
# NAVAL POSTGRADUATE SCHOOL

**MONTEREY, CALIFORNIA**

# THESIS

**OPENING THE APERTURE: HOLISTIC MITIGATION OPTIONS IN RESPONSE TO UAS THREATS**

by

Michael W. Young

September 2022

Co-Advisors: Nadav Morag (contractor)
Erik J. Dahl

THIS PAGE INTENTIONALLY LEFT BLANK

| REPORT DOCUMENTATION PAGE | | | *Form Approved OMB No. 0704-0188* |
|---|---|---|---|



| **1. AGENCY USE ONLY** *(Leave blank)* | **2. REPORT DATE** September 2022 | **3. REPORT TYPE AND DATES COVERED** Master's thesis |
|---|---|---|

| **4. TITLE AND SUBTITLE** OPENING THE APERTURE: HOLISTIC MITIGATION OPTIONS IN RESPONSE TO UAS THREATS | **5. FUNDING NUMBERS** |
|---|---|
| **6. AUTHOR(S)** Michael W. Young | |
| **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** Approved for public release. Distribution is unlimited. | **12b. DISTRIBUTION CODE** A |
|---|---|

**13. ABSTRACT (maximum 200 words)**

A synchronized collection of intelligence and investigative capacities, such as would be required to holistically mitigate the emerging threat from unmanned aircraft systems, does not currently exist within the United States government. Furthermore, the entities that do possess the authority, knowledge, and experience to respond are working within largely independent environments. This thesis seeks to identify the best method to collectivize individual agency strengths, unifying intelligence and investigative capacities into one juggernaut-level response against UAS threats. To address this, working groups, task forces, and single agency designation were chosen as potential options specifically for their historical precedence and likelihood of success. Each was compared according to their ability to embrace two defining characteristics: collaboration and commitment. The outcome of the analysis determined that the task force model was ultimately the most effective means to address UAS threats holistically. It mitigates the challenges associated with current technology and legal restrictions by utilizing intelligence and investigative operational capabilities to properly address each of the six steps within the UAS kill chain, all within an environment of high collaboration and commitment. The conclusions and accompanying recommendations outlined in this thesis provide a definitive direction as well as a rational plan of implementation.

| **14. SUBJECT TERMS** FBI, UAS, drone, task force, intelligence, investigations | **15. NUMBER OF PAGES** 105 |
|---|---|
| | **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.**

# OPENING THE APERTURE: HOLISTIC MITIGATION OPTIONS IN RESPONSE TO UAS THREATS

Michael W. Young
Unit Chief, Federal Bureau of Investigation
BA, Pennsylvania State University, 1997

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
September 2022**

Approved by: Nadav Morag
Co-Advisor

Erik J. Dahl
Co-Advisor

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

THIS PAGE INTENTIONALLY LEFT BLANK

# ABSTRACT

A synchronized collection of intelligence and investigative capacities, such as would be required to holistically mitigate the emerging threat from unmanned aircraft systems, does not currently exist within the United States government. Furthermore, the entities that do possess the authority, knowledge, and experience to respond are working within largely independent environments. This thesis seeks to identify the best method to collectivize individual agency strengths, unifying intelligence and investigative capacities into one juggernaut-level response against UAS threats. To address this, working groups, task forces, and single agency designation were chosen as potential options specifically for their historical precedence and likelihood of success. Each was compared according to their ability to embrace two defining characteristics: collaboration and commitment. The outcome of the analysis determined that the task force model was ultimately the most effective means to address UAS threats holistically. It mitigates the challenges associated with current technology and legal restrictions by utilizing intelligence and investigative operational capabilities to properly address each of the six steps within the UAS kill chain, all within an environment of high collaboration and commitment. The conclusions and accompanying recommendations outlined in this thesis provide a definitive direction as well as a rational plan of implementation.

THIS PAGE INTENTIONALLY LEFT BLANK

# TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

# LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

# LIST OF ACRONYMS AND ABBREVIATIONS

| | |
|---|---|
| 2D | two dimensional |
| 3D | three dimensional |
| BOP | Bureau of Prisons |
| CBP | Customs and Border Protection |
| CBRNE | chemical, biological, radiological, nuclear, explosive |
| CISA | Cybersecurity and Infrastructure Security Agency |
| CONUS | continental United States |
| COTS | commercial off the shelf |
| C-UAS | counter unmanned aircraft systems |
| DASH | Drone Anti-Submarine Helicopter |
| DEA | Drug Enforcement Administration |
| DHS | Department of Homeland Security |
| DIY | do it yourself |
| DJI | Da Jiang Innovations |
| DOD | Department of Defense |
| DOE | Department of Energy |
| DOJ | Department of Justice |
| EO/IR | electro-optical/infrared |
| EXCOM | executive committee |
| F2T2EA | find, fix, track, target, engage, and assess |
| FAA | Federal Aviation Administration |
| FBI | Federal Bureau of Investigation |
| FCC | Federal Communications Commission |
| FEMA | Federal Emergency Management Agency |
| FPS | Federal Protective Service |
| GCS | ground control station |
| GNSS | global navigation satellite system |
| HIDTA | high intensity drug trafficking area |
| IED | improvised explosive device |
| ISIS | Islamic State of Iraq and Syria |

| | |
|---|---|
| JCO | Joint Counter-small Unmanned Aircraft Systems Office |
| JTTF | Joint Terrorism Task Force |
| LAWS | Lethal autonomous weapons systems |
| NSSE | national special security events |
| OCDETF | organized crime drug enforcement task force |
| RDTE | research development testing evaluation |
| RF | radio frequency |
| ROAD | retired on active duty |
| SEAR | special event assessment rating |
| SOCOM | Special Operations Command |
| STEM | science, technology, engineering, mathematics |
| TFO | task force officer |
| TSA | Transportation Security Administration |
| UAE | United Arab Emirates |
| UAH | University of Alabama in Huntsville |
| UAS | unmanned aircraft systems |
| UAS Kill Chain | 1) plan; 2) acquire components; 3) test; 4) pre-operational surveillance; 5) attack; and 6) escape |
| USCG | United States Coast Guard |
| USMS | United States Marshals Service |
| USSS | United States Secret Service |
| WMD | weapons of mass destruction |

# EXECUTIVE SUMMARY

A synchronized collection of intelligence and investigative capacities, such as would be required to holistically mitigate the emerging threat from Unmanned Aircraft Systems, does not currently exist within the United States government. Furthermore, the entities which do possess the authority, knowledge, and experience to respond are working within largely independent environments. Some of this is mandated under current legal restrictions, however, there is also an underlying political current of selfishness permeating throughout.

This thesis seeks to identify the best method to collectivize individual agency strengths, unifying intelligence and investigative capacities into one juggernaut level response against UAS threats. The three main problems exposed within this body of research consist of current technology limitations, legal impediments, and a myopic focus upon one aspect of the UAS Kill Chain, a six-step process through which nefarious individuals plot an attack. Working groups, task forces, and single agency designation were the options chosen specifically for their historical precedence and likelihood of success. Each was compared according to their ability to embrace two defining characteristics: collaboration and commitment.

Working Groups were reviewed first and eventually discounted. While they possess a high level of collaboration, the level of commitment required to be effective in the UAS threat environment is extraordinarily low. Additionally, working groups are already prevalent throughout the federal, state, and local governments, which makes them appear more akin to status quo than innovative option.

Task forces were reviewed second and could not be ignored. Task forces possess a high level of collaboration and commitment, unlike working groups. Task force models also have a history of success at incorporating intelligence and investigative operations against other significant threats such as terrorism, organized crime, and narcotics.[1]

[1] Robert A. Martin, "The Joint Terrorism Task Force: A Concept That Works," *FBI Law Enforcement Bulletin* 68, no. 3 (March 1999): 23–27, ProQuest.

Single agency designation was the final option to be analyzed. In terms of commitment, this choice rated extremely high due to it being solely responsible for both the success, and failures, of its actions. Unfortunately, single agency designation ranks correspondingly very low regarding collaboration.

The outcome of the analysis determined that the task force model was ultimately the most effective means to address UAS threats holistically. It mitigates the challenges associated with current technology and legal restrictions by utilizing intelligence and investigative operational capabilities to properly address each of the six steps within the UAS Kill Chain, all within an environment of high collaboration and commitment.

The recommendations outlined in this thesis provide direction and a rational plan of implementation. It begins with a national, *administrative* task force component to develop policy and would be mirrored at the state level to ensure continuity. With administrative and policy requirements accounted for, a national, *operational* task force component, in equal partnership with the administrative side, would be created to action those policy obligations via strategy development containing mission-oriented objectives and achievable milestones. This would also be mirrored at the state level.

# ACKNOWLEDGMENTS

It has been an honor to work toward and now complete my master's thesis for the Naval Postgraduate School's Center for Homeland Defense and Security. While I completed the direct work within this program, there are several people who deserve to be thanked for their contribution to my success:

To my Family — Thank you. I am so blessed to have you all as my greatest allies and sources of encouragement throughout the past 18 months. I want to particularly thank my beautiful wife for her patience and understanding as I spent many late nights and weekends consumed by schoolwork.

To Nadav and Erik — Thank you both for all your time, assistance, and encouragement as I went through this process. I was very fortunate to secure you both as my advisors.

To the Federal Bureau of Investigation — Thank you for electing me to represent our agency and carry on the tradition of excellence.

To my CHDS cohort 2101/2102 — Thank you for the opportunity to go through this program with each one of you. It has been a distinct pleasure and I now count you as my friends.

To the CHDS faculty and staff — Thank you for providing a wonderful graduate experience. Your vested interest in my success was instrumental in getting me through such a challenging program.

THIS PAGE INTENTIONALLY LEFT BLANK

# I. INTRODUCTION

## A. PROBLEM STATEMENT

Today, most countries appropriately categorize Unmanned Aircraft Systems (UAS), or drones as they are more commonly referred to, as a lethal autonomous weapons system (LAWS). Most systems rate this designation because of the sophisticated technology employed as the command-and-control mechanism for the overall platform, as well as the attached sensors and deadly payload options available. So lethal is this platform that the international community actively seeks a consensus as to its legality, both from a research standpoint and in potential deployment on any future battlefields. Acquiring UAS platforms is legal, relatively low-cost, and lacks adequate oversight. Continuing advances in command-and-control software, as well as obstacle avoidance technology, make such devices extremely user-friendly.

Terrorists and Transnational Criminal Organizations continue to employ UAS platforms as an innovative method of achieving their goals. International terrorist groups, such as ISIS, have been deploying UAS to attack their adversaries for several years now.[1] More recently, Mexican drug cartels have also started using UAS platforms to transport illegal narcotics across our shared border and assassinate rivals, politicians, and the police.[2] From a proximity standpoint, the UAS threat is approaching the United States and, therefore, can no longer be ignored. To be blunt, the American response to this encroachment currently lacks a consolidated strategy incorporating stakeholder agencies and units from all levels of government, synchronized with academic and private sector partners.

The FBI, as part of that American response, currently lacks a scientifically focused, centralized apparatus dedicated to intelligence, investigations, and operational response

[1] Kentaro Hoshiko, "ISIS' Drone Fleet," *The Intelligencer* (blog), May 17, 2017, https://www.phc.edu/intelligencer/isis-drone-fleet.

[2] John P. Sullivan, Robert J. Bunker, and David A. Kuhn, "Mexican Cartel Tactical Note #38: Armed Drone Targets the Baja California Public Safety Secretary's Residence in Tecate, Mexico | Small Wars Journal," Small Wars Journal, August 6, 2018, https://smallwarsjournal.com/jrnl/art/mexican-cartel-tactical-note-38-armed-drone-targets-baja-california-public-safety.

against emerging technology threats such as UAS platforms. As one of several Department of Justice (DOJ) agencies, this dynamic creates significant problems with coordination, logistics, and defining individual responsibilities; all of which signal a more substantial homeland security gap within the entire U.S. government. Along with the DOJ, the Department of Homeland Security (DHS), the Department of Defense (DOD), and the Department of Energy (DOE) make up the four entities Congressionally authorized to address UAS threats since they all experience them.[3] Besides their current inability to legally address the UAS threat, state, local, and tribal law enforcement agencies are also grappling with the proper response.

The consequences of siloed efforts among competing agencies include an incomplete threat picture because any intelligence gathered remains raw, largely unseen by those who can best exploit it. This unprocessed intelligence leads to investigative agencies that, without proper context, cannot take appropriate action. The reluctance to categorize UAS platforms effectively—meaning labeling them as an entirely new risk modality or incorporating them into existing threat paradigms—further complicates the threat picture. This gap exacerbates confusion and conflict among agencies competing for areas of responsibility.

An incomplete threat picture—coupled with lost investigative opportunities and undefined areas of responsibility—leads to an ineffective or even non-existent response capability. With an emerging threat such as UAS, the technology advances so rapidly that any attempt to get ahead of it is almost impossible. This accelerated rate of change makes effective intelligence and investigations vital components of the overall mitigation strategy. Without these two essential components, responsive action becomes untenable. This is because the preferred method of response against these unique threats currently entails already deployed C-UAS operators and equipment at a fixed venue which,

[3] "Interagency Issues Advisory on Use of Technology to Detect and Mitigate Unmanned Aircraft Systems," Justice News, August 17, 2020, https://www.justice.gov/opa/pr/interagency-issues-advisory-use-technology-detect-and-mitigate-unmanned-aircraft-systems.

unfortunately, only addresses one step (attack) of the overall UAS Kill Chain model, whilst completely ignoring the others.[4]

A kill chain model has traditionally been utilized by the United States military to address threats by showcasing their intended response methodology as a sequence of chronological steps. In 2011, Lockheed Martin, an American cleared defense contractor, modified the military's kill chain model to address cyber security threats, and in doing so, coined the term, cyber kill chain.[5] Their version of a kill chain differed in one significant way from the military's model, specifically in terms of the viewpoint espoused. Instead of looking at the kill chain as a step-by-step threat response model, Lockheed Martin presented the enemy's tactics in a step-by-step process, culminating in the actual attack itself. In doing so, it allowed strategists to not only identify the enemy's practices but analyzed approaches to counter their methodology as well.

Kill chain models can possess a variety of different characteristics such as threat modality, point-of-view, and component quantity. Given the sheer volume of variables available to both the military response model and the cyber threat perspective, it is important to understand the style differences between action and reaction. Kill chain models that focus upon the action (of the perpetrator) provide context to the specific threat modality, as well as the overall threat picture, because those actions tend to track along a similar course from initiation to incident. Alternatively, models that emphasize reaction (of the responder), as the military model does, exclude any information regarding adversarial tactics necessary to formulate an effective response. This is because it provides no background nor targeting methodology from which to correctly apply a reactionary kill chain model to.

To properly address the threat from drones, the UAS Kill Chain in Figure 1 was developed as the preferred model for the research to be conducted: 1) PLAN; 2) AQUIRE

---

[4] Bhargav Patel and Dmitri Rizer, *Counter-Unmanned Aircraft Systems Technology Guide*, CUAS-T-G-1 (Washington, DC: Department of Homeland Security, 2020), https://www.dhs.gov/sites/default/files/publications/c-uas-tech-guide_final_28feb2020.pdf.

[5] "What Is the Cyber Kill Chain? Process & Model," Cybersecurity 101: The Fundamentals of Cybersecurity, April 22, 2021, https://www.crowdstrike.com/cybersecurity-101/cyber-kill-chain/.

COMPONENTS; 3) TEST; 4) PRE-OPERATIONAL SURVEILLANCE; 5) ATTACK; 6) ESCAPE. This specific model eschews the military response version of kill chains in favor of the enemy tactics viewpoint developed by Lockheed Martin because UAS platforms are an emerging threat and, unlike conventional warfare equipment such as a tank or rocket propelled grenade, there is much to learn about the drone threat before an ultra-effective and cohesive response strategy can be properly implemented.

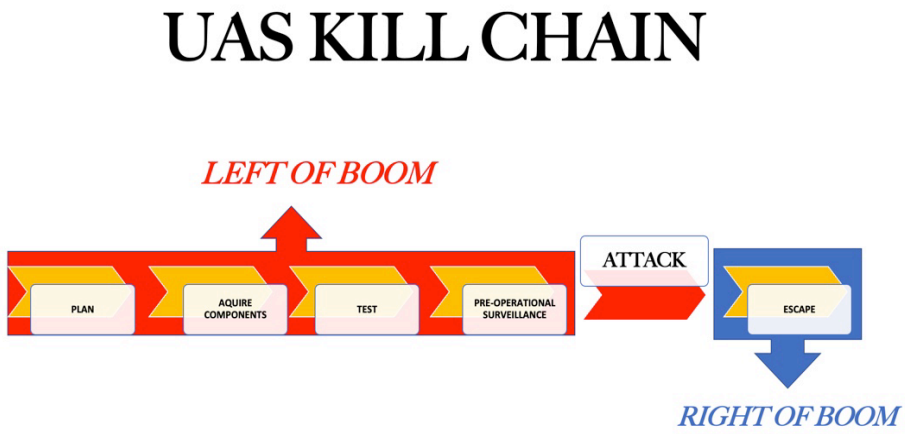


Figure 1. Unmanned Aircraft Systems Kill Chain

## B. RESEARCH QUESTION

How can the United States most effectively consolidate inter-agency resources and maximize both investigative and intelligence capacities to holistically address all six components of the UAS Kill Chain model?

## C. LITERATURE REVIEW

This literature review will first evaluate existing literature regarding the two main kill chain models in an effort to determine research scope viability. Once a determination is made in reference to the UAS threat environment specifically, additional literature will be reviewed to ascertain what, if any, components of the preferred kill chain model have been directly addressed within any Counter Unmanned Aircraft Systems (C-UAS) strategy currently being employed by the United States government. Finally, the remaining

commentary reveals what is being overlooked within that same literature as well. Academic, civilian government, and military sectors are the literature sources, thus intended to ensure a robust analysis.

## D. KILL CHAIN MODEL TYPES: ACTION VS. REACTION

Kill chains define the overall process of an attack, with the most effective examples displaying a fluctuating number of steps leading up to and following the attack itself. As previously stated, kill chain models are often constructed from the viewpoint of either the perpetrator or the responder, and are as varied as their origin and purpose. Overwhelmingly, the vast majority stem from either military strategy or within the cyber threat domain.

From a purely military perspective, author Adam Hebert asserted the need for Air Force assets to reduce the overall time necessary to move through the F2T2EA cycle, referring to it simply as the kill chain. This cycle refers to Find, Fix, Track, Target, Engage, and Assess.[6] The F2T2EA model tends to favor responsive actions that benefit from an opportunistic loitering functionality as opposed to the attacker's operational build-up. In other words, Hebert's claims fail to provide any behaviors to counter, preferring instead to define responsive actions to some unidentified threat.

The cyber kill chain, on the other hand, more closely resembles a structure that, if appropriately modified, could significantly benefit C-UAS response activities. It essentially provides a theoretical framework from which cyber security professionals can better understand the threat, as well as develop a mitigation strategy to deploy against the targeted hacker. Generally, the cyber kill chain consists of eight steps: Reconnaissance, Intrusion, Exploitation, Privilege Escalation, Lateral Movement; Obfuscation/Anti-forensics, Denial of service; and Exfiltration.[7] These steps, as affirmed by Hospelhorn,

---

[6] Adam J. Hebert, Hebert, Adam, "Compressing the Kill Chain," *Air Force Magazine*, March 1, 2003, https://www.airforcemag.com/article/0303killchain/.

