYSTEMS

by

Jason Knight

December 2019

Co-Advisors: John W. Rollins (contractor)
Erik J. Dahl

Approved for public release. Distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE	Form Approved OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC 20503.

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE December 2019	3. REPORT TYPE AND DATES COVERED Master's thesis

4. TITLE AND SUBTITLE COUNTERING UNMANNED AIRCRAFT SYSTEMS	5. FUNDING NUMBERS
6. AUTHOR(S) Jason Knight	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT	12b. DISTRIBUTION CODE
Approved for public release. Distribution is unlimited.	A

13. ABSTRACT (maximum 200 words)

Since 2015, the unmanned aircraft system (UAS) market has exploded; once an exclusively military domain, it is now also aimed at the private and public sectors. As a consequence, the availability of inexpensive UAS platforms that can be weaponized or outfitted with surveillance equipment has also become an attractive tool to terrorists and criminals. This thesis examines the question, How can local law enforcement protect their communities from UASs operated by careless hobbyists, criminals, and other nefarious actors, such as foreign and domestic terrorists? This thesis assessed the risk UASs pose to public safety, examined counter-UAS (C-UAS) technology currently available, and explored the limitations of C-UAS technology when deployed over urban areas. The thesis found that although the threat UAS platforms pose to urban areas is credible, C-UAS measures are available that local law enforcement can use to mitigate the risk. However, the thesis found that some forms of C-UAS technology have limitations when deployed over urban areas. In conclusion, the thesis recommends that local law enforcement consider UAS threats when conducting jurisdictional risk assessments, explore C-UAS technology and its limitations before procurement and implementation, and develop a C-UAS strategy that ensures measures taken are necessary, effective, and appropriate. The thesis provides a decision matrix to assist local law enforcement in their efforts to develop a C-UAS strategy.

14. SUBJECT TERMS	15. NUMBER OF PAGES
drone, UAV, UAS, unmanned aerial system, unmanned aircraft system, unmanned aerial vehicle, unmanned aircraft vehicle, counter UAS, counter UAV, counter drone, state, local	107
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UU

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

COUNTERING UNMANNED AIRCRAFT SYSTEMS

Jason Knight
Police Lieutenant, Deputy Emergency Manager/Homeland Security Coordinator,
Oklahoma City Police Department
BS, University of Central Oklahoma, 1995

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)

from the

NAVAL POSTGRADUATE SCHOOL
December 2019

Approved by: John W. Rollins
Co-Advisor

Erik J. Dahl
Co-Advisor

Erik J. Dahl
Associate Professor, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Since 2015, the unmanned aircraft system (UAS) market has exploded; once an exclusively military domain, it is now also aimed at the private and public sectors. As a consequence, the availability of inexpensive UAS platforms that can be weaponized or outfitted with surveillance equipment has also become an attractive tool to terrorists and criminals. This thesis examines the question, How can local law enforcement protect their communities from UASs operated by careless hobbyists, criminals, and other nefarious actors, such as foreign and domestic terrorists? This thesis assessed the risk UASs pose to public safety, examined counter-UAS (C-UAS) technology currently available, and explored the limitations of C-UAS technology when deployed over urban areas. The thesis found that although the threat UAS platforms pose to urban areas is credible, C-UAS measures are available that local law enforcement can use to mitigate the risk. However, the thesis found that some forms of C-UAS technology have limitations when deployed over urban areas. In conclusion, the thesis recommends that local law enforcement consider UAS threats when conducting jurisdictional risk assessments, explore C-UAS technology and its limitations before procurement and implementation, and develop a C-UAS strategy that ensures measures taken are necessary, effective, and appropriate. The thesis provides a decision matrix to assist local law enforcement in their efforts to develop a C-UAS strategy.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I. INTRODUCTION....1
A. LITERATURE REVIEW....2
1. Exploring UAS Capabilities, Limitations, and Risks....3
2. Exploring C-UAS Technologies for Hometown Security....7
3. The Case for a State and Local C-UAS Strategy....9
B. RESEARCH METHODOLOGY....12
C. CHAPTER OUTLINE....13

II. THE EVOLVING UAS THREAT TO HOMETOWN SECURITY....15
A. CARELESS AND MALEVOLENT UAS OPERATIONS....15
1. Careless UAS Operations....16
2. Malevolent UAS Operations....22
B. UAS TARGETS AND THEIR VULNERABILITIES....30
1. Targets....30
2. Target Vulnerabilities....34
C. SUMMARY....36

III. ACTIVE AND PASSIVE C-UAS MEASURES....39
A. PASSIVE COUNTERMEASURES....40
B. ACTIVE COUNTERMEASURES....44
C. SUMMARY....51

IV. IMPLEMENTATION OF C-UAS TECHNOLOGY....53
A. LIMITATIONS OF CURRENT C-UAS TECHNOLOGY....53
B. UNINTENDED CONSEQUENCES OF C-UAS MISSIONS....59
C. SUMMARY....62

V. RECOMMENDATIONS AND CLOSING THOUGHTS....65
A. RECOMMENDATIONS....65
1. Local Law Enforcement Risk Assessments Should Identify Gaps in Capabilities to Detect, Track, Interdict, and Disrupt Careless and Malevolent UAS Operations....65
2. Local Law Enforcement Should Explore Their Options to Bolster Capabilities to Detect, Track, Interdict, and Disrupt Malevolent and Careless UAS Platforms....66
3. Local Law Enforcement Should Understand that C-UAS Measures Have Limitations; therefore, the Deployment of

Such Measures Must Be Necessary, Effective, and Appropriate to Safely Counter the Threat 67
B. CLOSING THOUGHTS 69
1. Limited Scope of Paper 69
2. Future Research Opportunities 70

LIST OF REFERENCES 71

INITIAL DISTRIBUTION LIST 85

LIST OF FIGURES

Figure 1. C-UAS Decision Matrix 69

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

Table 1. Passive C-UAS Technologies 43

Table 2. Active C-UAS Technologies 50

Table 3. Limitations of Passive C-UAS Technology.....58

Table 4. Limitations of Active C-UAS Technology.....59

Table 5. Unintended Consequences of C-UAS Missions 62

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ACLU	American Civil Liberties Union
AMA	Academy of Model Aeronautics
CIKR	critical infrastructure and key resources
C-UAS	Counter Unmanned Aircraft System
DHS	Department of Homeland Security
DHS S&T	Department of Homeland Security Science and Technology Directorate
DoD	Department of Defense
DOE	Department of Energy
DOJ	Department of Justice
EO	electro-optical
FAA	Federal Aviation Administration
FBI	Federal Bureau of Investigation
FOD	foreign object debris
GNSS	global navigation satellite system
GPS	global positioning system
GTFS	Ghoul Tool Full Spectrum
IACP	International Association of Chiefs of Police
IED	improvised explosive device
IR	infrared
ISIS	Islamic State in Iraq and Syria
NDAA	National Defense Authorization Act
NPS	Naval Postgraduate School
OKC	Oklahoma City
PERF	Police Executive Research Forum
RF	radio frequency
S&T	Science and Technology Directorate
U.K.	United Kingdom
U.S.	United States
UAS	unmanned aircraft system

UPS	United Parcel Service
WMD	weapon of mass destruction
WRWA	Will Rogers World Airport

EXECUTIVE SUMMARY

The January 2015 crash of a small quadcopter, also referred to as a drone, on the White House grounds not only prompted a lockdown but left many questioning the risks drones pose to public safety.[1] Although an apparent accident due to careless operation, the incident highlights the vulnerabilities of even the most secured infrastructure to an unmanned aircraft system (UAS), such as a drone.[2] Since 2015, the UAS market has exploded; once an exclusively military domain, it is now also aimed at hobbyists, and the private and public sectors for recreational or mission specific operations. As a consequence, the availability of current and forthcoming inexpensive UAS platforms that can be weaponized or outfitted with surveillance equipment have also become an attractive tool to terrorists and criminals with nefarious intentions. In 2018, Congress recognized the potential threat drones pose to homeland security and passed the National Defense Authorization Act (NDAA) extending limited active counter-UAS (C-UAS) authority to the Department of Defense and Department of Energy.[3] However, the authority granted by Congress to use counter-drone technologies did not include local law enforcement agencies. This exclusion, in addition to the lack of a unified C-UAS strategy, leaves local law enforcement oblivious to potential UAS risks that can cause U.S. cities to remain vulnerable to nefarious UAS operations.[4]

This thesis answers the question of: How can local law enforcement protect their communities from UASs operated by careless hobbyists, criminals, and other nefarious actors, such as foreign and domestic terrorists? To answer this question, this thesis first

---

[1] Jack Nicas, "Criminals, Terrorists Find Uses for Drones, Raising Concerns," *Wall Street Journal*, January 28, 2015, http://www.wsj.com/articles/criminals-terrorists-find-uses-for-drones-raising-concerns-1422494268.

[2] Alejandro Sanchez and Cameron McKibben, "Worst Case Scenario: The Criminal Use of Drones," *Council on Hemispheric Affairs*, 1, February 2, 2015, http://www.coha.org/worst-case-scenario-the-criminal-use-of-drones/.

[3] Jason Snead, John-Michael Seibler, and David Inserra, *Establishing a Legal Framework for Counter-Drone Technologies*, Backgrounder No. 3305 (Washington, DC: Heritage Foundation, 2018), 1, https://www.heritage.org/sites/default/files/2018-04/BG3305_1.pdf.

[4] Ryan J. Wallace and Jon M. Loffi, "Examining Unmanned Aerial System Threats & Defenses: A Conceptual Analysis," *International Journal of Aviation, Aeronautics, and Aerospace* 2, no. 4 (2015): 2, https://doi.org/10.15394/ijaaa.2015.1084.

assesses the risks UASs pose to public safety by analyzing the capabilities of UAS platforms and incidents of careless and malevolent UAS operations. Next, this thesis examines the C-UAS technology currently available and identifies both passive and active C-UAS measures that local law enforcement can deploy to enhance prevention and protection capabilities, such as detecting, tracking, interdicting, or disrupting a threatening UAS platform. Finally, this thesis researches the limitations of C-UAS technology to provide situational awareness of unintended consequences associated with deploying the measures over America's hometowns.

Although legislative challenges associated with granting active C-UAS authority were beyond the scope of this thesis, several options enabling local law enforcement to enhance their capabilities to detect and track careless and malevolent UAS operations were identified. This thesis provides three recommendations to assist local law enforcement efforts in developing a C-UAS strategy. First, the threat of careless and malevolent UAS operations exposes a growing risk to not only national security but also America's hometowns. Metropolitan areas across the nation are dependent on various systems, networks, and other assets critical to the local government's ability to serve and protect the public. Additionally, many cities across the homeland regularly plan and host various outdoor special events throughout the year for their communities. Examples include parades, athletic competitions, holiday celebrations, and other entertainment events. Local law enforcement plays an important role in ensuring critical infrastructure and planned events within their communities remain functional and resilient. Therefore, it is recommended that local law enforcement assess their community's critical infrastructure and other planned events for vulnerabilities to UAS platforms and develop prevention and protection strategies to address both careless and malevolent UAS operations. Second, local law enforcement should explore their options to bolster capabilities to detect, track, interdict, and disrupt malevolent and careless UAS platforms. In addition to traditional practices employed by local law enforcement to protect their communities, a number of countermeasures supported by advanced technology are available to enhance prevention and protection capabilities further. C-UAS measures can be classified into two categories: passive and active countermeasures. While passive C-UAS measures are designed to detect and track a UAS, active C-UAS measures are backed by

technology that enables the jamming of radio frequency signals, spoofing of global positioning system communications, and the deployment of lasers and kinetic devices, such as netting to destroy or capture an unauthorized drone. The examination of active C-UAS measures available on the open market reveals that if authority is granted to state and local government, local law enforcement will have more options and greater capabilities to counter careless and malicious UAS operations over their communities. The third recommendation is that local law enforcement should understand that C-UAS technology has limitations; therefore, the deployment of this technology must be necessary and appropriate to counter the UAS threat effectively. Therefore, to ensure that the deployment of C-UAS measures remain necessary, appropriate, and effective to counter a UAS threat, local law enforcement should provide a continuum of options officers may use in their missions to counter UAS threats. This thesis provides a C-UAS decision matrix that ensures redundancy in prevention and protection capabilities and enables law enforcement personnel the ability to assess the risk a UAS poses to a critical infrastructure and key resources or an event, and then decide which countermeasures to deploy. Even though legislative challenges associated with granting active C-UAS authority were beyond the scope of this thesis, several options enabling local law enforcement to enhance their capabilities to detect and track careless and malevolent UAS operations were identified. The combination of passive C-UAS with regulatory measures can facilitate the development of a C-UAS strategy to counter drones within America's hometowns and enhance protection and prevention capabilities.

The threat posed by unmanned and often autonomous systems, on land and water, are also likely to increase. Therefore, research in the future should focus not only on enabling the defeat of UAS platforms, but also other unmanned systems and automated technologies supporting travel on land, and both on and under water. A comparison government study of other democratic nations may expose legislation that can be modeled within the United States. Additionally, research of drone and other autonomous vehicle threats around the world and the responses to those threats may be beneficial in identifying best practices for deterring, detecting, tracking, interdicting, and disrupting careless or malevolent autonomous vehicle operations within urban areas.

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

The academic excellence displayed by the faculty and staff of the Naval Postgraduate School's Center for Homeland Defense and Security is second to none. Without the continuous encouragement and support from Dr. Lauren Wollman and the professional guidance of my thesis co-advisors Dr. Erik Dahl and John Rollins, completion of this thesis would not have been possible. I am blessed to have been graced with the opportunity to work with all of you while participating in the master's program.

I have been humbled by cohort 1803/1804, a selection of amazing individuals who exhibit admirable professionalism. Backed by a tenacious will to improve the homeland security enterprise, you display courageous dedication to explore and provide clarity to the blurred lines between securing the homeland while also protecting our democracy. It has been an honor to experience this journey with you, and thank you for all that you have taught me.

Embarking on and completing this journey would not have been possible without the support and encouragement of Dr. Dean Findley of the University of Central Oklahoma, Captain Pat Byrne (ret.) of the Oklahoma City Police Department, and Director Kim Ed Carter of the Oklahoma Office of Homeland Security. The initial nudge to explore this program followed by continued expressions of confidence in me with your calls and words of encouragement during the program will never be forgotten. I am also grateful for the support of Chief Bill Citty (ret.) of the Oklahoma City Police Department who entrusted me with the responsibility of representing the Oklahoma City Police Department. Furthermore, my success would not have been possible without the support of the staff of the Oklahoma City Office of Emergency Management who graciously filled gaps in the daily missions of our office while I was away.

It is to God that I owe the greatest thankfulness, for without his grace nothing is possible. His vision for my life story continues to be filled with overwhelming blessings. Behind each of my success stories stands two strong women of God. Mom, you engrained in my soul from a young age, a sense of grit to never give up. My tenacious character to

never stop is owed to you. Becca, no words can truly describe what you mean to me, as you are the worldly gift God placed in my path so many years ago to make me a better person. Your persistent faith guides our family and gives me the confidence to explore such opportunities that test my own faith. Your willingness to place many things on hold over the past 18 months and your listening ear allowed me to spend countless hours completing the necessary assignments and research required to succeed in this program. You complete my soul, and as a team, we reached the top of yet another mountain.

Finally, to Emily, Tanner, and Kelsey, who gave up so much time with their dad. My hope is that as you watched me traverse this program while juggling life, you learn to embrace such opportunities and appreciate the benefits of hard work. You make me proud. Keep moving forward, never give up, and never stop learning.

I. INTRODUCTION

The January 2015 crash of a small quadcopter, also referred to as a drone, on the White House grounds not only prompted a lockdown but left many questioning the risks drones pose to public safety.[1] Although an apparent accident due to careless operation, the incident highlights the vulnerabilities of even the most secured infrastructure to an unmanned aircraft system (UAS), such as a drone.[2] Since 2015, the UAS market has exploded; once an exclusively military domain, it is now also aimed at hobbyists, and the private and public sectors for recreational or mission specific operations. As a consequence, the availability of current and forthcoming inexpensive UAS platforms that can be weaponized or outfitted with surveillance equipment has also become an attractive tool to terrorists and criminals with nefarious intentions. In 2018, Congress recognized the potential threat drones pose to homeland security and passed the National Defense Authorization Act (NDAA) that extended limited active counter-UAS (C-UAS) authority to the Department of Defense (DoD) and Department of Energy (DOE).[3] However, the authority granted by Congress to use counter-drone technologies did not include local law enforcement agencies. This exclusion, in addition to the lack of a unified C-UAS strategy, leaves local law enforcement oblivious to potential UAS risks that can cause U.S. cities to remain vulnerable to nefarious UAS operations.[4]

This thesis examines the question of: How can local law enforcement protect their communities from UASs operated by careless hobbyists, criminals, and other nefarious

---

[1] Jack Nicas, "Criminals, Terrorists Find Uses for Drones, Raising Concerns," *Wall Street Journal*, January 28, 2015, http://www.wsj.com/articles/criminals-terrorists-find-uses-for-drones-raising-concerns-1422494268.

[2] Alejandro Sanchez and Cameron McKibben, "Worst Case Scenario: The Criminal Use of Drones," *Council on Hemispheric Affairs*, 1, February 2, 2015, http://www.coha.org/worst-case-scenario-the-criminal-use-of-drones/.

[3] Jason Snead, John-Michael Seibler, and David Inserra, *Establishing a Legal Framework for Counter-Drone Technologies*, Backgrounder No. 3305 (Washington, DC: Heritage Foundation, 2018), 1, https://www.heritage.org/sites/default/files/2018-04/BG3305_1.pdf.

[4] Ryan J. Wallace and Jon M. Loffi, "Examining Unmanned Aerial System Threats & Defenses: A Conceptual Analysis," *International Journal of Aviation, Aeronautics, and Aerospace* 2, no. 4 (2015): 2, https://doi.org/10.15394/ijaaa.2015.1084.

actors, such as foreign and domestic terrorists? Local law enforcement entities have become well versed in adapting to the evolving threat environment, but disruptive technology, such as an armed UAS, can be a game-changer in public safety.[5] Local law enforcement has robust safety and security plans to defend against the threat environment and secure two-dimensional perimeters surrounding large-scale events and critical infrastructure. Yet, the proliferation of UAS technology, coupled with impressive capabilities to carry surveillance equipment, weapons, and other illicit items, has created a need to secure the three-dimensional space surrounding these same events and infrastructure. The capability to utilize C-UAS technology to detect, deter, and interrupt a UAS threatening outdoor open-access events, critical infrastructure, and strategic police operations, would enhance local law enforcement's protection of the three-dimensional space.[6] Before embarking on developing a local C-UAS strategy, however, these agencies need clarity about the threat posed by illicit drone use, how the threat can be countered, and key elements to consider before implementing a C-UAS strategy.

A. LITERATURE REVIEW

This literature review begins with an analysis and discussion of literature exposing UAS capabilities, limitations, and risks associated with armed or surveillance equipped UAS platforms posing a threat to public safety and critical infrastructure. Next, a review of literature about C-UAS technology explores deployment strategies and the challenges associated with countering a UAS in America's hometowns. Finally, C-UAS legislation and policy literature is reviewed to examine the need for C-UAS authority at the state and local levels of government. Key sources in the literature come from professional organizations, research firms, academia, the technology industry, and federal governmental agencies.

---

[5] Nicas, "Criminals, Terrorists Find Uses for Drones, Raising Concerns."

[6] Arthur Holland Michel, *Counter-Drone Systems 2018* (Washington, DC: The Center for the Study of the Drone at Bard College, 2018), 23, https://dronecenter.bard.edu/publications/counter-drone-systems/.

1. Exploring UAS Capabilities, Limitations, and Risks

The technology industry offers an abundance of information about UAS capabilities and provides examples of innovative ways a UAS can enhance business models and bolster public safety capabilities around the world.[7] For example, technology specialist Christina Mercer, who writes for Techworld, praises the capability of UAS platforms that allow Amazon and the United Parcel Service (UPS) to be more efficient in delivering products to customers.[8] In the same article, Mercer also applauds China's use of drones to bolster its ability to deliver food supplies in Shanghai.[9] *MIT Technology Review*, whose stated mission is to facilitate better-informed decisions about technology, applauds researchers' efforts in 2018 to enhance public safety protection capabilities by programming a drone to herd birds out of the airspace around airports.[10] Like the technology industry, research documents and academic literature also approve of impressive UAS capabilities that can enhance public safety missions. For example, in his 2018 thesis, Wee Leong Lee discusses the critical task of identifying and removing foreign object debris (FOD) on airport runways and suggests that tasking a UAS with FOD identification will not only reduce man hours but also enhance aircraft safety and prevent more accidents on runways.[11]

Professional organizations and other research forums, such as the National Police Foundation, the International Association of Chiefs of Police (IACP), and the Police Executive Research Forum (PERF), concur with technology experts and academia that advancements in UAS technology can improve public safety missions. For example, as early as 2009, PERF released a law enforcement technology needs assessment report,

---

[7] Christina Mercer-Myers, "How Are Drones Used?," Techworld, July 30, 2019, https://www.techworld.com/picture-gallery/apps-wearables/best-uses-of-drones-3605145/.

[8] Mercer-Myers.

[9] Mercer-Myers.

[10] Erin Winick, "Researchers Taught a Drone to Herd Birds Away from Airports," *MIT Technology Review*, August 7, 2018, https://www.technologyreview.com/the-download/611834/researchers-taught-a-drone-to-herd-birds-away-from-airports/.

[11] Wee Leong Lee, "Assessment of Foreign Objet Debris Management Using Group 1 Unmanned Aerial Systems" (master's thesis, Naval Postgraduate School, 2018), 1–2, https://calhoun.nps.edu/handle/10945/60426.

which stated that drones should be considered a promising technology for future police use.[12] More recently, in a 2017 Police Foundation blog, Chief Burguan of the San Bernardino Police Department, urges police departments to embrace UAS technology and employ the technology to assist with processing crime scenes, search and rescue operations, and high-risk police actions.[13]

However, unlike the industry experts and professional law enforcement organizations, many in academia, along with civil liberty advocacy groups, also note the tension presented associated with protecting civil liberties when deploying UAS technologies for domestic law enforcement missions. Jeanie Moore's 2014 Naval Postgraduate School (NPS) thesis raises concerns about privacy and argues the importance of law enforcement to develop a clear vision and a collaborative strategy to guide the use of UAS platforms in the national airspace.[14] Another 2014 NPS thesis, by Barcley Stamey, supports Moore's contentions and emphasizes that although the use of a UAS can improve law enforcement's vantage point and may reduce response times, these advantages may come at the cost of minimizing civil liberties in America.[15] Furthermore, Brian Smith argues in his 2016 NPS thesis that the use of UAS platforms by domestic law enforcement is promising, yet at the same time, is potentially problematic.[16] Smith concludes his thesis by suggesting that the use of UAS technology by domestic law enforcement is essentially

---

[12] Christopher S. Koper, Bruce G. Taylor, and Bruce E. Kubu, *Law Enforcement Technology Needs Assessment* (Washington, DC: Police Executive Research Forum, 2009), 1, https://www.policeforum.org/assets/docs/Free_Online_Documents/Technology/law%20enforcement%20technology%20needs%20assessment%202009.pdf.

[13] Jarrod Burguan, "Drones Help Augment a Police Department's Capabilities to Fight Crime," *National Police Foundation* (blog), April 28, 2017, https://www.policefoundation.org/drones-help-augment-a-police-departments-capabilities-to-fight-crime/.

[14] Jeanie Moore, "Da Vinci's Children Take Flight: Unmanned Aircraft Systems in the Homeland" (master's thesis, Naval Postgraduate School, 2014), 1, https://calhoun.nps.edu/handle/10945/41420.

[15] Barcley W. Stamey, "Domestic Aerial Surveillance and Homeland Security: Should Americans Fear the Eye in the Sky?" (master's thesis, Naval Postgraduate School, 2014), 1, https://calhoun.nps.edu/handle/10945/41466.