[7] Sarah Hospelhorn, Hospelhorn, Sarah, "What Is the Cyber Kill Chain and How to Use It Effectively," *Inside Out Security* (blog), June 20, 2016, https://www.varonis.com/blog/cyber-kill-chain.

clearly demonstrate adversarial actions from which an effective response can subsequently be formulated.

To summarize, current literature provides a window to show how flexible kill chain models have the capacity to be, particularly considering that the available options are as varied as the individual attack considerations. On one end of the spectrum is Hebert's F2T2EA model, which is classic military response strategy. As the pendulum swings toward the opposite end, the model described by Hospelhorn eschews a traditional response viewpoint due to the cyber attack's emergence as a relatively new type of technological threat.

Each model has its own merits and environmental applicability. Unfortunately, even though the collected works have thus far illustrated just how flexible the kill chain model is, and its potential pertinence to the UAS threat environment, the literature's major shortcoming is that authors like Hebert and Hospelhorn have failed to connect those two appropriately. Even when authors do make that correlation, they apply the improper model to the environment. For instance, authors Hebert, Van Bossuyt, Tang, and Hale all consistently employ the military F2T2EA model, which basically means the entire process begins the moment the UAS is launched and ends once the attack has been completed.[8] As previously asserted with Hebert's material, this model subscribes to the reactionary viewpoint, meaning it provides no threat context, thus eliminating any holistic understanding of the attack. This completely removes the ability to adapt customized response solutions to the unique nature of these types of attacks, which the cyber-based model provides. Applying the action-oriented (cyber-based) model throughout the remainder of this study, the following six steps have been developed and will be utilized as the UAS Kill Chain: Plan; Acquire components; Test; Pre-operational surveillance; Attack; and Escape.

[8] Choon Seng Tan, Douglas L. Van Bossuyt, and Britta Hale, "System Analysis of Counter-Unmanned Aerial Systems Kill Chain in an Operational Environment," *Systems* 9, no. 4 (2021): 1–27, https://doi.org/10.3390/systems9040079.

## E. CIVILIAN GOVERNMENT POLICY LITERATURE

One specific example, cited by the Department of Homeland Security (DHS) on page 13 of its C-UAS Tech Guide, showcases a C-UAS processing chain model with the following stages: detect, locate/track, classify/identify, and mitigate. This literature addresses the immediate threat situation faced by the C-UAS operator.[9] On pages 4–5 of the June 25, 2020, DHS Office of Inspector General report, specific agencies within DHS have essentially adopted this same department-level strategy to include the United States Secret Service (USSS), the United States Coast Guard (USCG), Customs and Border Protection (CBP), as well as the Federal Protective Service (FPS).[10]

As previously stated, these two pieces of DHS literature directly address the attack step of the UAS Kill Chain. More to the point, when an attack occurs, DHS' C-UAS processing chain model is immediately applied as the attack occurs and assumes that defensive resources are already available on site. Because the UAS Kill Chain consists of six components, and not just one, the literature, therefore, fails to capture the entire UAS threat picture and, ultimately, fails to holistically address the problem.

## F. MILITARY POLICY LITERATURE

Unlike the previously mentioned DHS C-UAS processing chain model, author Joseph Lacdan describes the Department of Defense's new C-UAS strategy as a compilation of three wide-ranging components: Ready the Force, Defend the Force, and Build the Team.[11] Ready the Force means implementing a risk-based approach using C-UAS systems specific to each unique environment. Defend the Force implies the creation and implementation of standard operating procedures, as well as synchronized training

---

[9] Patel and Rizer, *Counter-Unmanned Aircraft Systems Technology Guide*.

[10] Joseph V. Cuffari, *DHS Has Limited Capabilities to Counter Illicit Unmanned Aircraft Systems*, OIG-20-43 (Washington, DC: Department of Homeland Security Office of Inspector General, 2020), https://permanent.fdlp.gov/gpo144914/OIG-20-43-Jun20.pdf.

[11] Joseph Lacdan, "Army to Lead New DOD Strategy against Drone Attacks," Army News Service, www.army.mil, January 11, 2021, https://www.army.mil/article/242276/army_to_lead_new_dod_strategy_against_drone_attacks.

across each of the service branches. Build the Team seeks to increase collaboration among the services, other government organizations, and foreign allies.

This piece of literature moves beyond the DHS C-UAS approach previously mentioned, contending that a more broad-based strategy is necessary for success against the threat. Although the first two components purely address the attack step within this study's UAS Kill Chain, the third may have some potential applicability to additional aspects of the overall process. Despite that, the most significant issue with this piece of literature is the failure to explain any of those three components in sufficient detail. For example, the Build the Team portion neither thoroughly explains specific types of collaboration nor provides examples. Although partnership might create opportunities to address the other five steps within the UAS threat kill chain, the literature lacks specificity about how the military might exploit those opportunities.

Author Matthew Tedesco also loosely follows the DHS C-UAS strategy, focusing primarily on C-UAS equipment's ability to address an immediate attack yet again.[12] Within that same article, Tedesco also correctly points out the need to re-examine and improve C-UAS tactics, training, and policies in coordination with each branch of service. Despite those additional considerations, which coincide with Lacdan's DOD article, the author neglects to include any of the remaining five steps within the UAS Kill Chain process. Tedesco even references a kill chain, stating, "If the soldier can confirm the UAS is a threat, this is the first step in the UAS defense kill chain."[13] Although identification—as the first step within DHS' C-UAS processing chain model—coincides with the author's assertion, the remaining text conspicuously lacks any additional actions within his self-titled defense kill chain concept. In other words, the literature again fails to address anything left or right of boom.

---

[12] Matthew T. Tedesco, "Countering the Unmanned Aircraft Systems Threat," *Military Review* 95, no. 6 (December 2015): 64–69, https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20151231_art012.pdf.

[13] Tedesco, 68.

## G. ACADEMIC LITERATURE

Moving from military to academic authors, Wang, Liu, and Song discuss specific challenges within the C-UAS environment but remain, like Lacdan and Tedesco, completely fixated upon C-UAS equipment as the prioritized response to drone threats.[14] When discussing the challenges within the article for *IEEE Aerospace and Electronic Systems Magazine*, the authors identify the disadvantages of each method, that is, the effectiveness of the C-UAS equipment *within* each mitigation method.[15] Yet again, the authors address no consideration on the left or right of boom within the article. As previously pointed out, a narrow focus on elements of the immediate attack phase, as Wang, Liu, and Song did, showcases yet another missed opportunity within the associated literature to address the entire UAS Kill Chain.[16]

Travis Cline and J. Eric Dietz's article for Embry Riddle Aeronautical University's *International Journal of Aviation, Aeronautics, and Aerospace* discusses the limited effectiveness of fixed C-UAS mitigation equipment as drone speeds increase beyond the ability to respond successfully within a small area.[17] Using a prison environment as their chosen testbed, both authors assert the "goal of a fixed facility C-UAS system is to mitigate the threat, or in this case, prevent overflights of the facility." [18] Cline and Dietz likewise produce a work limited in scope to the attack scenario itself, much like the other authors.

## H. LITERATURE REVIEW SUMMARY

The military kill chain model is flawed in reference to the UAS threat environment because it sees the problem merely from a responsive standpoint when the perpetrator actions have yet to be properly identified and analyzed. This is appropriate when the threat

---

[14] Jian Wang, Yongxin Liu, and Houbing Song, "Counter-Unmanned Aircraft System(s) (C-UAS): State of the Art, Challenges and Future Trends," *IEEE Aerospace and Electronic Systems Magazine* 36, no. 3 (March 2021): 4–29, https://doi.org/10.1109/MAES.2020.3015537.

[15] Wang, Liu, and Song.

[16] Wang, Liu, and Song.

[17] Travis Cline and J. Dietz, "Agent Based Modeling for Low-Cost Counter UAS Protocol in Prisons," *International Journal of Aviation, Aeronautics, and Aerospace* 7, no. 2 (2020): 1–17, https://doi.org/10.15394/ijaaa.2020.1462.

[18] Cline and Dietz, 13.

is conventional and well known, however, UAS platforms, as an emerging technology, are more suited to the cyber kill chain model because it is purely focused upon the perpetrator's actions. The current UAS threat is comparable to the resurgence of Improvised Explosive Devices (IED) during the Global War on Terror. This rebirth was due to IED technical innovations, such as radio control systems, which allowed remote detonation and thus increased the device's effectiveness on and off the battlefield.[19] In fact, the author, Roger Davies, sees UAS platforms as an innovative example of technological progression for IEDs because they can remotely deliver the explosive device with extraordinary accuracy.[20]

After determining which kill chain model is best for the UAS threat environment, the other major shortcoming identified within the prevailing literature remains the author's inability to enhance their focus beyond the expansion of one single step of the UAS kill chain model, as was shown back in Figure 1. How this single step is ultimately labeled, whether it be an attack, engagement, or exploitation is, ultimately, irrelevant. What is important is that the literature's myopic perspective unquestionably fails to include the entire threat picture, meaning it omits data regarding the nefarious activity perpetrated before and after the attack, preferring to concentrate solely upon the attack itself. The four steps defined by the UAS Kill Chain model that transpire prior to a UAS attack (left of boom), as well as the single step afterward (right of boom) showcase multiple opportunity gaps not addressed, or even identified, within the reviewed literature.

## I. RESEARCH DESIGN

Determining the most appropriate methodology to holistically understand the process by which UAS attacks are carried out is only the first step. The environment must also be defined to the greatest extent possible, which would necessarily include the overall threat picture, the modalities, and the geography, and the current challenges. With the methodology and environment outlined, the next step is to identify alternative options to

[19] Roger Davies, "The History of the IED Explained," AOAV – Action on Armed Violence, October 15, 2020, https://aoav.org.uk/2020/the-history-of-the-ied-explained/.

[20] Davies.

address the threat. Those options must incorporate strategy options and define stakeholder responsibilities. Strategy options are necessary because they showcase and effectively analyze the potential to maximize intelligence and investigative capacity through inter-agency consolidation of resources. Distinguishing stakeholder responsibilities ensures that consolidation occurs by preventing operational overlap and exploiting individual strengths.

This thesis moves well beyond the parochial focus presently being entertained as an answer to one of the most challenging risks our country has ever faced. Unmanned aircraft systems are a true dual-use platform, constantly upgraded by advancing technology, uncomplicated acquisition, and relatively simplistic flight control characteristics that when combined make them an incredibly lethal weapon. Specifically, the research design will analyze the three most realistic options beyond the status quo, in terms of precedence and viability, to consolidate individual efforts across the United States government, exploiting strengths, reducing vulnerabilities, and substantially improving response coverage and value. These options are long term, strategic solutions because the proliferation of UAS is highly unlikely to diminish over time. Each was purposely selected because they have been successfully utilized, to one degree or another, in the past by government as a joint threat response.

Option one is to form a federally based UAS threat working group, which will allow robust participation by all relevant agency stakeholders. Other names for a working group include advisory committees, commissions, and even panels. When taken together, there are literally hundreds of working group type collaborative efforts to be found within the federal system. For instance, there are currently almost fifty different committees within the U.S. Congress alone.[21] The working group option is quite popular because it provides a relatively simple method of bringing multiple agencies together to analyze a specific problem set and may be particularly helpful when faced with an emerging threat, such as from UAS platforms. As such, this option tends to be quite effective when clarifying the threat picture requires opening new lines of communication.

[21] United States Congress, "Committees of the U.S. Congress," Library of Congress, accessed July 24, 2022, https://www.congress.gov/committees.

Option two is to form a UAS task force, modeled along the lines of a Joint Terrorism Task Force (JTTF). This option literally takes the working group model to an entirely new level of commitment because participants collectively agree to move well beyond mere communication. Task Force formation demands partner agency commitment of substantial resources to tackle the problem in the form of funding, personnel, and time. Unlike a working group, which would not confer any type of jurisdictional authority, the task force option would allow state, local, and tribal law enforcement entities to participate as federally deputized task force officers (TFO). Just as with the working groups, there are significant numbers and types of federal task forces. For example, there are over 170 different FBI led Violent Gang Task Forces spread across the United States.[22]

Option three is to designate a single agency as the lead entity to address UAS threats. This option moves to the far end of the commitment spectrum, which began with the least involved working group choice before continuing to the middle task force option. In terms of commitment, the working group and task force options pale in comparison to single agency designation, however, that is not the only difference. Single agency designation also takes a completely different stance as it relates to collaboration, eschewing direct partnership equities in favor of a single point of accountability and control. This option also provides a single point of failure. There are several agencies that lead law enforcement efforts against a particular threat, however, one of the best known is the Drug Enforcement Administration (DEA), which was created in 1973 to combat the illegal drug trade.[23]

Each of these three options will be compared in terms of commitment and collaboration levels. Regarding overall commitment, the willingness of an agency to provide funding for equipment, personnel, physical space, and training will be assessed. Collaboration, on the other hand, will be measured by an agency's willingness to join forces, cooperating with one another to achieve unified goals, as well as sharing in the

22 "Violent Gang Task Forces," What We Investigate, accessed May 6, 2022, https://www.fbi.gov/investigate/violent-crime/gangs/violent-gang-task-forces.

23 "Our History," Drug Enforcement Administration, accessed May 6, 2022, https://www.dea.gov/about/history.

accountability for potential success, and failure. With these two metrics identified, the highest rated option should necessarily be the one with both the highest level of commitment and the highest level of collaborative effort. To help quantify what can truly only be labeled as qualitative metrics, the following graph in Figure 2 has been created to provide a visual reference. Once the necessary research has been conducted, each option will be assigned a number corresponding to the level of commitment and collaboration necessary for the United States to most effectively consolidate inter-agency resources to combat the threat from UAS platforms. The higher the number for each, the more effective the option will be when both metrics are combined.

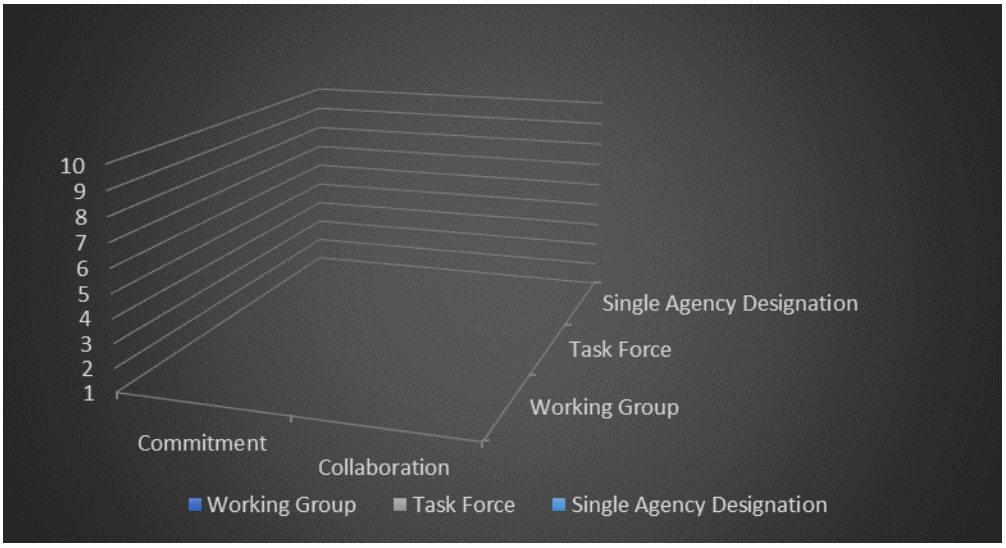


Figure 2. Federal UAS Threat Response Options

## J. CONCLUSION

This chapter defined the problem, reviewed the currently available literature, and defined the research parameters. The following five chapters will now showcase the research and analysis necessary to properly understand the overall problem, identify potential solutions, and ultimately determine the best path forward for the United States government. Specifically, chapter two will identify the UAS threat picture, providing threat modalities as well as specific threat geography. Chapter three will then provide an overview of the current C-UAS efforts within the military, civilian, and foreign sectors.

Chapter four analyzes C-UAS technology, legal authority, and the UAS Kill Chain, along with any associated challenges. Chapter five details the introduction of three inter-agency consolidation options: working group, task force, and designated agency. Chapter six summarizes the research by providing the requisite conclusions, recommendations, and opportunities for future research.

# II. UAS THREAT PICTURE

## A. THREAT MODALITIES

Before any intimation of response can be conceptualized, the overall threat environment must be identified and understood to the greatest extent possible. This comprehensive awareness will then provide the foundation upon which strategy can be most effectively crafted. Between commercial-off-the-shelf (COTS) and do-it-yourself (DIY) UAS platforms, a criminal or terrorist has nearly endless options at his or her disposal. The following are just a few drone characteristics that might be considered: quadcopters versus fixed wing, battery versus fuel, autonomous capability, speeds well in excess of one hundred miles an hour, ranges that can easily move into multiple hours, and substantial lift capacity. Taking these performance attributes together within what realistically amounts to a nearly unrestrained airspace, and it becomes increasingly clear as to why UAS platforms possess so much potential for lethality.

Beyond the considerable functionality of the UAS platform itself, the various types of attachments and payloads must also be considered. Depending upon the attack requirements, UAS platforms may have sophisticated cameras aboard to conduct surveillance against law enforcement authorities, or even advanced projectile weaponry to conduct mass killings. CBRNE materials can also easily be transported as payload, radically expanding the any potential kill radius. The drone itself could be utilized as a weapon similar to the kamikaze planes piloted by the Japanese during World War Two.

The actual environment itself is a large component requiring interpretation. What happens in one area of the world does not necessarily mean it occurs everywhere else. There is a certain line of thinking within government circles that tends to believe what happens overseas may eventually make its way to the United States. In other words, attacks on foreign soil may preview what is coming to America.

The last piece of the puzzle has to do with challenges currently faced within the overall UAS threat picture. Specifically, those challenges encountered while attempting to respond effectively, which include technology, legality, and lack of strategic focus.

## B. CBRNE PAYLOAD TYPES

Weapons of mass destruction modalities center upon five general areas: chemical, biological, radiological, nuclear, and explosives. Each one has the potential for incredible lethality and, save the nuclear option, is relatively easy to deploy aboard UAS platforms. The following sections break down each area in relation to the drone environment.

### 1. Chemical

Chemical weapons have been used throughout history, but the first large scale attack occurred in 1915 during World War One. Chlorine, Mustard, and other chemical agents killed over 90,000 people by war's end.[24] Fast forward over a hundred years and, despite long-standing international agreements prohibiting their use, chemical weapons are still being used in places like Syria.[25]

With the introduction of UAS platforms, chemical weapons now possess a superior means of transport and deployment. Drones improve chemical weapons dispersal, which previously experienced reduced reliability with other forms of deployment, such as crop dusters, particularly when forced to take into consideration certain weather conditions and foliage. This is because, unlike those crop dusters that rely upon indiscriminate, blanket coverage, UAS platforms have available sensor technology to minimize waste and improve targeting focus.[26] Chemical weapons and drone technology is the marriage made in hell, so to speak, as their relationship significantly increases overall lethality.

There are current reports circulating about the possibility that the Russians have begun using chemical weapons against the Ukrainians. One report, authored by Poppy Wood, alleges the Russians recently used a drone to deploy chemical weapons against

---

[24] "History: Looking Back Helps Us Look Forward," About Us: We Want to Live in a World Free of Chemical Weapons, accessed February 14, 2022, https://www.opcw.org/about/history.

[25] Hollis Rammer, "OPCW Confirms Chemical Weapons Use in Syria," *Arms Control TODAY*, August 2021, https://www.armscontrol.org/act/2021-07/news-briefs/opcw-confirms-chemical-weapons-use-syria.