[16] Brian T. Smith, "Ethics on the Fly: Toward a Drone-Specific Code of Conduct for Law Enforcement" (master's thesis, Naval Postgraduate School, 2016), 2, https://calhoun.nps.edu/handle/10945/48476.

a debate about the future of law enforcement and the cost of security in a post-9/11 society.[17]

While the majority of the literature about UAS technology focuses on enhanced capabilities and privacy issues, some traction has been reached in discussions about their limitations, the risks they may pose to public safety, and the importance of regulating UAS operation in airspace. A 2018 internationally peer-reviewed article in *Drones* discusses the use of drones for surveillance and recommends that surveillance missions should consider obstacles, such as limited range and flight restrictions forbidding drone operations, in areas that fall within no-flight zones.[18] Although this article refers to flight restrictions as obstacles, others in the technological industry recognize the positive impacts of flight restrictions and how UAS regulations can secure the airspace. A 2018 report from *MIT Technology Review* concurs that standards for drone operations can help facilitate safer airspace and establish accountability for drone operators.[19] Trade journals, too, have weighed in on discussions surrounding drone operations accountability and potential risks of illicit drone use. A 2017 article in *Air and Space Power Journal* recognizes that key advances in UAS technology, such as speed, maneuverability, and ease of operation, may expose vulnerabilities of traditional security strategies and are precisely what might attract potential adversaries.[20] Authors Thomas Palmer and John Geis specifically identify vulnerabilities of traditional security strategies, such as high fencing and small arms defense, in protecting critical infrastructure from a UAS.[21]

---

[17] Smith, 71.

[18] Tauã M. Cabreira, Lisane B. Brisolara, and Paulo R. Ferreira Jr., "Survey on Coverage Path Planning with Unmanned Aerial Vehicles," *Drones* 3, no. 1 (2019): 1–4, https://doi.org/10.3390/drones3010004.

[19] Charlotte Jee, "The First Worldwide Drone Standards Have Been Unveiled to Keep Aircraft Safe," *MIT Technology Review*, November 22, 2018, https://www.technologyreview.com/the-download/612460/the-first-worldwide-drone-standards-have-been-unveiled-to-keep-aircraft-safe/.

[20] Thomas S. Palmer and John P. Geis II, "Defeating Small Civilian Unmanned Aerial Systems to Maintain Air Superiority," *Air & Space Power Journal* 31, no. 2 (Summer 2017): 102–18, https://www.airuniversity.af.edu/Portals/10/ASPJ_Spanish/Journals/Volume-29_Issue-4/2017_4_07__palmer_s_eng.pdf.

[21] Palmer and Geis, 105.

More recently, law enforcement organizations have begun to recognize the potential threat unregulated and illicit UAS use poses to public safety. A January 2019 "Tech Talk" sponsored by the IACP argues that drones are both useful and challenging. IACP contends that unauthorized drones should be considered a threat as they may be piloted by a hobbyist unknowingly causing a risk to public safety or a hostile who is intent on surveying police actions or deploying weapons.[22] A 2018 article published by the American Military University exposes how gangs in America are using drones to counter law enforcement operations, which supports IACP's contention.[23] In the report, Federal Bureau of Investigation (FBI) Agent Mazel describes how a hostage rescue team was compromised when a criminal gang deployed a low-flying, high-speed swarm of drones over the team.[24]

Although most sources agree that advanced UAS platforms are beneficial, some, such as academia and law enforcement, have identified unintended consequences. Academic literature supports the use of drones by domestic law enforcement but argues that the lack of oversight may lead to an encroachment on civil liberties concerning privacy and the protection of unreasonable search and seizure. On the other hand, law enforcement agencies and professional organizations have begun to realize the potential dangers of illicit drone use and consider drones to be potential threats to public safety and police operations. For example, to bolster protection of the 2019 Super Bowl in Atlanta, Georgia, local authorities declared a "No Drone Zone" around the venue leading up to the game and restricted the airspace during the game.[25] As a result of these protective measures and other

---

[22] Joerg Lamprecht, "Tech Talk: Drone Safety and Defense Start with Detection," *Police Chief*, January 1, 2019, http://www.policechiefmagazine.org/tech-talk-drone-safety-and-defense-start-with-detection/.

[23] Robert Brzenchek, "How Gangs Are Using Drones to Disrupt Law Enforcement," In Public Safety, May 21, 2018, https://inpublicsafety.com/2018/05/how-gangs-are-using-drones-to-disrupt-law-enforcement/.

[24] Brzenchek.

[25] Brendan O'Brien, "Six Drones Confiscated in Atlanta Ahead of Super Bowl," *Reuters*, February 3, 2019, https://www.reuters.com/article/us-football-nfl-superbowl-drones-idUSKCN1PR0PL.

non-disclosed C-UAS measures, six unauthorized drones were confiscated leading up to the event.[26]

In summary, the literature review of UAS capabilities, limitations, and risks reveals agreement that UAS technology capabilities are promising for both private and public safety missions. The literature begins to scratch the surface of the limitations of UAS technologies with a consensus that they should be regulated. Moreover, although the literature acknowledges UAS technology can pose risks to both civil liberties and public safety, justifying the need for C-UAS strategies, it stops short of discussing ways local law enforcement should plan and prepare for its malevolent use. Therefore, additional research is necessary to inform local law enforcement about C-UAS options and guide the development of a C-UAS strategy.

2. Exploring C-UAS Technologies for Hometown Security

In light of the growing concern of illicit drone use, a new market for counter-drone systems has emerged, commonly referred to as C-UAS technology. C-UAS technology is used to detect and interrupt or interdict a UAS.[27] The Department of Homeland Security (DHS) recognizes the need to counter nefarious drones, and since 2016, the DHS Science and Technology Directorate (S&T) has worked to assist homeland security partners with the development, testing, and use of C-UAS technology.[28] DHS S&T contends that although numerous C-UAS solutions are available, most have not been tested in America's hometown environments, which has resulted in little analysis of how these systems perform in an urban setting.[29] In their 2018 Heritage Foundation report, Jason Snead, John-Michael Seibler, and David Inserra agree with DHS S&T assertions. They claim that many commercially available C-UAS technologies were designed for military battlefields and

---

[26] Alexis Stevens, "Enforcing 'No Drone Zone' near the Super Bowl Is Tough for Authorities," *Atlantic Journal-Constitution*, February 1, 2019, https://www.ajc.com/news/crime--law/enforcing-drone-zone-near-the-super-bowl-tough-for-authorities/q5p3QFMiXHgHW8Q7h6ueuL/.

[27] Michel, *Counter-Drone Systems 2018*, 1.

[28] Department of Homeland Security, "Snapshot: Countering Unmanned Aerial Systems in Urban Environments," Science and Technology, May 11, 2018, https://www.dhs.gov/science-and-technology/news/2018/05/11/snapshot-c-uas-urban-environments.

[29] Department of Homeland Security.

not considered practical in domestic airspace, especially over a densely populated urban area.[30] A 2018 report from the Center for the Study of the Drones at Bard College found that over 200 C-UAS platforms are available around the globe.[31] Michel Holland, from the Center for the Study of the Drone at Bard College, contends with both DHS and the authors of the Heritage Foundation report, that although a variety of necessary detection and interdiction techniques are available, each comes with practical challenges for field operations.[32] Holland, however, also argues that problems associated with the effectiveness and reliability of C-UAS technology in field operations can be attributed to "a lack of common standards" within the C-UAS industry.[33] Holland contends that without international standards, the likelihood exists that C-UAS technology varies significantly in areas of performance and reliability, and also poses safety concerns, especially over civilian airways.[34]

Practical challenges associated with deploying C-UAS technology in urban areas can be compounded by legal challenges as well. In addition to the lack of effective urban area deployment capabilities, Holland argues that clear legislative measures guiding the policy development for using C-UAS technology are necessary.[35] According to Holland, C-UAS platforms designed to interdict a drone through signal jamming are currently illegal or heavily restricted in the United States.[36] In their 2018 Heritage Foundation report, Snead, Seibler, and Inserra also agree with the Bard College scholars' contentions of legal challenges associated with using C-UAS technology. The authors argue that legal authority to use C-UAS technology is vague and Congress should "expand the limited drone authority" given with the 2017 and 2018 NDAAs.[37] For example, Snead, Seibler, and

---

[30] Snead, Seibler, and Inserra, *Establishing a Legal Framework for Counter-Drone Technologies*, 5.

[31] Michel, *Counter-Drone Systems 2018*, 1.

[32] Michel, 1.

[33] Michel, 1.

[34] Michel, 9.

[35] Michel, 1.

[36] Michel, 8.

[37] Snead, Seibler, and Inserra, *Establishing a Legal Framework for Counter-Drone Technologies*, 1.

Inserra claim that although Congress recognized the growing UAS threat, the 2017–2018 NDAA falls short of extending C-UAS authority to state and local law enforcement agencies, which are often the first to respond to significant public safety threats.[38] The literature represented in this review seems to agree that while C-UAS technology has exploded in recent years, it is not effective within America's hometowns. The authors cite reasons for such ineffectiveness as a lack of industry standards to ensure urban-area applications and the lack of legal authority guiding state and local law enforcement deployment of C-UAS technology.

3. The Case for a State and Local C-UAS Strategy

The debate surrounding drone operations and the legal considerations of using them are not new. In a 2015 journal article by the *Seattle Journal of Environmental Law*, author Kurt Smith argues that to mitigate malevolency and protect airspace, Federal Aviation Administration (FAA) regulation, drone registration, and drone monitoring capabilities should be pursued.[39] During recent discussions about C-UAS technology, a controversial issue is whether a drone can be legally interdicted and brought down from airspace, and if it can, who should have the deciding authority. The FAA considers a drone to be an aircraft and under current federal law, 18 U.S.C. § 32, it is illegal to disrupt or take down an aircraft.[40] Although Joseph Vacek, a researcher and aerospace law teacher at the University of North Dakota School of Law, recognizes both federal law and the potential threat of illicit drones, he argues that active C-UAS implementation should remain an option in response to a perceived drone threat.[41]

---

[38] Snead, Seibler, and Inserra, 9.

[39] Kurt W. Smith, "Drone Technology: Benefits, Risks, and Legal Considerations," *Seattle Journal of Environmental Law* 5, no. 1 (2015): 293, https://digitalcommons.law.seattleu.edu/sjel/vol5/iss1/12.

[40] "U.S.C. Title 18—Crimes and Criminal Procedure," U.S. Government Publishing Office, accessed August 7, 2019, https://www.govinfo.gov/content/pkg/USCODE-2011-title18/html/USCODE-2011-title18-partI-chap2-sec32.htm.

[41] Joseph J. Vacek, "Counter-UAS Applications Illegal under 18 U.S.C. § 32 Are Justified When Using a Reasonably Defensible Counter-UAS Strategy that Incorporates Risk and Compliance Categorizations," *North Dakota Law Review* 93, no. 3 (2018): 502, https://law.und.edu/law-review/issues/93/93-3.html.

Additionally, Congress recognizes the potential threat drones pose to homeland security and provides legislative support to protect against the threat. In early 2018, Congress passed the NDAA giving C-UAS authority to the DOE and the DoD.[42] In June 2018, DHS, FBI, and FAA personnel testified before the Senate Homeland Security and Government Affairs Committee, arguing that the 2018 Bill's C-UAS authority should be extended to DHS and the Department of Justice (DOJ).[43] In response to the June 6, 2018, Senate hearing, the American Civil Liberties Union (ACLU) questioned whether additional DHS or DOJ C-UAS authority is necessary. In its letter to the Committee Chair, Senator Johnson, the ACLU contends that extending authorities under the NDAA Act of 2018 would allow DHS and DOJ to take unnecessary extreme action that can result in the unlawful seizure of private property.[44] Furthermore, the ACLU argues that the bill is too vague, and fails to ensure appropriate oversight to protect civil liberties.[45] During the hearing, committee Chair Senator Johnson, along with other committee members, recognized the ACLU claims and the importance of protecting civil rights. However, many committee members refute the ACLU's claims and have expressed concerns that the bill is too limited, which leaves America's state and local jurisdictions vulnerable to UAS threats.[46] During both opening statements and throughout the testimonies, Chair Senator Johnson repeatedly emphasized that the 2018 bill is "very" limited, and is simply the "first step" in protecting the American people against the UAS threat.[47] Senator Hassan noted during the hearing that state and local responders would likely be the first responders to a UAS threat and would not have time to wait for DHS or the FBI to deploy C-UAS resources

---

[42] Snead, Seibler, and Inserra, *Establishing a Legal Framework for Counter-Drone Technologies*, 1.

[43] "S. 2836, the Preventing Emerging Threats Act of 2018: Countering Malicious Drones," U.S. Senate Committee on Homeland Security & Governmental Affairs, pt, 2:04:01, 2018, https://www.hsgac.senate.gov/hearings/s-2836-the-preventing-emerging-threats-act-of-2018-countering-malicious-drones.

[44] Faiz Shakir and Neema Singh Guliani, "ACLU Opposes S.2836," June 6, 2018, https://www.aclu.org/letter/aclu-opposition-preventing-emerging-threats-act-2018-countering-malicious-drones.

[45] Shakir and Guliani, 2.

[46] U.S. Senate Committee on Homeland Security & Governmental Affairs, "S. 2836, the Preventing Emerging Threats Act of 2018: Countering Malicious Drones," pt. 01:05:07.

[47] U.S. Senate Committee on Homeland Security & Governmental Affairs, pt. 00:18:43–00:20:35.

to an event or incident.[48] DHS's Undersecretary for Intelligence and Analysis, David Glawe, gave testimony during the hearing that gave merit to Senator Hassan's concerns. Glawe emphasized that although extending authority under the bill to DHS and the DOJ would enhance coordination with state and local authorities, these partners would have difficulty detecting nefarious UAS threats, and unless resources were already on scene and ready, C-UAS capabilities of the federal government would be ineffective.[49] Concerning guidelines to protect both drone operators, civil rights, and public safety, committee members expressed concern about the effectiveness of FAA regulations concerning UAS operations. When answering how the regulations would support protecting the American public from nefarious drones, FAA representative Angela Stubblefield gave merit to the senators' concerns claiming that regulatory measures are effective only for compliant drone operators.[50]

A 2015 research article from the *International Journal of Aviation, Aeronautics, and Aerospace* recognizes that not everyone will be compliant. Authors Ryan Wallace and Jon Loffi, who after exploring intentional and illicit uses of a UAS, conclude that UAS platforms provide terrorists and criminals with an applicable tool to further malevolent intentions threatening public safety.[51] These two scholars emphasize the need for public safety personnel to remain vigilant to illicit UAS operations.[52] Although the aforementioned sources and discussions within the federal government, academia, and civil libertarians overwhelmingly reveal a gap in C-UAS capability and authority at state and local levels, the literature also exposes the need for effective legislation that provides

---

[48] U.S. Senate Committee on Homeland Security & Governmental Affairs, pt. 56:15.

[49] Senate Committee on Homeland Security and Governmental Affairs, *Joint Testimony of the Honorable David J. Glawe, Under Secretary for Intelligence and Analysis, U.S. Department of Homeland Security, Hayley Chang, Deputy General Counsel, S. 2836, the Preventing Emerging Threats Act of 2018: Countering Malicious Drones* (Washington, DC: Department of Homeland Security, 2018), 9, https://www.hsgac.senate.gov/imo/media/doc/Testimony-Glawe%20and%20Chang-2018-06-061.pdf.

[50] U.S. Senate Committee on Homeland Security & Governmental Affairs, "S. 2836, the Preventing Emerging Threats Act of 2018: Countering Malicious Drones," pt. 1:06:47.

[51] Wallace and Loffi, "Examining Unmanned Aerial System Threats & Defenses," 24.

[52] Wallace and Loffi, 24.

oversight for protection of civil liberties when deploying C-UAS technology in America's hometowns.

B. RESEARCH METHODOLOGY

Research conducted for this thesis maintains a limited scope and focuses on how local governments can protect their communities from malevolent or careless UAS operations. Therefore, to assess the risk of UAS operations, this thesis begins by first examining the threat UAS technology poses to local communities. Next, the research assesses options local governments have to mitigate their community's vulnerability to UAS operations. The assessment looks at C-UAS technology supporting passive measures to detect and track threatening drones, and active measures to interdict and or disrupt a UAS. Finally, research explores the limitations and potential consequences of implementing C-UAS technology in America's hometowns.

Researching literature exposing the evolving threat posed by malevolent or careless UAS operations will aid the reader in devising a local C-UAS strategy. Exploring incidents involving both careless UAS operations and threatening or nefarious UAS operations can provide the reader situational awareness of UAS threats to public safety. Furthermore, assessing targets of careless or malevolent UAS operations will qualify the threat, by identifying vulnerabilities of America's cities, and their critical infrastructure and key resources to unauthorized drones.

Due to the explosion of UASs operating within the national airspace, federal, state, and local governments have passed various regulations, legislation, and ordinances to ensure a safe airspace, and protect the public's safety and right to privacy on the ground. However, a detailed analysis of the legal issues surrounding UAS and C-UAS operations is beyond the scope of this thesis. Instead, this thesis contains research focusing on C-UAS technology available today to provide the reader insight into how a UAS can be countered passively or actively. For example, issuing a temporary flight restriction over a designated geographical area is considered a passive UAS countermeasure while the deployment of radio frequency (RF) jamming technology to interdict and disrupt a UAS is considered an active C-UAS practice.

Finally, this thesis researches elements to consider prior to procuring and implementing C-UAS technology. The research focuses on implementation challenges, associated with active and passive countermeasures when deployed within an urban environment. Research can enlighten the reader about operational limitations of deploying C-UAS technology in populated cities and towns within the United States.

The thesis concludes by synthesizing the research in the previous chapters to provide the reader with a framework to take action. The final chapter assists the reader in creating a C-UAS strategy that accounts for risk mitigation, while employing C-UAS technology to protect local communities. The chapter provides recommendations for developing a relevant necessary and appropriate C-UAS strategy to protect America's hometowns against malevolent and careless UAS threats.

C. CHAPTER OUTLINE

Chapter I provides an overview of the evolving technology associated with unmanned aircraft and the challenges local law enforcement face when protecting their communities from nefarious UAS operations. The chapter expands on the potential risk posed by UAS operations because of their availability and ease of operation in almost any environment, and asks how local law enforcement can protect their communities from a UAS. Chapter I describes the research methodology employed for this thesis, and concludes with a literature review exploring both UAS and C-UAS technology, and the legal and regulatory measures regarding C-UAS technology deployment, within America's hometowns.

Chapter II provides the reader with situational awareness to bring the threat into focus for local public safety planning efforts. Chapter II examines incidents involving UAS platforms that threaten the publics' safety to guide local law enforcement's efforts to assess their communities' risks to the threat. The risk assessment conducted in this chapter examines the intention, motivation, capabilities, and history of the threat. Additionally, the assessment identifies target vulnerabilities and the consequences of the incidents and attacks. Furthermore, Chapter II helps local law enforcement develop preparedness plans and mitigation measures to lessen their communities' risk to UAS operations.

Chapter III focuses on C-UAS technology. The chapter identifies passive and active countermeasure technology designed to detect and interdict a threatening UAS. Due to the limited scope of this thesis, legal issues surrounding C-UAS authority is not included in Chapter III.

Chapter IV researches issues to consider before implementing C-UAS technology. For example, the research examines limitations of C-UAS technology and identifies potential unintended consequences associated with interdicting a drone over urban areas. The research conducted in this chapter can assist the reader in developing a C-UAS policy, as well as creating operational procedures to implement a local C-UAS strategy.

Chapter V emphasizes the need for local C-UAS strategies and provides the reader with recommendations that can help develop a C-UAS strategy. Applying the recommendations to a local C-UAS strategy can enhance a jurisdiction's capability to protect from careless or malevolent UAS threats. The chapter concludes the paper with closing thoughts highlighting the limited scope of the paper and considerations for future research opportunities.

II. THE EVOLVING UAS THREAT TO HOMETOWN SECURITY

A. CARELESS AND MALEVOLENT UAS OPERATIONS

The impressive capabilities exhibited by UAS platforms attract more followers and users for both legitimate business objectives and pure entertainment purposes.[53] The proliferation of small, inexpensive UAS platforms in production and sold around the world serve as yet another example of extraordinary technological advances aimed to enhance business ventures while also providing an attractive toy for the hobbyist. Even without malicious intent, a careless hobbyist can unintentionally invade another's privacy, encroach upon critical infrastructure, and even interfere with manned aircraft.[54]

Unfortunately, individuals, and organizations with malevolent intent have also capitalized on impressive UAS capabilities.[55] The malicious use of UAS platforms has become a useful tool for criminals, terrorists, and lone wolf actors.[56] UAS platforms supporting drones with respectable payload capacities are able to support surveillance equipment and are being used as vehicles to move weapons and other illicit goods.[57] Furthermore, what is even more alarming is the occurrence of weaponized UAS technology used to conduct physical attacks.[58] Since UAS technology has become another tool to bolster terrorist and criminal activity both globally and domestically, public safety officials

---

[53] Nicas, "Criminals, Terrorists Find Uses for Drones, Raising Concerns," 1.

[54] Nicas, 1–2.

[55] John P. Sullivan and Robert J. Bunker, "Mexican Cartel Strategic Note No. 18: Narcodrones on the Border and Beyond," *Small Wars Journal*, 1, March 28, 2016, https://www.hsdl.org/?abstract&did=791699.

[56] "DHS Releases UAS Threats on Critical Infrastructure Video," *Security*, May 10, 2019, https://www.securitymagazine.com/articles/90214-dhs-releases-uas-threats-on-critical-infrastructure-video.

[57] Justin Ling, "Someone Used a Drone to Deliver a Handgun into a Notorious Canadian Prison," Vice News, December 14, 2015, https://news.vice.com/en_us/article/gy9wnj/someone-used-a-drone-to-deliver-a-handgun-into-a-notorious-canadian-prison.

[58] Colin P. Clarke, "Approaching a 'New Normal': What the Drone Attack in Venezuela Portends," *The RAND Blog* (blog), August 13, 2018, https://www.rand.org/blog/2018/08/approaching-a-new-normal-what-the-drone-attack-in-venezuela.html.

should begin to recognize the emerging threats, safety, and privacy concerns drones pose to states and municipalities within the United States.[59]

Although UAS technology is impressive and can enhance everyday life, careless and malevolent operations pose both a hazard, and at times, threats to the public's safety. This chapter studies incidents involving UAS operations that endangered the public's safety. Whether deemed accidental or intentional, this analysis can qualify the potential danger improper UAS operations pose and emphasize the need for local law enforcement to enhance preparedness efforts.

1. Careless UAS Operations

a. Hobbyists

With drones becoming a regular occupier of airspace, operators of UAS platforms find themselves intentionally and unintentionally pushing the limits of safe flight operations.[60] Although the 2015 crash of a small quadcopter on the White House grounds was deemed accidental, the incident heightened concerns of public safety officials.[61] The incident supports statements made in the 2105 DHS Commercial Facilities Sector Specific Plan acknowledging UAS technology as an emerging threat to critical infrastructure.[62] Even without malicious intent or motivation to cause harm, the government employee operating the drone exposed a capability gap in White House security.[63] The security breach at the White House in 2015 was not an intended threat to the facility or personnel, but the carelessness of a UAS hobbyists in the early morning hours introduced a new challenge that for which the Secret Service was not prepared. The UAS platform operated

---

[59] Nicas, "Criminals, Terrorists Find Uses for Drones, Raising Concerns," 1.

[60] Arthur Holland Michel and Dan Gettinger, *Drone Incidents: A Survey of Legal Cases* (Washington, DC: Center for the Study of Drone, Bard College, 2017), 1, https://dronecenter.bard.edu/drone-incidents/.

[61] Nicas, "Criminals, Terrorists Find Uses for Drones, Raising Concerns," 1.