[26] Zackary Kallenborn and Philipp Bleek, "Drones of Mass Destruction: Drone Swarms and the Future of Nuclear, Chemical, and Biological Weapons," War on the Rocks, February 14, 2019, https://warontherocks.com/2019/02/drones-of-mass-destruction-drone-swarms-and-the-future-of-nuclear-chemical-and-biological-weapons/.

Ukrainian fighters in the city of Mariupol.[27] Ground forces reported symptoms included sore eyes and nausea which, although far from conclusive, is consistent with health effects of certain chemical weapons. Despite chemical weapons being considerably cheaper and, ultimately, less effective than some other WMD threats such as nuclear weapons, their deployment nonetheless is likely to create mass disruption amongst the targeted populace.[28]

### 2. Biological

Biological weapons have a long history of illicit use dating as far back as 1347, when Mongols used dead bodies afflicted with plague to initiate what became a nearly five year long pandemic that killed approximately 33 percent of Europe's population.[29] Biological and chemical weapons tend to possess similar methods of deployment, with one such technique being particularly popular with biological toxins, is in the form of an aerosol.[30] Da-Jiang Innovations, or DJI as they are more commonly known, is the world's leading manufacturer of commercial and hobbyist drones. Their AGRA line of agricultural drones can easily spray large swaths of land with several types of farming specific products such as pesticides and fertilizers.[31] What makes these types of drones so beneficial to the farming industry also makes them a fantastic transport and deployment platform for ricin and anthrax. The cameras and obstacle avoidance software, which are currently available, greatly enhance this type of discriminate dispersal performance by improving targeting and retaining potency while also reducing the risk of airborne dilution.

---

[27] Poppy Wood, "UK Intelligence Examining Reports of Russia Chemical Attack in Ukraine Will Be Scouring Flight Paths for Drone," iNews, April 12, 2022, https://inews.co.uk/news/world/western-intelligence-drones-alleged-chemical-weapons-attack-1571749.

[28] "Biological, Chemical, & Other Non-Nuclear Threats," Federation of American Scientists, accessed May 7, 2022, https://fas.org/issues/biological-chemical-and-other-non-nuclear-threats/.

[29] *Britannica*, s.v. "biological weapon," November 27, 2017, https://www.britannica.com/technology/biological-weapon

[30] *Britannica, "Biological* weapon."

[31] DJI Enterprise, "The Use of Drones in Agriculture Today," *DJI Enterprise* (blog), September 18, 2021, https://enterprise-insights.dji.com/blog/drones-in-agriculture.

### 3. Radiological

In the Spring of 2015, a Japanese national flew a small, quadcopter UAS carrying soil laced with small amounts of a radioactive substance onto the roof of the Japanese Prime Minister's private residence.[32] That substance was Cesium-137, which is a radioactive by-product of fission within nuclear reactors.[33] The perpetrator's intent was to protest the Prime Minister's decision to restart two nuclear reactors less than five years after the Fukushima disaster.[34]

The acquisition of Cesium-137 is not quite as difficult as one might think since it has several commercial uses in medicine, industrial gauges, and measurement devices.[35] Just over two years ago, the *Los Angeles Times* wrote an article detailing the potential for terrorists to weaponize enough Cesium-137 from just one common medical device to contaminate up to ten square miles of a large city. The device is called an irradiator and is used by medical professionals to sterilize blood and tissue. Each one contains roughly double the amount of radioactive substance necessary to infect the urban grid area just mentioned.[36] Given the potential levels of radioactivity and heat given off, UAS platforms are an excellent way to minimize the criminal or terrorist's exposure. This type of scenario can easily be taken several steps further by simultaneously deploying several drones throughout a large city, each strafing well populated streets with a legally purchased drop mechanism containing lethal amounts of stolen Cesium-137.

### 4. Nuclear

Even within military applications, the combination of UAS and nuclear payloads is highly unlikely, however, it is not without precedence. The concept of unmanned aircraft

---

[32] Will Ripley, "Drone with Radioactive Material Found on Japanese Prime Minister's Roof," CNN, April 22, 2015, https://www.cnn.com/2015/04/22/asia/japan-prime-minister-rooftop-drone/index.html.

[33] "Radionuclide Basics: Cesium-137," Radiation Protection, July 5, 2022, https://www.epa.gov/radiation/radionuclide-basics-cesium-137.

[34] Ripley, "Drone with Radioactive Material Found on Japanese Prime Minister's Roof."

[35] Environmental Protection Agency, "Radionuclide Basics."

[36] David Willman and Melody Petersen, "Terrorists Could Make a Dirty Bomb from This Common Medical Device," *Los Angeles Times*, December 27, 2019, https://www.latimes.com/politics/story/2019-12-27/cesium-137-dirty-bomb.

with nuclear payloads actually dates back to 1962, when the U.S. Navy was searching for solutions to address the Soviet Union's proliferation of nuclear submarines. Enter the Gyrodyne QH-50 D.A.S.H. (Drone Anti-Submarine Helicopter), which became famous as the first autonomous aircraft to enter military service. For anti-submarine duties, the QH-50 could be deployed with either conventional torpedoes or a nuclear depth bomb aboard.[37] The specific nuclear equipped payload was called the Mk-57, a relatively light-weight tactical nuclear bomb weighing approximately 500 pounds.[38]

Although there is no currently known use of a nuclear equipped drone, there are other aspects of this relationship worth exploring. For instance, on July 3, 2018, the environmental group, Greenpeace, piloted a drone dressed as the comic book hero, Superman, into the wall of the spent fuel storage pool at the Bugey Nuclear Plant near Lyon, France. Greenpeace asserted their action was intended to expose the security vulnerabilities of nuclear power plants, particularly given that they were constructed in the seventies without accounting for new threats.[39]

### 5. Explosive

There is no shortage of examples for explosive payloads being deployed from UAS platforms. By 2017, fifteen different terrorist groups had produced videos using explosive laden drones.[40] In fact, even back in 2016, the SOCOM Commander at the time labeled terrorist operated, small UAS platforms as the most complex threat to address on the battlefield for his soldiers.[41] One only need look at the daily news emanating from the

---

[37] Rebecca Maksel, "D.A.S.H. Goes to War," *Air & Space Magazine*, March 2012, https://www.smithsonianmag.com/air-space-magazine/dash-goes-to-war-23369442/.

[38] "Chart of Strategic Nuclear Bombs," Nuclear Weapons in the Strategic Air Command Arsenal, accessed February 17, 2022, http://www.strategic-air-command.com/weapons/nuclear_bomb_chart.htm.

[39] Jack Loughran, "Greenpeace Crashes Superman Drone into French Nuclear Power Plant," *E&T*, July 4, 2018, https://eandt.theiet.org/content/articles/2018/07/greenpeace-crashes-superman-drone-into-french-nuclear-power-plant/.

[40] "Drones and the IED Threat," Reliefweb, July 26, 2017, https://reliefweb.int/report/world/drones-and-ied-threat.

[41] David Larter, "SOCOM Commander: Armed ISIS Drones Were 2016's 'Most Daunting Problem," Defense News, May 16, 2017, https://www.defensenews.com/digital-show-dailies/sofic/2017/05/16/socom-commander-armed-isis-drones-were-2016s-most-daunting-problem/.

Middle East to understand this threat continues to proliferate, despite advances in C-UAS equipment. Saudi Arabia, Yemen, Iraq, UAE, and now the Ukraine are but a few of the countries dealing with explosive laden drones on a recurring basis. These attacks are no longer confined to the Middle East either.

India is now beginning to experience their own drone attacks, with one well-publicized event that took place on June 27, 2021. Two drones dropped explosives into the Indian Air Force Base at Jammu, injuring several service members and causing property damage.[42] The article asserted that no drone components were identified following the attack, which suggests the payload was dropped and the UAS was able to fly away, showcasing a textbook example of why these platforms are so effective.

Mexico, a close southern neighbor to the United States, is seeing an enormous uptick in the number of violent incidents involving drones. Cartels are combining this form of emerging technology with tactical precision to attack civilian and government rivals with increasingly effective results. Cartel use of drones is a natural progression from contraband transport across borders and reconnaissance that began over a decade ago.[43]

On July 7, 2021, the Haitian President, Jovenel Moïse, was assassinated at his residence by gunfire, however, the attackers also dropped grenades from drones overhead in an apparent attempt to ensure the job was finished.[44] One final example that occurred within the United States involved a man named Jason Muzzicato, who was arrested and

---

[42] Ramachandran, Sudha, "Drone Attacks on Military Installation Rattle India's Security Establishment," *The Diplomat*, June 30, 2021, https://thediplomat.com/2021/06/drone-attacks-on-military-installation-rattle-indias-security-establishment/.

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

[44] Jacqueline Charles and Jay Weaver, "Grenade-Dropping Drones, a Paranoid President, Guards Who Ran: Latest on Haiti Assassination," *Miami Herald*, September 19, 2021, https://www.miamiherald.com/news/nation-world/world/americas/article254275213.html.

eventually convicted for, amongst other things, utilizing a UAS platform to drop explosive devices onto property owned by his former girlfriend.[45]

## C. KAMIKAZE DRONES

Rather than using a drop mechanism or agricultural spray drone to release lethal payloads and escape, the relatively low cost of commercial-off-the-shelf (COTS) UAS platforms makes the fire and forget option potentially more viable. The University of Alabama in Huntsville (UAH) led an eighteen-month long study to understand the injury effects of a drone colliding with a human being. UAH found that the great variability in platform size, performance, and bodily impact areas complicated definitive injury risk assessment.[46]

Attaching an explosive device to the drone that explodes upon impact is another story altogether. What makes this scenario so unique is the platform's ability to loiter from above for significant periods, waiting for the perfect second to attack with incredible accuracy. This Precision can be significantly enhanced via new technology such as facial recognition, allowing a single individual to be targeted rather than an entire crowd.[47]

## D. WEAPONIZATION

The weaponization of UAS platforms presents one of the most lethal threats to homeland security. Foreign nations have already built and deployed this type of drone, with Turkey being just one of many examples. Their Songar drone is armed with a 5.56mm rifle capable of firing up to 200 rounds as either single, 15 round burst, or fully automatic.

---

45 "Northampton County Man Sentenced to Five Years for Using Drone to Harass Ex-Girlfriend, Illegally Possessing Bombs and Guns," U.S. Attorneys Eastern District of Pennsylvania News, September 24, 2020, https://www.justice.gov/usao-edpa/pr/northampton-county-man-sentenced-five-years-using-drone-harass-ex-girlfriend-illegally.

46 "ASSURE Announces Results of UAH-Led Drone Ground Collision Study," University of Alabama in Huntsville News, August 14, 2019, https://www.uah.edu/news/news/assure-announces-results-of-uah-led-drone-ground-collision-study.

47 Ken Dilanian, "Kamikaze Drones: A New Weapon Brings Power and Peril to the U.S. Military," NBC News, December 6, 2021, https://www.nbcnews.com/news/military/kamikaze-drones-new-weapon-brings-power-peril-u-s-military-n1285415.

Sophisticated camera stabilization technology allows accuracy within 15cm at 200m range. If that is not enough, a grenade launcher can be added to the platform, along with the rifle.[48]

There is no need for this level of sophistication, however, as a University of Connecticut student successfully attached a fully functioning pistol, as well as a flame thrower, to a drone back in 2015.[49] His creations sparked significant interest on YOUTUBE but also got him expelled from the school. There is no shortage of videos with different types of pistols and rifles being fired remotely from a drone via the ground control station.

## E. SURVEILLANCE/RECONNAISSANCE

UAS platforms are an excellent method of mobile surveillance and reconnaissance, as evidenced by their continued deployment with militaries around the world, as far back as the Vietnam War.[50] Today, the abundance of available cameras, sensors, and stabilization software offered make them a comparatively cost-effective solution with minimal disadvantages. Camera options include such things as high definition, live feed video and infrared in day or night conditions. Sensors include light and radio wave detection, as well as heat signature capabilities.[51]

This technological competence makes drone flights over critical infrastructure a serious problem within the United States and abroad. Optional targets for surveillance activities may include certain military bases, chemical plants, nuclear plants, government laboratories, and various components of the transportation sector, particularly commercial airports. Activities like these are so concerning to the Cybersecurity and Infrastructure

---

48 "SONGAR Armed Drone System," Army Technology, September 1, 2020, https://www.army-technology.com/projects/songar-armed-drone-system/.

49 John Moritz, "Former CT College Student behind Viral 'Flying Gun' Video Has Convictions Overturned," CT Insider, November 30, 2021, https://www.ctinsider.com/news/article/Former-CT-college-student-behind-viral-Flying-16662141.php.

50 Kashyap Vyas, "A Brief History of Drones: The Remote Controlled Unmanned Aerial Vehicles (UAVs)," Interesting Engineering, June 29, 2020, https://interestingengineering.com/a-brief-history-of-drones-the-remote-controlled-unmanned-aerial-vehicles-uavs.

51 "Drones/Unmanned Aerial Vehicles," Street Level Surveillance, August 28, 2017, https://www.eff.org/pages/dronesunmanned-aerial-vehicles.

Security Agency (CISA) is keenly aware of the situation and, as such, works directly with these entities to proactively address the threat.[52] In an attempt to defend against this type of criminal activity, Israel's Ben Gurion University is actively conducting research into methods to both identify, and potentially circumvent, efforts to illicitly record a specific location and/or person via drone cameras.[53]

Drones can, and have been, used for corporate espionage as well. UAS platforms can easily bypass any physical security barriers and their potential electronic payloads are then able to bypass cyber security protocols and hack into a private company's database. Major corporations, including Apple and Tesla, have experienced this very thing and there are likely many more who have not been as open about the experience.[54]

## F. SWARMS

The final, and perhaps most daunting, homeland security challenge to be discussed is drone swarms. Take any one of the previously mentioned drone threat types and imagine, if you can, the exponential increase in lethality as they deploy in multiples of five, ten, or even a hundred at one time. The ability to strike multiple targets with such precise synchronization and accuracy, by one nefarious individual, is nearly unparalleled.

A drone swarm is generally controlled in one of three ways: manual, semi-autonomous, or fully autonomous. In terms of a manually controlled drone swarm, one example might have multiple operators independently controlling single drones but operating in coordination with each other to achieve their objective(s). A semi-autonomous drone swarm, on the other hand, could be controlled by one operator in two different ways. The first occurs when a single operator utilizes a control algorithm to operate multiple drones. With this method, the drones may or may not communicate with each other. The

---

[52] "Unmanned Aircraft Systems (UAS) - Critical Infrastructure," Cybersecurity and Infrastructure Security Agency, accessed February 21, 2022, https://www.cisa.gov/uas-critical-infrastructure.

[53] "First Technique to Detect Illicit Drone Video Filming Demonstrated by BGU and Weizmann Institute Researchers," Ben Gurion University of the Negev, January 14, 2018, https://in.bgu.ac.il/en/pages/news/Game-of-Drones.aspx.

[54] Claire Scott, "Corporate Espionage by Drone: Why Corporations Need Better Physical and Legal Protections" (University, MS: University of Mississippi, School of Law, January 24, 2021), https://papers.ssrn.com/abstract=3772434.

second method is a "lead – follow" scenario where an operator controls the lead drone while the other worker/slave drones follow based upon an onboard control algorithm.

A fully autonomous swarm operation, generally considered to be the most advanced of the three, may also occur in one of two different ways. The first involves multiple UAS communicating with each other to operate in coordination, but independent of an operator based upon a centralized control algorithm. The second type allows the swarm drones to operate independent of an operator, and without inter-drone communication, based upon a de-centralized algorithm. This type of algorithm even allows the swarm to continue operations after one or more of the drones are lost. Both versions rely upon advanced onboard obstacle avoidance sensors, working in conjunction with the algorithms.[55]

## G. THREAT GEOGRAPHY

After looking at the examples provided in the previous sections, it is obvious the threat from drones is not confined to any one part of the world. In spite that fact, there are areas that tend to have higher rates of attack than others. Two regions, in particular, seem to have much higher concentrations of drone related attacks.

## H. FOREIGN

The first in within the Middle East where, according to one study, the region has spent approximately $1.5 billion on UAS platforms over the past five years. This assertion does not include Israel, a country that prefers not to share this type of data with potential adversaries, and who is generally considered to be the most advanced nation in the area with this type of technology.[56] This regional proliferation appears to be increasing along

[55] Anam Tahir et al., "Swarms of Unmanned Aerial Vehicles — A Survey," *Journal of Industrial Information Integration* 16 (December 1, 2019): 1–7, https://doi.org/10.1016/j.jii.2019.100106.

[56] Cathrin Schaer and Kersten Knipp, "Can Drone Warfare in the Middle East Be Controlled?," Deutsche Welle, January 7, 2021, https://www.dw.com/en/can-drone-warfare-in-the-middle-east-be-controlled/a-58111069.

with the advancements in drone technology as well as those who pilot them, whether they be funded directly by other nations, their proxies, or others with less political clout.[57]

The other geographic region experiencing a substantial increase in drone-related attacks is Central America. Having seen their viability as a surveillance/reconnaissance platform, as well as their successful use in the Middle East, Mexican cartels are now beginning to use drones to attack rivals, the military, the police, and even politicians.[58] The escalation thus far has been so intense, the cartel's drone operators have become known as *droneros.*[59]

In 2018, Venezuelan President, Nicolas Maduro, was targeted for assassination by two drones carrying almost five pounds of C-4 explosive. Maduro's administration later accused political opponents of being behind the attack, however, there does not appear to be much in the way of proof as to the veracity of their claim.[60] Maduro is not the only senior foreign politician to come face to face with a drone. In 2013, an unarmed drone, piloted by a protestor, flew within a few feet of German Chancellor Angela Merkel during a political gathering. The fact that it crashed right in front of her before any security personnel responded shows the lack of understanding as to their lethality.[61]

## I. DOMESTIC

Drone incidents within the United States have been somewhat less alarming, however, there are many who justifiably believe that what first occurs overseas tends to

---

[57] Federico Borsari, *The Middle East's Game of Drones: The Race to Lethal UAVs and Its Implications for the Region's Security Landscape* (Milan: Italian Institute for International Political Studies, 2021), https://www.ispionline.it/sites/default/files/pubblicazioni/borsari_analisi_26.01.2021.pdf.

[58] Mark Stevenson, "Mexican Army: Explosive Drone Attacks in at Least 3 States," Media, AP News, April 21, 2021, https://apnews.com/article/latin-america-cb836518d514b68850607a1eca24a7bd.

[59] "Mexican Cartels Now Use IEDs as Well as Bomb-Dropping Drones," Voice of America, February 5, 2022, https://www-voanews-com.cdn.ampproject.org/c/s/www.voanews.com/amp/mexican-cartels-now-use-ieds-as-well-as-bomb-dropping-drones-/6427770.html.

[60] Erin Kelly, "Venezuela Drone Attack: Here's What Happened with Nicolas Maduro," *USA TODAY*, August 6, 2018, https://www.usatoday.com/story/news/politics/2018/08/06/venezuela-drone-attack-nicolas-maduro-assassination-attempt-what-happened/913096002/.

[61] Sean Gallagher, "German Chancellor's Drone 'Attack' Shows the Threat of Weaponized UAVs," Ars Technica, September 18, 2013, https://arstechnica.com/information-technology/2013/09/german-chancellors-drone-attack-shows-the-threat-of-weaponized-uavs/.

eventually make its way into the United States. Domestic drone incidents are still quite varied, ranging from contraband drops into prisons, to crashes with manned aircraft, to hampering firefighting and law enforcement efforts. Dedrone.com listed well over 200 significant drone related incidents within the United States and counting.[62] Although domestically, the United States currently lags behind other countries in drone attack lethality, their ease of acquisition and use, coupled with plenty of overseas examples to draw inspiration from, should only serve to increase their potential for nefarious use.