[62] Department of Homeland Security, *2015 Commercial Facilities Sector-Specific Plan: An Annex to the NIPP 2013* (Washington, DC: Department of Homeland Security, 2015), 10, https://www.dhs.gov/sites/default/files/publications/nipp-ssp-government-facilities-2015-508.pdf.

[63] Michael S. Schmidt and Michael D. Shear, "A Drone, Too Small for Radar to Detect, Rattles the White House," *New York Times*, January 27, 2015, https://www.nytimes.com/2015/01/27/us/white-house-drone.html.

by the hobbyist that included a small drone flying at a low altitude was not detected by the radar system designed to alert security personnel of airborne objects within the White House airspace.[64] The incident highlights how easy it is to penetrate one of the most secure facilities in the country with a drone capable of conducting surveillance, or even worse, launching an attack. UAS hobbyists not only have an interest in accessing critical infrastructure for purposes of capturing photographs and video not possible from the ground, but they also seek the opportunity to gain access to outdoor events to capture aerial photographs and videos. Although the FAA, law enforcement, and stadium owners and operators have worked to secure the airspace above their events, the risk persists. On May 21, 2017, an unauthorized drone hovered over thousands of fans at a Major League baseball game in San Diego for several minutes before crashing down into the stands.[65] According to stadium security and media outlets, the drone crashed near some fans and did not cause any injuries.[66] In an April 2019 incident, a drone was observed hovering over Fenway Park during a Boston Red Sox baseball game.[67] The drone did not crash, but because of the threat to the public's safety, the incident resulted in a joint investigation between local and federal entities to determine whether the juvenile operating the drone should face criminal charges.[68] Like other incidents, criminal intent was not found. However, such careless UAS operations remain a challenge for critical infrastructure owners and operators who work to mitigate threats and hazards likely to cause mass casualty incidents on the ground at outdoor venues.

---

[64] Schmidt and Shear.

[65] Fitz Tepper, "The FAA Gets a Case Study with a Drone Crash inside an MLB Stadium," TechCrunch, May 23, 2017, http://social.techcrunch.com/2017/05/23/the-faa-gets-a-case-study-with-a-drone-crash-inside-an-mlb-stadium/.

[66] Mark J. Burns, "MLB Responds after Drone Makes Petco Park Crash Landing during San Diego Padres Game," SportTechie, May 22, 2017, https://www.sporttechie.com/gopro-karma-drone-makes-crash-landing-at-petco-park-during-san-diego-padres-game/.

[67] David Shepardson, "FAA to U.S. Airports: Do Not Install Drone Countermeasures on Your Own," *Reuters*, May 8, 2019, https://www.reuters.com/article/us-usa-drones-airports/faa-to-u-s-airports-do-not-install-drone-countermeasures-on-your-own-idUSKCN1SE2QZ.

[68] Scott Gleeson, "Police Identify Juvenile Who Flew Drone at Fenway Park during Red Sox Game," *USA Today*, April 14, 2019, https://usatodayhss.com/2019/fenway-park-drone-red-sox-game.

b. Commercial Aerial Photography

Commercial aerial photography is another legitimate purpose for UAS platforms. According to its 2019–2039 aerospace forecast, the FAA predicts that 21 percent of UAS systems operating in the airspace film outdoor athletic events, entertainment venues, and private ceremonies.[69] Many of these systems are operated by commercial entities hired by a third party to capture still photos and record video of the events. Commercial aerial photography has enhanced surveillance capabilities with UAS platforms. Coupled with their ease of operation and accessibility, UAS platforms equipped with onboard camera systems continue to grow in popularity. The commercial and residential real-estate markets, critical infrastructure owners and operators, and commercial aerial photographers also employ UAS technology to further business operations and promote sales.[70]

Operating drones over crowds of people at outdoor, open access events, and around critical infrastructure can provide impressive still and video images. However, these operations also pose a risk to the public's safety. On Saturday, June 28, 2015, while capturing video over a Pride Parade in Seattle, Washington, the owner of an aerial footage company crashed his drone into the side of a commercial facility, which caused the drone to fall to the ground injuring two people.[71] Paul Skinner, who was later convicted of reckless endangerment, a misdemeanor charge, was operating the DJI Phantom 3 quadcopter.[72] The drone, equipped with surveillance equipment, captured approximately one minute of video from an altitude near 185 feet before crashing into a 50-story commercial building.[73] According to local media reports, the $1,200.00 drone had an 18-

---

[69] Federal Aviation Administration, *FAA Aerospace Forecast 2019–2039* (Washington, DC: Federal Aviation Administration, 2019), 50, https://www.faa.gov/data_research/aviation/aerospace_forecasts/.

[70] Kathryn Zickuhr, Elias Stahl, and Nicole DuPuis, *Cities and Drones: What Cities Need to Know about Unmanned Aerial Vehicles (UAVs)* (Washington, DC: National League of Cities, 2016), 1, https://www.nlc.org/sites/default/files/2016-12/NLC%20Drone%20Report.pdf.

[71] Steve Miletich, "Pilot of Drone that Struck Woman at Pride Parade Gets 30 Days in Jail," *Seattle Times*, February 24, 2017, https://www.seattletimes.com/seattle-news/crime/pilot-of-drone-that-struck-woman-at-pride-parade-sentenced-to-30-days-in-jail/.

[72] Tim Wright, "If You Crash a Drone, You Might Land Yourself in Jail: The Story Behind a Recent Landmark Conviction," *Air & Space Magazine*, August 2017, https://www.airspacemag.com/flight-today/36_aug2017-uav-criminal-180963942/.

[73] Wright.

inch wingspan and weighed only two pounds.[74] The investigation of the accident showed no malicious intent, but the crash highlights the consequence of reckless UAS operations over populated, urban areas and the likely endangerment of the public's safety on the ground.[75]

c. Encounters and Close Calls in the Crowded Airspace

While public safety personnel work to ensure the public's safety on the ground, when a UAS is flown irresponsibly, this carelessness can also put lives at risk in the air. Pilots of manned aircraft continue to report incidents of encounters with UAS platforms at an alarming rate. A 2015 study by the Center for the Study of the Drone at Bard College reported 921 incidents of manned aircraft reporting drone encounters in the U.S. Airspace System between December 2013 and September 2015.[76] The study divided the 921 drone encounter incidents into two categories. The first category, close encounters, are reports of drones operating within 500 feet of manned aircraft and may have resulted in evasive action by the manned aircraft to avoid a collision.[77] The second category, labeled as sightings, involves incidents where a drone was observed flying above the legal ceiling or near an airport, but did not pose an imminent risk to the aircraft.[78] The study concluded that 327 incidents were close calls while 594 were classified as sightings.[79] The Bard College study reinforces the FAA's concern of crowded airspace. Data gathering for the study ended August 21, 2015, but according to the FAA, reports of UAS sightings and close calls by manned aircraft continue to climb.[80] According to the FAA, an intense increase in UAS

---

[74] Miletich, "Pilot of Drone That Struck Woman at Pride Parade Gets 30 Days in Jail."

[75] Betsy Lillian, "Seattle Court Orders Jail Time for 'Reckless Endangerment' Drone Incident," Unmanned Aerial, February 24, 2017, https://unmanned-aerial.com/seattle-court-orders-jail-time-for-reckless-endangerment-drone-incident.

[76] Dan Gettinger and Arthur Holland Michel, *Drone Sightings and Close Encounters: An Analysis* (Washington, DC: The Center for the Study of the Drone at Bard College, 2015), 5, https://dronecenter.bard.edu/drone-sightings-and-close-encounters/.

[77] Gettinger and Michel, 5.

[78] Gettinger and Michel, 5.

[79] Gettinger and Michel, 5.

[80] Gettinger and Michel, 5.

sightings by pilots, citizens, and law enforcement has occurred since 2017.[81] Since the FAA receives over 100 reports each month, it continues to encourage the public's help in discouraging reckless UAS operations.[82]

Both the Bard College study and reports by the FAA continue to be challenged. Representatives from organizations, such as the Academy of Model Aeronautics (AMA), argued that data used to formulate the report were misrepresentations and even exaggerated.[83] According to the AMA, the rhetoric used within the title of the 2015 FAA report sensationalized sightings as meaning close calls requiring manned aircraft to take evasive actions to avoid mid-air collisions.[84] In their examination of the 2015 FAA report, the AMA determined that evasive action by the manned aircraft was taken in only 10 of the 764 reports.[85] Although the AMA argues the validity of the FAA data, it recognizes the need to sustain a safe airspace. The AMA emphasized the importance of educating the public about safe UAS operations and believed the data could be helpful in guiding future policy conversations to mitigate safety risks.[86] Even though organizations, such as the AMA, government agencies, such as the FAA, and academia may argue data reliability, other academic research gives merit to the general concern about UAS occupying the airspace. The 2016 research project from Australia's RMIT University studied 150 drone incidents around the world and concluded that 64 percent of the incidents between 2006 and 2016 were caused by technical problems rather than operational error.[87] The majority

---

81 "UAS Sightings Report, Unmanned Aircraft Systems," Federal Aviation Administration, July 22, 2019, https://www.faa.gov/uas/resources/public_records/uas_sightings_report/.

82 Federal Aviation Administration.

83 Academy of Model Aeronautics, *A Closer Look at the FAA's Drone Data* (Muncie, IN: Academy of Model Aeronautics, 2105), 2–3, https://www.modelaircraft.org/sites/default/files/gov/docs/AMAAnalysis-Closer-Look-at-FAA-Drone-Data_091415.pdf.

84 Academy of Model Aeronautics, 4.

85 Academy of Model Aeronautics, 3.

86 Academy of Model Aeronautics, 14.

87 "Tech Issues Cause Most Drone Accidents: Research," RMIT University, August 24, 2016, https://www.rmit.edu.au/news/newsroom/media-releases-and-expert-comments/2016/august/tech-issues-cause-most-drone-accidents--research.

of technical issues identified were related to the UAS communications links.[88] The 2016 study emphasized the need for airworthiness requirements for UAS platforms to help reduce the risk of accidents or incidents.[89]

As concerns surrounding UAS operations crowding airspace and flying near U.S. airports continue, the aerospace community has become more vigilant of UAS activity and its effect on the safety and security of the transportation sector. Recently, multiple incidents have occurred where UAS operations have directly affected the transportation sector. In December 2018, drones were observed flying near Gatwick, the second busiest airport in the United Kingdom (U.K.).[90] The incident resulted in the suspension of air traffic causing significant flight disruptions in the country for three consecutive days.[91] Even after the airport suspended flights, transportation officials reported an additional 40 sightings of drones in the area of the airport.[92] In all, 67 sightings were reported during the shutdown at Gatwick in December 2018.[93] Although law enforcement did not recognize the incident to be terror related, they did consider it a deliberate operation of drones around the airport that resulted in hundreds of cancelled flights and disrupted travel for over 110,000 passengers.[94] As a result of the incident, the no-fly zone around U.K.'s airports was deemed inadequate.[95] More recently, Germany's busiest air travel hub was forced to ground flights for nearly an hour after a UAS sighting was reported near Frankfurt

---

[88] RMIT University.

[89] RMIT University.

[90] "What Are the Busiest Airports in the UK?—We List the Top 20," Inside Flyer UK, January 24, 2018, https://insideflyer.co.uk/2018/01/what-are-the-busiest-airports-in-the-uk/.

[91] Shepardson, "FAA to U.S. Airports."

[92] Robert Wall, "Gatwick Resumes Flights Once Again After Drone Scare; U.K's Second-Busiest Airport Begins Returning to Normal Operations Comes After Sighting of Another Drone," *Wall Street Journal*, December 22, 2018, http://search.proquest.com/docview/2159531786/citation/6E7A280EAB674A70PQ/1, ProQuest.

[93] Chris Stokel-Walker, "Why Drones Cause Airport Chaos," *New Scientist* 241, no. 3213 (January 19, 2019): 10, https://doi.org/10.1016/S0262-4079(19)30100-9.

[94] Matthew Weaver et al., "Military Called in to Help with Gatwick Drone Crisis," *The Guardian*, December 20, 2018, https://www.theguardian.com/uk-news/2018/dec/19/gatwick-flights-halted-after-drone-sighting.

[95] Weaver et al.

airport.[96] Even though landings and takeoffs at the airport were stopped for only one hour, the UAS sighting caused 48 airborne commercial flights to be diverted and another 143 cancellations.[97] Both incidents serve as examples of how careless and malicious UAS operations not only endanger lives, but can also disrupt the critical infrastructure transportation systems sector.

2. Malevolent UAS Operations

> We do know that terrorist organizations have an interest in using drones. We have seen that overseas already with some frequency. I think that the expectation is that it is coming here imminently.
>
> —FBI Director Christopher Wray, September 27, 2017[98]

a. The Conveyance of Illicit Goods

UAS technology has become an effective tool enabling drug cartels to move drugs from Mexico to the United States by avoiding traditional ports of entry or underground tunneling systems.[99] U.S. law enforcement and border patrol entities have not only reported incidents of drones used to smuggle illicit goods across the U.S. border, but have also noted an upward trend in the use of drones to defeat access control measures and deliver illicit goods into prisons within the United States.[100] In 2017, research published from the Center for the Study of the Drone suggests that the use of UAS platforms to

---

[96] Arno Schuetze and Tassilo Humme, "Air Traffic at Frankfurt Airport Resumes after Drone Sighting...," Reuters, May 8, 2019, https://www.reuters.com/article/us-germany-drones-frankfurt-airport-idUSKCN1SF0IU.

[97] "Update: 143 Flights Cancelled at Frankfurt Airport Due to Drone Sighting," The Local, accessed May 18, 2019, https://www.thelocal.de/20190509/disruption-after-frankfurt-airport-halts-flights-due-to-drone-sighting.

[98] Arthur Holland Michel and Dan Gettinger, *Drone Year in Review: 2017*, 7, 2018, https://dronecenter.bard.edu/projects/other-projects/drone-year-in-review-2017/.

[99] Stephen Dinan, "Drones Become Latest Tool Drug Cartels Use to Smuggle Drugs into U.S.," *Washington Times*, August 20, 2017, https://www.washingtontimes.com/news/2017/aug/20/mexican-drug-cartels-using-drones-to-smuggle-heroi/.

[100] Nicas, "Criminals, Terrorists Find Uses for Drones, Raising Concerns."

smuggle illicit items into correctional facilities is on the rise around the world.[101] The 2017 report documented three cases of drone smuggling in the United States between 2013 and 2016.[102] The earliest of the three cases occurred in Georgia where four individuals attempted to smuggle tobacco products into a state prison.[103] According to national media reports, the four individuals were arrested by the Calhoun County Sheriff's Office after a corrections officer at Calhoun State Prison reported a small rotary-wing drone hovering over the prison yard.[104] After a search of the area, the sheriff's office located the individuals and their vehicle, gained consent to search the vehicle, and recovered the drone and approximately two pounds of tobacco wrapped in plastic bundles to be dropped by the drone into the prison.[105] In 2015, a maximum security prison in Maryland exposed its vulnerability to UAS platforms after two individuals were apprehended and sentenced to 13 years in prison for multiple contraband drops with a drone into the Western Correctional Institution.[106] According to local media reports, during a surveillance mission related to an ongoing investigation by prison authorities, the two Maryland residents were found outside the state prison complex with a small quadcopter drone, a firearm, pornography, tobacco and the synthetic drug, K2.[107] Furthermore, the investigation revealed that an inmate coordinated the contraband delivery, which was one of several drone drops, each securing an estimated profit of $6,000.00.[108]

To coordinate such drone drops, communication between those inside prisons and those on the outside must occur. A 2016 incident in Georgia sheds some light on how illicit

---

[101] Michel and Gettinger, *Drone Incidents*, 6.

[102] Michel and Gettinger, *Drone Incidents*, 1.

[103] Michel and Gettinger, 6.

[104] Lindsay Perez, "Drone Tries to Sneak Contraband into Georgia Prison," NBC News, November 27, 2013, http://www.nbcnews.com/news/world/drone-tries-sneak-contraband-georgia-prison-flna2D11665517.

[105] Perez.

[106] Michel and Gettinger, *Drone Incidents*, 6.

[107] Alison Knezevich and Ian Duncan, "Drone Intercepted near Maryland Prison, Officials Say," *Baltimore Sun*, August 25, 2015, https://www.baltimoresun.com/news/crime/bs-md-prison-drone-20150824-story.html.

[108] Michel and Gettinger, *Drone Incidents*, 6.

drone drops enables communication between inmates and the outside world. In September 2016, 16 people in Georgia were indicted for using drones to smuggle cellphones into a state prison to coordinate drug and other illicit good trafficking.[109] After a two-year investigation by the U.S. Attorney's Office of the Southern District of Georgia, an Organized Crime Drug Enforcement Task Force uncovered the conspiracy in which the 16 defendants operated and equipped drones to smuggle cell phones to co-conspirators incarcerated in the Georgia corrections facility.[110] Incarcerated conspirators used the phones to facilitate drug deals outside of the prison via Facebook and PayPal accounts, and to enable drug distribution within the correctional facility while also promoting a climate of fear within the prison system.[111] As a result of these aforementioned incidents, it is logical to believe that traditional checkpoints and other physical security measures at critical infrastructures, such as correctional facilities, are ineffective against drones carrying and delivering illicit items into the prison system. Thus, some prison authorities continue to combat this challenge by enhancing existing perimeter fence with barbed wire, netting, and in some cases, birds of prey.[112] Other correctional facilities have opted to use technology to detect unauthorized drones in the area and attempt to locate both the operator and illicit objects that may have landed on prison property.[113]

b. Reconnaissance, Surveillance, Intelligence, and Interference

Terrorist organizations, such as the Islamic State in Iraq and Syria (ISIS), have realized the benefits of UAS technology to enhance intelligence gathering and bolster their

---

[109] Michel and Gettinger, 6.

[110] "16 Defendants Indicted on Federal Drug Trafficking Charges," United States Department of Justice, Office of the United States Attorneys, Southern District of Georgia, September 28, 2016, https://www.justice.gov/usao-sdga/pr/16-defendants-indicted-federal-drug-trafficking-charges.

[111] United States Department of Justice, Office of the United States Attorneys, Southern District of Georgia.

[112] Tilly Rubens, "Drug-Smuggling Drones: How Prisons Are Responding to the Airborne Security Threat," IFSEC Global, February 8, 2018, https://www.ifsecglobal.com/drones/drug-smuggling-drones-prisons-airborne-security-threat/.

[113] Luke Dormehl, "Prisons Are Fighting Back against Contraband-Dropping Drones," Digital Trends, July 20, 2018, https://www.digitaltrends.com/cool-tech/airwarden-drone-survaillance/.

reconnaissance missions.[114] In 2014, ISIS released surveillance video that included aerial video footage of disputed territory and still images of a Syrian Army military base.[115] The use of small UAS platforms by terrorist's organizations abroad has be recognized by America's armed forces tasked with protecting the nation's security. Some believe the threat posed by a UAS operated by terrorists has created tactical and operational capability gaps within the U.S. military.[116]

The use of UAS technology by terrorists and criminals is not just a national security matter. UAS technology has also become a tool for criminals and gangs in cities around the world including America's hometowns. In as early as 2012, drug cartels were conducting counter surveillance on law enforcement at the U.S.-Mexico border.[117] Since 2012, criminal enterprises, such as gangs, have realized the benefits of using drones to monitor law enforcement activity and missions.[118] In 2017, a criminal gang used a swarm of drones to harass an FBI hostage rescue team.[119] Few details are available surrounding this incident due to its law enforcement sensitive classification. Nevertheless, according to one report, the incident was a collaborative effort by several UAS operators who not only flew drones directly at the FBI hostage rescue team members, but also provided live video surveillance of the agents' positions and movements via YouTube to fellow gang members inside the target of the investigation.[120]

---

[114] Counter Extremism Project, *Digital Developments: Extremists' Use of Modern Communications Tools* (London: Counter Extremism Project, 2019), 11, https://www.counterextremism.com/sites/default/files/Digital%20Developments_031819.pdf.

[115] Jeff Stone, "Does ISIS Have Drones? Propaganda Footage Shows Aerial View of Syrian Raqqa Army Base," *International Business Times*, August 25, 2014, https://www.ibtimes.com/does-isis-have-drones-propaganda-footage-shows-aerial-view-syrian-raqqa-army-base-video-1668474.

[116] David Oliver, "The Flying IED Threat," *Military Technology* 42, no. 5 (May 2018): 67–70, Ebsco.

[117] Ray Downs, "Australian Drug Gang Suspected of Using Drone to Monitor Police," UPI, June 30, 2017, https://www.upi.com/Top_News/World-News/2017/06/30/Australian-drug-gang-suspected-of-using-drone-to-monitor-police/2911498801791/.

[118] Rob Thurbron, "Criminals Used Swarm of Drones to Disrupt FBI Hostage Raid," TechSpot, May 4, 2018, https://www.techspot.com/news/74466-criminals-used-swarm-drones-disrupt-fbi-hostage-raid.html.

[119] Thurbron.

[120] Thurbron.

Malicious UAS operations can also interfere with public safety operations other than law enforcement, such as within the fire services sector of public safety. Many cases of drones disrupting wildland firefighting operations in the United States have been documented.[121] The U.S. Forest Service reported that in 2018, at least 17 drone incursions occurred, 13 of which resulted in the shutdown of firefighting efforts to save life and property.[122] As of July 11, 2019, the U.S. Forest Service has reported four reports of public drone incursions that resulted in the shutdown of two firefighting operations.[123] If a drone collides with firefighting aircraft, it may cause a serious or fatal accident; therefore, when a drone is identified near a scene, firefighting efforts are halted.[124] Halting firefighting operations during wildland firefighting operations can allow the fire to intensify, which then endangers both firefighters on the ground, as well as the property and lives they are trying to protect.[125] Such incidents not only further highlight the difficulty to secure critical infrastructure and outdoor public events, but also causes concern for how to protect public safety operations from not only counter surveillance operations, but also interference.

c. Weaponized Operations

At a special operation forces conference in the Spring of 2017, General Raymond Thomas, the then-Commanding General of U.S. Special Operations Command, referred to terrorists' use of drones for deadly attacks as "fourth-generation warfare."[126] General Thomas shared with the audience that ISIS was able to purchase 70 drones, modify and arm them with 40-mm weapons, and fire them at identified targets, which resulted in the

---

[121] Charles Werner, "Using Drones in the Fire Service," *Firehouse; Fort Atkinson*, 86, April 2015, http://search.proquest.com/docview/1685183092/abstract/CA0B5C8500FE4FC3PQ/1, ProQuest.

[122] Managing the Land, "If You Fly, We Can't," U.S. Forest Service, accessed July 11, 2019, https://www.fs.fed.us/managing-land/fire/uas/if-you-fly.

[123] National Interagency Fire Center, "Unmanned Aircraft Systems (UAS or Drones)," Drones and Wildfires, accessed July 11, 2019, https://www.nifc.gov/drones/.

[124] National Interagency Fire Center.

[125] U.S. Forest Service, "If You Fly, We Can't."

[126] John Ubaldi, "Will Terror Organizations Use Drones to Attack the U.S.?," In Homeland Security, May 15, 2019, https://inhomelandsecurity.com/drones-attack-us/.

halt of daily operations in Iraq for a 24-hour period.[127] Some believe that weaponized drone use by terror organizations in the Middle East also serves as a warning of the potential threat to U.S. hometowns. In 2018, FBI Director Christopher Wray told the Senate Homeland Security and Governmental Affairs Committee he was confident that terrorists would use UAS technology to attack vulnerable targets likely to result in mass casualties within the United States.[128] Director Wray gave context to his assessment by stating that because of continued efforts by terrorists, such as ISIS and Al Qaida, transnational criminal organizations, such as MS-13 and Mexican drug cartels, to weaponize UAS platforms, other malevolent actors within the United States may be inspired to conduct like attacks.[129] Recognition of the potential threat has caused U.S. public safety entities, especially law enforcement, to recognize the ease of purchasing off-the-shelf drones and turning them into weapons.[130] Weaponized UAS platforms remain a persistent threat.[131] Between 2011 and January 2015, several attempts by terrorists to launch drone attacks against U.S. interests at home and abroad were foiled, as well as against other countries, such as Germany, Spain, and Egypt.[132]

It appears as though no region is safe from nefarious UAS operations. In 2012, Rezwan Feredaus was sentenced to federal prison after the FBI disrupted his plan to fill jet-powered, remote-controlled model aircraft with explosives and crash them into the Capitol and Pentagon using global positioning system (GPS) guided technology.[133] Looking abroad, in 2013, the political Pirate Party in Germany used a drone to intimidate

---

[127] Ubaldi.

[128] Christopher A. Wray, *Statement of Christopher A. Wray, Director, Federal Bureau of Investigation, before the Committee on Homeland Security and Governmental Affairs, United States Senate* (Washington, DC: Department of Justice, 2018), 8, https://www.hsgac.senate.gov/imo/media/doc/Testimony-Wray-2018-10-10.pdf.

[129] Wray, 8.

[130] Andy Pasztor and Dustin Volz, "Worries Mount over Ability to Weaponize Drones," *Wall Street Journal*, August 7, 2018, https://www.wsj.com/articles/worries-mount-over-drone-safety-after-venezuela-attack-1533601121.

[131] Nicas, "Criminals, Terrorists Find Uses for Drones, Raising Concerns."

[132] Nicas.

[133] Wray, *Statement of Christopher A. Wray*, 8.

Chancellor Angela Merkel while attending an outdoor event.[134] In 2015, Yasua Yamamoto from Japan turned himself into authorities and admitted that as a protest against nuclear power, he attached a container of radioactive sand retrieved from the 2011 Fukushima nuclear power plant disaster to a drone and landed it on the prime minister's office.[135] Furthermore, the 2017 Conflict Armament Research report monitoring the Islamic State's armament capabilities claimed that the group's sophisticated development of weapons can be compared to those of national military forces and has the wiliness to adapt their weapons to innovative UAS technology for future use in theaters beyond Iraq.[136] Additionally, in 2017, it was discovered that terrorist groups, such as ISIS, were developing an improvised explosive device (IED) that could be transported to strategic locations by a UAS and dropped on specific targets.[137] One example of a weaponized UAS attack using explosives was the 2018 attempt to assassinate the Venezuelan President with IED-laden drones that created mass panic and fear among a large crowd of Venezuelan people.[138] A second and more recent incident of a terrorist attempting to weaponize an unmanned vehicle was in 2019 in the United Kingdom. On July 12, 2019, a jury in the U.K. Sheffield Crown Court found Farhad Salah guilty after his arrest for plotting the terrorist attack.[139] The investigation by police uncovered evidence of Salah's affiliation with ISIS and his

---

[134] Patrice Deschênes, "The Rise of the Drones: Technological Development of Miniaturised Weapons and the Challenges for the Royal Canadian Navy," *Canadian Military Journal* 19, no. 2 (Spring 2019): 51, http://www.journal.forces.gc.ca/Vol19/No2/PDF/CMJ192Ep51.pdf.

[135] Stanley White, "Japanese Man Arrested for Landing Drone on PM's Office in Nuclear Protest," Reuters, April 24, 2015, https://www.reuters.com/article/us-japan-nuclear-drone-idUSKBN0NG04520150425.

[136] Ahmed Aboulenein, "Islamic State Developing New Weapons despite Losses: Arms Monitor," *Reuters*, April 26, 2017, https://www.reuters.com/article/us-mideast-crisis-iraq-arms-idUSKBN17S20N.

[137] "Timeline: The Rise, Spread, and Fall of the Islamic State," Wilson Center, April 30, 2019, https://www.wilsoncenter.org/article/timeline-the-rise-spread-and-fall-the-islamic-state.

[138] Dan Falvey, "Panic in Venezuela as 'Drone Attack' Explosions Hit during Speech by President Maduro," Express, August 5, 2018, https://www.express.co.uk/news/world/999021/venezuela-explosion-caracas-Nicolas-Maduro-speech-panic-terror.

[139] Kylie Bielby, "Terrorists Look to Drones and Driverless Cars to Avoid Martyrdom," Homeland Security Today, July 13, 2019, https://www.hstoday.us/subject-matter-areas/counterterrorism/terrorists-look-to-drones-and-driverless-cars-to-avoid-martyrdom/.

intention to arm an unmanned vehicle with explosives so that he could detonate the bomb remotely to avoid martyrdom.[140]

Reports of weaponized or explosive laden UAS platforms within the United States remain minimal; however, a terrorist's ability to deliver and release explosives from drones raises a concern whether the United States is capable of defending against these threats abroad and within the homeland.[141] In his 2019 thesis exploring 21st century crime, Kevin Peters' research sustains that criminals and other malevolent actors are capable of leveraging existing UAS technology to build unmanned, intelligent aerial weaponized systems in the United States.[142] Peters contends that the homeland security enterprise should develop an appreciative inquiry into the advancement of this potential weapons system.[143] Peters' research supports earlier research distributed by the Naval Postgraduate School in 2018. Aaron Schmersahl conducted research on the use of drones along the U.S.-Mexico border and his thesis concludes that the threat of weaponized drones in the airspace is no longer a novel threat.[144] Schmersahl contends that the threat is a serious concern for homeland security disciplines.[145]

Recent suspicious acts may serve as a valid warning about the likelihood of the threat in the homeland's near future. A series of explosions that rocked a quiet community in Pennsylvania may substantiate 2017 claims by FBI Director Wray that America remains vulnerable to an imminent UAS threat.[146] Although considered speculation by local law enforcement, residents of the Northampton County community in Pennsylvania believe

---

[140] Bielby.

[141] Oliver, "The Flying IED Threat," 1.

[142] Kevin M. Peters, "21st Century Crime: How Malicious Artificial Intelligence Will Impact Homeland Security" (master's thesis, Naval Postgraduate School, 2019), 2, https://www.hsdl.org/?abstract&did=825201.

[143] Peters, 2.

[144] Aaron R. Schmersahl, "Fifty Feet above the Wall: Cartel Drones in the U.S.-Mexico Border Zone Airspace, and What to Do about Them" (master's thesis, Naval Postgraduate School, 2018), 95, https://www.hsdl.org/?abstract&did=811367.

[145] Schmersahl, 95.

[146] Chuck Ross, "FBI Director Discusses Threat of Terrorist Drones," YouTube, 2017, video, :35, https://www.youtube.com/watch?v=GpR2z4-vYJ4&feature=youtu.be.

that a drone dropped explosives into their neighborhood.[147] Local media interviewed residents and local law enforcement and were told that at least 10 explosions were heard during overnight hours and several undetonated devices had been located in front yards between March 2019 and June 2019.[148] Such incidents further support academic research suggesting that the likelihood of weaponized aerial systems threatening America's hometowns is on the rise.[149]

B. UAS TARGETS AND THEIR VULNERABILITIES

Careless or malevolent UAS operations within America's hometowns can threaten the public's safety, as well as the critical infrastructure necessary for a community to remain civil. The following section further frames the risk careless and malicious UAS operations can pose to America's hometowns by identifying likely targets of careless or malevolent UAS operations. Additionally, this section identifies potential targets' vulnerabilities that can result in negative consequences affecting local communities in terms of loss life, economy, and psychological fear. Achieving an understanding of likely targets, their vulnerabilities, and potential consequences can enable emergency planners and local law enforcement to have a better understanding of their community's risk to threatening drones. This knowledge enlightens situational awareness and can enhance jurisdictional risk assessments within America's hometowns by ensuring appropriate mitigation measures are developed to protect their communities from both careless and malevolent UAS operations.

1. Targets

a. Open Access Outdoor Events

Throughout the year, venues in hometowns across the United States host various outdoor events including athletic competitions, concerts, parades, and other celebrations or

---

[147] Jamie Stover, "Explosions Leaving Many on Edge in Northampton County," WFMZ-TV 69 News, June 6, 2019, https://www.wfmz.com/news/lehigh-valley/explosions-leaving-many-on-edge-in-northampton-county/1083883100.

[148] Stover.

[149] Peters, "21st Century Crime," 2.

special events. Furthermore, every state in the nation hosts larger events that occur on or around the same date each year, such as Florida's Daytona Beach Bike Week, and New York's Times Square New Years.[150] As noted earlier in this chapter, these activities, such as sporting events, can be targets of careless and malicious UAS operations.[151] As these events are open access, outdoors, sometimes symbolic, and are publicized to residents and visitors in and around the hometowns, they are often highly visible to the general public. Attendance of these events can range from under 100 to millions of people, which creates the potential for a mass casualty incident.

UAS hobbyist and commercial operators are attracted to these events because of their ability to launch low-cost, consumer grade drones capable of taking high definition video and high-resolution aerial photos over the event to provide live or recorded bird's eye images. Surveying crowds with a drone from above enables them to remain mobile while capturing phenomenal video and photos not possible from ground level.[152] Although this type of surveillance offers benefits to include monitoring crowd behavior at a concert, fair, or parade, tracking lead runners of a marathon, and documenting weddings or other ceremonies for historical purposes, they can also pose a risk to participants on the ground.[153]

Malevolent actors are attracted to outdoor planned events due to open access, the yearly reoccurrence of the events, the likelihood of creating a mass casualty incident, and the opportunity of receiving national exposure. Terrorists and others with criminal intentions recognize the negative effects an intentional attack may have on the host jurisdiction, its residents, as well as its visitors. For many years, terrorists and other malevolent actors have chosen vehicles as the weapon of choice when launching an attack on open access events. For example, in 2010, an issue of al-Qaeda's *Inspire* magazine included an article dedicated to the use of a pickup truck as the ultimate "mowing machine"

---

[150] "Largest Events in Each State," Genfare, accessed July 12, 2019, https://www.genfare.com/resources/largest-events-state/.

[151] Tepper, "The FAA Gets a Case Study with a Drone Crash inside an MLB Stadium."

[152] Michel and Gettinger, *Drone Incidents*, 2.

[153] Miletich, "Pilot of Drone That Struck Woman at Pride Parade Gets 30 Days in Jail."

to mow down pedestrians.[154] Although law enforcement and others within the security community have adopted risk mitigation measures, such as protective bollards to protect the public from vehicle ramming attacks at large outdoor events, they may have inadvertently transferred the risk to a threat from above.[155] A 2014 report from the RAND Corporation contends that a nail bomb dropped by a drone over a crowded outdoor event would produce similar effects of the Boston marathon attack.[156] The capability of an intentional UAS attack on a large outdoor event was validated in 2017 after a drone flew over not one, but two professional football games in California, and dropped anti-media propaganda onto the fans.[157] The two incidents demonstrated the ease of using UAS technology to deliver and drop potential weapons over a crowd to create mass casualties.[158] What may be even more troubling is the creation of a weapon of mass destruction (WMD) using a UAS to transport chemical or biological agents and disperse them over a large, outdoor event. Researchers from the RAND Corporation contend that al-Qaeda, along with other terrorist organizations, continue to inspire followers to engineer a WMD and launch an attack in the West.[159] Whether such an attack resulted in mass casualties, the attempt alone could perpetuate the fear of terrorism within the United States.[160]

---

[154] Julie Shain, "Cars and Trucks as Weapons of Terror," *Tech and Terrorism* (blog), April 7, 2017, https://www.counterextremism.com/blog/cars-and-trucks-weapons-terror.

[155] Mike Ventiere, II, "Soft Targets: Stemming the Tide of Vehicle Ramming Attacks," *Security Technology Executive* 27, no. 3 (August 2017): 17, ProQuest.

[156] Lynn E. Davis et al., *Armed and Dangerous?* (Santa Monica, CA: RAND, 2014), 7, https://www.rand.org/pubs/research_reports/RR449.html.

[157] Lea Gabrielle, "Drone Drops Leaflets over Football Stadiums, Raising Security Concerns," Fox News, November 27, 2017, https://www.foxnews.com/tech/drone-drops-leaflets-over-football-stadiums-raising-security-concerns.

[158] Charles Werner, "Drones: The Need for Counter-Technology," *Firehouse*, 1, February 2018, http://search.proquest.com/docview/1989496569/abstract/BF5592D978FB4EEAPQ/1, ProQuest.

[159] Colin P. Clarke, "Approaching a 'New Normal': What the Drone Attack in Venezuela Portends," *The RAND Blog* (blog), August 13, 2018, https://www.rand.org/blog/2018/08/approaching-a-new-normal-what-the-drone-attack-in-venezuela.html.

[160] Clarke.

b. Critical Infrastructure

DHS has identified 16 sectors recognized as critical infrastructure whose continuity of operations is vital to the security, economy, and public health of the nation.[161] Although every city within the United States may not have infrastructure considered critical from a national perspective, every locale is supported by various physical or virtual assets, systems, and networks critical to their own mission. As a result of their geographical locations, level of visibility, accessibility, types of materials on site, and population capacity, they may be vulnerable to careless or malicious UAS operations that could result in grave consequences in terms of loss of life, financial loss, and psychological damage within the community. Due to their versatility and impressive operational capabilities, UASs can easily evade detection and other protection measures at critical infrastructure, which creates new challenges for owners and operators.[162] Examples include commercial facilities and entertainment venues supporting a viable local economy; communications towers that ensure interoperable communications; emergency services responsible for prevention, protection, response and recovery missions; energy and water treatment assets providing water and electrical utility needs, and transportation assets that facilitate the movement of goods and people. In a 2016 National League of Cities research report focusing on UAS platforms and their effects on municipal government, researchers discovered a gap in measures to protect critical infrastructure within the nation's hometowns from careless and malicious drone operations. The report contends that due to a lack of FAA regulations prohibiting the operations of UAS platforms near critical infrastructure, physical assets, such as power plants, prisons, and refineries remain vulnerable.[163]

---

[161] "Infrastructure Security," Department of Homeland Security, July 16, 2012, https://www.dhs.gov/topic/critical-infrastructure-security.

[162] Department of Homeland Security, *Unmanned Aircraft Systems: Addressing Critical Infrastructure Security Challenges, Fact Sheet* (Washington, DC: Department of Homeland Security, 2017), 1, https://www.dhs.gov/sites/default/files/publications/uas-ci-challenges-fact-sheet-508.pdf.

[163] Zickuhr, Stahl, and DuPuis, *Cities and Drones*, 33.

2. Target Vulnerabilities

a. Geographic Location

In terms of vulnerabilities associated with the geographical location of the target, law enforcement, special event planners, and critical infrastructure owners should stay aware of the level of visibility of the target and the types of materials that may be stored inside or near critical infrastructure or outdoor events. Assessing the level of visibility is a measurement of both the symbolic importance and awareness of the existence of the target to the general public. For example, an asset of symbolic importance, such as a national monument, may have a regional or national level of visibility, while only local residents may know of the existence of a municipal water treatment facility. A critical asset of symbolic importance and high visibility may be more vulnerable than the asset known only locally. Furthermore, assessing the presence of hazardous materials either stored or used at a specific critical infrastructure facility or near a planned outdoor venue is also important. Depending on the specific location, type and amount of hazardous material present, an accident or attack could complicate response and recovery operations and increase the likelihood of a mass casualty incident.

b. Impact within and outside of the Jurisdiction

Another factor to consider when assessing the vulnerability of a target is the measurement of the criticality of the asset, system, or network to local, regional, and international communities.[164] A careful assessment of the target's value to the economy and government services essential to the continuity of government are key to understanding the potential impact the loss or damage of the target may have both within and outside of the jurisdiction. Airports, for example, serve a critical role within the transportation sector by connecting people, goods, and services around the world.[165] In Oklahoma City (OKC), the City of Oklahoma City owns three airports. Will Rogers World Airport (WRWA) is

---

[164] Ionuţ Alin Cîrdei, "Improving the Level of Critical Infrastructure Protection by Developing Resilience," *Land Forces Academy Review* 23, no. 4 (December 1, 2018): 238, https://doi.org/10.2478/raft-2018-0028.

[165] Kimberly Arsenault, "The Threats to Transportation Infrastructure: Airports at Risk," In Homeland Security, April 4, 2017, https://inhomelandsecurity.com/transportation-infrastructure-airport/.

the largest of the three airports that combines daily freight, commercial, military, corporate, and general aviation.[166] The disruption to the airspace around OKC's WRWA due to a UAS could have a major impact on the transportation sector both locally and nationally. For safety reasons, the FAA may suspend air travel in and out of the airport that then results in cancellations and delays of flights around the country. On the other hand, a UAS operating within the airspace of a smaller municipal airport, such as Wiley Post Airport in OKC, may only have a local or regional affect to air travel in and out of OKC. Wiley Post serves as a reliever airport to WRWA and serves primarily corporate and business aviation.[167]

c. Access Control

Since the three dimensional perimeter around critical infrastructure and outdoor planned events can be difficult to secure, the level of access a UAS has to a potential target is often unlimited. The mere fact that many of these events and infrastructure are open access, they remain more vulnerable to careless or malevolent UAS operations. Security personnel and event planners should remain knowledgeable of the air domain around these targets and create partnerships with the FAA that has authority over the airspace.[168] Unfortunately, no single mitigation action can completely eliminate the risk.[169] Obtaining a restriction on the airspace around a target can help mitigate the threat. However, although airspace can be restricted at times to prevent UAS operations in or near a potential target, the regulations are only effective to those who both understand and abide by them.

d. Potential for Mass Casualties

Determining the vulnerability of a mass casualty incident at a planned event or within the realms of critical infrastructure focuses on the population capacity at the target site, as well as the potential for mass casualties within a defined radius of the target.

---

166 "Department of Airports/Airport Trust," Wiley Post Airport, accessed July 14, 2019, http://wileypostairport.com/Page/AirportsTrust.

167 Wiley Post Airport.

168 Department of Homeland Security, *Unmanned Aircraft Systems*, 1.

169 Department of Homeland Security, 1.

Targets, such as sporting events, may have a population capacity in the thousands, while other targets, such as a power plant, may have less than 100 personnel on site at any given time. Based on the number of spectators, players, and employees at a packed football game, casualties may potentially number in the thousands, while at the power plant, less than 100 casualties may occur as the result of a weaponized UAS assault. However, when looking at the potential for collateral mass casualties, an attack on a power plant causing the loss of power, may affect an entire jurisdiction, whereas the attack on the football stadium remains somewhat localized.

DHS contends that a real concern exists about drones and their use by malevolent actors, such as terrorists, to launch mass casualty attacks over large groups of people.[170] Terrorists and other nefarious actors view large, open access, outdoor events, and critical infrastructure within the transportation sector as target rich environments because with little effort they can produce mass casualties.[171] DHS further supports its concern with a brief look at the history of flight in general and the tactical advantage of launching an attack from the sky, and argues that it is not unreasonable to accept that evolving technology will support capable UAS operations effective in launching attacks from the air.[172] Cathy Lanier, National Football League Chief Security Officer, agrees with DHS. Lanier has stated that technology demands public safety's rapid adaptability to the evolving threat environment, and that, "the speed of change" keeps her up at night.[173]

C. SUMMARY

Advances in technology continue to expand beyond imaginations of the general public. What was once a tool used by military forces overseas as a force multiplier in conducting surveillance and completing tactical missions is now a relatively available and

---

[170] CISA Infrastructure Security Division, "Unmanned Aircraft Systems (UAS)—Critical Infrastructure," 00:46–00:56, Department of Homeland Security, accessed July 14, 2019, https://www.dhs.gov/cisa/uas-critical-infrastructure.

[171] Jonathan R. White, *Terrorism and Homeland Security*, 7th ed. (Belmont, CA: Cengage Learning, 2012), 151.

[172] CISA Infrastructure Security Division, "Unmanned Aircraft Systems (UAS)," 00:57–01:25.

[173] CISA Infrastructure Security Division, 01:26–01:37.

inexpensive tool available to anyone. Technological advances have enabled designers of UAS platforms to create small, light, and nimble drones, equipped with capabilities attractive to both hobbyists, and unfortunately, nefarious actors. Furthermore, the ensuing proliferation of UAS platforms in the sky over America's hometowns has created a crowded airspace and significant challenges on the ground to protect privacy, property, and lives from careless and malevolent flight operations.

UAS that operate in careless or threatening manners have become a concern for public safety entities and owners and operators of potential targets, such as critical infrastructure and open-access outdoor planned events. UAS platforms expose vulnerabilities of these targets and require those responsible for maintaining safe and secure cities to include UAS platforms as a likely threat to lives, property, and the continuity of a civil society. Although hobbyists may have no intent to harm, careless UAS operations to obtain aerial footage of events, people, and infrastructure can interrupt critical transportation sectors, such as air travel, and also threaten the safety of people on board manned aircraft or attending an outdoor event.

Although no impactful malevolent UAS attack has occurred within the United States, subject matter experts within the homeland security project warn of future attacks. Both DHS and the FBI express concern for the future threat of nefarious UAS operations within America. UAS platforms have proven capabilities to deliver illicit goods into U.S. prisons. Moreover, as UAS technology has become a useful tool for public safety to monitor criminal activity, it has also become a tool of counter-surveillance for the criminal element. However, what may be more alarming is an emergence of weaponized UAS platforms within this nation's hometowns. As the criminal element and terrorists leverage existing UAS technology to build unmanned, intelligent, weaponized systems, those tasked with hometown security must acknowledge their communities' risk and work to mitigate vulnerabilities of targets, such as outdoor, open access events, and critical infrastructure exposed to nefarious UAS operations.

THIS PAGE INTENTIONALLY LEFT BLANK

III. ACTIVE AND PASSIVE C-UAS MEASURES

With an increase in use of UAS technology around the globe and the recognition that careless or malevolent UAS operations are likely, a growing interest has arisen in research and development of counter-drone technology.[174] Furthermore, the awareness of UASs traversing the airspace above America's hometowns along with the occurrences of careless and weaponized drones, has some American law enforcement executives exploring options their agencies have to protect from the threat.[175] C-UAS measures can be defined as prevention and protection capabilities enhanced through innovative technological systems designed to detect or interdict UAS platforms.[176]

Much like the UAS market, the C-UAS market is rapidly advancing in an attempt to maintain pace. In 2017, the Institute for Defense Analysis produced a five-year outlook of trends in UAS and C-UAS technology. Their analysis concluded that although technology supporting the detection and tracking of UAS platforms would grow steadily, the evolving development of UAS capabilities would likely create new capability gaps in protection from careless and malevolent UAS operations.[177] According to a 2018 Bard College study of C-UAS technology, over 230 C-UAS systems are available, produced by 155 manufacturers around the world.[178] Although most C-UAS technology systems produced today are typically designed to either detect or interdict, innovations have made it possible for some systems to be capable of both counter measures using ground-based, hand-held, or UAS-based platforms.[179] As of this research, the reader should understand that the authorization for state and local law enforcement to deploy C-UAS measures to

---

[174] CISA Infrastructure Security Division, 03:49–04:04.

[175] Michael Hamann, "Can You Legally Counter a Drone?," *Police Magazine*, November 16, 2018, http://www.policemag.com/486684/can-you-legally-counter-a-drone.

[176] Michel, *Counter-Drone Systems 2018*, 1.

[177] James Herrera, Jason A. Dechant, and E. K. Green, *Technology Trends in Small Unmanned Aircraft Systems (SUAS) and Counter-UAS: A Five Year Outlook*, IDA Paper P-8823 (Alexandria, VA: Institute for Defense Analysis, 2017), iv, https://apps.dtic.mil/dtic/tr/fulltext/u2/1047506.pdf.

[178] Michel, *Counter-Drone Systems 2018*, 1.

[179] Michel, 11–18.

detect, track, interdict, or disrupt a UAS is limited. Although some forms of detection and tracking are legal, C-UAS measures employing active counter-drone technology remain illegal with a few exceptions.[180] A comprehensive legal analysis of C-UAS technology goes beyond the scope of this thesis. The narrow scope of this thesis researches counter-drone technology to provide local law enforcement executives an idea of its future use within local jurisdictions once C-UAS authority is expanded to first responders at all levels of government throughout America.