## J. CONCLUSION

This chapter provides an in-depth look at just how lethal drones can truly be when unleashed by nefarious actors. It begins with an overview of the various threat types a UAS platform could be employed as including, amongst other things, specific payloads, and sensor technology. It ends with threat geography around the world, showcasing examples of UAS attacks in several different countries like Mexico, which is in very close proximity to the United States. Given the potential lethality of this dual-use technology, and verified attack incidents occurring closer and closer to home, the United States must not take this threat lightly or risk being caught off-guard in what could be described as a September 10th mentality.

62 "Map of Worldwide Drone Incidents," Worldwide Drone Incidents, accessed February 21, 2022, https://www.dedrone.com/resources/incidents/all?bd17d29f_page=2.

# III. REVIEW AND ANALYSIS OF CURRENT C-UAS EFFORTS

This chapter analyzes what the United States currently possesses in terms of C-UAS capabilities across the federal government. It begins with how the Department of Defense addresses the drone threat. The second portion looks at the civilian federal government response from the Departments of Energy, Justice, and Homeland Security. The final section diverts from the American response by reviewing the current C-UAS strategy from the United Kingdom. This is not meant to compare national strategies because the United States does not possess a national C-UAS strategy, whereas the British government does.

## A. MILITARY/UNIFORMED SERVICE EFFORTS

DOD is the fourth department authorized to conduct C-UAS activities inside the United States. Within the overall military apparatus, the designated lead for small UAS platform counter activities is the Joint Counter-small Unmanned Aircraft Systems Office (JCO), which was established in early 2020. The JCO is led by a two-star general with the mission to establish policy, identify obligations, assemble resources, and develop preparedness as part of a multi-service, consolidation of C-UAS military strategy. This strategy will address drone threats at home and abroad, working with military and civilian UAS stakeholders.[63]

Although the current C-UAS strategy employed by the United States military, as shown in Figure 3, has been discussed briefly within the Literature Review, it is important to analyze it further. As such, the three main goals, or Lines of Effort, as the Army describes them, will be broken down individually to ensure clarity. Those three parts are as follows: 1) Ready the Force; 2) Defend the Force; and 3) Build the Team.[64]

---

63 "Joint Counter-Small Unmanned Aircraft Systems Office," STAND-TO!, August 27, 2021, https://www.army.mil/standto/archive/2021/08/27/.

64 Department of Defense, *Counter-Small Unmanned Aircraft Systems Strategy* (Washington, DC: Department of Defense, 2021), 11, https://media.defense.gov/2021/Jan/07/2002561080/-1/-1/1/department-of-defense-counter-small-unmanned-aircraft-systems-strategy.PDF.

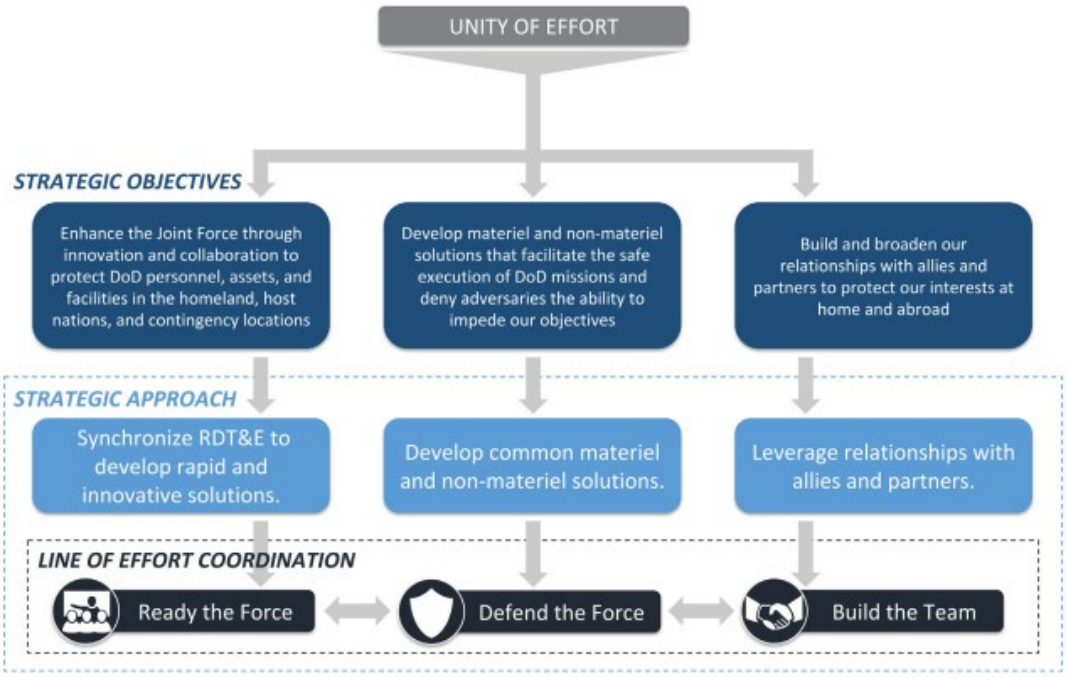


Figure 3. Current Department of Defense C-UAS Strategy.[65]

## B. READY THE FORCE

There are four main components within this specific Line of Effort. In general terms, a Line of Effort is military jargon for smaller, achievable milestones that showcase forward movement within an overarching operational strategy.[66] The first is to develop threat assessments that provide a more thorough UAS threat picture, allowing for the identification of requirements. The second is to coordinate and speed up the progress of C-UAS technology. The third is to synchronize C-UAS equipment and software architecture amongst a wide variety of situations. The fourth is to create a shared C-UAS Test and Evaluation procedures and principles.[67]

---

[65] Source: Department of Defense, 11.

[66] Joint Chiefs of Staff, *Joint Planning*, JP 5-0 (Washington, DC: Joint Chiefs of Staff, 2020), GL-11, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp5_0.pdf.

[67] Department of Defense, *Counter-Small Unmanned Aircraft Systems Strategy,* 10–11.

### 1. UAS Threat Picture Identification

This component ensures coordination within DOD's specific intelligence apparatus, as well as with the overall intelligence community to provide a more cohesive understanding of the total threat picture. This will allow senior commanders to identify current risks while also preparing for any emerging threats. Continuously improving pre-emptive and reactionary response capacity by intelligence personnel is vital to battlefield success.[68]

### 2. C-UAS Technology Progression

With the UAS threat picture identified, the DOD will use it to manage the risk from drone threats. This will include the development of robust C-UAS capabilities wherever the American military is deployed. This capability advancement will incorporate subject matter expertise from all branches of the department.[69]

### 3. C-UAS Technology Synchronization

C-UAS systems much be adaptable to different environments and conditions. They must also possess the capacity for true integration with each other to ensure the most effective response is available to commanders. Integration, however, must encompass more than just the hardware aspects of reactionary intent. Shared requirements will also increase the DOD's ability to remain nimble in the face of a rapidly evolving threat.[70]

### 4. C-UAS Test and Evaluation Criteria

Between the UAS threat picture identification and the subject matter expertise within DOD, service branches will work together to address UAS threats wherever and whenever the need arises. Formalized analytical criteria will be utilized to ensure

[68] Department of Defense, 12.

[69] Department of Defense, 13.

[70] Department of Defense, 13.

deployment commonality amongst all services. This will be accompanied by functional testing to validate operational competence.[71]

## C. DEFEND THE FORCE

Defend the Force is comprised of three main components. The first is to provide shared C-UAS competencies across all branches of service. The second is to create functional models and policy to increase the military's advantage against rivals. The third is to create training principles, improve current curriculum, and ensure the shared training objectives satisfy individual service requirements.[72]

### 1. Shared C-UAS competencies

Combining individual needs from each service branch into one common requirement set will distribute costs more effectively amongst stakeholders. Collaborative efforts will take advantage of both aggressive and protective capabilities by creating a coordinated set of standard operating procedures. These can then be applied across all operational environments, providing the United States an opportunity to benefit significantly against its adversaries.[73]

### 2. Functional Policy to Increase Advantage

These policies will address everything from humanitarian efforts through full-scale war, and everything in between. They should also provide the potential for inclusive, multi-service efforts in suitable situations, highlighting the importance of shared territorial efforts. Policy guidance should effectively categorize options to either stop or diminish threats.[74]

---

[71] Department of Defense, 13.

[72] Department of Defense, 14.

[73] Department of Defense, 14.

[74] Department of Defense, 14–15.

### 3. Improve Training

Training must become focused upon collaborative efforts, replacing individual needs and requirements that reduced collective capabilities. Additionally, current training must be enhanced and expanded to meet emerging threats and technologies associated with UAS platforms. Despite the need for effective collaboration, training must still address individual challenges within each environment and service branch area of responsibility.[75]

## D. BUILD THE TEAM

Build the Team is also comprised of three main components. The first is to collaborate with other federal entities as well as civilian groups to accelerate shared C-UAS capabilities against the drone threat. The second is to enhance liaison opportunities with foreign partners to ensure a more effective response overseas. The third is to liaise with federal law enforcement to unify efforts within the United States.[76]

### 1. Collaborate to Improve

DOD intends to establish new and/or improved partnerships within their department, as well as amongst external stakeholders inside the greater National Security apparatus. This endeavor will necessarily include alliances with cleared defense contractors as part of a concerted effort to improve production as C-UAS technology progresses. In doing so, DOD, along with its partners, will be well postured to address a wide breadth of UAS threats inside the United States and abroad.[77]

### 2. Liaise with Foreign Partners

This internal liaison must extend to foreign partners as well since they will likely experience similar threats from UAS platforms. The creation and disclosure of strategies that benefit both the United States and its allies will only increase DOD's ability to protect its substantial overseas assets. In addition to the sharing of policy considerations, the DOD

---

[75] Department of Defense, 15.

[76] Department of Defense, 16.

[77] Department of Defense, 16.

will expedite opportunities to provide allied countries with the industrial results of American research on C-UAS technology.[78]

### 3. Synchronize with Domestic Partners

Finally, DOD intends to marry up its C-UAS efforts with American law enforcement entities to bolster intelligence collection and analysis, as well as the resulting potential for prosecution of nefarious individuals, particularly those who operate drones in and around shared DOD-civilian boundaries. This proactive approach will greatly reduce the potential to be caught off guard, regardless of what side of the fence the incident occurs on. As with other partners, collaboration will also entail the sharing of what is sure to be substantial costs in terms of research and development of C-UAS capability.[79]

## E. SUMMARY

Out of the ten specifically mentioned components of the DOD C-UAS strategy, only one specifically addresses anything resembling either *left or right of boom*. The identification of the overall UAS threat picture, discussed at the very beginning of this chapter, is the singular component with any ancillary connection to the UAS Kill Chain. By creating an accurate representation of the UAS threat picture, it necessarily includes current intelligence already accumulated as well as compelling new data collection. Although by no means sufficient in its own right, the latter may present additional opportunities to spot potential informants and detect the actual perpetrator(s). This is specifically where DOD's C-UAS strategy has potential application to the UAS Kill Chain. Intelligence analysis, current informant debriefing, prospective source recognition, and investigative operations all provide *left of boom* opportunities to uncover and potentially disrupt UAS-based attacks before they occur.

[78] Department of Defense, 17.

[79] Department of Defense, 17.

## F. CIVILIAN C-UAS STRATEGY

For C-UAS activities within the United States civilian government, authority has been divided amongst three departments: DOJ, DHS, and DOE. DOJ and DHS both receive their authority from the same congressional authority, that being 6 U.S.C. § 124n (Protection of certain facilities and assets from unmanned aircraft).[80] DOE, like DOD, receives its own authority and, as such, will be discussed first.

### 1. Department of Energy

DOE receives its authority from 50 U.S.C. § 2661 (Protection of certain nuclear facilities and assets from unmanned aircraft). Although similar to 124n, 2661 specifically provides the Secretary of Energy with legal authority deploy C-UAS resources to protect DOE assets within the United States and its territories.[81] The available literature regarding C-UAS strategy for DOE is much less robust than the other three departments. For instance, the *C-UAS Implementation Storyline* explicitly details their plan of action to implement a C-UAS program including 65 steps within seven individual sections.[82] Rather than an overarching mitigation strategy, it appears to be a how-to guide for addressing the attack step only versus an overarching strategy that confronts any other aspects of the UAS Kill Chain model. This limits DOE's ability to identify and respond to UAS threats.

### 2. Department of Justice

DOJ released three different administrative pieces of policy regarding anything UAS related. The first one is titled, "Department of Justice Policy on the Use of Unmanned Aircraft Systems" (9-95.100). This details the use of UAS platforms by agencies comprising the DOJ, to include amongst other things compliance, scope, and training. It does not, however, contain anything whatsoever about C-UAS operations.

---

[80] Protection of Certain Facilities and Assets from Unmanned Aircraft, *U.S. Code* 6 (2018) §§ 124n, https://www.law.cornell.edu/uscode/text/6/124n.

[81] Protection of Certain Nuclear Facilities and Assets from Unmanned Aircraft, *U.S. Code* 50 (2012) §§ 2661, https://www.law.cornell.edu/uscode/text/50/2661.

[82] Julian James Atencio and Carolynn P. Scherer, *Counter Unmanned Aircraft System (CUAS) Implementation Storyline*, LA-UR-20-25040 (Los Alamos, NM: Los Alamos National Laboratory, 2020), https://doi.org/10.2172/1638609.

The second, "Preventing Threats Act of 2018" (9-95.200), summarizes the Congressional authority for DOJ (and DHS) to conduct C-UAS operations. It does not provide any information indicative of an overarching implementation strategy. It is slated to sunset later in 2022 and, as such, will require reauthorization, an alternative, or be allowed to die on the vine, so to speak.

The third, "Technology to Detect and Mitigate Unmanned Aircraft Systems" (9-95.300), provides additional guidance to those public and private sector entities regarding C-UAS criminal and regulatory provisions.[83] More than anything, this policy piece essentially attempts to clarify the legal language contained within the Preventing Emerging Threats of 2018. What it really does is let those who were not granted C-UAS authority understand just how much trouble they face by engaging in C-UAS activities on their own.

After review of all three, it is evident that the DOJ does not currently have, or does not publicly acknowledge, an enterprise-wide, holistic C-UAS strategy. This realization puts them in the same substandard situation as the much smaller DOE, and squarely behind DOD's more enviable determination to fully address the UAS threat. Given the significance of DOJ's C-UAS authorities, which one could argue encompasses significantly more of the homeland security mission than DOE, the lack of a comprehensive mitigation strategy to action the aforementioned 124n policy is unacceptable.

### 3. Department of Homeland Security

DHS provides their current C-UAS methodology on page 13 of the Counter Unmanned Aircraft Systems Technology Guide.[84] Referred to as their C-UAS Processing Chain, DHS moves along a four-piece structure as follows: 1) Detect; 2) Locate/Track; 3) Classify/Identify; and 4) Mitigate. Although this may loosely resemble the UAS Kill Chain, it is only set up to address one of those six steps.

---

[83] "9-95.000 – Unmanned Aircraft Systems (UAS)," Justice Manual, November 26, 2019, https://www.justice.gov/jm/9-95000-unmanned-aircraft-systems-uas.

[84] Patel and Rizer, *Counter-Unmanned Aircraft Systems Technology Guide*.

The DHS Processing Chain only addresses the attack step with the overall UAS Kill Chain. This means the four steps representing *left of boom* as well as the sixth step signifying *right of boom* are completely ignored. While this plan is absolutely appropriate to deal with the actual attack itself, it makes two noteworthy assumptions. The most significant one is that this course of action assumes there are C-UAS assets on site and prepared to respond. Given the severely limited C-UAS authority, assets, and operators available, this assumption is untenable.

A second assumption is that technology is going to save the day, so to speak. Although providing a suite of C-UAS technologies has the best potential to mitigate the attack once it has commenced, it is not fool-proof. As technology advances on both sides, there will be counters to the counter, and so on. Given this reality, it would be wise to consider whatever prevention potential there is before the drone takes flight, i.e., *left of boom*.

## G. SUMMARY

After review of the three civilian departments authorized to conduct C-UAS operations, it is apparent they lack a cohesive, comprehensive strategy to address hostile drone activity. This is complete opposition to what the DOD has instituted. Despite having similar Congressional authority to the U.S. military, DOE, DOJ, and DHS prefer to focus singularly upon the immediate threat, meaning the attack itself. This is an interesting perspective to take considering the increased potential for collateral damage, particularly within the urban CONUS environments DOJ and DHS are likely to find themselves operating within.

## H. FOREIGN C-UAS STRATEGY

To provide some strategy comparison between the United States and a foreign government, the United Kingdom was chosen. As a critical partner to American law enforcement interests, the British no doubt understand the threat capabilities of UAS platforms. Ample evidence of this can be found within their Counter Unmanned Aircraft Strategy, which was crafted by the United Kingdom's Home Office as a vital homeland security component of official government policy. What is particularly striking about this

strategy is the praise-worthy, proactive intent to provide a unified purpose for both government and industry, thus facilitating an environment of collaboration, productiveness, and a suitable return on investment.[85]

The C-UAS strategy crafted by the United Kingdom is broken down into four main components: 1) Acquire a comprehensive UAS threat picture; 2) Initiate a holistic response approach to address illegal drone use; 3) Cultivate effective liaison with the commercial sector to improve quality; and 4) enable law enforcement and others to respond effectively with the proper gear, legal authority, education, and oversight. Each of these components will be discussed individually, and at length, throughout the remainder of this section.[86]

### 1. UAS Threat Picture Acquisition

It is quite difficult to properly prepare for, and effectively respond to, a threat you cannot first adequately define. Therefore, to accomplish this objective, the United Kingdom chose to prioritize UAS threats by actor and/or target by harnessing the expertise of individual elements across the entire internal government apparatus, as well as the valued external nation-state partners who face similar problems. These efforts include proactive intelligence analysis and investigative operations to identify unaddressed gaps within the overall threat picture. When appropriate, the government will approach and partner with academic and commercial entities to increase subject matter expertise regarding the increased capability of terrorists and criminals to manipulate commercial-off-the-shelf (COTS) UAS platforms. Continuous and effective engagement with public and private sector organizations to educate and increase awareness of potential security threats posed by drones will act as a force multiplier to bolster government and industry security needs.[87]

---

[85] Secretary of State for the Home Department, "UK Counter-Unmanned Aircraft Strategy," Home Office, October 21, 2019, https://www.gov.uk/government/publications/uk-counter-unmanned-aircraft-strategy.

[86] Secretary of State for the Home Department, 5.

[87] Secretary of State for the Home Department, 9–13.

### 2. National Mitigation Strategy

What may indeed be the most important aspect of how the United Kingdom addresses the UAS threat is the importance its government places upon the need for a national C-UAS mitigation strategy, something the United States has, thus far, failed to implement. Given the myriad drone target vulnerabilities present within the United Kingdom at any one time, and the finite C-UAS resources currently available, the British Government accurately chose to develop and implement what they described as a "Full Spectrum" approach to mitigating UAS threats. This includes multiple layers of proactive risk management ranging from intelligence collection and analysis to law enforcement investigations synchronized with community service announcements, increased public alertness, and improved C-UAS capabilities.[88]

Taking this direction allows multiple facets of public and private sector entities to present a united front against those intent upon harming the United Kingdom and its interests by appropriately applying individual talents and resources to satisfy operational gaps. An all-encompassing strategy such as this means the United Kingdom is indeed looking left and right of boom, or more to the point, well beyond just the actual physical phase of the attack itself. This is a reasonable and mature position to take relative to emerging threats like UAS platforms because their inherent complexity makes effective response very difficult for a single agency to undertake.