Providing an analysis of C-UAS technologies can help state and local law enforcement determine the best option they have to bolster capabilities to detect, interdict, interrupt, and disrupt careless and malevolent UAS operations in their hometowns. The chapter first examines passive countermeasures, such as detection and tracking. The second section of this chapter examines active countermeasures. Specific active countermeasures reviewed are those with capabilities to interdict, and in some cases, disrupt a threatening UAS to take control of the aircraft when it enters airspace above protected assets and large-scale planned events.

A. PASSIVE COUNTERMEASURES

Common passive C-UAS measures center on strategies to detect and track UAS platforms. These countermeasures are aimed to recognize the UAS manufacturer and model number, and identify the operator. The FAA contends that the two most important ways to address careless or malevolent UAS operations include the identification of the operator and timely notification of the incident to the FAA.[181] Furthermore, the FAA considers law enforcement as best positioned to detect a UAS in the airspace above their communities, and are likely to be the first government agency to make contact with the operator.[182]

---

[180] Hamann, "Can You Legally Counter a Drone?"

[181] Federal Aviation Administration, *Law Enforcement Guidance for Suspected Unauthorized UAS Operations* (Washington, DC: Department of Transportation, 2018), 6.

[182] Federal Aviation Administration, 6.

Unfortunately, most state and local law enforcement agencies are capable of only monitoring the airspace above their communities through the eyes of personnel assigned to physical security assignments. Law enforcement's emphasis on suspicious activity reporting within the community and assigning personnel the additional responsibility of surveying threats in the airspace over critical infrastructure and key resources (CIKR), or planned outdoor events, can be effective, but even if spotted by law enforcement officers on the ground, the intentions of the operator remain elusive.[183] However, with the assistance of passive C-UAS technology facilitating advanced detection and tracking capabilities, risk assessments may be enhanced, which provides exact operator location and identification, and the delivery of this information to the FAA.

The first line of defense against a threatening UAS is early detection and identification.[184] C-UAS technology designed to detect a UAS employs radar, RF, electro-optical (EO), infrared (IR), and acoustic technologies to detect the presence of drones in the airspace.[185] C-UAS technology that emits radar to detect UAS radio frequency signals, or that is equipped with electro-optical, infrared, or acoustic detection capabilities, aids the naked eye in the early detection of potential UAS threats. Radar technology exposes objects invisible to the naked eye under certain conditions due to weather, lack of daylight, and distance.[186] The technology behind radar detecting systems not only detects objects in airspace, but can also measure the distance, direction of travel, velocity of the object, its physical parameters, and course.[187]

In addition to detection, C-UAS systems equipped with EO/IR and acoustic technologies can also help public safety track a drone's flight pattern and guide public safety personnel to the careless or malevolent operator of the UAS platform. EO/IR

---

[183] Stevens, "Enforcing 'No Drone Zone'."

[184] Alexander Solodov et al., "Analyzing the Threat of Unmanned Aerial Vehicles (UAV) to Nuclear Facilities," *Security Journal* 31, no. 1 (February 2018): 312, https://doi.org/10.1057/s41284-017-0102-5.

[185] Michel, *Counter-Drone Systems 2018*, 4.

[186] "Radar Principle," Radar Basics, accessed July 28, 2019, http://www.radartutorial.eu/01.basics/Radar%20Principle.en.html.

[187] Radar Basics.

imaging has been used extensively for threat detection as this technology enables the detection of a targeted threat in both daytime and low-light or nighttime conditions.[188] These systems are designed to not only recognize radar signature, but also RF emittance, visual and heat signatures, and actual noise produced by the drone's motors.[189]

The use of passive C-UAS technology is growing and its use can be found in and around CIKR and planned events around the country. In 2015, the Boston Police Commissioner confirmed the use of C-UAS technology for the Boston Marathon. Boston Police Department partnered with DroneShield whose drone detection system used omnidirectional microphones to compare sounds with acoustic signatures associated with common consumer drones.[190] More recently, during the 2018 Professional Golfers Association tour in Scottsdale, Arizona, Dedrone RF sensing technology was deployed. The C-UAS technology assisted local authorities in detecting approximately 36 unauthorized drones intruding over the area of the golf tournament.[191] According to media reports, Dedrone's C-UAS detection and tracking capabilities supported by RF and Wi-Fi sensors, included cameras and audio sensors to collect data on drones in the area, such as make, model, and flight paths.[192] The Scottsdale, Arizona, police department claimed that deploying drone detection technology enabled them to provide another layer of protection from unauthorized drones, which presented a safety hazard to tournament participants and spectators.[193] Finally, this past year, during the 2019 Super Bowl in Atlanta, Georgia, law enforcement collaborated at the federal, state, and local levels to also deploy drone

---

[188] Byeong Hak Kim et al., "V-RBNN Based Small Drone Detection in Augmented Datasets for 3D LADAR System," *Sensors* 18, no. 11 (2018): 3825, https://doi.org/10.3390/s18113825.

[189] Michel, *Counter-Drone Systems 2018*, 4.

[190] Shawn Musgrave, "Boston Police Set Up 'Drone Shields' along the 2015 Marathon Route," Vice, April 22, 2015, https://www.vice.com/en_us/article/ezv83k/boston-police-set-up-drone-shields-along-the-2015-marathon-route.

[191] Sally French, "A Bunch of People Are Illegally Flying Drones around the PGA Tour Right Now," *The Drone Girl* (blog), February 2, 2018, http://thedronegirl.com/2018/02/02/bunch-people-illegally-flying-drones-around-pga-tour-right-now/.

[192] French.

[193] Stephanie Olmo, "Scottsdale Police Using Drone Detection Technology at Waste Management Phoenix Open," Fox 10 Phoenix, February 1, 2018, http://www.fox10phoenix.com/news/arizona-news/scottsdale-police-using-drone-detection-technology-at-waste-management-phoenix-open.

detection technology. It was reported that they identified 54 unauthorized drones operating near the Mercedes-Benz Stadium during the super bowl weekend.[194]

This thesis argues that combining both traditional law enforcement surveillance strategies with C-UAS technology can enhance detection and tracking capabilities. Furthermore, combining the technology with traditional police practices can enable law enforcement to meet the FAA's assumptions that local law enforcement is best positioned to detect unauthorized UAS. Table 1 shows passive C-UAS technology and a summary of its prevention and protection capabilities currently available to assist state and local law enforcement's efforts to protect the public's safety from careless or malevolent drone operations.

Table 1. Passive C-UAS Technologies[195]

Technology	Capability
Radar	Use of conventional radar systems to scan a defined airspace for drones. The radar system scans for radar signatures emitted from a UAS to provide early warning of the presence of a drone in a defined airspace.
Radio-frequency (RF)	Scans the airspace for the specific band of frequencies most drones operate within and uses algorithms from RF emitting devices in the airspace that may be drones.
Electro-optical (EO)/Infrared (IR)	EO technology that detects drones within the airspace based on a visual signature. IR detects a drone in the airspace based on its heat signature.
Acoustic	Technology capable of matching the sound produced by a drone's motor to a specific sound within a library of sounds created by drones.
Combination of C-UAS Technologies	The integration of one or more technologies to enable enhanced detection capability. Can increase the accuracy of detection.

[194] Anna Giaritelli, "Super Bowl Saw 54 Drone Incursions: Homeland Security," *Washington Examiner*, April 10, 2019, https://www.washingtonexaminer.com/news/super-bowl-saw-54-drone-incursions-homeland-security.

[195] Michel, *Counter-Drone Systems 2018*, 4.

B. ACTIVE COUNTERMEASURES

Active C-UAS measures are designed to interdict and disrupt a threatening UAS by employing RF jamming, GPS jamming, spoofing, and kinetic countermeasures, such as laser weapons systems, and the deployment of netting.[196] Since the authority to use these countermeasures remains limited to military and federal entities, state, and local public safety agencies remain deficient in their ability to interdict and disrupt threatening drones.[197] While waiting for federal legislation to grant local law enforcement the authority to take active counter measures against threatening drones, state and local public safety executives should expand their awareness of active C-UAS technologies. Acquiring a basic understanding of the technology behind C-UAS jamming measures can provide public safety officials insight into how this technology can help stop a potential accident or drone attack within America's hometowns if C-UAS authority is extended to their level of government.

C-UAS jamming systems interdict and disrupt RF and GPS signals making up the communications loop of UAS platforms. An example of RF jamming interdiction technology is found in the Ghoul Tool Full Spectrum (GTFS) hand-held jammer. The GTFS is part of the Gould Tool line of drone countermeasures offered by Florida-based Invisible Interdiction Inc. intended for use by the military, law enforcement, and other counter-terror organizations.[198] The GTFS works by interrupting command and control radio links between the drone pilot and the drone.[199] While the GTFS is designed to jam drone control frequencies and force the drone to go home, other C-UAS systems are able to not only interrupt, but can disrupt the UAS enabling law enforcement to safely down the

---

[196] Michel, *Counter-Drone Systems 2018*, 4.

[197] Joseph De Avila, "New York Police Seek Authority to Take down Drones," *Wall Street Journal*, February 17, 2019, https://www.wsj.com/articles/new-york-police-seek-authority-to-take-down-drones-11550419320.

[198] "The Ghoul Tool Full Spectrum (GTFS) Hand-Held Drone Countermeasure Has Arrived!," sUAS News, August 29, 2018, https://www.suasnews.com/2018/08/the-ghoul-tool-full-spectrum-gtfs-hand-held-drone-countermeasure-has-arrived/.

[199] sUAS News.

drone for recovery.[200] For example, the DroneGun Tactical platform employs RF and GPS jamming technology to not only interrupt command and control between the drone and pilot, but also gives law enforcement control over the drone to perform a controlled landing in a safe location.[201] With the ability to land the drone, law enforcement is more likely to safely recover the drone, and possibly render a potential nefarious UAS safe. Additionally, armed with the capability of returning the drone back to the starting point can assist with identifying the operator.[202]

In its most basic design, a hand-held C-UAS jamming system has frequency specific antennas and a transmitter to emit an appropriate jamming signal to a drone overhead. The jamming signals disrupt frequencies and communication links necessary for controlling the drone and receiving video from the drone. Hand-held jamming C-UAS systems are simple and easy to operate. Many hand-held C-UAS systems are connected to a rifle platform enabling an operator of the system the ability to aim at a specific target while transmitting the jamming signals. The platform includes a panel with a power switch and dials enabling the operator to dial in appropriate frequencies. On-board re-chargeable batteries power the systems. The RF jamming capability requires three circuits, the RF circuit, a tuning circuit, and the power supply circuit.[203] The components of the transmitter's RF circuitry include a voltage controlled oscillator and a tuning circuit.[204] The oscillator, powered by an on-board linear amplifier, enables the system the ability to sweep the specific bands, as the tuning circuit drives the oscillator.[205] Essentially, all the components that make up a hand-held C-UAS jamming device are packaged in an easy to

---

200 "UAV Detection—Drone Electronic Defeat Systems," Invisible Interdiction, accessed December 2, 2018, https://invisidiction.com/.

201 "DroneGun Tactical," DroneShield, accessed December 2, 2018, https://www.droneshield.com/dronegun-tactical/.

202 DroneShield.

203 Ahmad Jisrawi, "Drones Jammer. A Simple Drone Jammer Designed to Hack Unwelcomed Civilian Drones within Your Backyard Range," DocPlayer, 1, accessed October 10, 2019, https://docplayer.net/7556467-Drones-jammer-a-simple-drone-jammer-designed-to-hack-unwelcomed-civilian-drones-within-your-backyard-range.html.

204 Jisrawi, 2.

205 Jisrawi, 2.

deploy platform to make them an appealing tool for first responder agencies. Although it is readily available on the open market, C-UAS jamming technology is only one of several C-UAS measures to consider.

Global Navigation Satellite Systems (GNSS) directing UAS flight navigation can be vulnerable beyond signal blocking and jamming technologies described previously.[206] Many current UAS platforms make use of affordable and small integrated circuits to take advantage of the navigational accuracy provided by GNSS and the associated United States' GPS satellites that makes them also vulnerable to spoofing.[207] In 2019, an analysis report published by the Center for Advanced Defense Studies concluded that GNSS attacks, such as spoofing, are becoming viable measures to disrupt effectively communication signals necessary for accurate time and navigation data.[208] GNSS spoofing differs from jamming. Instead of simply drowning out satellite signals with noise, spoofing is the act of transmitting false signals that imitate the true satellite system signals received by a GNSS receiver, which causes it to receive false position and timing data.[209] More specifically, spoofing technology transmits counterfeit GPS signals to disrupt the communication links between a drone and its controller.[210] Fortunately, most commercially available drones in the market today use civil GPS much like what is used in cellular phones, automobile navigation, and watches. Civil GPS is different from military GPS in that it is not encrypted and is more vulnerable to C-UAS spoofing measures.[211] Therefore, since commercial GPS receivers found in most UAS platforms

---

[206] Center for Advanced Defense Studies, *Above Us Only Stars: Exposing GPS Spoofing in Russia and Syria* (Washington, DC: C4ADS, 2019), 3, https://www.c4reports.org/aboveusonlystars.

[207] "How GPS Drone Navigation Works," Drone Omega, accessed July 29, 2019, https://www.droneomega.com/gps-drone-navigation-works/.

[208] Center for Advanced Defense Studies, *Above Us Only Stars*, 3.

[209] U.S. Air Force, "Information about GPS Jamming," GPS, accessed July 30, 2019, https://www.gps.gov/spectrum/jamming/.

[210] Andrew J. Kerns et al., "Unmanned Aircraft Capture and Control via GPS Spoofing," *Journal of Field Robotics* 31, no. 4 (August 2014): 617, https://doi.org/10.1002/rob.21513.

[211] AirMap, "Security and the Drone-of-Things," *AirMap* (blog), April 13, 2016, https://www.airmap.com/security-drone-of-things/.

available to the public are not equipped with strong spoofing defense systems, C-UAS spoofing technology may also be a viable option for state and local law enforcement.[212]

Another approach to counter UAS platforms is to deploy kinetic countermeasures, such as anti-missile laser technology.[213] Since at least 1973, laser weapons systems have proven their effectiveness in taking down airborne objects.[214] The military continues to exercise C-UAS measures including defense contractor's use of lasers to defend against UAS threats during the military's 2015 Back Dart exercise.[215] More recently, high-energy technologies, such as laser beams used to interdict and disrupt a single UAS, have also shown some promise in defending against swarms of drones.[216] Major Andrew Sanders' 2017 U.S. Army Command and General Staff College monograph titled Drone Swarms, substantiates this claim by stating that swarms of drones are vulnerable to both C-UAS jamming technologies and lasers.[217] In January 2019, Raytheon claimed that their high-energy laser disrupted 45 drones, some of which were part of a swarm of drones, during a U.S. Army exercise in New Mexico.[218]

Although the complex explanation of a radar weapons system is beyond the scope of this thesis, a basic explanation of how laser technology can be used against airborne objects, such as a single UAS or a swarm of drones, can be found in laser weapon systems deployed with the U.S. Army's Mobile Expeditionary High Energy Laser Program. The

---

[212] Logan Kugler, "Why GPS Spoofing Is a Threat to Companies, Countries," *Communications of the ACM* 60, no. 9 (September 2017): 18, https://doi.org/10.1145/3121436.

[213] Ray Coulombe, "Drone Zone," *Security Technology Executive* 27, no. 3 (August 2017): 10, ProQuest.

[214] David Hambling, "Drones Fight Back against Laser Weapons: And They Might Be Winning," *Popular Science*, November 4, 2016, https://www.popsci.com/laser-guns-are-targeting-uavs-but-drones-are-fighting-back/.

[215] David M. Hall, "Not the Drones You're Looking for: Civil Drones Invading Stability Operations" (master's thesis, School of Advanced Air and Space Studies, Air University, 2016), 2, https://www.hsdl.org/?abstract&did=822552.

[216] "Bad to the Drone—This System Helps to Clip the Wings of Malicious Unmanned Aircraft," Raytheon, May 5, 2019, https://www.raytheon.com/news/feature/bad-drone.

[217] Andrew William Sanders, "Drone Swarms" (monograph, Leavenworth, KS: School of Advanced Military Studies, U.S. Army Command and General Staff College, 2017), 28, https://apps.dtic.mil/dtic/tr/fulltext/u2/1039921.pdf.

[218] Raytheon, "Bad to the Drone."

system can be mounted to a vehicle or a tripod, and with the assistance of an on-board power generating source, can neutralize small UASs.[219] Such laser weapons systems enable operators to track and disrupt an object, such as a UAS with directed energy produced by laser technology.[220] Another benefit of laser technology to counter threatening UAS operations is that laser technology does not rely on the identification of UAS navigation systems; therefore, it can be effective against a UAS that has been modified with self-contained guidance.[221] Manufacturers claim that such laser systems can perform as a standalone measure or be paired with other defense systems providing an effective, accurate, and economical solution to defeat threats to a range of at least 22 miles.[222] Some common benefits of laser technology include:[223]

- Speed of light interface
- Line of sight target engagement
- Very rapid re-engagement capability
- Multiple target engagements
- Single shot accuracy

Furthermore, because of their compact size, a single operator could deploy small laser weapons systems. The basic components of a laser weapons system includes a battery, an on-board water chiller system, a commercially available laser with a specially designed

---

[219] Todd South, "This Laser Could Help Marines Knock down Drones on the Fob or on the Move," *Marine Corps Times*, September 29, 2018, https://www.marinecorpstimes.com/news/your-marine-corps/2018/09/29/this-laser-could-help-marines-knock-down-drones-on-the-fob-or-on-the-move/.

[220] Boeing, "Silent Strike: Boeing's Compact Laser Weapons System Tracks and Disables UAVs," Boeing Defense, August 27, 2015, https://www.boeing.com/features/2015/08/bds-compact-laser-08-15.page.

[221] Palmer and Geis, "Defeating Small Civilian Unmanned Aerial Systems to Maintain Air Superiority," 107.

[222] Robert Farago, "New from Boeing: Compact Laser Weapon System," The Truth about Guns, July 7, 2015, https://www.thetruthaboutguns.com/new-from-boeing-compact-laser-weapon-system/.

[223] David H. Titterton, *Military Laser Technology and Systems* (Boston, MA: Artech House, 2015), 241–42.

beam director, that can be broken down into four separate parts for transport.[224] A key takeaway of such laser systems is that a once complex weapons system is now becoming available as a somewhat portable unit less burdensome to deploy.

While laser technology remains somewhat complex, other kinetic counter measures offer a low-tech, simple option. The term "drone catcher" is a C-UAS technology involving the use of nets that can be deployed from a traditional firearm platform, remotely from a shoulder-mounted weapon resembling a rocket launcher, or via an attack drone that pursues a targeted drone and launches a net to capture the drone.[225] As early as 2017, net-filled shotgun shells were being offered to military and police as anti-drone rounds.[226] In their most basic form, the .12 gauge shotgun shells contain a compressed net with weights that when deployed are designed to entangle with the drone and its motors, which then renders it paralyzed.[227] The launching of nets to entangle a threatening drone overhead are also meant to disrupt a threatening UAS, much like a traditional scattergun, but capture rather than destroy the drone. The concept behind kinetic C-UAS measures, such as nets, is that once the net captures the target drone, either it falls from the airspace, or if caught by another drone, is transported to a safe area and landed to mitigate any threat.[228]

This countermeasure has been marketed as a simple method to deal with threatening drones and has been used as force multiplier in securing critical infrastructure and key resources around the world. After a drone with trace amounts of radiation was intercepted in 2015 over the Japanese prime minister's office, Tokyo's police force stepped up C-UAS measures. By December that year, the police force had added a fleet of UAS platforms with

---

[224] Farago, "New from Boeing."

[225] Donovan Alexander, "Drone Hunters: 9 of the Most Effective Anti-Drone Technologies for Shooting Drones out of the Sky," Interesting Engineering, January 22, 2019, https://interestingengineering.com/drone-hunters-9-of-the-most-effective-anti-drone-technologies-for-shooting-drones-out-of-the-sky.

[226] Matthew Humphries, "U.S. Air Force Orders Anti-Drone Net-Filled Shotgun Shells," PCMAG, March 14, 2017, https://www.pcmag.com/news/352360/us-air-force-orders-anti-drone-net-filled-shotgun-shells.

[227] Andy Greenberg, "Watch a Test of Anti-Drone Weapons, from Shotguns to Superdrones," *Wired*, July 26, 2017, https://www.wired.com/story/watch-anti-drone-weapons-test/.

[228] "How Countries Counter the Drone Threat," BBC News, December 21, 2018, https://www.bbc.com/news/technology-46639099.

drones that carry large nets to their riot teams, which allowed trained officers the ability to catch unauthorized drones in midair flying over sensitive locations.[229] In 2016, a shoulder-mounted system, SkyWall, was deployed in Berlin as a protective measure during President Obama's visit.[230] According to an associate professor of mechanical engineering at Michigan Technological University, a drone catcher is a simple autonomous system that enables the effective pursuit and capture of unauthorized drones.[231]

Table 2 summarizes currently available active C-UAS technology to assist state and local law enforcement in protecting the public's safety from careless or malevolent drone operations.

Table 2. Active C-UAS Technologies[232]

Technology	Capability
RF and GNSS Jamming	Disrupts radio frequency or satellite communications links, such as GPS used by a UAS platform for navigation. A disruption of the communications systems causes the drone to either drop to the ground or return home. Disrupting the satellite link interrupts the drone's navigation and can also cause it to hover in place.
Spoofing	Spoofing can be referred to as protocol manipulation, which makes it possible to take control of a threatening drone by hijacking satellite communications links and disrupting a drone's navigational capabilities.
Laser	Actively directing energy at a specific drone in the airspace to destroy portions of the drones frame and cause it to crash.
Netting	Deploying nets and projectiles into the airspace to entangle, capture, or destroy a drone while in the flight.
Combination of C-UAS Technologies	Common interdiction technologies that can work in tandem to interdict or disrupt a UAS include both RF and GNSS jamming technologies.

[229] Rhiannon Williams, "Tokyo Police Are Using Drones with Nets to Catch Other Drones," *Telegraph*, December 11, 2015, https://www.telegraph.co.uk/technology/2016/01/21/tokyo-police-are-using-drones-with-nets-to-catch-other-drones/.

[230] Jason Reagan, "SkyWall Protects Obama from Potential Drone Threats," DroneLife, November 28, 2016, https://dronelife.com/2016/11/28/germany-skywall-protects-obama-potential-drone-threats/.

[231] Marcia Goodrich, "Drone Catcher: 'Robotic Falcon' Can Capture, Retrieve Renegade Drones," Michigan Tech News, January 7, 2016, https://www.mtu.edu/news/stories/2016/january/drone-catcher-robotic-falcon-can-capture-retrieve-renegade-drones.html.

[232] Michel, *Counter-Drone Systems 2018*, 4.

C. SUMMARY

The FAA considers UASs to be aircraft. Therefore, it is illegal for state and local law enforcement to deploy active C-UAS measures to damage, destroy, or disable an unauthorized drone.[233] As a result, C-UAS options for state and local law enforcement remain limited to passive measures that enable only detection and tracking.[234] Some argue that state and local law enforcement need tools to not only detect, but also interdict and disrupt careless and malevolent drones.[235] The argument supports the idea that protection strategies to counter UAS platforms not be limited to one countermeasure. In fact, many suggest C-UAS strategies include the use of a combination of C-UAS measures. For example, whether the goal is to detect and track, or interdict and disrupt, many, including those from within the DoD, recommend that a system-of-systems approach is necessary to counter a UAS effectively before it strikes.[236] While the federal government continues to debate C-UAS authority for state and local law enforcement, it is important for police executives throughout America's hometowns to increase their knowledge of what may one day become a countermeasure their departments are authorized to use.

---

[233] "U.S.C. Title 18."

[234] Herrera, Dechant, and Green, *Technology Trends in Small Unmanned Aircraft Systems (SUAS) and Counter-UAS*, 33.

[235] Jason Snead, "It's Time to Empower Police to Stop Drone Threats," Heritage Foundation, June 26, 2019, https://www.heritage.org/crime-and-justice/commentary/its-time-empower-police-stop-drone-threats.

[236] Palmer and Geis, "Defeating Small Civilian Unmanned Aerial Systems to Maintain Air Superiority," 111.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. IMPLEMENTATION OF C-UAS TECHNOLOGY

The previous chapter provided an overview of available C-UAS technology and its intended detection, tracking, interdiction, and interruption capabilities. Although the capabilities appear promising, the reader should understand that C-UAS platforms have traditionally been designed for military and federal missions to enhance national security and secure America's borders.[237] Therefore, before obtaining C-UAS authority, procuring C-UAS technologies and developing a C-UAS strategy, state and local law enforcement executives should consider C-UAS limitations and the potential consequences when implemented over urban areas within America's hometowns. This research can help in the creation of doctrine supporting strategy and policy development when the C-UAS debate comes to fruition and if C-UAS authority is extended to state and local law enforcement. The chapter begins by examining limitations of C-UAS technology in support of successful prevention and protection missions. The chapter concludes with potential consequences associated with detection and tracking, and interdicting or interrupting UAS operations above urban areas. As mentioned in previous chapters, although the authorized use of C-UAS technology by state and local law enforcement agencies continues to be deliberated within the federal arena, an analysis of the legal issues remains outside of the scope of this thesis.[238]

A. LIMITATIONS OF CURRENT C-UAS TECHNOLOGY

It can be argued that the first line of defense is perimeter security.[239] It can also be argued that with the proliferation of UASs within the airspace, traditional intrusion detection practices including fencing and closed circuit television to ensure perimeter security may be ineffective.[240] Therefore, effective mitigation of the threat posed by either

---

[237] Snead, Seibler, and Inserra, *Establishing a Legal Framework for Counter-Drone Technologies*, 5.

[238] Snead, Seibler, and Inserra, 1.

[239] James Gompers, "The First Line of Defense," American City and County, December 1, 2004, https://www.americancityandcounty.com/2004/12/01/the-first-line-of-defense/.

[240] Wallace and Loffi, "Examining Unmanned Aerial System Threats & Defenses," 2.

careless or malevolent UAS operations begins with the ability to detect the presence of a drone within the three-dimensional perimeter surrounding critical infrastructure and planned events vulnerable to a drone.

Since detection can be considered a critical capability of perimeter security, state and local law enforcement may first consider C-UAS detection systems when developing a strategy to counter careless or malevolent UAS operations. Passive C-UAS measures employing radar, RF, or EO/IR sensing technologies can enhance physical overwatch to detect and track threatening UASs overhead. However, these C-UAS technologies are not without limitations. Commercially available drones are often built on small platforms that are agile, log impressive flight ranges and times, and are capable of operating at low altitudes at speeds close to 100 mph.[241] Small drones flown at lower altitudes can be hard to detect by radar and other detection sensing technologies.[242] Take, for example, radar technology that may not be calibrated correctly to detect small objects like the DJI Phantom drone that landed on the White House grounds in 2015.[243]

Likewise, other passive C-UAS technologies, such as RF and EO/IR sensing, can be optimal when operated within a clear skyline and uncluttered background, but if an operator of a threatening drone is navigating in an overcast, cloudy airspace, or among tall trees and other environmental barriers, radar, RF and EO/IR become less effective.[244] The physical landscape surrounding the area being protected can provide cover and concealment for a threatening drone, and thus impede the direct line of sight necessary for successful EO/IR and RF detection.[245] For example, if a threatening drone passes behind a tall building or a swarm of small drones is among other airborne objects, such as birds, passive C-UAS technologies may lose their ability to detect and track the drones and will

---

[241] David J. Praisler, *Counter-UAV Solutions for the Joint Force* (Maxwell Air Force Base, AL: Air War College, Air University, 2017), 8, https://apps.dtic.mil/docs/citations/AD1037984.

[242] Michel, *Counter-Drone Systems 2018*, 6.

[243] Schmidt and Shear, "A Drone, Too Small for Radar to Detect, Rattles the White House."

[244] Kim et al., "V-RBNN Based Small Drone Detection in Augmented Datasets for 3D LADAR System," 3.

[245] Michel, *Counter-Drone Systems 2018*, 6.

likely be unable to distinguish the drones from other airborne debris, such as birds, accurately.[246]

Furthermore, technologies analyzing acoustics within the environment to detect unauthorized drones may have limitations due the quantity and quality of microphones on board and their tolerance of ambient noises.[247] For example, the effectiveness of acoustic detection can be decreased by distance and environmental factors, such as wind and background noises commonly heard in urban environments.[248] Perhaps a prevailing limitation of acoustic C-UAS systems is their limited internal library of sounds emitted only by commonly used drones of today. With continuous advancements in technology and the birth of modified or new UAS platforms, a traditional library of drone systems not updated regularly may fall deaf to new systems entering the commercial market.[249]

Unfortunately, according to the FAA, nationally recognized standards for passive C-UAS technologies that detect unauthorized UAS are lacking.[250] Additionally, the FAA contends that passive C-UAS technologies lack the ability to determine the operational intent or the level of threat posed by an unauthorized UAS detected overhead.[251] This limitation is important to accept because the ability of passive C-UAS systems to detect a drone overhead may not be enough to protect the public's safety adequately. For example, during a 2015 Major League Baseball All-star Game, DHS deployed a passive C-UAS detection system that proved successful in detecting several unauthorized drones flying

---

[246] Arthur Holland Michel, *Counter-Drone Capabilities in the Middle East and Beyond: A Primer*, Policywatch 3045 (Washington, DC: Washington Institute for Near East Policy, 2018), 6, https://www.washingtoninstitute.org/policy-analysis/view/counter-drone-capabilities-in-the-middle-east-and-beyond-a-primer.

[247] Wallace and Loffi, "Examining Unmanned Aerial System Threats & Defenses," 17–18.

[248] Ismail Guvenc et al., "Detection, Tracking, and Interdiction for Amateur Drones," *IEEE Communications Magazine* 56, no. 4 (April 2018): 75–81, https://doi.org/10.1109/MCOM.2018.1700455.

[249] Michel, *Counter-Drone Capabilities in the Middle East and Beyond*.

[250] Federal Aviation Administration, *Unmanned Aircraft System Detection—Technical Considerations* (Washington, DC: Federal Aviation Administration, 2019), 1, https://www.faa.gov/airports/airport_safety/media/Attachment-3-UAS-Detection-Technical-Considerations.pdf.

[251] Federal Aviation Administration, 1.

over the game.[252] However, concerns grew after the system detected the drones because law enforcement and security personnel realized they had no capability to interdict or disrupt the drones to protect the fans.[253]

As local law enforcement and others responsible for securing airspace above critical infrastructure and large-scale planned events search for active C-UAS technologies to fill capability gaps in their protection missions, they should understand that active C-UAS also has its limitations. Although active C-UAS technology is intended to interdict and disrupt UAS communications links, they too have proven ineffective in certain environments.[254] In 2018, when rogue drones were detected within the restricted airspace of Gatwick International Airport, officials attempted to mitigate the threat with C-UAS jamming technology.[255] Due to the airport environment, officials had to be mindful that the jamming technology was not pointed at or near other authorized airborne objects, such as manned aircraft. Some argue that it is very difficult in busy airspace to account for multiple variables, such as speed, travel direction, and the altitude of the target drone, while also ensuring C-UAS jamming measures do not affect other RF and GPS signals.[256] In other words, the operator of jamming technology must be well trained and capable of maintaining situational awareness of the entire airspace within the scope of the C-UAS jamming mission.

C-UAS spoofing technology, as described in Chapter III, aims to disrupt communication signals that provide accurate time and navigation data critical to UAS operations. However, although most commercially available UAS utilize line of sight communications via RF and GPS signals, they can be customized with accelerometers and

---

[252] Mark Pomerleau, "Drones: Findable but Not Stoppable," GCN, June 3, 2015, https://gcn.com/articles/2015/06/03/drone-detection.aspx.

[253] Michael S. Schmidt and Michael D. Shear, "Drones Spotted, but Not Halted, Raise Concerns," *New York Times*, January 29, 2015, https://www.nytimes.com/2015/01/30/us/for-super-bowl-and-big-games-drone-flyovers-are-rising-concern.html.

[254] Jeremy Jensen, "Drone Jammer 101—An Inside Look at Counter UAS Technology," UAV Coach, May 30, 2019, https://uavcoach.com/drone-jammer/.

[255] Jen Colton, "The Limitations of RF Jammers for Stopping Rogue Drones," *Fortem News* (blog), March 26, 2019, https://fortemtech.com/blog/rf-jamming-limitations-rogue-drones/.

[256] Colton.

gyroscopes to maneuver via an inertial navigation system.[257] If a UAS is customized with an onboard inertial navigation system, it can maneuver without a RF or GPS communication link, which makes spoofing and jamming C-UAS measures ineffective.[258]

Unfortunately, even with their impressive history, the effectiveness of laser weapons systems may be limited by environmental factors, such as weather, smoke, and other airborne debris.[259] The use of C-UAS technology employing laser weapons systems can also be limited by operator competencies, as well as the complexity of laser technology. Due to the limited time needed to engage a threatening UAS and the requirement of precise operator skill in keeping the laser on target, the effectiveness of laser systems can be decreased.[260] Therefore, often faced with a limited amount of time to assess the level of threat and engage a drone, and the uncertainties of the atmosphere, a skilled operator competent in accurate beam deployment is necessary for successful disruption missions.

Regarding kinetic C-UAS measures, the use of technology, such as a net gun to intercept a drone or to arm an interceptor drone with a net gun to chase and capture a drone, seems to be gaining popularity. The drone net gun can be described as a slingshot device that with the aid of compressed air, releases a net into the air from the ground to capture a drone overhead.[261] According to one prevalent net gun manufacturer who markets its net guns for catching animals, its net gun has an effective range of 35 feet.[262] On the other hand, another manufacture who markets its technology as a simple and cost effective way

---

[257] J. L. Weston and D. H. Titterton, "Modern Inertial Navigation Technology and Its Application," *Electronics Communication Engineering Journal* 12, no. 2 (April 2000): 49–64, https://doi.org/10.1049/ecej:20000202.

[258] Praisler, *Counter-UAV Solutions for the Joint Force*, 12.

[259] Palmer and Geis, "Defeating Small Civilian Unmanned Aerial Systems to Maintain Air Superiority," 107.

[260] Titterton, *Military Laser Technology and Systems*, 242.

[261] Hillary Schaub and Darrell M. West, "Six Ways to Disable a Drone," *TechTank* (blog), March 16, 2016, https://www.brookings.edu/blog/techtank/2016/03/16/six-ways-to-disable-a-drone/.

[262] "Net Gun|Net Launcher|Net Shooter—The World's #1 Net Gun Provider!," The Net Gun Store, accessed August 10, 2019, https://thenetgunstore.com/.

to capture unwanted drones claims effective ranges out to approximately 49 feet.[263] In 2016, Michigan Technological University developed an interceptor drone that it claims can chase down unauthorized drones and deploys a tethered net to capture the drone and recover it in a safe manner.[264] However, the effective range of the interceptor drone is reported to be limited to 40 feet.[265] As noted earlier in this paper, counter drone operations often have a limited time frame to assess a potential threat and take protective measures. Therefore, the effectiveness of countering an unauthorized drone with kinetic measures, such as deploying a net from either a gun on the ground or an interceptor drone, is dependent on the competency of the C-UAS operator. Furthermore, some argue that because today's drones are capable of reaching speeds over 100 miles per hour, they are too quick for human pilots of interceptor drones to catch.[266] Table 3 shows the limitations of passive C-UAS technology, while Table 4 shows the limitations of active C-UAS technology.

Table 3. Limitations of Passive C-UAS Technology

Passive C-UAS	Limitations
Radar	Smaller drones may be hard to detect.
Radio-frequency (RF), Electro-Optical (EO)/Infrared (IR), Acoustic	Cloudy, overcast skylines and the existence of other airborne debris or birds may decrease effectiveness of RF, EO/IR, and acoustic technologies.

263 "NetGun X1," Drone Defence, accessed August 10, 2019, https://www.dronedefence.co.uk/products/netgun-x1/.

264 Jay Bennett, "Drone-Mounted Net Cannon Snags Other Drones with Ease," *Popular Mechanics*, January 12, 2016, https://www.popularmechanics.com/flight/drones/a18942/michigan-tech-drone-mounted-net-cannon/.

265 Bennett.

266 Stephen Nellis, "Drone-Catchers Emerge on a New Aerial Frontier," Reuters, March 21, 2017, https://www.reuters.com/article/us-usa-drone-hunter-idUSKBN16S1IT.

Table 4. Limitations of Active C-UAS Technology

Active C-UAS	Limitations
RF and GNSS Jamming	Environmental factors, such as crowded airspace, make deployment of jamming technologies difficult because of multiple variables, such as speed, direction of travel, and altitude of the target drone, and the existence of authorized aircraft in the area vulnerable to signal jamming.
Spoofing	UASs with inertial navigation systems can be immune to spoofing technologies since GPS signals are not necessary for successful navigation.
Laser	Can be limited due to environmental factors, such as weather and smoke in the atmosphere, and because of a limited interaction time to engage a threatening drone, the operator of C-UAS laser technology must be well trained to achieve an accurate beam deployment.
Netting	Limited range of approximately 49 feet. With drone speeds reaching over 100 mph, interceptor drones may not actually be able to catch threatening drones.

B. UNINTENDED CONSEQUENCES OF C-UAS MISSIONS

C-UAS technologies can be complex. Therefore, before procuring and implementing C-UAS within the homeland, public safety entities should assess the potential consequences of detecting, tracking, and if necessary, removing a UAS from the airspace.[267] Although passive C-UAS technologies seem to be the only current counter measure authorized for state and local law enforcement, they are not absolute and have their drawbacks. Additionally, as state and local law enforcement grow more aware of UAS threats and seek to enhance their agency's options to protect actively against careless and malevolent UAS operations, they must understand that active C-UAS measures can have significant consequences when deployed within their urban communities.

According to Arthur Holland Michael with the Center for the Study of the Drone, C-UAS detection systems can generate both false negatives and positives.[268] As with any technology used to protect the public, false alarms can have negative consequences.

[267] CISA Infrastructure Security Division, 04:04–04:12.

[268] Michel, *Counter-Drone Systems 2018*, 6.

Although a false report from EO/IR detection technology that senses a bird rather than a drone may be a nuisance, radar systems with reduced sensitivity to reduce alarms from non-UAS platforms can result in missing the detection of small UAS threats.[269] Either of these consequences over time, could reduce overall confidence in the technology's accuracy.

With a growing interest in RF jamming technology to interdict and disrupt an unauthorized UAS, the readers should combine their understanding of how the technology works and what the potential for collateral damage is. To be effective, the noise emitting from an RF jammer must be at a power level high enough to cover up the radio communication signal between the drone and the pilot. This counter measure has the potential to cause collateral damage to authorized users of the same airspace by unintentionally interrupting their communications systems as well.[270] Unintentionally jamming communications signals of other RF enabled systems can be dangerous when other radio signals are disrupted.[271] Even with growing concerns about UAS flights near CIKR, such as airports and sports arenas, the FAA cautions the use of countermeasures without federal consent because of the risk of interfering with commercial aircraft.[272] For example, as late as May 2019, the FAA continued to warn against the use of active C-UAS technologies with interdiction capabilities because of the hazard they pose to air navigation.[273] This issue is important to consider because as with many urban areas, the likelihood of helipads at area trauma centers makes C-UAS jamming and spoofing measures risky to critical navigational aids of manned aircraft, such as medical helicopters.

---

[269] Solodov et al., "Analyzing the Threat of Unmanned Aerial Vehicles (UAV) to Nuclear Facilities," 314.

[270] Colton, "The Limitations of RF Jammers for Stopping Rogue Drones."

[271] João Antunes, "What Do You Need to Know about Anti-Drone and Counter Drone Technology?," Commercial UAV News, March 13, 2018, https://www.expouav.com/news/latest/need-know-anti-drone-counter-drone-technology/.

[272] Shepardson, "FAA to U.S. Airports."

[273] John R. Dermody, *Updated-Information-UAS-Detection-Countermeasures-Technology-Airports* (Washington, DC: Office of Airports Safety and Standards, Federal Aviation Administration, 2019), 1, https://www.faa.gov/airports/airport_safety/media/Updated-Information-UAS-Detection-Countermeasures-Technology-Airports-20190507.pdf.

Manned aircraft may not be the only thing affected by active C-UAS technologies, such as spoofing or jamming signals. According to David Silver of the Aerospace Industries Association, instances have occurred in which the disruption of radio wave communications have not only caused the loss of autopilot systems of manned aircraft, but have also caused doors of commercial businesses to randomly open and close.[274] Local law enforcement should consider the consequences of unintentionally disabling security measures put in place by private businesses and private residences to protect their personal property.

As pointed out by Arthur Holland Michael and others, many of today's active C-UAS systems can be too dangerous to deploy over crowded urban areas.[275] For example, an overarching consequence of kinetic means to counter a threating drone is the possibility of causing a drone to fall to the ground, damaging other property, or worse, further endangering the public's safety.[276] What could be even more alarming are the potential consequences of deploying an active C-UAS measure against a weaponized drone. The use of a kinetic counter strategy, such as a laser weapons system or netting technology against a weaponized drone, could inadvertently detonate explosives or expose the public to weapons of mass destruction, such as chemical, biological, or radiological agents.[277]

Another potential consequence of interdicting and disrupting UAS platforms is improper evidence collection. Whether photographic or other visual evidence, such as video, the FAA considers this evidence essential to its investigations of unlawful UAS operations and believes that local law enforcement is best positioned to secure such evidence.[278] State and local law enforcement should remain cognizant of the need for the

---

[274] Calvin Biesecker, "Military Counter-UAS Efforts Creating Framework for Other U.S. Agencies," *Rotor & Wing International*, July 12, 2018, https://www.rotorandwing.com/2018/07/12/military-counter-uas-efforts-creating-framework-u-s-agencies/.

[275] Michel, *Counter-Drone Systems 2018*, 7.

[276] Michel, 6.

[277] Snead, Seibler, and Inserra, *Establishing a Legal Framework for Counter-Drone Technologies*, 5.

[278] Meredith Tracey, *Law Enforcement Guide for Suspected Unauthorized UAS Operations* (Washington, DC: Federal Aviation Administration, 2015), 7, https://www.faa.gov/uas/resources/policy_library/media/FAA_UAS-PO_LEA_Guidance.pdf.

proper handling of drones and associated UAS platforms that may be detected, as they may be dangerous or require collection as evidence that needs to be handled properly.[279] Table 5 shows the unintended consequences of both passive and active C-UAS missions.

Table 5. Unintended Consequences of C-UAS Missions

Passive C-UAS	Unintended Consequences
• Radar • Radio-frequency (RF) • Electro-Optical (EO)/Infrared (IR) • Acoustic	Generation of false negatives and false positives creating low confidence in the technologies capabilities that results in complacency and the potential to miss credible UAS threats.
Active C-UAS	**Unintended Consequences**
• RF and GNSS Jamming • Spoofing	Collateral damages, such as interference with authorized manned aircraft and their navigational aids or radio waves, supported security measures taken by businesses and individuals within an urban environment.
• Laser • Netting	The complete destruction of or loss of control of UAS platforms, which causes a drone to fall from the sky endangering life and property on the ground, exposes the public to on board weapons of mass destruction, and results in the loss of properly gathered and handled evidence.

C. SUMMARY

Most can agree that C-UAS technology is evolving rapidly and that CIKR owners and operators, as well as government agencies, remain critical stakeholders in ensuring that the systems supporting C-UAS technology can efficiently and safely protect the public's safety.[280] Even though a vast market of commercially available C-UAS options is available, most have not undergone appropriate testing in urban areas.[281] Events like the unauthorized drones within the protected airspace of Gatwick International Airport

[279] CISA Infrastructure Security Division, 04:33–06:30.

[280] Herrera, Dechant, and Green, *Technology Trends in Small Unmanned Aircraft Systems (SUAS) and Counter-UAS*, 33.

[281] "Countering Unmanned Aerial Systems in Urban Environments," ECN, May 11, 2018, ProQuest.

revealed that the deployment of one single C-UAS technology falls short of providing the necessary mitigation to reduce the risks.[282] Additionally, although authorities were able to detect drones impeding on a 2015 Major League baseball game, the incident exposed gaps in capabilities to prevent a mass casualty attack effectively had the UAS operations had an attack mission.[283]

Although state and local law enforcement will continue to explore options to increase prevention and protection capabilities against unauthorized drones, implementation issues are challenging both procurement and policy development to support C-UAS use. Currently, the most significant challenge faced by local law enforcement in using C-UAS systems is the legal constraints restricting their use.[284] In addition to legal constraints, many practical and policy challenges may exist that local law enforcement administration should consider prior to purchasing, testing, and implementing C-UAS technology. The lack of standards within the C-UAS industry creates reliability and effectiveness issues. Questioning the reliability and effectiveness of C-UAS systems, combined with the absence of legal guidelines for use by state, local, tribal and territorial law enforcement, creates uncertainty and hesitation by these agencies to procure, develop policy, and implement this technology. Nevertheless, the development of C-UAS technology is extremely fluid, and with a growing concern of malevolent drone attacks, legal constraints will likely be addressed while industry standards continue to improve.

---

[282] Joel Griffin, "The Counter-Drone Conundrum," Security Info Watch, January 15, 2019, https://www.securityinfowatch.com/perimeter-security/robotics/anti-drone-technologies/article/21042411/the-counterdrone-conundrum.

[283] Schmidt and Shear, "Drones Spotted, but Not Halted, Raise Concerns."

[284] Federal Aviation Administration, *Law Enforcement Guidance for Suspected Unauthorized UAS Operations*, 5.

THIS PAGE INTENTIONALLY LEFT BLANK

V. RECOMMENDATIONS AND CLOSING THOUGHTS

A. RECOMMENDATIONS

While state and local law enforcement that make up the frontlines of homeland security stand by for lawmakers to empower them with the authority to engage in active C-UAS missions, they should not sit idle. To help justify their authority, local law enforcement executives across America should embark on a proactive approach to develop doctrine ensuring their C-UAS strategies are relevant, necessary, and appropriate.[285] The following recommendations are intended to support local law enforcement efforts in the development of a C-UAS strategy to bolster their overall mission of protecting the public's safety from disruptive technology, such as careless or malicious UAS threats.

1. Local Law Enforcement Risk Assessments Should Identify Gaps in Capabilities to Detect, Track, Interdict, and Disrupt Careless and Malevolent UAS Operations

Traditional risk assessment doctrine focuses on mitigating risks from natural hazards, technological hazards, and human-caused, intentional acts.[286] Although the DHS threat and hazard identification and risk assessment process accounts for a broad spectrum of threats and hazards, the threat of careless or malevolent UAS operations presents a new challenge for local law enforcement.[287] The impressive capabilities designed within UAS platforms combined with a growing interest in the use of drones, gives merit to the likelihood of on-going incidents involving UAS platforms threatening the public's safety within the United States.

---

[285] Jason Snead and John-Michael Seibler, "Legal Framework for Counter-Drone Operations Is Critical to the Future," Heritage Foundation, July 3, 2018, https://www.heritage.org/defense/commentary/legal-framework-counter-drone-operations-critical-the-future.

[286] Department of Homeland Security, *Threat and Hazard Identification and Risk Assessment (THIRA) and Stakeholder Preparedness Review (SPR) Guide*, Comprehensive Preparedness Guide (CPG) 201, 3rd ed. (Washington, DC: Department of Homeland Security, 2018), 11, https://www.fema.gov/media-library-data/1527613746699-fa31d9ade55988da1293192f1b18f4e3/CPG201Final20180525_508c.pdf.