### 3. Drone Industry Partnership

The United Kingdom works in partnership with the C-UAS commercial manufacturers to make sure they understand the government's needs. This mutually beneficial relationship includes research/development/testing/evaluation (RDTE), official endorsements, standard operating procedures, an awareness of the dynamic legal environment and nature, as well as the eventual integration of this specialized technology into the national economy.[89] The government's transparency is intended to at least

[88] Secretary of State for the Home Department, 15–17.

[89] Secretary of State for the Home Department, 19–22.

minimize, if not prevent, wasted time, effort, and money for both them and their private industry associates.

### 4. Effective Response

To satisfy this last component, the United Kingdom will increase the quantity and quality of C-UAS operators charged with an effective response proficiency. This includes the latest C-UAS equipment and software, a measured increase in UAS specific law enforcement authorities, a variety of physical security improvements, a nationalized drone response capability, and the potential for non-government entities to legally deploy C-UAS resources. That last piece would likely be exemplified in specific situations such as private ownership of critical infrastructure and large, open-air entertainment venues. All by itself, this unique aspect is worthy of considerable reflection as it is something that truly sets the United Kingdom apart from its peers.

Beyond what has already been stated, one final, but no less important, aspect of this specific component is the deliberate intention to stream-line authority to deploy C-UAS equipment, an action that will greatly improve response effectiveness.[90] Bureaucratic red tape in the form of an excessively long line of signature approvals would unnecessarily hamper efforts, exacerbating an already uncertain situation with no real margin for error. This is yet another unique characteristic of how the United Kingdom's government intends to address the UAS threat, and something the United States has failed to consider.

## I. CONCLUSION

This chapters provides an overview of current C-UAS efforts by both the United States military and civilian federal law enforcement. Additionally, this chapter ends with a single example of how a foreign strategic partner, the United Kingdom, deals with threats from UAS platforms within their borders. Moving forward, chapter four will consider the technical, legal, and UAS Kill Chain challenges that currently affect response efforts.

[90] Secretary of State for the Home Department, 23–25.

# IV. CURRENT CHALLENGES

UAS platform lethality is only half of the homeland security challenge, with the other half being the appropriate government response. Regarding the former, there is realistically very little ability to holistically stop, or even minimize, the performance characteristics of drones or their lethal payloads. Drones are a true, dual-use technology and, as such, the positive benefits they eventually provide will only fuel societal interest in advancing their capabilities, thus, outweighing any caution regarding their potential for nefarious use.

The latter, on the other hand, is both legitimate and reasonable. Defining and implementing an appropriate government response, however, is not without several noteworthy challenges. This chapter dives into three of those challenges currently faced by the United States as it seeks to organize its response strategy. The first deals with the technological capabilities and limitations of operational C-UAS equipment. The second directly confronts the current legal authorities for C-UAS operations, with specificity toward DOJ and DHS, due to the co-mingled and wide-ranging nature of their authorities. The third, and final, challenge is centered upon the UAS Kill Chain as the basis for holistic mitigation.

## A. TECHNICAL CONSIDERATIONS

The first challenge to be discussed has to do with the Counter-Unmanned Aircraft Systems (C-UAS) equipment and software employed as part of that government response. Although it will be discussed further within the next section, it is relevant to understand the significant legal limitations regarding its use. To be more specific, there are only four federal departments with current congressional authority to deploy counter-unmanned aircraft systems (C-UAS) equipment: the Department of Justice (DOJ), the Department of Homeland Security (DHS), the Department of Defense (DOD), and the Department of Energy (DOE), all of which share similar authorities within the United States.

Also comparable between the four is their immediate response strategy, which is generally divided into two distinct phases of operation, that being the initial *detect/track*

and subsequent *mitigation*. For example, the Department of Homeland Security's C-UAS response strategy is shown in Figure 4.[91] The other three departments incorporate similar response strategies.


Figure 4. Department of Homeland Security C-UAS Response Strategy.[92]

The four most common C-UAS *detect/track* sensors are 1) Radio Frequency (RF); 2) Radar; 3) Electro-Optical/ Infrared cameras (EO/IR); and 4) Acoustic. These sensors may provide the C-UAS operator with the potential ability to determine UAS presence, location, classification, and identification, subject to individual equipment capabilities and legal authorities.[93]

For mitigation, which is the direct interdiction of a UAS to neutralize its threat potential, there are two types of techniques that may be employed: 1) kinetic; and 2) non-kinetic. For kinetic means, options include drone-on-drone collisions, projectiles, net/ entanglement systems, laser beams, and high-power microwave pulse. For non-kinetic means, options include RF and GNSS jamming, Spoofing, and Dazzling.[94]

## B. HOW IT WORKS

### 1. Radio Frequency (RF)

RF, as shown in Figure 5, may be a passive sensor that possesses an antenna and a computer to receive and analyze electronic communications between the drone and the ground control stations (GCS). RF can identify certain models and manufacturers, as well

[91] Patel and Rizer, *Counter-Unmanned Aircraft Systems Technology Guide*.

[92] Source: Patel and Rizer, 13.

[93] Patel and Rizer, *Counter-Unmanned Aircraft Systems Technology Guide*.

[94] Patel and Rizer, 22–24.

as locating the signal's transmission origin from either the drone and/or the GCS. This is accomplished by comparing the drone with a UAS radio signature library, which must be updated periodically to remain relevant.[95]

Figure 5. Radio Frequency Model

### 2. Radar

Radars, as shown in Figure 6, are an active sensor because they transmit a specific radio signal out to the drone and subsequently detect the reflected signal. Radars can be 2D (provide direction and distance) or 3D (provide direction, distance, and altitude).[96]

Figure 6. Radar Model

### 3. Electro-Optical/Infrared (EO/IR) Camera

EO/IR digital video cameras, as shown in Figure 7, are passive sensors that collect data within both visible and infrared light spectrums. They can detect RF silent drones as

[95] Patel and Rizer, 18.

[96] Patel and Rizer, 16.

well as identify and classify UAS. EO/IR cameras are often used as a secondary detection option along with primary sensors such as radar or RF.[97]

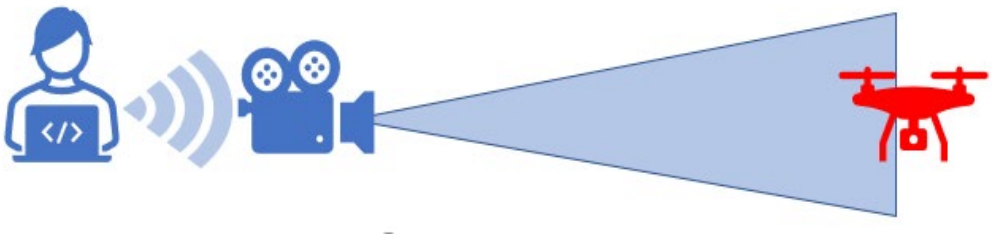

Figure 7. Electro-Optical/Infrared Camera Model

### 4. Acoustic

Figure 8 showcases acoustic sensors, which are passive and utilize extremely sensitive microphones in conjunction with sophisticated audio analysis software to detect, track, and identify drones from the sound of their motors and propellers.[98]

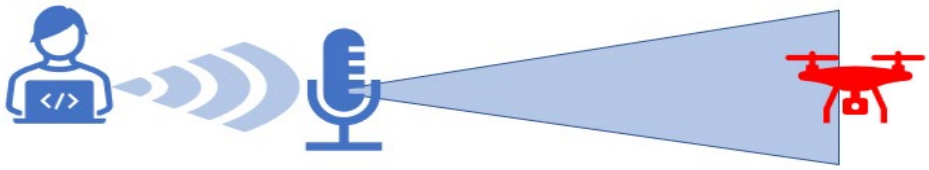

Figure 8. Acoustic Model

### 5. RF/GNSS Jamming

For RF jamming, which is depicted in Figure 9, this means disrupting the communications link between the UAS and the GCS. For GNSS jamming, the satellite link is disrupted, causing the drone to lose its spatial awareness.[99]

[97] Patel and Rizer, 19.

[98] Patel and Rizer, 19.

[99] Patel and Rizer, 23.

Figure 9. Radio Frequency Jamming

### 6. Spoofing:

With spoofing (Figure 10), the C-UAS operator either acts as a man-in-the middle, essentially becoming what the UAS believes is the legitimate GCS or spoofing the GNSS signal to send the UAS off from its intended course.[100]

Figure 10. Spoofing Model

### 7. Dazzling

In Figure 11, this technique utilizes a laser to blind or distract the sensors aboard a UAS rather than destroy the drone like some other laser systems. This type can, however, destroy the sensitive optical sensors attached to the UAS.[101]

---

[100] Patel and Rizer, 24.

[101] Philip Butterworth-Hayes, "'Drone Dazzling Counter-UAS Equipment Installed on U.S. Navy Warship' – News Report," Unmanned airspace, February 24, 2020, https://www.unmannedairspace.info/counter-uas-systems-and-policies/drone-dazzling-counter-uas-equipment-installed-on-us-navy-warship-news-report/.

Figure 11. Dazzling Model

## C. ASSOCIATED CHALLENGES

The greatest challenge to be discussed regarding C-UAS equipment and software is its ability to potentially disrupt other types of electronic communications systems. Of particular concern is the jamming and spoofing equipment, which the Federal Communications Commission (FCC) has a significant problem with. This is because these methods of mitigation have the very real potential to interfere with a variety of things normally found in its localized environment, such as communication signals, power company equipment, manned aircraft navigation systems, wireless internet, and even 5G.[102] Jamming technology might even violate the communications Act of 1934, which largely prohibits technology that will interfere with legal, radio-based communications.[103]

That type of interference brings another challenge into focus, that being the liability aspect. Utilizing these mitigations systems, whether kinetic or non-kinetic, have the legitimate potential to cause damage and/or injury. Every time C-UAS operators disable a drone in flight with a kinetic device, it immediately begins an uncontrolled descent. This means the UAS will impact with whatever is in its way at the time…Another aircraft, a private residence, a vehicle, a person.

One exception to this is the drone net/entanglement systems, such as the Drone Hunter system offered by Fortem Technologies. Essentially, the Drone Hunter identifies, pursues, and eventually captures a rogue drone with a sophisticated net entanglement

[102] Rob Thompson, "The Problems with Counter UAS (CUAS): How to Move the Industry Forward," sUAS News - The Business of Drones, April 23, 2018, https://www.suasnews.com/2018/04/the-problems-with-cuas-how-to-move-the-industry-forward/.

[103] David M. Krueger, "Drone Federalism Act Seeks to Curb Call for 'Anti-Drone' Technology," Lexology, September 21, 2017, https://www.lexology.com/library/detail.aspx?g=2ebbeb3c-eb91-465e-ab48-de253fd12179.

system, before landing it safely.[104] There are a variety of companies, in addition to Fortem, who are in the process of building and testing these types of mitigation systems. Some potential issues that have been identified in association with these systems include target discrimination, angle of attack, as well as speed and agility characteristics. In contrast, non-kinetic mitigation may induce less liability since the electronic confusion caused tends to make the UAS hover, land in a controlled descent, or return to home. Despite offering a better margin of safety, the ability of non-kinetic systems to land a rogue UAS platform safely is not guaranteed

## D. LEGAL AUTHORITY/JURISDICTION

Currently, the application of C-UAS technology within the United States is severely limited by Congressional law. DOJ and DHS are both given specific authorization under 6 U.S. Code 124n.[105] DOD is singularly provided its authorization to conduct C-UAS operations within the United States only under 10 U.S. Code 130i.[106] Although a much smaller department, the DOE is given similar authority within the United States and its territories under 50 U.S. Code 2661.[107] Each of these set forth very specific parameters under which each department may operationally deploy C-UAS systems and equipment.

For DHS and DOJ, the statute specifically covers assets for Coast Guard (USCG), Customs and Border Protection (CBP), Secret Service (USSS), Federal Protective Service (FPS), Federal Bureau of Investigation (FBI), U.S. Marshals Service (USMS), Bureau of Prisons (BOP), DOJ itself, and the Federal Courts. Additionally, the law covers National Special Security Events (NSSE) and Special Event Assessment Rating (SEAR) events, as well as activities with either an investigative purpose or national security threat. The final piece covers any special requests made by a state governor or the state attorney general. DOD and DOE authority are like each other in that they pertain individually to assets under

104 "DroneHunter® F700," Fortem Technologies, accessed September 26, 2021, https://fortemtech.com/products/dronehunter/.

105 Protection of Certain Facilities and Assets from Unmanned Aircraft, *U.S. Code* 6 (2018) §§ 124n,

106 Protection of Certain Facilities and Assets from Unmanned Aircraft, *U.S. Code* 10 (2021) §§ 130i, https://www.law.cornell.edu/uscode/text/10/130i.

107 Protection of Certain Nuclear Facilities and Assets from Unmanned Aircraft.

each department's control. The major difference between them and the first two mentioned is there is no consideration for assistance outside of their specific assets, such as for a local entity.

Although the multi-department jurisdiction described above may sound extensive, it really is not. Under 124n, which applies to two very large departments (DOJ and DHS), the statute fails to specifically account for every single agency within either department. Furthermore, when compared to all the other agencies within the federal government not afforded C-UAS authority, the current jurisdiction begins to look considerably less comprehensive. At the state and local levels, the situation is even more problematic because the sole mechanism to even request protection rests singularly with either DOJ or DHS. What this also means is that there is no delegation whatsoever of C-UAS authority, from those specifically designated federal authorities, to any state or local law enforcement agencies.

National Special Security Events (NSSE) and Special Event Assessment Rating (SEAR) events are also eligible for coverage, but are prioritized, and at the mercy of very limited resources. The NSSE designation is determined by the DHS Secretary in close consultation with the USSS, the FBI, the Federal Emergency Management Agency (FEMA, and others.[108] SEAR ratings are also determined by DHS after federal, state, and/ or local representatives make the formal request for a threat assessment to be conducted. Examples of SEAR rated activities include significant professional sporting events like the Major League World Series.[109]

Limited C-UAS resources, in terms of authority, equipment, and operators, is currently by design. The language within 124n specifically states that only employees, officers, and trained contractors of DOJ and DHS are authorized to conduct C-UAS

[108] "National Special Security Events Credentialing," Securing Events, accessed February 24, 2022, https://www.secretservice.gov/protection/events/credentialing.

[109] Department of Homeland Security, "Special Event Assessment Rating (SEAR) Events Fact Sheet" (Washington, DC: Department of Homeland Security, 2022), https://www.dhs.gov/publication/special-event-assessment-rating-sear-events-fact-sheet.

operations. This means that, as has been previously mentioned, state, local, and tribal law enforcement officers are specifically prohibited from such activities.

Although initially characterized as a challenge within the C-UAS environment, this situation should also be viewed as an opportunity because 124n is going to sunset in 2022. This presents an opportunity to correct shortcomings and expand capacity where appropriate. To accomplish this, there three components of 124n that should be amended to better suit a holistic mitigation strategy against UAS threats. The first two have already been discussed at length, those being the limited jurisdiction and the lack of delegation to state, local, and tribal law enforcement agencies. The third aspect pertains to the cumbersome approval process which requires written authority from either the Attorney General or the DHS Secretary, in consultation with the Transportation Secretary. This process is unnecessarily burdensome and should be delegated down to agency heads in the future.

## E. UAS KILL CHAIN FOCUS

As previously mentioned in Chapter One, the UAS Kill Chain model (Figure 12) specifically utilized within this document will consist of six steps: 1) Plan; 2) Acquire components; 3) Test; 4) Pre-operational surveillance; 5) Attack; and 6) Escape. Rather than showcase the government's mass-produced reactions, this model sequentially breaks down the totality of the perpetrator's actions into definable steps, from which government can then formulate a truly customized response. The challenge with this concept is two-fold: first, C-UAS response ideology must be moved away from its current myopic focus upon the Attack step singularly and, two, expand the U.S. government's philosophy by being equally inclusive to all six steps of the UAS Kill Chain. To understand the value of those six steps, each will be discussed individually as they relate to the overall process.

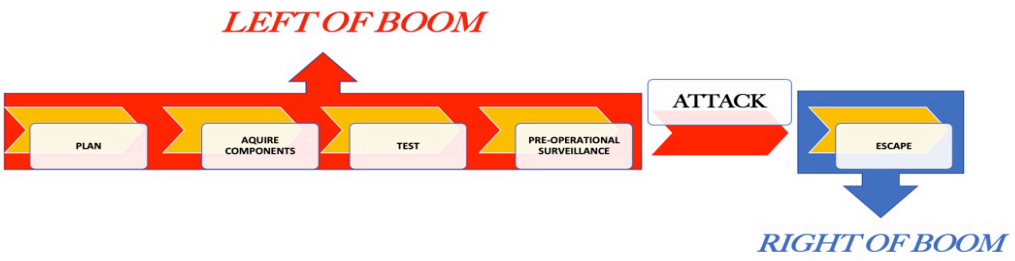


Figure 12. Unmanned Aircraft Systems Kill Chain

### 1. Left of Boom

Left of boom is government or military term often used to signify those activities leading up to an actual attack. Within the UAS Kill Chain, it refers specifically to the first four steps. This is a crucial period of time because there is a small window of opportunity to identify and disrupt the plot before the attack occurs.

#### *a. Plan*

Merriam Webster dictionary defines plan as "an orderly arrangement of parts of an overall design or objective."[110] Once a criminal or terrorist has made the decision, this is where they develop ideas to conduct the attack. This likely includes choosing the targeted location, the timetable, the choice of co-conspirators, the specific style of attack, the necessary weapons and equipment, as well as the method of escape, if any.

This step is rarely done in complete isolation, although there are exceptions, such as the 2017 mass shooting in Las Vegas where 58 people were killed. The FBI eventually closed that investigation without a clear understanding as to the shooter's motivations because he kept his intentions private and did not have an accomplice.[111] Because there is

[110] *Merriam Webster*, s.v. "plan," accessed February 27, 2022, https://www.merriam-webster.com/dictionary/plan.

[111] Vanessa Romo, "FBI Finds No Motive In Las Vegas Shooting, Closes Investigation," NPR National, January 29, 2019, https://www.npr.org/2019/01/29/689821599/fbi-finds-no-motive-in-las-vegas-shooting-closes-investigation.

so much to consider during this step, there is also legitimate potential for law enforcement to capitalize upon the main vulnerability, namely the choice of co-conspirators.

Once knowledge of the attack expands beyond the originator, it becomes more difficult to control that information, exposing the perpetrator to infiltration. Opportunities like this tend to involve an already embedded operational source or the penetration of a new source. Either way, the earlier law enforcement can directly engage, the better chance to prevent the attack from ever occurring.

### *b. Acquire Components*

A plan without the necessary equipment remains a plan. This step also depends upon the competence of the criminal or terrorist, and their potential accomplices. For example, certain lethal chemical and biological agents can be produced from a mixture of legally purchased substances. The same goes for some types of explosives. If the architect or his associates lack that knowledge, they will obviously need to attain it.

Those with the appropriate science, technology, engineering, and math (STEM) backgrounds will be sought after, but other factors may come into play when recruiting such as ethnicity or country of origin, as well as lack of societal and familial association.[112] This is by no means meant to be definitive nor exhaustive, however, it does provide the perpetrator with a few good starting points to consider.

In consideration of a UAS attack, luckily for the criminal or terrorist, the vast majority of drones as well as their individual components, and even a plethora of drop mechanisms, can be legally purchased in stores or via the internet. Imagine if mass panic was the goal. An operator could fly a drone into a large sports stadium full of fans and release talcum powder over everyone. Despite its non-toxic nature, the situation would likely induce mass hysteria, with several deaths and injuries resulting.