[287] Department of Homeland Security, 12.

The threat of careless and malevolent UAS operations exposes a growing risk to not only national security, but also America's hometowns. Metropolitan areas across the nation are dependent on various systems, networks, and other assets critical to the local government's ability to serve and protect the public. Additionally, many cities across the homeland regularly plan and host various outdoor special events throughout the year for their communities. Examples include parades, athletic competitions, holiday celebrations, and other entertainment events. Local law enforcement plays an important role in ensuring critical infrastructure and planned events within their communities remain functional and resilient. Therefore, it is recommended that local law enforcement assess their community's critical infrastructure and other planned events for vulnerabilities to UAS platforms and develop prevention and protection strategies to address both careless and malevolent UAS operations.

2. Local Law Enforcement Should Explore Their Options to Bolster Capabilities to Detect, Track, Interdict, and Disrupt Malevolent and Careless UAS Platforms

In addition to traditional practices employed by local law enforcement to protect their communities, a number of countermeasures are supported by advanced technology to enhance prevention and protection capabilities further. Specific prevention and protection capabilities that can be bolstered by C-UAS measures include detection, tracking, interdiction, and disruption. C-UAS measures can be classified into two categories, passive and active countermeasures. Passive C-UAS measures include traditional law enforcement practices of surveillance in which police are tasked with maintaining a watchful eye of both the two-dimensional and three-dimensional spaces surrounding an event, a key resource, or a critical facility. However, if a drone is detected and effectively tracked, with the aid of passive C-UAS technology, law enforcement's efforts to locate and identify the operator of the UAS may be expedited.

While passive C-UAS measures are designed to detect and track a UAS, active C-UAS measures are backed by technology that enables the jamming of RF signals, spoofing of GPS communications, and the deployment of lasers and kinetic devices, such as netting to destroy or capture an unauthorized drone. However, since UASs are considered aircraft

by the FAA, the authority to interdict and disrupt a drone remains limited to the DoD and other select federal law enforcement entities. Nevertheless, the examination of active C-UAS measures available on the open market reveals that if authority is granted to state and local government, local police will have more options and greater capabilities to counter careless and malicious UAS operations over their communities.

3. Local Law Enforcement Should Understand that C-UAS Measures Have Limitations; therefore, the Deployment of Such Measures Must Be Necessary, Effective, and Appropriate to Safely Counter the Threat

C-UAS technology is a rather young field, yet rapidly developing. Even though many C-UAS measures are available on the open market, most have been developed for the battlefield while only a few have been tested over urban areas. The technology behind C-UAS capabilities has its limitations, especially when deployed in a crowded airspace or above a densely populated area. Therefore, if local law enforcement were to receive full C-UAS authorization and deployed these countermeasures without first developing a healthy awareness of those limitations, negative consequences could result.

While the legal aspects of granting C-UAS authority to local law enforcement remains in debate, police executives should adhere to their sworn responsibilities to act on UAS threats with a necessary and appropriate use of counter force. C-UAS strategies for local law enforcement and their partners in public safety should include the deployment of a combination of C-UAS measures. First, they should strive to deter or discourage UAS operations near CIKR and other large-scale events to mitigate the risk of careless or malevolent UAS operations through public education campaigns about FAA regulations regarding the operation of UAS platforms, or requesting that the FAA restrict airspace around a CIKR or event. Additionally, local law enforcement could discourage UAS operations in designated areas by declaring the space around CIKR and events as a “no drone zone,” and encourage the public to report UAS activity.

When regulatory measures fail to mitigate the risk effectively, local law enforcement should have protocol adopted to guide detection, tracking, interdiction, and disruption measures. Whether the goal is to detect and track, or interdict and disrupt, local

law enforcement strategies should include a combination of options personnel can use that are both necessary and effective to counter the threat. Most law enforcement agencies have policies written to guide their use of force with a range of actions taken by police officers to stop a threat with only the appropriate and effective type of force necessary.[288] Likewise, to ensure that the deployment of C-UAS measures remain necessary, appropriate, and effective to counter a UAS threat, local law enforcement should provide a continuum of options officers may use in their missions to counter UAS threats.

C-UAS technology will continue to evolve, and in the future, is likely to become an effective tool for law enforcement at the federal, state, and local levels. A C-UAS decision matrix shown in Figure 1 can guide future decision making at the frontlines of hometown security when local communities are threatened by careless or malevolent UAS operations. To ensure redundancy in prevention and protection capabilities, the decision matrix can give law enforcement personnel the ability to assess the risk a UAS poses to their community and decide which countermeasures are necessary, effective, and appropriate to deploy.

Upon the discovery of a UAS within the airspace, officers should analyze the intention and capabilities of the threat based on location, timing, the existence of surveillance equipment, or other suspicious cargo on board, and whether the system is weaponized. Along with the initial assessment, officers continuously assess the risk the UAS poses to the public's safety or infrastructure. Based on the risk assessment, law enforcement is then able to use the C-UAS decision matrix to determine which C-UAS measure to deploy to detect, track, and if necessary, actively interdict and disrupt, the UAS platform appropriately.

---

288 "The Use-of-Force Continuum," National Institute of Justice, August 3, 2009, http://nij.ojp.gov/topics/articles/use-force-continuum.

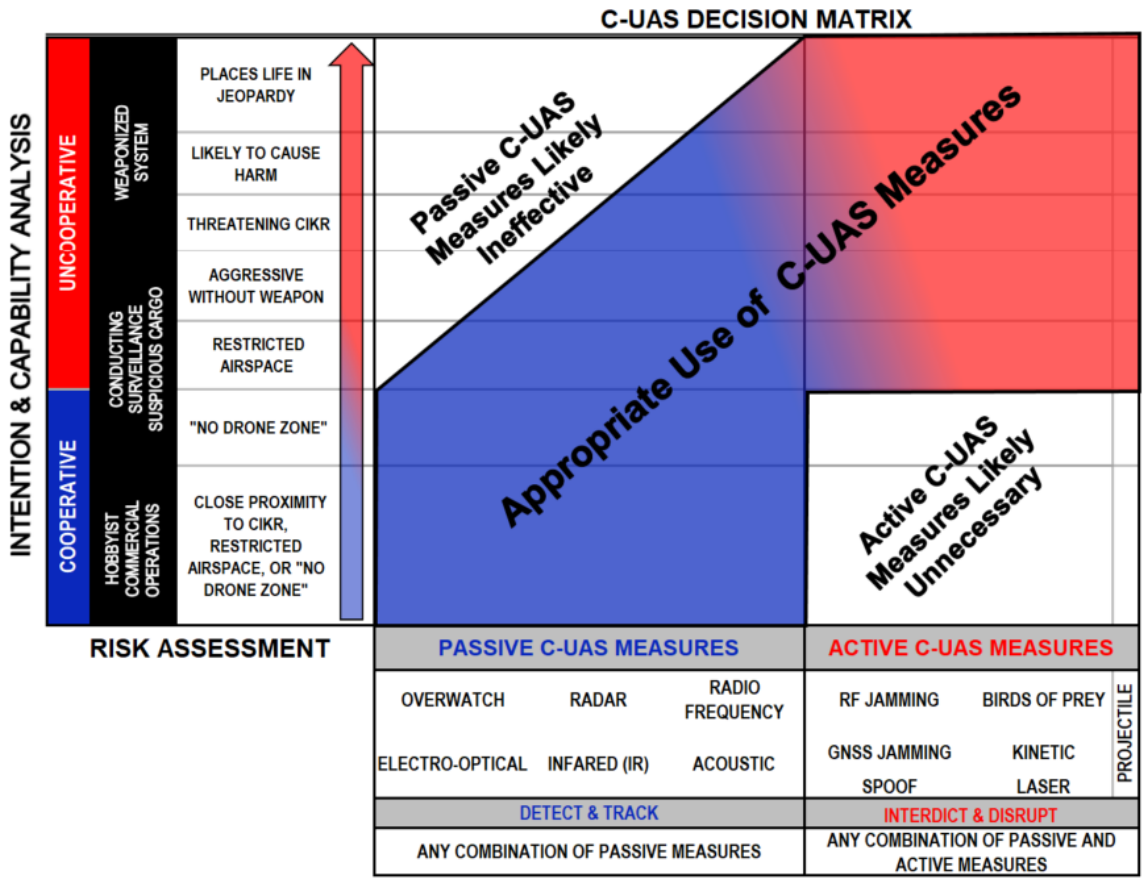

Figure 1. C-UAS Decision Matrix

B. CLOSING THOUGHTS

1. Limited Scope of Paper

Uncertainty can be dangerous, especially for people and assets needing protection from the threat of careless and malevolent UAS operations across America's landscape.[289] Unfortunately, until legal authority to deploy C-UAS technology to interdict and disrupt a threating drone actively is given to local law enforcement, police executives will most likely remain uncertain about the best way to protect their communities from the emerging threat posed by UAS platforms. Even though legislative challenges associated with granting active C-UAS authority were beyond the scope of this thesis, several options

[289] Snead, Seibler, and Inserra, *Establishing a Legal Framework for Counter-Drone Technologies*, 12.

enabling local law enforcement to enhance their capabilities to detect and track careless and malevolent UAS operations were identified. The combination of passive C-UAS with regulatory measures can facilitate the development of a C-UAS strategy to counter drones within America's hometowns and enhance protection and prevention capabilities.

2. Future Research Opportunities

The rapid pace of UAS technology is exciting, yet also alarming. As the New York Police Department's Deputy Commissioner Miller contended in May 2019, local law enforcement has found itself behind the curve in countering threatening UAS platforms.[290] Unfortunately, the threat posed by unmanned and often autonomous systems, on land and water, are also likely to increase. Therefore, research in the future should focus on not only enabling the defeat of UAS platforms, but also other unmanned systems and automated technologies supporting travel on land, and both on and under water. A comparison government study of other democratic nations may expose legislation that could be modeled within the United States. Additionally, research on drone and other autonomous vehicle threats around the world and the responses to those threats may be beneficial in identifying best practices for deterring, detecting, tracking, interdicting, and disrupting careless or malevolent autonomous vehicle operations within an urban environment.

[290] John J. Miller, "Local Efforts to Counter the Terror Threat in New York City: A Retrospective and a Roadmap," Homeland Security, Subcommittee on Intelligence and Counterterrorism (2019), 6, https://homeland.house.gov/hearings-and-markups/hearings/local-efforts-counter-terror-threat-new-york-city-retrospective-and.

LIST OF REFERENCES

Aboulenein, Ahmed. "Islamic State Developing New Weapons despite Losses: Arms Monitor." *Reuters*, April 26, 2017. https://www.reuters.com/article/us-mideast-crisis-iraq-arms-idUSKBN17S20N.

Academy of Model Aeronautics. *A Closer Look at the FAA's Drone Data*. Muncie, IN: Academy of Model Aeronautics, 2105. https://www.modelaircraft.org/sites/default/files/gov/docs/AMAAnalysis-Closer-Look-at-FAA-Drone-Data_091415.pdf.

AirMap. "Security and the Drone-of-Things." *AirMap* (blog), April 13, 2016. https://www.airmap.com/security-drone-of-things/.

Alexander, Donovan. "Drone Hunters: 9 of the Most Effective Anti-Drone Technologies for Shooting Drones out of the Sky." Interesting Engineering, January 22, 2019. https://interestingengineering.com/drone-hunters-9-of-the-most-effective-anti-drone-technologies-for-shooting-drones-out-of-the-sky.

Antunes, João. "What Do You Need to Know about Anti-Drone and Counter Drone Technology?." Commercial UAV News, March 13, 2018. https://www.expouav.com/news/latest/need-know-anti-drone-counter-drone-technology/.

Arsenault, Kimberly. "The Threats to Transportation Infrastructure: Airports at Risk." In Homeland Security, April 4, 2017. https://inhomelandsecurity.com/transportation-infrastructure-airport/.

BBC News. "How Countries Counter the Drone Threat." December 21, 2018. https://www.bbc.com/news/technology-46639099.

Bennett, Jay. "Drone-Mounted Net Cannon Snags Other Drones with Ease." *Popular Mechanics*, January 12, 2016. https://www.popularmechanics.com/flight/drones/a18942/michigan-tech-drone-mounted-net-cannon/.

Bielby, Kylie. "Terrorists Look to Drones and Driverless Cars to Avoid Martyrdom." Homeland Security Today, July 13, 2019. https://www.hstoday.us/subject-matter-areas/counterterrorism/terrorists-look-to-drones-and-driverless-cars-to-avoid-martyrdom/.

Biesecker, Calvin. "Military Counter-UAS Efforts Creating Framework for Other U.S. Agencies." *Rotor & Wing International*, July 12, 2018. https://www.rotorandwing.com/2018/07/12/military-counter-uas-efforts-creating-framework-u-s-agencies/.

Boeing. “Silent Strike: Boeing’s Compact Laser Weapons System Tracks and Disables UAVs.” Boeing Defense, August 27, 2015. https://www.boeing.com/features/2015/08/bds-compact-laser-08-15.page.

Brzenchek, Robert. “How Gangs Are Using Drones to Disrupt Law Enforcement.” In Public Safety, May 21, 2018. https://inpublicsafety.com/2018/05/how-gangs-are-using-drones-to-disrupt-law-enforcement/.

Burguan, Jarrod. “Drones Help Augment a Police Department’s Capabilities to Fight Crime.” *National Police Foundation* (blog), April 28, 2017. https://www.policefoundation.org/drones-help-augment-a-police-departments-capabilities-to-fight-crime/.

Burns, Mark J. “MLB Responds after Drone Makes Petco Park Crash Landing during San Diego Padres Game.” SportTechie, May 22, 2017. https://www.sporttechie.com/gopro-karma-drone-makes-crash-landing-at-petco-park-during-san-diego-padres-game/.

Cabreira, Tauã M., Lisane B. Brisolara, and Paulo R. Ferreira Jr. “Survey on Coverage Path Planning with Unmanned Aerial Vehicles.” *Drones* 3, no. 1 (2019): 1–38. https://doi.org/10.3390/drones3010004.

Center for Advanced Defense Studies. *Above Us Only Stars: Exposing GPS Spoofing in Russia and Syria*. Washington, DC: C4ADS, 2019. https://www.c4reports.org/aboveusonlystars.

Cîrdei, Ionuţ Alin. “Improving the Level of Critical Infrastructure Protection by Developing Resilience.” *Land Forces Academy Review* 23, no. 4 (December 1, 2018): 237–43. https://doi.org/10.2478/raft-2018-0028.

CISA Infrastructure Security Division. “Unmanned Aircraft Systems (UAS)—Critical Infrastructure.” Department of Homeland Security. Accessed July 14, 2019. https://www.dhs.gov/cisa/uas-critical-infrastructure.

Clarke, Colin P. “Approaching a ‘New Normal’: What the Drone Attack in Venezuela Portends.” *The RAND Blog* (blog), August 13, 2018. https://www.rand.org/blog/2018/08/approaching-a-new-normal-what-the-drone-attack-in-venezuela.html.

Colton, Jen. “The Limitations of RF Jammers for Stopping Rogue Drones.” *Fortem News* (blog), March 26, 2019. https://fortemtech.com/blog/rf-jamming-limitations-rogue-drones/.

Coulombe, Ray. “Drone Zone.” *Security Technology Executive* 27, no. 3 (August 2017): 10, 14. ProQuest.

Counter Extremism Project. *Digital Developments: Extremists' Use of Modern Communications Tools*. London: Counter Extremism Project, 2019. https://www.counterextremism.com/sites/default/files/Digital%20Developments_031819.pdf.

Davis, Lynn E., Michael J. McNerney, James S. Chow, Thomas Hamilton, Sarah Harting, and Daniel Byman. *Armed and Dangerous?* Santa Monica, CA: RAND, 2014. https://www.rand.org/pubs/research_reports/RR449.html.

De Avila, Joseph. "New York Police Seek Authority to Take down Drones." *Wall Street Journal*, February 17, 2019. https://www.wsj.com/articles/new-york-police-seek-authority-to-take-down-drones-11550419320.

Department of Homeland Security. *2015 Commercial Facilities Sector-Specific Plan: An Annex to the NIPP 2013*. Washington, DC: Department of Homeland Security, 2015. https://www.dhs.gov/sites/default/files/publications/nipp-ssp-government-facilities-2015-508.pdf.

———. "Infrastructure Security." July 16, 2012. https://www.dhs.gov/topic/critical-infrastructure-security.

———. "Snapshot: Countering Unmanned Aerial Systems in Urban Environments." Science and Technology, May 11, 2018. https://www.dhs.gov/science-and-technology/news/2018/05/11/snapshot-c-uas-urban-environments.

———. *Threat and Hazard Identification and Risk Assessment (THIRA) and Stakeholder Preparedness Review (SPR) Guide*. Comprehensive Preparedness Guide (CPG) 201. 3rd ed. Washington, DC: Department of Homeland Security, 2018. https://www.fema.gov/media-library-data/1527613746699-fa31d9ade55988da1293192f1b18f4e3/CPG201Final20180525_508c.pdf.

———. *Unmanned Aircraft Systems: Addressing Critical Infrastructure Security Challenges, Fact Sheet*. Washington, DC: Department of Homeland Security, 2017. https://www.dhs.gov/sites/default/files/publications/uas-ci-challenges-fact-sheet-508.pdf.

Dermody, John R. *Updated-Information-UAS-Detection-Countermeasures-Technology-Airports*. Washington, DC: Office of Airports Safety and Standards, Federal Aviation Administration, 2019. https://www.faa.gov/airports/airport_safety/media/Updated-Information-UAS-Detection-Countermeasures-Technology-Airports-20190507.pdf.

Deschênes, Patrice. "The Rise of the Drones: Technological Development of Miniaturised Weapons and the Challenges for the Royal Canadian Navy." *Canadian Military Journal* 19, no. 2 (Spring 2019): 51–56. http://www.journal.forces.gc.ca/Vol19/No2/PDF/CMJ192Ep51.pdf.

Dinan, Stephen. “Drones Become Latest Tool Drug Cartels Use to Smuggle Drugs into U.S.” *Washington Times*, August 20, 2017. https://www.washingtontimes.com/news/2017/aug/20/mexican-drug-cartels-using-drones-to-smuggle-heroi/.

Dormehl, Luke. “Prisons Are Fighting Back against Contraband-Dropping Drones.” Digital Trends, July 20, 2018. https://www.digitaltrends.com/cool-tech/airwarden-drone-survaillance/.

Downs, Ray. “Australian Drug Gang Suspected of Using Drone to Monitor Police.” UPI, June 30, 2017. https://www.upi.com/Top_News/World-News/2017/06/30/Australian-drug-gang-suspected-of-using-drone-to-monitor-police/2911498801791/.

Drone Defence. “NetGun X1.” Accessed August 10, 2019. https://www.dronedefence.co.uk/products/netgun-x1/.

Drone Omega. “How GPS Drone Navigation Works.” Accessed July 29, 2019. https://www.droneomega.com/gps-drone-navigation-works/.

DroneShield. “DroneGun Tactical.” Accessed December 2, 2018. https://www.droneshield.com/dronegun-tactical/.

ECN. “Countering Unmanned Aerial Systems in Urban Environments.” May 11, 2018. ProQuest.

Falvey, Dan. “Panic in Venezuela as ‘Drone Attack’ Explosions Hit during Speech by President Maduro.” Express, August 5, 2018. https://www.express.co.uk/news/world/999021/venezuela-explosion-caracas-Nicolas-Maduro-speech-panic-terror.

Farago, Robert. “New from Boeing: Compact Laser Weapon System.” The Truth about Guns, July 7, 2015. https://www.thetruthaboutguns.com/new-from-boeing-compact-laser-weapon-system/.

Federal Aviation Administration. *FAA Aerospace Forecast 2019–2039*. Washington, DC: Federal Aviation Administration, 2019. https://www.faa.gov/data_research/aviation/aerospace_forecasts/.

———. *Law Enforcement Guidance for Suspected Unauthorized UAS Operations*. Washington, DC: Department of Transportation, 2018.

———. “UAS Sightings Report, Unmanned Aircraft Systems.” July 22, 2019. https://www.faa.gov/uas/resources/public_records/uas_sightings_report/.

———. *Unmanned Aircraft System Detection—Technical Considerations*. Washington, DC: Federal Aviation Administration, 2019. https://www.faa.gov/airports/airport_safety/media/Attachment-3-UAS-Detection-Technical-Considerations.pdf.

French, Sally. “A Bunch of People Are Illegally Flying Drones around the PGA Tour Right Now.” *The Drone Girl* (blog), February 2, 2018. http://thedronegirl.com/2018/02/02/bunch-people-illegally-flying-drones-around-pga-tour-right-now/.

Gabrielle, Lea. “Drone Drops Leaflets over Football Stadiums, Raising Security Concerns.” Fox News, November 27, 2017. https://www.foxnews.com/tech/drone-drops-leaflets-over-football-stadiums-raising-security-concerns.

Genfare. “Largest Events in Each State.” Accessed July 12, 2019. https://www.genfare.com/resources/largest-events-state/.

Gettinger, Dan, and Arthur Holland Michel. *Drone Sightings and Close Encounters: An Analysis*. Washington, DC: The Center for the Study of the Drone at Bard College, 2015. https://dronecenter.bard.edu/drone-sightings-and-close-encounters/.

Giaritelli, Anna. “Super Bowl Saw 54 Drone Incursions: Homeland Security.” *Washington Examiner*, April 10, 2019. https://www.washingtonexaminer.com/news/super-bowl-saw-54-drone-incursions-homeland-security.

Gleeson, Scott. “Police Identify Juvenile Who Flew Drone at Fenway Park during Red Sox Game.” *USA Today*, April 14, 2019. https://usatodayhss.com/2019/fenway-park-drone-red-sox-game.

Gompers, James. “The First Line of Defense.” American City and County, December 1, 2004. https://www.americancityandcounty.com/2004/12/01/the-first-line-of-defense/.

Goodrich, Marcia. “Drone Catcher: ‘Robotic Falcon’ Can Capture, Retrieve Renegade Drones.” Michigan Tech News, January 7, 2016. https://www.mtu.edu/news/stories/2016/january/drone-catcher-robotic-falcon-can-capture-retrieve-renegade-drones.html.

Greenberg, Andy. “Watch a Test of Anti-Drone Weapons, from Shotguns to Superdrones.” *Wired*, July 26, 2017. https://www.wired.com/story/watch-anti-drone-weapons-test/.

Griffin, Joel. “The Counter-Drone Conundrum.” Security Info Watch, January 15, 2019. https://www.securityinfowatch.com/perimeter-security/robotics/anti-drone-technologies/article/21042411/the-counterdrone-conundrum.

Guvenc, Ismail, Farshad Koohifar, Simran Singh, Mihail L. Sichitiu, and David Matolak. “Detection, Tracking, and Interdiction for Amateur Drones.” *IEEE Communications Magazine* 56, no. 4 (April 2018): 75–81. https://doi.org/10.1109/MCOM.2018.1700455.

Hall, David M. “Not the Drones You’re Looking for: Civil Drones Invading Stability Operations.” Master’s thesis, School of Advanced Air and Space Studies, Air University, 2016. https://www.hsdl.org/?abstract&did=822552.

Hamann, Michael. “Can You Legally Counter a Drone?.” *Police Magazine*, November 16, 2018. http://www.policemag.com/486684/can-you-legally-counter-a-drone.

Hambling, David. “Drones Fight Back against Laser Weapons: And They Might Be Winning.” *Popular Science*, November 4, 2016. https://www.popsci.com/laser-guns-are-targeting-uavs-but-drones-are-fighting-back/.

Herrera, James, Jason A. Dechant, and E. K. Green. *Technology Trends in Small Unmanned Aircraft Systems (SUAS) and Counter-UAS: A Five Year Outlook*, IDA Paper P-8823. Alexandria, VA: Institute for Defense Analysis, 2017. https://apps.dtic.mil/dtic/tr/fulltext/u2/1047506.pdf.

Humphries, Matthew. “U.S. Air Force Orders Anti-Drone Net-Filled Shotgun Shells.” PCMAG, March 14, 2017. https://www.pcmag.com/news/352360/us-air-force-orders-anti-drone-net-filled-shotgun-shells.

Inside Flyer UK. “What Are the Busiest Airports in the UK?—We List the Top 20.” January 24, 2018. https://insideflyer.co.uk/2018/01/what-are-the-busiest-airports-in-the-uk/.

Invisible Interdiction. “UAV Detection—Drone Electronic Defeat Systems.” Accessed December 2, 2018. https://invisidiction.com/.

Jee, Charlotte. “The First Worldwide Drone Standards Have Been Unveiled to Keep Aircraft Safe.” *MIT Technology Review*, November 22, 2018. https://www.technologyreview.com/the-download/612460/the-first-worldwide-drone-standards-have-been-unveiled-to-keep-aircraft-safe/.

Jensen, Jeremy. “Drone Jammer 101—An Inside Look at Counter UAS Technology.” UAV Coach, May 30, 2019. https://uavcoach.com/drone-jammer/.

Jisrawi, Ahmad. “Drones Jammer. A Simple Drone Jammer Designed to Hack Unwelcomed Civilian Drones within Your Backyard Range.” DocPlayer. Accessed October 10, 2019. https://docplayer.net/7556467-Drones-jammer-a-simple-drone-jammer-designed-to-hack-unwelcomed-civilian-drones-within-your-backyard-range.html.

Kerns, Andrew J., Daniel P. Shepard, Jahshan A. Bhatti, and Todd E. Humphreys. “Unmanned Aircraft Capture and Control via GPS Spoofing.” *Journal of Field Robotics* 31, no. 4 (August 2014): 617–36. https://doi.org/10.1002/rob.21513.

Kim, Byeong Hak, Danish Khan, Ciril Bohak, Wonju Choi, Hyun Jeong Lee, and Min Young Kim. "V-RBNN Based Small Drone Detection in Augmented Datasets for 3D LADAR System." *Sensors* 18, no. 11 (2018): 3825. https://doi.org/10.3390/s18113825.

Knezevich, Alison, and Ian Duncan. "Drone Intercepted near Maryland Prison, Officials Say." *Baltimore Sun*, August 25, 2015. https://www.baltimoresun.com/news/crime/bs-md-prison-drone-20150824-story.html.

Koper, Christopher S., Bruce G. Taylor, and Bruce E. Kubu. *Law Enforcement Technology Needs Assessment*. Washington, DC: Police Executive Research Forum, 2009. https://www.policeforum.org/assets/docs/Free_Online_Documents/Technology/law%20enforcement%20technology%20needs%20assessment%202009.pdf.

Kugler, Logan. "Why GPS Spoofing Is a Threat to Companies, Countries." *Communications of the ACM* 60, no. 9 (September 2017): 18–19. https://doi.org/10.1145/3121436.

Lamprecht, Joerg. "Tech Talk: Drone Safety and Defense Start with Detection." *Police Chief*, January 1, 2019. http://www.policechiefmagazine.org/tech-talk-drone-safety-and-defense-start-with-detection/.

Lee, Wee Leong. "Assessment of Foreign Objet Debris Management Using Group 1 Unmanned Aerial Systems." Master's thesis, Naval Postgraduate School, 2018. https://calhoun.nps.edu/handle/10945/60426.

Lillian, Betsy. "Seattle Court Orders Jail Time for 'Reckless Endangerment' Drone Incident." Unmanned Aerial, February 24, 2017. https://unmanned-aerial.com/seattle-court-orders-jail-time-for-reckless-endangerment-drone-incident.

Ling, Justin. "Someone Used a Drone to Deliver a Handgun into a Notorious Canadian Prison." Vice News, December 14, 2015. https://news.vice.com/en_us/article/gy9wnj/someone-used-a-drone-to-deliver-a-handgun-into-a-notorious-canadian-prison.

Local, The. "Update: 143 Flights Cancelled at Frankfurt Airport Due to Drone Sighting." Accessed May 18, 2019. https://www.thelocal.de/20190509/disruption-after-frankfurt-airport-halts-flights-due-to-drone-sighting.

Managing the Land. "If You Fly, We Can't." U.S. Forest Service. Accessed July 11, 2019. https://www.fs.fed.us/managing-land/fire/uas/if-you-fly.

Mercer-Myers, Christina. "How Are Drones Used?." Techworld, July 30, 2019. https://www.techworld.com/picture-gallery/apps-wearables/best-uses-of-drones-3605145/.

Michel, Arthur Holland. *Counter-Drone Capabilities in the Middle East and Beyond: A Primer*. Policywatch 3045. Washington, DC: Washington Institute for Near East Policy, 2018. https://www.washingtoninstitute.org/policy-analysis/view/counter-drone-capabilities-in-the-middle-east-and-beyond-a-primer.

———. *Counter-Drone Systems 2018*. Washington, DC: The Center for the Study of the Drone at Bard College, 2018. https://dronecenter.bard.edu/publications/counter-drone-systems/.

Michel, Arthur Holland, and Dan Gettinger. *Drone Incidents: A Survey of Legal Cases*. Washington, DC: Center for the Study of Drone, Bard College, 2017. https://dronecenter.bard.edu/drone-incidents/.

———. *Drone Year in Review: 2017*, 2018. https://dronecenter.bard.edu/projects/other-projects/drone-year-in-review-2017/.

Miletich, Steve. "Pilot of Drone that Struck Woman at Pride Parade Gets 30 Days in Jail." *Seattle Times*, February 24, 2017. https://www.seattletimes.com/seattle-news/crime/pilot-of-drone-that-struck-woman-at-pride-parade-sentenced-to-30-days-in-jail/.

Miller, John J. "Local Efforts to Counter the Terror Threat in New York City: A Retrospective and a Roadmap." Homeland Security, Subcommittee on Intelligence and Counterterrorism (2019). https://homeland.house.gov/hearings-and-markups/hearings/local-efforts-counter-terror-threat-new-york-city-retrospective-and.

Moore, Jeanie. "Da Vinci's Children Take Flight: Unmanned Aircraft Systems in the Homeland." Master's thesis, Naval Postgraduate School, 2014. https://calhoun.nps.edu/handle/10945/41420.

Musgrave, Shawn. "Boston Police Set Up 'Drone Shields' along the 2015 Marathon Route." Vice, April 22, 2015. https://www.vice.com/en_us/article/ezv83k/boston-police-set-up-drone-shields-along-the-2015-marathon-route.

National Institute of Justice. "The Use-of-Force Continuum." August 3, 2009. http://nij.ojp.gov/topics/articles/use-force-continuum.

National Interagency Fire Center. "Unmanned Aircraft Systems (UAS or Drones)." Drones and Wildfires. Accessed July 11, 2019. https://www.nifc.gov/drones/.

Nellis, Stephen. "Drone-Catchers Emerge on a New Aerial Frontier." Reuters, March 21, 2017. https://www.reuters.com/article/us-usa-drone-hunter-idUSKBN16S1IT.

Net Gun Store, The. "Net Gun|Net Launcher|Net Shooter—The World's #1 Net Gun Provider!." Accessed August 10, 2019. https://thenetgunstore.com/.

Nicas, Jack. “Criminals, Terrorists Find Uses for Drones, Raising Concerns.” *Wall Street Journal*, January 28, 2015. http://www.wsj.com/articles/criminals-terrorists-find-uses-for-drones-raising-concerns-1422494268.

O’Brien, Brendan. “Six Drones Confiscated in Atlanta Ahead of Super Bowl.” *Reuters*, February 3, 2019. https://www.reuters.com/article/us-football-nfl-superbowl-drones-idUSKCN1PR0PL.

Oliver, David. “The Flying IED Threat.” *Military Technology* 42, no. 5 (May 2018): 67–70. Ebsco.

Olmo, Stephanie. “Scottsdale Police Using Drone Detection Technology at Waste Management Phoenix Open.” Fox 10 Phoenix, February 1, 2018. http://www.fox10phoenix.com/news/arizona-news/scottsdale-police-using-drone-detection-technology-at-waste-management-phoenix-open.

Palmer, Thomas S., and John P. Geis II. “Defeating Small Civilian Unmanned Aerial Systems to Maintain Air Superiority.” *Air & Space Power Journal* 31, no. 2 (Summer 2017): 102–18. https://www.airuniversity.af.edu/Portals/10/ASPJ_Spanish/Journals/Volume-29_Issue-4/2017_4_07__palmer_s_eng.pdf.

Pasztor, Andy, and Dustin Volz. “Worries Mount over Ability to Weaponize Drones.” *Wall Street Journal*, August 7, 2018. https://www.wsj.com/articles/worries-mount-over-drone-safety-after-venezuela-attack-1533601121.

Perez, Lindsay. “Drone Tries to Sneak Contraband into Georgia Prison.” NBC News, November 27, 2013. http://www.nbcnews.com/news/world/drone-tries-sneak-contraband-georgia-prison-flna2D11665517.

Peters, Kevin M. “21st Century Crime: How Malicious Artificial Intelligence Will Impact Homeland Security.” Master’s thesis, Naval Postgraduate School, 2019. https://www.hsdl.org/?abstract&did=825201.

Pomerleau, Mark. “Drones: Findable but Not Stoppable.” GCN, June 3, 2015. https://gcn.com/articles/2015/06/03/drone-detection.aspx.

Praisler, David J. *Counter-UAV Solutions for the Joint Force*. Maxwell Air Force Base, AL: Air War College, Air University, 2017. https://apps.dtic.mil/docs/citations/AD1037984.

Radar Basics. “Radar Principle.” Accessed July 28, 2019. http://www.radartutorial.eu/01.basics/Radar%20Principle.en.html.

Raytheon. “Bad to the Drone—This System Helps to Clip the Wings of Malicious Unmanned Aircraft.” May 5, 2019. https://www.raytheon.com/news/feature/bad-drone.

Reagan, Jason. “SkyWall Protects Obama from Potential Drone Threats.” DroneLife, November 28, 2016. https://dronelife.com/2016/11/28/germany-skywall-protects-obama-potential-drone-threats/.

RMIT University. “Tech Issues Cause Most Drone Accidents: Research.” August 24, 2016. https://www.rmit.edu.au/news/newsroom/media-releases-and-expert-comments/2016/august/tech-issues-cause-most-drone-accidents--research.

Ross, Chuck. “FBI Director Discusses Threat of Terrorist Drones.” YouTube, 2017. Video, 2:05. https://www.youtube.com/watch?v=GpR2z4-vYJ4&feature=youtu.be.

Rubens, Tilly. “Drug-Smuggling Drones: How Prisons Are Responding to the Airborne Security Threat.” IFSEC Global, February 8, 2018. https://www.ifsecglobal.com/drones/drug-smuggling-drones-prisons-airborne-security-threat/.

Sanchez, Alejandro, and Cameron McKibben. “Worst Case Scenario: The Criminal Use of Drones.” *Council on Hemispheric Affairs*, February 2, 2015. http://www.coha.org/worst-case-scenario-the-criminal-use-of-drones/.

Sanders, Andrew William. “Drone Swarms.” Monograph, Leavenworth, KS: School of Advanced Military Studies, U.S. Army Command and General Staff College, 2017. https://apps.dtic.mil/dtic/tr/fulltext/u2/1039921.pdf.

Schaub, Hillary, and Darrell M. West. “Six Ways to Disable a Drone.” *TechTank* (blog), March 16, 2016. https://www.brookings.edu/blog/techtank/2016/03/16/six-ways-to-disable-a-drone/.

Schmersahl, Aaron R. “Fifty Feet above the Wall: Cartel Drones in the U.S.-Mexico Border Zone Airspace, and What to Do about Them.” Master’s thesis, Naval Postgraduate School, 2018. https://www.hsdl.org/?abstract&did=811367.

Schmidt, Michael S., and Michael D. Shear. “A Drone, Too Small for Radar to Detect, Rattles the White House.” *New York Times*, January 27, 2015. https://www.nytimes.com/2015/01/27/us/white-house-drone.html.

———. “Drones Spotted, but Not Halted, Raise Concerns.” *New York Times*, January 29, 2015. https://www.nytimes.com/2015/01/30/us/for-super-bowl-and-big-games-drone-flyovers-are-rising-concern.html.

Schuetze, Arno, and Tassilo Humme. “Air Traffic at Frankfurt Airport Resumes after Drone Sighting...” Reuters, May 8, 2019. https://www.reuters.com/article/us-germany-drones-frankfurt-airport-idUSKCN1SF0IU.

Security. “DHS Releases UAS Threats on Critical Infrastructure Video.” May 10, 2019. https://www.securitymagazine.com/articles/90214-dhs-releases-uas-threats-on-critical-infrastructure-video.

Senate Committee on Homeland Security and Governmental Affairs. *Joint Testimony of the Honorable David J. Glawe, Under Secretary for Intelligence and Analysis, U.S. Department of Homeland Security, Hayley Chang, Deputy General Counsel, S. 2836, the Preventing Emerging Threats Act of 2018: Countering Malicious Drones*. Washington, DC: Department of Homeland Security, 2018. https://www.hsgac.senate.gov/imo/media/doc/Testimony-Glawe%20and%20Chang-2018-06-061.pdf.

Shain, Julie. "Cars and Trucks as Weapons of Terror." *Tech and Terrorism* (blog), April 7, 2017. https://www.counterextremism.com/blog/cars-and-trucks-weapons-terror.

Shakir, Faiz, and Neema Singh Guliani. "ACLU Opposes S.2836." June 6, 2018. https://www.aclu.org/letter/aclu-opposition-preventing-emerging-threats-act-2018-countering-malicious-drones.

Shepardson, David. "FAA to U.S. Airports: Do Not Install Drone Countermeasures on Your Own." *Reuters*, May 8, 2019. https://www.reuters.com/article/us-usa-drones-airports/faa-to-u-s-airports-do-not-install-drone-countermeasures-on-your-own-idUSKCN1SE2QZ.

Smith, Brian T. "Ethics on the Fly: Toward a Drone-Specific Code of Conduct for Law Enforcement." Master's thesis, Naval Postgraduate School, 2016. https://calhoun.nps.edu/handle/10945/48476.

Smith, Kurt W. "Drone Technology: Benefits, Risks, and Legal Considerations." *Seattle Journal of Environmental Law* 5, no. 1 (2015): 291–302. https://digitalcommons.law.seattleu.edu/sjel/vol5/iss1/12.

Snead, Jason, and John-Michael Seibler. "Legal Framework for Counter-Drone Operations Is Critical to the Future." Heritage Foundation, July 3, 2018. https://www.heritage.org/defense/commentary/legal-framework-counter-drone-operations-critical-the-future.

Snead, Jason, John-Michael Seibler, and David Inserra. *Establishing a Legal Framework for Counter-Drone Technologies*. Backgrounder No. 3305. Washington, DC: Heritage Foundation, 2018. https://www.heritage.org/sites/default/files/2018-04/BG3305_1.pdf.

Snead, Jason. "It's Time to Empower Police to Stop Drone Threats." Heritage Foundation, June 26, 2019. https://www.heritage.org/crime-and-justice/commentary/its-time-empower-police-stop-drone-threats.

Solodov, Alexander, Adam Williams, Sara Al Hanaei, and Braden Goddard. "Analyzing the Threat of Unmanned Aerial Vehicles (UAV) to Nuclear Facilities." *Security Journal* 31, no. 1 (February 2018): 305–24. https://doi.org/10.1057/s41284-017-0102-5.

South, Todd. “This Laser Could Help Marines Knock down Drones on the Fob or on the Move.” *Marine Corps Times*, September 29, 2018. https://www.marinecorpstimes.com/news/your-marine-corps/2018/09/29/this-laser-could-help-marines-knock-down-drones-on-the-fob-or-on-the-move/.

Stamey, Barcley W. “Domestic Aerial Surveillance and Homeland Security: Should Americans Fear the Eye in the Sky?.” Master’s thesis, Naval Postgraduate School, 2014. https://calhoun.nps.edu/handle/10945/41466.

Stevens, Alexis. “Enforcing ‘No Drone Zone’ near the Super Bowl Is Tough for Authorities.” *Atlantic Journal-Constitution*, February 1, 2019. https://www.ajc.com/news/crime--law/enforcing-drone-zone-near-the-super-bowl-tough-for-authorities/q5p3QFMiXHgHW8Q7h6ueuL/.

Stokel-Walker, Chris. “Why Drones Cause Airport Chaos.” *New Scientist* 241, no. 3213 (January 19, 2019): 10. https://doi.org/10.1016/S0262-4079(19)30100-9.

Stone, Jeff. “Does ISIS Have Drones? Propaganda Footage Shows Aerial View of Syrian Raqqa Army Base.” *International Business Times*, August 25, 2014. https://www.ibtimes.com/does-isis-have-drones-propaganda-footage-shows-aerial-view-syrian-raqqa-army-base-video-1668474.

Stover, Jamie. “Explosions Leaving Many on Edge in Northampton County.” WFMZ-TV 69 News, June 6, 2019. https://www.wfmz.com/news/lehigh-valley/explosions-leaving-many-on-edge-in-northampton-county/1083883100.

sUAS News. “The Ghoul Tool Full Spectrum (GTFS) Hand-Held Drone Countermeasure Has Arrived!.” August 29, 2018. https://www.suasnews.com/2018/08/the-ghoul-tool-full-spectrum-gtfs-hand-held-drone-countermeasure-has-arrived/.

Sullivan, John P., and Robert J. Bunker. “Mexican Cartel Strategic Note No. 18: Narcodrones on the Border and Beyond.” *Small Wars Journal*, March 28, 2016. https://www.hsdl.org/?abstract&did=791699.

Tepper, Fitz. “The FAA Gets a Case Study with a Drone Crash inside an MLB Stadium.” TechCrunch, May 23, 2017. http://social.techcrunch.com/2017/05/23/the-faa-gets-a-case-study-with-a-drone-crash-inside-an-mlb-stadium/.

Thurbron, Rob. “Criminals Used Swarm of Drones to Disrupt FBI Hostage Raid.” TechSpot, May 4, 2018. https://www.techspot.com/news/74466-criminals-used-swarm-drones-disrupt-fbi-hostage-raid.html.

Titterton, David H. *Military Laser Technology and Systems*. Boston, MA: Artech House, 2015.

Tracey, Meredith. *Law Enforcement Guide for Suspected Unauthorized UAS Operations*. Washington, DC: Federal Aviation Administration, 2015. https://www.faa.gov/uas/resources/policy_library/media/FAA_UAS-PO_LEA_Guidance.pdf.

U.S. Air Force. "Information about GPS Jamming." GPS. Accessed July 30, 2019. https://www.gps.gov/spectrum/jamming/.

U.S. Government Publishing Office. "U.S.C. Title 18—Crimes and Criminal Procedure." Accessed August 7, 2019. https://www.govinfo.gov/content/pkg/USCODE-2011-title18/html/USCODE-2011-title18-partI-chap2-sec32.htm.

U.S. Senate Committee on Homeland Security & Governmental Affairs. "S. 2836, the Preventing Emerging Threats Act of 2018: Countering Malicious Drones." 2018. https://www.hsgac.senate.gov/hearings/s-2836-the-preventing-emerging-threats-act-of-2018-countering-malicious-drones.

Ubaldi, John. "Will Terror Organizations Use Drones to Attack the U.S.?." In Homeland Security, May 15, 2019. https://inhomelandsecurity.com/drones-attack-us/.

United States Department of Justice, Office of the United States Attorneys, Southern District of Georgia. "16 Defendants Indicted on Federal Drug Trafficking Charges." September 28, 2016. https://www.justice.gov/usao-sdga/pr/16-defendants-indicted-federal-drug-trafficking-charges.

Vacek, Joseph J. "Counter-UAS Applications Illegal under 18 U.S.C. § 32 Are Justified When Using a Reasonably Defensible Counter-UAS Strategy that Incorporates Risk and Compliance Categorizations." *North Dakota Law Review* 93, no. 3 (2018): 499–519. https://law.und.edu/law-review/issues/93/93-3.html.

Ventiere, Mike II. "Soft Targets: Stemming the Tide of Vehicle Ramming Attacks." *Security Technology Executive* 27, no. 3 (August 2017): 17. ProQuest.

Wall, Robert. "Gatwick Resumes Flights Once Again After Drone Scare; U.K's Second-Busiest Airport Begins Returning to Normal Operations Comes After Sighting of Another Drone." *Wall Street Journal*, December 22, 2018. http://search.proquest.com/docview/2159531786/citation/6E7A280EAB674A70PQ/1. ProQuest.

Wallace, Ryan J., and Jon M. Loffi. "Examining Unmanned Aerial System Threats & Defenses: A Conceptual Analysis." *International Journal of Aviation, Aeronautics, and Aerospace* 2, no. 4 (2015): 1–32. https://doi.org/10.15394/ijaaa.2015.1084.

Weaver, Matthew, Damien Gayle, Patrick Greenfield, and Frances Perraudin. "Military Called in to Help with Gatwick Drone Crisis." *The Guardian*, December 20, 2018. https://www.theguardian.com/uk-news/2018/dec/19/gatwick-flights-halted-after-drone-sighting.

Werner, Charles. “Drones: The Need for Counter-Technology.” *Firehouse*, February 2018. http://search.proquest.com/docview/1989496569/abstract/BF5592D978FB4EEAPQ/1. ProQuest.

———. “Using Drones in the Fire Service.” *Firehouse; Fort Atkinson*, April 2015. http://search.proquest.com/docview/1685183092/abstract/CA0B5C8500FE4FC3PQ/1. ProQuest.

Weston, J. L., and D. H. Titterton. “Modern Inertial Navigation Technology and Its Application.” *Electronics Communication Engineering Journal* 12, no. 2 (April 2000): 49–64. https://doi.org/10.1049/ecej:20000202.

White, Jonathan R. *Terrorism and Homeland Security*. 7th ed. Belmont, CA: Cengage Learning, 2012.

White, Stanley. “Japanese Man Arrested for Landing Drone on PM’s Office in Nuclear Protest.” Reuters, April 24, 2015. https://www.reuters.com/article/us-japan-nuclear-drone-idUSKBN0NG04520150425.

Wiley Post Airport. “Department of Airports/Airport Trust.” Accessed July 14, 2019. http://wileypostairport.com/Page/AirportsTrust.

Williams, Rhiannon. “Tokyo Police Are Using Drones with Nets to Catch Other Drones.” *Telegraph*, December 11, 2015. https://www.telegraph.co.uk/technology/2016/01/21/tokyo-police-are-using-drones-with-nets-to-catch-other-drones/.

Wilson Center. “Timeline: The Rise, Spread, and Fall of the Islamic State.” April 30, 2019. https://www.wilsoncenter.org/article/timeline-the-rise-spread-and-fall-the-islamic-state.

Winick, Erin. “Researchers Taught a Drone to Herd Birds Away from Airports.” *MIT Technology Review*, August 7, 2018. https://www.technologyreview.com/the-download/611834/researchers-taught-a-drone-to-herd-birds-away-from-airports/.

Wray, Christopher A. *Statement of Christopher A. Wray, Director, Federal Bureau of Investigation, before the Committee on Homeland Security and Governmental Affairs, United States Senate*. Washington, DC: Department of Justice, 2018. https://www.hsgac.senate.gov/imo/media/doc/Testimony-Wray-2018-10-10.pdf.

Wright, Tim. “If You Crash a Drone, You Might Land Yourself in Jail: The Story Behind a Recent Landmark Conviction.” *Air & Space Magazine*, August 2017. https://www.airspacemag.com/flight-today/36_aug2017-uav-criminal-180963942/.

Zickuhr, Kathryn, Elias Stahl, and Nicole DuPuis. *Cities and Drones: What Cities Need to Know about Unmanned Aerial Vehicles (UAVs)*. Washington, DC: National League of Cities, 2016. https://www.nlc.org/sites/default/files/2016-12/NLC%20Drone%20Report.pdf.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California