The recruitment of subject matter experts as well as the required materials to conduct the attack, may create additional opportunities for law enforcement to identify,

[112] Jacqueline Smith, "Radicalization of Life Scientists to Terrorism" (master's thesis, Georgetown University, 2011), http://hdl.handle.net/10822/553586.

track, and ultimately, disrupt the planned attack. Again, much like the first step, as aspects of the plan become necessarily exposed, operational security diminishes, providing additional opportunities for law enforcement to manipulate the situation. This is where well-maintained law enforcement relationships with academic, commercial, and social institutions can pay big dividends.

#### *c. Test*

Like any scientific endeavor, testing is necessary to validate the concept (plan). In the case of a UAS attack, which will likely be carrying some form of CBRNE payload, the architect must test individual components by themselves first, and then in conjunction with each other. This means the payload modality must be tested to ensure it deploys properly either as an aerosol liquid or ignites, in the case of an explosive.

As for the UAS itself, it's performance might be well known, in the case of a COTS drone, however, if the platform is a DIY model, it will require significant testing to determine its viability and limits. Add to that a custom, or even a commercial drop mechanism, and the levels of complexity and difficulty continue to rise. Once, all these items are addressed, there is still the need to combine the payload with the UAS and make sure it deploys properly, on the correct target, and at the intended time.

This sort of testing would be very difficult to conceal and, as such, presents a third opportunity for plot discovery and subsequent disruption by law enforcement. Drone clubs and associated parks have members who are keen to avoid Federal Aviation Administration (FAA) scrutiny and would thus take immediate notice of foolish or blatantly dangerous behavior. More than likely, this type of unwanted activity would be reported to the FAA and/or the local police department. Again, seeking out and maintaining liaison relationships with these type of drone entities will only benefit government efforts, regardless of whether it simply encourages good citizen behavior or identifies a potential paid informant.

#### *d. Pre-operational Surveillance*

As the plot moves closer to the attack stage, pre-operational surveillance becomes necessary to determine certain characteristics about the venue itself. This includes the most

advantageous date and time to conduct the attack, as well as the most vulnerable locations within the targeted area. Other considerations include the operator's physical position, whether that be close proximity or remote, in addition to designation of post locations for any co-conspirators, identification of fixed surveillance camera sites, and probable uniformed law enforcement staging,

This is the stage where public awareness becomes critical to success. Ever since September 11, 2001, governments, at every level, have engaged communities with various awareness campaigns to partner against suspicious activity. DHS currently maintains a website dedicated to social vigilance with the *See Something, Say Something* slogan.[113] Venues around the country with large scale, special events planned should overtly and prominently display this type of message throughout the physical location, as well as with any associated social media outlets.

***e. Attack***

As has previously been mentioned, this is the phase where most of the civilian and military C-UAS strategy is focused. It is, no doubt, a vital piece within the overall UAS Kill Chain because it showcases the manifestation of the perpetrator's preparation. One of the problems with being so focused upon this particular component, however, is the narrow-minded assumption that C-UAS equipment and personnel are already on site, tracking, and ready to respond.

At this point within the UAS Kill Chain, the only option is mitigation, with the best scenario being a successful intercept prior to the means of attack being deployed. Again, this assumes C-UAS assets are present and operational. At worst, there are no accessible C-UAS assets, which given the restricted resources legally authorized and available, is the much more likely scenario within the United States.

113 "If You See Something, Say Something," Department of Homeland Security, accessed February 28, 2022, https://www.dhs.gov/see-something-say-something.

### 2. Right of Boom

Very few seem to ever discuss the other end of the spectrum, or *right of boom*, when it comes to attack models. However, there is much to be gained from taking this perspective. Depending upon what, if anything, was done *left of boom*, this may be the first-time law enforcement and intelligence officials are reacting to the attack.

Continuing with the actions of the criminal or terrorist, once the attack has been set in motion, he or she will try to escape, which also happens to be the last step within the UAS Kill Chain. A successful escape will likely mean the perpetrator is able to repeat the process all over again, beginning with the planning step. The stand-off capability with UAS platforms is part of what makes them so attractive to terrorist and criminal organizations because it is easier to avoid arrest, remaining free to do it all over again. This replication of the attack process also lends credibility to the UAS Kill Chain as a suitable model to both analyze and develop the most effective response to these unique threats.

The importance of this step to law enforcement cannot be over-emphasized. If *left of boom* has been completely ignored, this necessarily becomes the reactionary initiation point for investigative operations. Typical law enforcement actions are then taken, such as making the scene safe, collecting evidence, as well as conducting witness and victim interviews. Had consideration been taken for *left of boom*, the severity of the situation may have been significantly reduced, or even eliminated entirely.

## F. CONCLUSION

In summary, substantial challenges exist within the UAS threat picture across the United States, and it is quite difficult to disconnect them completely from one another. The challenge with C-UAS hardware and software is significant because there is no one sensor that acts as the *magic bullet* against drones. Even with a suite of sensors, there are absolutely no guarantees of successful mitigation. Additionally, even with the best equipment money can buy, it must be deployed with competent operators to be effective. Legal challenges consist of limited jurisdiction, a lack of delegation, and the cumbersome approval process. Limited jurisdiction curtails the federal response to very specific situations, leaving a multitude of soft targets uncovered and open to attack. A lack of

delegation prevents any non-designated law enforcement entity from assisting those relatively few who do possess the ability to deploy C-UAS resources. This means the thousands of state, local, tribal, and territorial police departments, that could act as significant force multipliers, end up standing idly by. Remaining ignorant of the UAS kill chain model by solely focusing upon the attack step will place the homeland security apparatus in an unenviable position when, not if, a criminal or terrorist decides to employ a drone, or drones, against any one of the large, open venue gatherings that occur each day around the United States.

THIS PAGE INTENTIONALLY LEFT BLANK

# V. INTER-AGENCY CONSOLIDATION

The purpose of this chapter is to identify and analyze several options for the United States government to consider as it confronts the UAS threat. The reality is, if time and space were not factors, an endless number of options could be assessed for viability. However, because those factors must be taken into consideration, three options, beyond the status quo, were specifically chosen to make this process manageable, and because they have been used in the past to provide a whole of government response to various homeland security threats. These specifically selected options include a working group, a task force, and single agency designation.

As previously stated within the Research Design section of Chapter One, each will be compared in terms of commitment and collaboration levels. For commitment, this again means the willingness of an agency to provide funding for equipment, personnel, physical space, and training. Collaboration is the measure of an agency's willingness to join forces, cooperating with one another to achieve unified goals, as well as sharing in the accountability for potential success, and failure. After the analysis is conducted, the best option will have the highest levels of commitment and collaborative effort, designated by a number from 1 to 10.

## A. OPTIONS

The UAS Kill Chain has already been analyzed in terms of its ability to holistically address those six steps a criminal or terrorist would likely take to carry out an attack. Bearing that model in mind, how can the United States most effectively consolidate inter-agency resources, maximizing both investigative and intelligence capacities to prevent, or at least substantially, mitigate a UAS attack? First, the United States must develop a nationally recognized strategy to address the threat posed by UAS platforms. Incorporating the UAS Kill Chain into that strategy also allows the United States to widen its aperture, looking *left of boom*, where it can exploit the planning, the acquisition of UAS components and payload, the testing, and any pre-operational surveillance. Additionally, it provides Americans with the ability to look *right of boom*, which includes the subject's escape.

The American government can no longer rely upon siloed efforts between individual departments, and their respective UAS stakeholder agencies, to effectively address emerging threats, specifically with something as complicated and lethal as drone technology. Similar to the United Kingdom, the American national strategy must be holistic and multi-layered in its approach by also synchronizing domestic and foreign intelligence collection with investigative activities. Meaningful collaboration efforts should be inclusive of the academic and commercial sectors as well to ensure a unified response is presented to the perpetrator(s).

The easiest way for the federal government to address the UAS threat is to simply continue operating as it has been for the past several years, with each department and associated stakeholder agency conducting business largely independent of each other. Collective discussions would occur between certain key players from time to time, however, C-UAS operational deployments will remain firmly in-house, so to speak. With this course of action, each entity maintains their own level of capability and deployment terms for C-UAS operations while almost completely forgoing any meaningful intelligence analysis or direct investigative activity except for, perhaps a few personnel, when available as collateral duty.

Going this route is obviously the easiest for the U.S. government because it necessitates no asset, operational, or policy changes whatsoever. There are no new costs incurred, no additional manpower requirements, or extra time expended. Everyone continues along by themselves, independently conducting very similar C-UAS operations.

On the positive side, by maintaining the status quo, it does allow specific agencies to address UAS threats entirely in support of their unique mission requirements, unimpeded by competing interests or some artificially imposed collaboration mandate. Take the United States Secret Service, for example, which deploys C-UAS assets in support of their executive protection mission. Or, DHS' Customs and Border Protection, which now counts

the defense of American borders against drone threats as one of its latest mission sets.[114] Any unnecessary collaborative efforts, enforced merely to showcase shallow liaison decrees would be appropriately disregarded.

Moving onto the negative side, by maintaining the status quo, it absolutely forgoes any potential for meaningful collaboration between agencies at the operational and strategic levels. This course of action will also likely eliminate, or severely restrict, any opportunities to exploit individual strengths, reduce operational overlap, as well as decrease the potential gain in collective efficiency and effectiveness.

### 1. Working Group

Working groups generally are formed to study an issue of importance so they can eventually make some type of recommendation(s) about how to appropriately address it. Government versions are no different, having been around for a long time, and for a variety of reasons. They are seen as a positive opportunity to bring together subject matter experts from different backgrounds as a more effective means to solve pressing problems. The UAS threat environment is no different.

#### *a. DOJ UAS Working Group*

DOJ already has a departmental UAS working group that is presided over by the Deputy Attorney General. This particular working group is the centralized mechanism within DOJ for all UAS and C-UAS issues. As such, all internal DOJ agencies and offices have representation within this assembly.[115]

---

[114] Linda Canfield and Jonathan R. Cantor, *Privacy Impact Assessment for the United States Secret Service Special Operations Division Counter-Unmanned Aircraft Systems in Support of United Nations General Assembly*, DHS/USSS/PIA-025 (Washington, DC: Department of Homeland Security, 2019), https://www.dhs.gov/publication/dhsussspia-025-united-states-secret-service-special-operations-division-counter-unmanned.

[115] "Unmanned Aircraft Systems," Office of Legal Policy, April 29, 2022, https://www.justice.gov/olp/unmanned-aircraft-systems.

### *b. TSA C-UAS Working Group*

The Transportation Security Administration (TSA) stood up a C-UAS Technology Working Group in June 2019. It is co-managed by both DHS and DOJ, with TSA representing the former and the FBI acting on behalf of DOJ. Over twenty agencies are represented with nearly 160 individual participants.[116]

### *c. FAA UAS EXCOM*

The Federal Aviation Administration (FAA) chairs the UAS EXCOM or UAS executive committee which brings stakeholders together to discuss drone research and development, policy, and techniques. This working group is intended to address issues emanating from UAS integration into the national airspace. Beyond the typical members, this committee also counts the National Aeronautics and Space Administration (NASA), as well as the Departments of Commerce and Interior, respectively. UAS EXCOM began back in 2009 and was intended to assist the DOD with UAS integration into the U.S. national airspace.[117]

### *d. Pros*

As previously stated, working groups can be a positive way to bring together subject matter experts from a variety of departments, agencies, and units to discuss whole-of-government problems. There are two characteristics of working groups that make them worthwhile, at least at the outset of defining a threat. The first is that the process of creating one necessarily identifies all the relevant stakeholders. The second, which is sequential to the first, is that working groups are a particularly effective method of opening new communication lines between various government entities.

---

116 Transportation Security Administration, "Counter-Unmanned Aircraft Systems (C-UAS) Program Briefing," in *Asia-Pacific Economic Cooperation (APEC 2021)* (New Zealand, 2021), http://mddb.apec.org/Documents/2021/TPTWG/AEG-TM1/21_tptwg_aeg_tm1_002.pdf.

117 "Federal Government Expands UAS Partnerships," Department of Transportation, March 16, 2016, https://www.faa.gov/newsroom/federal-government-expands-uas-partnerships.

### *e. Cons*

Taking the opposite (negative) perspective, working groups abound at the federal, state, and local levels of government, which tends to dilute their individual importance and anticipated effectiveness. As it currently stands, even with the plethora of working groups focused upon UAS issues, many of which contain the same member agencies and representatives, individual efforts persist. This is quite evident when one considers that the American government still does not possess a single, all-encompassing, permanent body of oversight for UAS matters. Until that happens, meaningful efforts will remain largely independent amongst distinct UAS stakeholders.

There are two observations to consider regarding the working group option. One is that, given the multi-year existence of numerous UAS working groups, it is reasonable to include their presence as part of the status quo. The second is that because UAS technology is advancing so rapidly, the potential threat has also increased exponentially as well. One could conclude that the American response has not kept pace with the growing threat. Bearing these observations in mind, unless someone comes up with a better method to make the working group model more effective than it currently is, as least as far as it relates to UAS threats, the United States response to drone threats will remain unremarkable for the foreseeable future.

## 2. Task Force

A second choice along our government options continuum to combat the UAS threat is the task force model. Although working groups tend to exist more at the surface level in terms of true investment, they do assist by, at least, helping to identify the true stakeholders. Strap-hangers, or those deemed not crucial, tend to start out strong, but over time, their commitment generally begins to decline.

Once the proverbial wheat is separated from the chaff, and assuming collaborative intentions are, and remain legitimate, there is real potential for those national and regional working groups to eventually morph into enhanced task forces. In general, a task force is formed to increase interaction and synchronization between two or more law enforcement entities, permitting individual agencies to traverse jurisdictional lines, thus increasing their

collective effectiveness against a particular crime or threat.[118] Examples of current task forces include DOJ's Organized Crime Drug Enforcement Task Forces (OCDETF), the Drug Enforcement Administration's High Intensity Drug Trafficking Areas (HIDTA), the U.S. Marshals Fugitive Task Force, and the FBI's Joint Terrorism Task Force.

Task force officers (TFO) generally serve for at least one year; however, many serve for five years and longer. Non-federal TFOs continue to collect their salary from their parent department, but all overtime and related equipment are paid for by the lead federal agency.[119] The physical location of the task force is also generally maintained and funded by the lead agency as well. TFO status confers federal jurisdiction, significantly increasing each member's authority to enforce laws at the local, state, and federal levels. In one particular study conducted of nearly 30 law enforcement agencies within the state of Texas, 38% felt their task force participation was successful and 41% felt their participation was very successful.[120] Despite the uniqueness of the study, its results provide a fairly significant validation of the task force model, even without knowledge of the exact level of participation, which tends to vary between agencies.

The decision to create or implement a task force is based upon an assessment of the situation to determine its appropriateness. Task forces can, and are, formed for a wide variety of reasons beyond just law enforcement threats, with just two immediate examples being education and healthcare. Despite the specific subject matter differences, there are certain reasons for forming a task force that transcends the isolated problem to be addressed. For instance, task forces allow parent agencies to focus upon one prioritized issue while still having the capability to handle day-to-day responsibilities. Additionally, a

118 "Evaluating the Task Force Model," *TELEMASP Bulletin* 9, no. 3 (June 2002): 1–7, ProQuest.

119 James Casey, "Managing Joint Terrorism Task Force Resources," *FBI Law Enforcement Bulletin* 73, no. 11 (November 2004): 1–6, ProQuest.

120 TELEMASP Bulletin, "Evaluating the Task Force Model."

smaller group tends to be more agile than the larger enterprise. Finally, task forces have the ability to synchronize individual strengths of members for collective benefit.[121]

### *a. Pros*

The implementation of a task force offers several benefits. For one thing, it creates buy-in to the overall concept and goals. Regarding national task forces, despite a single federal entity taking lead over the task force, there are constant opportunities for each TFO to directly contribute to both the ongoing process and the expectant success of the group. Second, it spreads the overall costs of the endeavor for vital operating components like manpower, time, and equipment, across multiple agencies, preventing any one department from shouldering the entire burden by themselves. This can be a game changer in terms of response capability, particularly for small departments, as it allows them to punch far above their respective weights, so to speak.

Third, as the professional relationships between TFOs and their federal counterparts development, and optimistically improve over time, the egocentric turf war style attitudes would correspondingly diminish. This results in member actions becoming more cohesive, leading to greater interest in accomplishing the task force's collective goals versus those of their parent departments. The subsequent successes can then be legitimately shared amongst all participating agencies.

### *b. Cons*

Of course, task forces are not immune from problems either. For one thing, depending upon how the partner agencies view their involvement, they might either send their best and brightest, or see the task force as a dumping ground for personnel who are either very inexperienced, troublemakers, and who are derisively referred to as ROAD or retired on active duty. While this selfishly benefits the department by ridding itself of their

[121] Community Tool Box, "Section 3. Developing Multisector Task Forces or Action Committees for the Initiative," Learn a Skill Chapter 9. Developing an Organizational Structure for the Initiative, accessed May 22, 2022, https://ctb.ku.edu/en/table-of-contents/structure/organizational-structure/multisector-task-forces/main.

sub-par employees, it obviously reduces the effectiveness of the task force, and its ability to have a positive impact against the threat.

This leads into another potential issue with turnover. If the task force is saddled with the type of personnel just mentioned, quick turnover can be a blessing as the potential to wreak havoc is limited. On the other hand, if the TFO is a high performer, the parent agency might want them back as soon as possible. This is obviously not advantageous for the task force because their capability is diminished. Turnover also creates a loss of institutional knowledge similar to removing senior enlisted cadre from vital training billets and, thus, losing their ability to mentor students.

One final potential problem the task force model may experience is agility, or the lack thereof. Task forces, by their very nature, must remain agile, able to pivot in response to various changes within the threat. The more institutionalized a task force becomes, the more it begins to resemble a cumbersome, bureaucratic behemoth, unable to rapidly adjust and transform as necessary. Nimbleness is as much a necessary component of the task force model as is its component's collectivized strength. This means keeping the structure lean, but possessing the capacity for augmentation when necessary, such as during the attacks of September 11, 2001.

### 3. Designated Agency

A third course of action to consider is the designation of one federal agency to address the UAS threat. This may be the most complicated path to take of the three options discussed here because it involves the transfer of existing authority, whether explicit within the Preventing Emerging Threats Act of 2018, or simply assumed by other agencies. With multiple agencies already involved in the UAS threat environment, this could be a difficult direction to go. Not to mention the fact that that agency will shoulder the future success, and failure, of any UAS attack and/or operation. Luckily, this path has already been previously utilized by the Federal Government with some measure of success.

### *a. Drug Enforcement Administration*

The Drug Enforcement Administration (DEA) is one such agency under the DOJ. Their mission statement is as follows:

> The mission of the Drug Enforcement Administration (DEA) is to enforce the controlled substances laws and regulations of the United States and bring to the criminal and civil justice system of the United States, or any other competent jurisdiction, those organizations and principal members of organizations, involved in the growing, manufacture, or distribution of controlled substances appearing in or destined for illicit traffic in the United States; and to recommend and support non-enforcement programs aimed at reducing the availability of illicit controlled substances on the domestic and international markets.[122]

While other agencies possess the authority to investigate and prosecute drug crimes, the DEA is widely considered to be the lead agency, regardless of government level throughout the United States.

### *b. United States Secret Service*

The United States Secret Service (USSS) is another agency with a highly specialized, singular mission, that being executive protection. As with drugs, there are other agencies who conduct these types of operations, however, there is little doubt as to what agency comes to mind when bodyguard responsibilities are mentioned. To be fair, the USSS also conducts investigations into financial crimes and related activities, but they are world-renown for their protection capabilities. Their mission encompasses these two aspects as follows:

> We have an integrated mission of protection and financial investigations to ensure the safety and security of our protectees, key locations, and events of national significance. We also protect the integrity of our currency and investigate crimes against the U.S. financial system committed by criminals around the world and in cyberspace.[123]

---

122 "DEA Mission Statement," Mission, accessed March 15, 2022, https://www.dea.gov/about/mission.

123 "About Us," United States Secret Service, accessed March 15, 2022, https://www.secretservice.gov/about/overview.

### *c. Customs and Border Protection*

One final example is DHS' Customs and Border Protection (CBP). Although now combined with Customs, the Border Patrol also has a very focused mission, this time entirely dedicated to securing the U.S. borders. Their mission statement is the most succinct of the three and is as follows: "Protect the American people, safeguard our borders, and enhance the nation's economic prosperity."[124] The CBP are considered the first line of defense when it comes to homeland security responsibilities.

### *d. Pros*

As far as single agency designation goes, there are some potential benefits. For one thing, it would allow a multitude of other enforcement and regulatory agencies that currently expend limited resources, in terms of funding, personnel, and time, to re-focus their efforts upon other mission related activities. It may also reduce, or even possibly eliminate, any inter-agency conflicts about jurisdiction, which is a legitimate problem, even between units within the very same agency. A single agency would also increase accountability, improve management, and reduce operational response ambiguity.

### *e. Cons*

Conversely, any attempts by a single agency to assert this singular position of authority would certainly cause major conflict across the whole of government. DOD, DOE, DHS, and DOJ have already invested considerable resources into their respective C-UAS programs. Individual agencies or offices have also been officially designated as the lead agency with their respective departments. Examples include the FBI within DOJ and the JCO within DOD. Others have simply assumed departmental authority despite not being specifically mentioned within any specific one of the four Congressional authorities.

124 "About CBP," U.S. Customs and Border Protection, February 24, 2022, https://www.cbp.gov/about.

## B. CONCLUSION

As has been shown, there are multiple ways for the United States government to consolidate inter-agency resources, thereby maximizing the intelligence and investigative capacities necessary to meet and defeat the threat from UAS platforms. One option is the working group model, which as has been shown, is part of the current status quo, in the sense that there are already a multitude of UAS working groups at each level of government. This would seem to be a reasonable strategy considering there has not yet been a major attack of any kind on American soil utilizing a drone as either the weaponized payload's designated method of delivery or as the weapon itself. When looked at through the lens of commitment, there is little or no willingness of the associated agencies to fund equipment, personnel, physical space, or training, at least not beyond what is normally required to conduct day-to-day, enterprise-wide business. This means the working group model rates a two (2) on a scale of ten (10) for commitment. Collaboration, on the other hand, is quite high as evidenced by the typically high number of participants, thereby providing a rating of six (6), as shown in Figure 10.

Moving beyond the Working Group option is the task force model. It is a tried-and-true government method of addressing a variety of law enforcement threats from criminal to terrorism, and everything in between. It has the legitimate potential to provide a measure of stability usually reserved for the agency designation option, but without having to completely undo any currently existing legal authorities or intra-agency administrative rules. There is also real potential for all participating task force members to contribute in a meaningful way that accomplishes the collective goals while allowing individual agencies and departments to share the credit for operational successes.

Task forces possess a rather high level of commitment compared to the working group model. This is because prospective agencies must have *skin in the game* to participate. At the very least, personnel must be seconded to the task force but very often, there are additional costs involved. As was previously mentioned, some federal agencies, like the FBI, pay most the task force's operating costs but parent agencies must still sacrifice to reap the collective benefits. Bearing this in mind, the task force model is rated at a seven (7) for commitment, as it moves far beyond the bare accoutrements entertained

by working groups. Collaboration within the task force model is also obviously very high as the centralized purpose is to join forces with other agencies to enhance effectiveness and efficiency. As such, the task force rating is slightly higher at eight (8).

Moving beyond the working group and task force models, the U.S. government could simply go all in and either create an entirely new agency, or select an existing agency, to take the lead on all things UAS. There is precedence for both options as previously described in the single agency designation section. Given the severity of UAS attacks currently occurring around the world, with special consideration given to the Middle East and now more recently, along the Southwest border with Mexico, this may be a prudent strategy to get ahead of the threat.

Single agency designation takes commitment to entirely new level because that enterprise assumes sole responsibility for all funding, personnel allocation, infrastructure, and training. There is no higher form of commitment and, thus, it receives the highest rating of ten (10) to reflect that. Collaboration, with the single agency designation, falls to the opposite end of the spectrum. This is because, as per its name, there is no overt intention to collaborate with external entities, at least not in any meaningful way. This is not to say that there will be absolutely no liaison or temporary partnership opportunities, it just means the designated agency will take the lead for all activities relating to the threat, as well as any responsive actions deemed appropriate. This includes responsibility for all subsequent successes and any potential failures. With this understanding, single agency designation receives the lowest rating of zero (0) as shown in Figure 13.

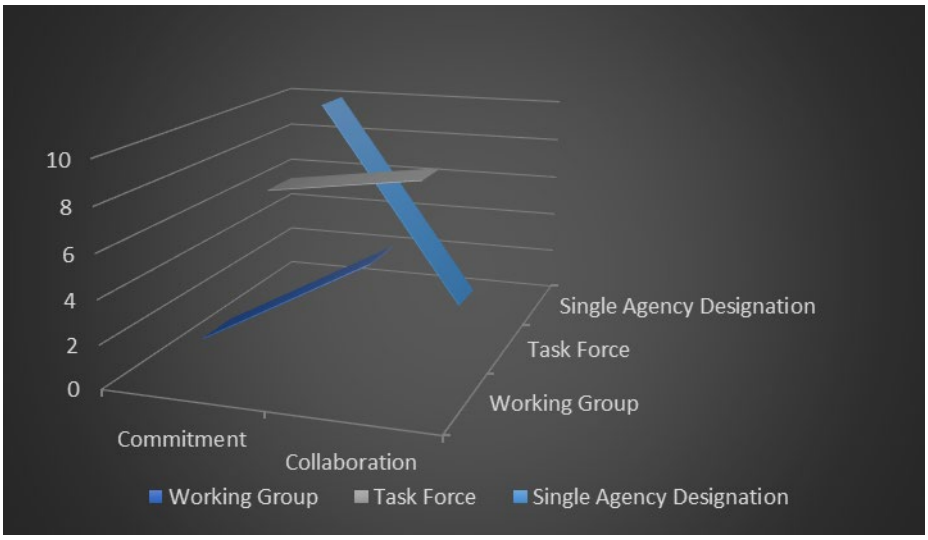


Figure 13. Federal UAS Threat Response Options

THIS PAGE INTENTIONALLY LEFT BLANK

# VI. RECOMMENDATIONS AND CONCLUSIONS

## A. RESEARCH CONCLUSION

There are two main conclusions to be drawn from the research conducted. The first is that the United States must stop looking at the actual drone attack itself as the only relevant activity to be addressed by homeland security officials. Throughout Chapter Three of this document, the current C-UAS strategy, employed by United States government civilian and military components, has been exposed for its narrow-minded approach and significant deficiency in terms of holistic mitigation posture. This is because, as has been shown in Chapter Two, the process by which a criminal or terrorist conducts a UAS attack cannot possibly be encompassed solely within the time frame of the physical attack itself. There are multiple steps being ignored, prior to and just after that attack, which must be appropriately considered as well. Those steps, which were analyzed within the last section of Chapter Four, are sequentially identified within the UAS Kill Chain model and have been analyzed throughout this document.

Figure 11 showcases the differences between what is currently accepted as C-UAS strategy and the UAS Kill Chain. Furthermore, that existing response strategy is completely reliant upon technology, showcased in Chapter Three, to counter the threat within a very specific interval, that being from the time the drone takes operational flight until it is brought down by C-UAS operators. This is a tragic mistake because it utilizes an extraordinarily limited tactical response to address a nearly unrestricted strategic problem as presented in Chapter Two. Even more depressing is the fact that very few sites across the United States are legally hardened on a temporary basis, and even fewer are likely to possess permanent response capabilities. This means that, given the plethora of potential targets throughout this country, nearly all could legitimately be considered soft. Responsibility for this situation is due, in no small part, to the current federal legal restrictions regarding who can deploy and operate, as well as where, which was discussed in the second section of Chapter Four.

This reality must be dealt with much more effectively. The only way to truly increase that effectiveness is by consolidating inter-agency resources to maximize the intelligence, investigative, and C-UAS capacities to holistically address the UAS Kill Chain. Law enforcement and intelligence personnel must incorporate *left* and *right of boom* in their mitigation response to ensure a holistic strategy is first developed and then deployed. This reality was what precipitated the need to analyze the three main response options identified within Chapter Five.

Utilizing the UAS Kill Chain provides an outline for moving well beyond current, purely reactive tactical responses. Another significant benefit is that it should force individual departments and agencies to work together, ending the siloed efforts amongst them. As Cody Minks (2018) mentioned in his thesis, "information silos cause trouble for innovation and success across various organizations…which make sharing information and collaboration almost impossible."[125]

The second conclusion to be drawn came from an in-depth analysis of the three UAS threat response options first presented within the Research Design section of Chapter One. This determination resulted from the comparison in Chapter Five, which found that, despite the legitimate viability of each option, only one vastly improves upon existing practice, while also deftly navigating the politically charged minefield of United States government jurisdiction. To be clear, all were individually viewed through the lens of historical precedence and then assessed for operational veracity. Worthy consideration of the previously stipulated commitment and collaboration aspects from Chapter One negates the potential for serious impact by either the working group or single agency designation models. This is because each is significantly lacking in one or the other necessary aspects of measurement.

The first model to be reviewed was the working group, which was eventually determined to be part of the current status quo for the simple reason that so many already exist, and at all levels of government, yet none of them have contributed anything remotely

[125] Minks, Cody, "Hacking the Silos: Eliminating Information Barriers between Public Health and Law Enforcement" (master's thesis, Naval Postgraduate School, 2018), 18–19, http://hdl.handle.net/10945/58345.

responsive to the overall UAS Kill Chain model. To put it simply, the working group model lacks authentic commitment. The second option was the task force model, which properly balanced commitment and collaboration, rating high in both categories. It provides equal parts breadth and depth, thus, addressing an asymmetrical threat as lethal as UAS platforms have the propensity to be. By its very design, a task force collectivizes vital, individual strengths from different departments, agencies, and units to properly address the UAS threat.

Moving on to the third and final option, a single agency designation, which was also entertained but, ultimately, rejected because despite ranking high in commitment, it ranked low in collaboration. Additionally, and by no means inconsequential to this discussion, those turf conscious agencies who currently possess C-UAS authority are very unlikely to cede any of it to one agency, particularly if it is not them. Essentially, this means legitimate collaboration is absent or severely limited when a single agency designation model is commissioned to address a threat.

By analyzing Figure 14, the task force model possesses all the requisite partners to holistically address every step of the UAS Kill Chain, rather than just the C-UAS assets for the attack itself. A hybridized task force will provide the framework to successfully synchronize inter-agency resources against UAS threats in much the same way a Joint Terrorism Task Force has for over four decades.

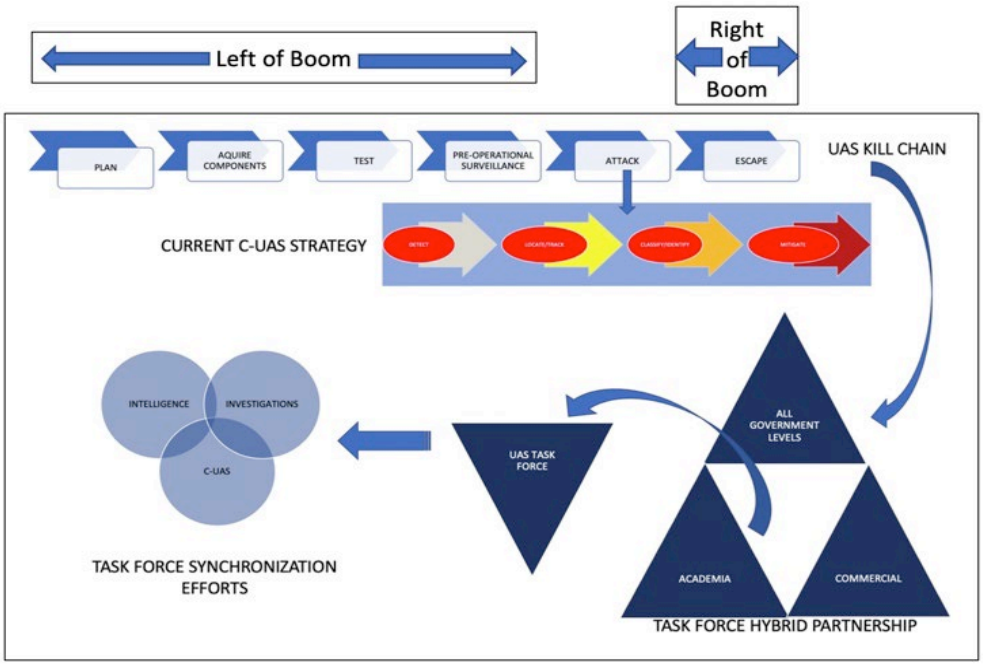


Figure 14. UAS Kill Chain Synchronization with Task Force Model

## B. RECOMMENDATIONS

In consideration of the research presented, which is 1) intended to identify problems associated with the current C-UAS tactics utilized by the United States government and, 2) provide the most effective, corrective solution, thereby maximizing strategic response operations, the following four steps are recommended to assist with the development and implementation of a holistic mitigation approach that reaches across all levels of government.

### 1. Step One

The first step is to designate a national, administrative task force comprised of stakeholder personnel from individual agencies and units within each of the four authorized C-UAS departments (DOJ, DOD, DHS, and DOE). In addition, prominent subject matter experts from academic institutions of distinction and recognized commercial entities should be included as well. A dynamic leadership structure must be put in place with the ability to adjust and transform along with the threat. This will ensure the ensuing United States UAS mitigation policy is not stifled with *best practices* mediocrity, but rather

welcoming of a much more provocative approach that not only embraces but demands innovation.

Embracing the national model, each state should follow by creating single, administrative task force with state-wide law enforcement agencies who work in tandem with regionally based academic and commercial partners, thus, maintaining a legitimate and shared presence within both the UAS and C-UAS environments. The lead member should have direct access to, and meaningful representation within, the national, administrative UAS working group. This ensures state, local, tribal, and territorial interests are not ignored or overlooked at the national level.

### 2. Step Two

Once the national and state structures are set up, a federal level C-UAS policy needs to be created, one which is broad enough to incorporate all six steps of the UAS Kill Chain, but also inclusive enough to remain cognizant of localized interests. The national administrative task force, working together with their state counterparts, would be responsible for crafting this policy. This means that beyond devising the objectives and framework necessary to formulate a comprehensive national policy, reduced scale versions should be crafted to implement those principles in a consistent manner by individual states, thus ensuring sufficient cohesion throughout the United States. The national C-UAS policy should transcend department, agency, and even unit responsibilities to ensure the United States government presents a united front in response to this emerging homeland security threat.

Policy formation must be done in close coordination with Congress to ensure the legal framework supports it by not only increasing C-UAS authority but also incorporating sufficient criminal penalties for illicit use. As the severity of the illegal activity increases, so must the corresponding consequences. With few exceptions, the vast majority of potential penalties are currently regulatory in nature and are, singularly enforced by the FAA.[126] Criminal penalties do currently exist but are not yet sufficient to deal with the

126 "Offices," Security and Hazardous Materials Safety, accessed March 24, 2022, https://www.faa.gov/about/office_org/headquarters_offices/ash/ash_offices.

plethora of threat options identified throughout this document. For example, one applies to those who interfere with manned aircraft and particularly near airports under 18 U.S. Code § 39B – *Unsafe operation of unmanned aircraft*.[127] Another example is 18 U.S. Code § 40A – *Operation of unauthorized unmanned aircraft over wildfires*, which obviously applies to those who operate a drone during emergency wildfire suppression activities conducted by firefighters and other first responders.[128]

### 3. Step Three

With a national policy and accompanying legal framework in place, an on-the-ground entity will be required to craft and, subsequently, implement an operational strategy. This is where the operational component of the national task force comes into play as a valued and equal partner to the administrative piece. It is the mechanism by which policy, strategy, and operations synchronize to holistically address the threat across the entire UAS Kill Chain. It could be modeled along the lines of the FBI's Joint Terrorism Task Force but hybridized with subject matter experts from academic and commercial entities as well. This will increase the task force's ability to pivot in tandem with the threat itself, remaining resilient and ready to respond as the technology improves, making UAS platforms more lethal over time.

Prior to any consideration of deployment activities, a strategy must first be created to transform the policy's conceptualized vision into actionable mission sets with defined objectives and achievable milestones. Specifically, the operational component of the UAS task force will design a coherent strategy that focuses upon the operational implementation of those vital homeland security interests first identified by the national policy. It should also incorporate all aspects of the UAS Kill Chain into each individually identified line of effort. These essential endeavors specifically pertain to training requirements, intelligence collection and analysis, investigations, source identification and cultivation, research, and development, as well as testing and evaluation.

---

[127] Unsafe Operation of Unmanned Aircraft, *U.S. Code* 18 (2018) §§ 39B, https://www.law.cornell.edu/uscode/text/18/39B.

[128] Operation of Unauthorized Aircraft over Wildfires, U.S. Code 18 (2018) §§ 40A, https://www.law.cornell.edu/uscode/text/18/40A.

Realistically, the UAS threat response must be led by the government; however, success will not be realized without meaningful inclusion from academic and commercial entities as well. Non-traditional partnership inclusion is nothing new to the United States, nor to its large-scale threat strategies. A good example of this is the current counterterrorism strategy. Throughout the document, it consistently calls for collaboration with non-traditional entities to include private sector groups that help protect communications technology and enhance cyber security. Also mentioned are prevention, intervention, and re-integration platforms.[129] Although these entities may be non-traditional in the sense that they are not of intelligence, law enforcement, or military origin, their presence and purpose is, as was previously stated, not without precedence. Given the potential lethality of the UAS threat, which rapidly increases with each technological innovation, existing response methodology simply will not do. This threat requires a custom solution.

#### 4. Step Four

Once those national components are in place, the next step is to create localized operational task forces within each state, or region, to ensure recognition and inclusivity of valued, non-federal law enforcement agencies. These would be modeled after the national structure, partnering with the administrative component, and would necessarily include law enforcement elements from state, local, corrections, and fusion cell entities to ensure true diversity. Only by working together at all levels of government, with non-traditional partners in an operational task force environment, versus the limited efficacy of a working group model, or the isolationist approach of single agency designation, will the United States government succeed at creating a truly proactive and holistic response against emerging UAS threats.

---

[129] Donald J. Trump, *National Counterterrorism Strategy for the United States of America* (Washington, DC: White House, 2018), https://www.dni.gov/files/NCTC/documents/news_documents/NSCT.pdf.

## C. FUTURE RESEARCH

Regarding future research, if the goal is to address any limitations identified during this analytical process, it would be to encourage more study that directly incorporates this type of UAS Kill Chain model. To be sure, there is nothing new utilized within this research, meaning there is obvious and well-documented interest in C-UAS tactics as well as joint task force operations. There is even some literature where those two subjects intersect, however, none of it overlays those two subjects along a kill chain model. If the United States intends to properly prepare for and effectively respond to the UAS threat, more focused research needs to be conducted by both scholars and practitioners that properly incorporates left and right of boom.

## D. SUMMARY

Acknowledging that a problem exists is only the first step. This research was, thus, partially undertaken to address numerous shortcomings within the C-UAS approach currently utilized by the United States government as identified within Chapter Four. Recognition without resolution, however, is essentially worthless. As such, Chapter Five's analysis of that research subsequently identified the best solution to address those shortcomings. One important contribution this research provided was significantly increased awareness of the overall UAS threat environment, well beyond just the immediate confrontation. This narrow-minded emphasis placed upon the attack step that is currently espoused by C-UAS stakeholders throughout the federal government resembles a September 10th mentality that homeland security practitioners cannot justify nor afford. We must work together, developing and deploying a potent, pro-active operational response strategy sufficient to successfully mitigate the UAS threat now, and in the future.

# LIST OF REFERENCES


Action on Armed Violence. "Drones and the IED Threat." Reliefweb, July 26, 2017. https://reliefweb.int/report/world/drones-and-ied-threat.

Army Technology. "SONGAR Armed Drone System." Army Technology, September 1, 2020. https://www.army-technology.com/projects/songar-armed-drone-system/.

Associated Press. "Mexican Cartels Now Use IEDs as Well as Bomb-Dropping Drones." Voice of America, February 5, 2022. https://www-voanews-com.cdn.ampproject.org/c/s/www.voanews.com/amp/mexican-cartels-now-use-ieds-as-well-as-bomb-dropping-drones-/6427770.html.

Atencio, Julian James, and Carolynn P. Scherer. *Counter Unmanned Aircraft System (CUAS) Implementation Storyline*. LA-UR-20-25040. Los Alamos, NM: Los Alamos National Laboratory, 2020. https://doi.org/10.2172/1638609.

Ben Gurion University of the Negev. "First Technique to Detect Illicit Drone Video Filming Demonstrated by BGU and Weizmann Institute Researchers." Ben Gurion University of the Negev, January 14, 2018. https://in.bgu.ac.il/en/pages/news/Game-of-Drones.aspx.

Borsari, Federico. *The Middle East's Game of Drones: The Race to Lethal UAVs and Its Implications for the Region's Security Landscape*. Milan: Italian Institute for International Political Studies, 2021. https://www.ispionline.it/sites/default/files/pubblicazioni/borsari_analisi_26.01.2021.pdf.

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

Butterworth-Hayes, Philip. "'Drone Dazzling Counter-UAS Equipment Installed on U.S. Navy Warship' – News Report." Unmanned airspace, February 24, 2020. https://www.unmannedairspace.info/counter-uas-systems-and-policies/drone-dazzling-counter-uas-equipment-installed-on-us-navy-warship-news-report/.

Canfield, Linda, and Jonathan R. Cantor. *Privacy Impact Assessment for the United States Secret Service Special Operations Division Counter-Unmanned Aircraft Systems in Support of United Nations General Assembly*. DHS/USSS/PIA-025. Washington, DC: Department of Homeland Security, 2019. https://www.dhs.gov/publication/dhsussspia-025-united-states-secret-service-special-operations-division-counter-unmanned.

Casey, James. “Managing Joint Terrorism Task Force Resources.” *FBI Law Enforcement Bulletin* 73, no. 11 (November 2004): 1–6. ProQuest.

Charles, Jacqueline, and Jay Weaver. “Grenade-Dropping Drones, a Paranoid President, Guards Who Ran: Latest on Haiti Assassination.” *Miami Herald*, September 19, 2021. https://www.miamiherald.com/news/nation-world/world/americas/article254275213.html.

Cline, Travis, and J. Dietz. “Agent Based Modeling for Low-Cost Counter UAS Protocol in Prisons.” *International Journal of Aviation, Aeronautics, and Aerospace* 7, no. 2 (2020): 1–17. https://doi.org/10.15394/ijaaa.2020.1462.

Community Tool Box. “Section 3. Developing Multisector Task Forces or Action Committees for the Initiative.” Learn a Skill Chapter 9. Developing an Organizational Structure for the Initiative. Accessed May 22, 2022. https://ctb.ku.edu/en/table-of-contents/structure/organizational-structure/multisector-task-forces/main.

CrowdStrike. “What Is the Cyber Kill Chain? Process & Model.” Cybersecurity 101: The Fundamentals of Cybersecurity, April 22, 2021. https://www.crowdstrike.com/cybersecurity-101/cyber-kill-chain/.

Cuffari, Joseph V. *DHS Has Limited Capabilities to Counter Illicit Unmanned Aircraft Systems*. OIG-20-43. Washington, DC: Department of Homeland Security Office of Inspector General, 2020. https://permanent.fdlp.gov/gpo144914/OIG-20-43-Jun20.pdf.

Customs and Border Protection. “About CBP.” U.S. Customs and Border Protection, February 24, 2022. https://www.cbp.gov/about.

Cybersecrutiy & Infrastructure Security Agency. “Unmanned Aircraft Systems (UAS) – Critical Infrastructure.” Cybersecurity and Infrastructure Security Agency. Accessed February 21, 2022. https://www.cisa.gov/uas-critical-infrastructure.

Davies, Roger. “The History of the IED Explained.” AOAV – Action on Armed Violence, October 15, 2020. https://aoav.org.uk/2020/the-history-of-the-ied-explained/.

Dedrone. “Map of Worldwide Drone Incidents.” Worldwide Drone Incidents. Accessed February 21, 2022. https://www.dedrone.com/resources/incidents/all?bd17d29f_page=2.

Department of Defense. *Counter-Small Unmanned Aircraft Systems Strategy*. Washington, DC: Department of Defense, 2021. https://media.defense.gov/2021/Jan/07/2002561080/-1/-1/1/department-of-defense-counter-small-unmanned-aircraft-systems-strategy.pdf.

Department of Homeland Security. “If You See Something, Say Something.” Department of Homeland Security. Accessed February 28, 2022. https://www.dhs.gov/see-something-say-something.

———. “Special Event Assessment Rating (SEAR) Events Fact Sheet.” Washington, DC: Department of Homeland Security, 2022. https://www.dhs.gov/publication/special-event-assessment-rating-sear-events-fact-sheet.

Department of Justice. “9-95.000 – Unmanned Aircraft Systems (UAS).” Justice Manual, November 26, 2019. https://www.justice.gov/jm/9-95000-unmanned-aircraft-systems-uas.

———. “Interagency Issues Advisory on Use of Technology to Detect and Mitigate Unmanned Aircraft Systems.” Justice News, August 17, 2020. https://www.justice.gov/opa/pr/interagency-issues-advisory-use-technology-detect-and-mitigate-unmanned-aircraft-systems.

———. “Northampton County Man Sentenced to Five Years for Using Drone to Harass Ex-Girlfriend, Illegally Possessing Bombs and Guns.” U.S. Attorneys Eastern District of Pennsylvania News, September 24, 2020. https://www.justice.gov/usao-edpa/pr/northampton-county-man-sentenced-five-years-using-drone-harass-ex-girlfriend-illegally.

———. “Unmanned Aircraft Systems.” Office of Legal Policy, April 29, 2022. https://www.justice.gov/olp/unmanned-aircraft-systems.

Dilanian, Ken. “Kamikaze Drones: A New Weapon Brings Power and Peril to the U.S. Military.” NBC News, December 6, 2021. https://www.nbcnews.com/news/military/kamikaze-drones-new-weapon-brings-power-peril-u-s-military-n1285415.

DJI Enterprise. “The Use of Drones in Agriculture Today.” *DJI Enterprise* (blog), September 18, 2021. https://enterprise-insights.dji.com/blog/drones-in-agriculture.

Drug Enforcement Administration. “DEA Mission Statement.” Mission. Accessed March 15, 2022. https://www.dea.gov/about/mission.

———. “Our History.” Drug Enforcement Administration. Accessed May 6, 2022. https://www.dea.gov/about/history.

Electronic Frontier Foundation. “Drones/Unmanned Aerial Vehicles.” Street Level Surveillance, August 28, 2017. https://www.eff.org/pages/dronesunmanned-aerial-vehicles.

Environmental Protection Agency. “Radionuclide Basics: Cesium-137.” Radiation Protection, July 5, 2022. https://www.epa.gov/radiation/radionuclide-basics-cesium-137.

"Evaluating the Task Force Model." *TELEMASP Bulletin* 9, no. 3 (June 2002): 1–7. ProQuest.

Federal Aviation Administration. "Federal Government Expands UAS Partnerships." Department of Transportation, March 16, 2016. https://www.faa.gov/newsroom/federal-government-expands-uas-partnerships.

———. "Offices." Security and Hazardous Materials Safety. Accessed March 24, 2022. https://www.faa.gov/about/office_org/headquarters_offices/ash/ash_offices.

Federal Bureau of Investigation. "Violent Gang Task Forces." What We Investigate. Accessed May 6, 2022. https://www.fbi.gov/investigate/violent-crime/gangs/violent-gang-task-forces.

Federation of American Scientists. "Biological, Chemical, & Other Non-Nuclear Threats." Federation of American Scientists. Accessed May 7, 2022. https://fas.org/issues/biological-chemical-and-other-non-nuclear-threats/.

Fortem Technologies. "DroneHunter® F700." Fortem Technologies. Accessed September 26, 2021. https://fortemtech.com/products/dronehunter/.

Gallagher, Sean. "German Chancellor's Drone 'Attack' Shows the Threat of Weaponized UAVs." Ars Technica, September 18, 2013. https://arstechnica.com/information-technology/2013/09/german-chancellors-drone-attack-shows-the-threat-of-weaponized-uavs/.

Headquarters, Department of the Army, Deputy Chief of Staff, G-3/5/7. "Joint Counter-Small Unmanned Aircraft Systems Office." STAND-TO!, August 27, 2021. https://www.army.mil/standto/archive/2021/08/27/.

Hebert, Adam. "Compressing the Kill Chain." *Air Force Magazine*, March 1, 2003. https://www.airforcemag.com/article/0303killchain/.

Hoshiko, Kentaro. "ISIS' Drone Fleet." *The Intelligencer* (blog), May 17, 2017. https://www.phc.edu/intelligencer/isis-drone-fleet.

Hospelhorn, Sarah. "What Is the Cyber Kill Chain and How to Use It Effectively." *Inside Out Security* (blog), June 20, 2016. https://www.varonis.com/blog/cyber-kill-chain.

Joint Chiefs of Staff. *Joint Planning*. JP 5-0. Washington, DC: Joint Chiefs of Staff, 2020. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp5_0.pdf.

Kallenborn, Zackary, and Philipp Bleek. "Drones of Mass Destruction: Drone Swarms and the Future of Nuclear, Chemical, and Biological Weapons." War on the Rocks, February 14, 2019. https://warontherocks.com/2019/02/drones-of-mass-

destruction-drone-swarms-and-the-future-of-nuclear-chemical-and-biological-weapons/.

Kelly, Erin. "Venezuela Drone Attack: Here's What Happened with Nicolas Maduro." *USA TODAY*, August 6, 2018. https://www.usatoday.com/story/news/politics/2018/08/06/venezuela-drone-attack-nicolas-maduro-assassination-attempt-what-happened/913096002/.

Krueger, David M. "Drone Federalism Act Seeks to Curb Call for 'Anti-Drone' Technology." Lexology, September 21, 2017. https://www.lexology.com/library/detail.aspx?g=2ebbeb3c-eb91-465e-ab48-de253fd12179.

Lacdan, Joseph. "Army to Lead New DOD Strategy against Drone Attacks." Army News Service. www.army.mil, January 11, 2021. https://www.army.mil/article/242276/army_to_lead_new_dod_strategy_against_drone_attacks.

Larter, David. "SOCOM Commander: Armed ISIS Drones Were 2016's 'Most Daunting Problem.'" Defense News, May 16, 2017. https://www.defensenews.com/digital-show-dailies/sofic/2017/05/16/socom-commander-armed-isis-drones-were-2016s-most-daunting-problem/.

Loughran, Jack. "Greenpeace Crashes Superman Drone into French Nuclear Power Plant." *E&T*, July 4, 2018. https://eandt.theiet.org/content/articles/2018/07/greenpeace-crashes-superman-drone-into-french-nuclear-power-plant/.

Maksel, Rebecca. "D.A.S.H. Goes to War." *Air & Space Magazine*, March 2012. https://www.smithsonianmag.com/air-space-magazine/dash-goes-to-war-23369442/.

Martin, Robert A. "The Joint Terrorism Task Force: A Concept That Works." *FBI Law Enforcement Bulletin* 68, no. 3 (March 1999): 23–27. ProQuest.

Minks, Cody. "Hacking the Silos: Eliminating Information Barriers between Public Health and Law Enforcement." Master's thesis, Naval Postgraduate School, 2018. http://hdl.handle.net/10945/58345.

Moritz, John. "Former CT College Student behind Viral 'Flying Gun' Video Has Convictions Overturned." CT Insider, November 30, 2021. https://www.ctinsider.com/news/article/Former-CT-college-student-behind-viral-Flying-16662141.php.

Organisation for the Prohibition of Chemical Weapons. "History: Looking Back Helps Us Look Forward." About Us: We Want to Live in a World Free of Chemical Weapons. Accessed February 14, 2022. https://www.opcw.org/about/history.

Patel, Bhargav, and Dmitri Rizer. *Counter-Unmanned Aircraft Systems Technology Guide*. CUAS-T-G-1. Washington, DC: Department of Homeland Security, 2020. https://www.dhs.gov/sites/default/files/publications/c-uas-tech-guide_final_28feb2020.pdf.

Ramachandran, Sudha. "Drone Attacks on Military Installation Rattle India's Security Establishment." *The Diplomat*, June 30, 2021. https://thediplomat.com/2021/06/drone-attacks-on-military-installation-rattle-indias-security-establishment/.

Rammer, Hollis. "OPCW Confirms Chemical Weapons Use in Syria." *Arms Control TODAY*, August 2021. https://www.armscontrol.org/act/2021-07/news-briefs/opcw-confirms-chemical-weapons-use-syria.

Ripley, Will. "Drone with Radioactive Material Found on Japanese Prime Minister's Roof." CNN, April 22, 2015. https://www.cnn.com/2015/04/22/asia/japan-prime-minister-rooftop-drone/index.html.

Romo, Vanessa. "FBI Finds No Motive In Las Vegas Shooting, Closes Investigation." NPR National, January 29, 2019. https://www.npr.org/2019/01/29/689821599/fbi-finds-no-motive-in-las-vegas-shooting-closes-investigation.

Schaer, Cathrin, and Kersten Knipp. "Can Drone Warfare in the Middle East Be Controlled?" Deutsche Welle, January 7, 2021. https://www.dw.com/en/can-drone-warfare-in-the-middle-east-be-controlled/a-58111069.

Scott, Claire. "Corporate Espionage by Drone: Why Corporations Need Better Physical and Legal Protections." University, MS: University of Mississippi, School of Law, January 24, 2021. https://papers.ssrn.com/abstract=3772434.

Secretary of State for the Home Department. "UK Counter-Unmanned Aircraft Strategy." Home Office, October 21, 2019. https://www.gov.uk/government/publications/uk-counter-unmanned-aircraft-strategy.

Smith, Jacqueline. "Radicalization of Life Scientists to Terrorism." Master's thesis, Georgetown University, 2011. http://hdl.handle.net/10822/553586.

Stevenson, Mark. "Mexican Army: Explosive Drone Attacks in at Least 3 States." Media. AP News, April 21, 2021. https://apnews.com/article/latin-america-cb836518d514b68850607a1eca24a7bd.

Strategic-Air-Command. "Chart of Strategic Nuclear Bombs." Nuclear Weapons in the Strategic Air Command Arsenal. Accessed February 17, 2022. http://www.strategic-air-command.com/weapons/nuclear_bomb_chart.htm.

Sullivan, John P., Robert J. Bunker, and David A. Kuhn. “Mexican Cartel Tactical Note #38: Armed Drone Targets the Baja California Public Safety Secretary’s Residence in Tecate, Mexico | Small Wars Journal.” Small Wars Journal, August 6, 2018. https://smallwarsjournal.com/jrnl/art/mexican-cartel-tactical-note-38-armed-drone-targets-baja-california-public-safety.

Tahir, Anam, Jari Boling, Mohammad-Hashem Haghbayan, Hannu Toivonen, and Juha Plosila. “Swarms of Unmanned Aerial Vehicles — A Survey.” *Journal of Industrial Information Integration* 16 (December 1, 2019): 1–7. https://doi.org/10.1016/j.jii.2019.100106.

Tan, Choon Seng, Douglas L. Van Bossuyt, and Britta Hale. “System Analysis of Counter-Unmanned Aerial Systems Kill Chain in an Operational Environment.” *Systems* 9, no. 4 (2021): 1–27. https://doi.org/10.3390/systems9040079.

Tedesco, Matthew T. “Countering the Unmanned Aircraft Systems Threat.” *Military Review* 95, no. 6 (December 2015): 64–69. https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20151231_art012.pdf.

Thompson, Rob. “The Problems with Counter UAS (CUAS): How to Move the Industry Forward.” sUAS News – The Business of Drones, April 23, 2018. https://www.suasnews.com/2018/04/the-problems-with-cuas-how-to-move-the-industry-forward/.

Transportation Security Administration. “Counter-Unmanned Aircraft Systems (C-UAS) Program Briefing.” In *Asia-Pacific Economic Cooperation (APEC 2021)*. New Zealand, 2021. http://mddb.apec.org/Documents/2021/TPTWG/AEG-TM1/21_tptwg_aeg_tm1_002.pdf.

Trump, Donald J. *National Counterterrorism Strategy for the United States of America*. Washington, DC: White House, 2018. https://www.dni.gov/files/NCTC/documents/news_documents/NSCT.pdf.

United States Congress. “Committees of the U.S. Congress.” Library of Congress. Accessed May 6, 2022. https://www.congress.gov/committees.

United States Secret Service. “About Us.” United States Secret Service. Accessed March 15, 2022. https://www.secretservice.gov/about/overview.

———. “National Special Security Events Credentialing.” Securing Events. Accessed February 24, 2022. https://www.secretservice.gov/protection/events/credentialing.

University of Alabama in Huntsville. “ASSURE Announces Results of UAH-Led Drone Ground Collision Study.” University of Alabama in Huntsville News, August 14, 2019. https://www.uah.edu/news/news/assure-announces-results-of-uah-led-drone-ground-collision-study.

Vyas, Kashyap. “A Brief History of Drones: The Remote Controlled Unmanned Aerial Vehicles (UAVs).” Interesting Engineering, June 29, 2020. https://interestingengineering.com/a-brief-history-of-drones-the-remote-controlled-unmanned-aerial-vehicles-uavs.

Wang, Jian, Yongxin Liu, and Houbing Song. “Counter-Unmanned Aircraft System(s) (C-UAS): State of the Art, Challenges and Future Trends.” *IEEE Aerospace and Electronic Systems Magazine* 36, no. 3 (March 2021): 4–29. https://doi.org/10.1109/MAES.2020.3015537.

Willman, David, and Melody Petersen. “Terrorists Could Make a Dirty Bomb from This Common Medical Device.” *Los Angeles Times*, December 27, 2019. https://www.latimes.com/politics/story/2019-12-27/cesium-137-dirty-bomb.

Wood, Poppy. “UK Intelligence Examining Reports of Russia Chemical Attack in Ukraine Will Be Scouring Flight Paths for Drone.” iNews, April 12, 2022. https://inews.co.uk/news/world/western-intelligence-drones-alleged-chemical-weapons-attack-1571749.

# INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California