Emerging Drone Risks and Protective Measures: A Study on the Western Interconnection Electrical Grid

Dissertation Manuscript

Submitted to National University

School of Business and Economics

in Partial Fulfillment of the

Requirements for the Degree of

DOCTOR OF PHILOSOPY IN BUSINESS ADMINISTRATION

by

JUSTIN WERNER

San Diego, California

November 2025

Approval Page

Abstract

The rapid growth of low-cost unmanned aerial vehicles (UAVs) has introduced new risks for U.S. critical infrastructure. The problem to be addressed by this study will be the threat that current and emerging aerial drone technologies pose to the Western Interconnection electrical power grid, as perceived by subject matter experts (SME) from the U.S. Department of Energy (DOE), the Federal Energy Regulatory Commission (FERC), and the Western Electricity Coordinating Council (WECC). The purpose of this descriptive qualitative study is to analyze and identify the severity of risk posed by current and emerging commercial aerial drone technology to America's Western Interconnection Electrical Grid Infrastructure. Data were gathered via an IRB-approved anonymous survey of 24 subject matter experts (SMEs) with follow-up interviews. Open-ended responses addressed (a) perceived UAV risk levels, (b) SME concern, and (c) adequacy of counter-UAS measures and interagency coordination. Thematic analysis revealed that SMEs view the grid as vulnerable due to gaps in detection, statutory authorities, and coordinated response protocols. Most rated current protections only slightly or moderately effective, with no SME identifying safeguards as highly effective; interagency coordination was assessed as minimal to moderate. Findings highlight the need for stronger policies and cross-agency collaboration. Recommendations include integrating counter-UAS scenarios into training, expanding statutory authorities, and investing in layered detection and mitigation systems. The study contributes stakeholder-driven insights at the unclassified level and offers guidance for regulators and practitioners seeking to strengthen energy infrastructure security against evolving aerial threats.

Acknowledgements

This dissertation represents the culmination of years of dedication, perseverance, and support from those who have stood beside me throughout this journey. It is with deep gratitude that I recognize the individuals whose encouragement, guidance, and sacrifices made this work possible.

To my wife, your steadfast love, patience, and belief in me have been the foundation upon which this accomplishment rests. You carried burdens and made sacrifices that allowed me to pursue this demanding goal, and for that I am forever grateful. To my children, your joy and curiosity continually inspired me to press forward. I hope this work serves as an example to you both of what can be achieved with perseverance and determination.

To my parents, I thank you both for instilling in me the values of hard work, resilience, and commitment. Your unwavering support and encouragement throughout my life provided the foundation for every step of this academic and professional journey.

To my dissertation committee, I extend my sincere appreciation. To my chair, Dr. Dave Lowery, thank you for your steady guidance, thoughtful critiques, and mentorship that kept me focused and accountable. To Dr. Leila Sopko and Dr. Jeremy Buchanan, thank you for your invaluable insights, feedback, and support throughout this process. Each of you has played an essential role in shaping the quality and rigor of this dissertation.

Finally, to all who offered encouragement, whether through words and/or support, I am indebted to you. This work is not solely my own but the result of a community of family, mentors, and colleagues who stood with me every step of the way.

Table of Contents

Chapter 1: Introduction 1

- Statement of the Problem 5
- Purpose of the Study 6
- Introduction to Theoretical Framework 7
- Introduction to Research Methodology and Design (Nature of the Study) 10
- Research Questions 11
- Significance of Study 12
- Definitions of Key Terms 13
- Summary 18

Chapter 2: Literature Review 20

- Theoretical Framework 23
- Other Considered Theories 26
- Stakeholder Theory 30
- Technology Risk Assessment 34
- Technical Capabilities 49
- Critical Infrastructure Protection (CIP) 60
- Regulatory Adaptation to Technological Advancements 69
- Summary 74

Chapter 3: Research Method 77

- Research Methodology and Design (Nature of the Study) 79
- Population and Sample 89
- Instrumentation 96
- Study Procedures 99
- Data Analysis 100
- Assumptions 105
- Limitations 108
- Delimitations 110
- Ethical Assurances 112
- Summary 115

Chapter 4: Findings 116

- Trustworthiness of the Data 118
- Results 123
- Evaluation of Findings 164
- Summary 172

Chapter 5: Implications, Recommendations, and Conclusion 174

- Implications 175
- Recommendations for Practice 183

Recommendations for Future Research 185
Conclusion 186

References 187

Appendix A Search Terms, Combinations, and Categories 205

Appendix B History of Drone Technology Development 212

Appendix C Study Letter Outlining Research Instrumentation and Eligibility Criteria 213

Appendix D Online Anonymous Survey Consent 215

Appendix E Consent Letter for Adult One-on-One Interview Zoom Participants 217

Appendix F Survey/Interview Questions Specific to Each Research Question 221

List of Tables

Table 1 Listing of SME non-identifiable demographics 125
Table 2 Listing of the two Individual 'Second Wave' Interviewees 160
Table 3 Top Three Themes for Research Question #1 165
Table 4 Top Theme for Research Question #2 167
Table 5 Top Three Theme for Research Question #3 169

List of Figures

Figure 1 Key UAV Technology Building Blocks 38
Figure 2 Overview of Chronology of Drone Technology Terms 48
Figure 3 Overview of the 5 Levels of Drone Autonomy 53
Figure 4 Gender of Online Survey Participants 126
Figure 5 Age of Online Survey Participants 127
Figure 6 Education Level of Online Survey Participants 128
Figure 7 Relevant Professional Experience of Online Survey Participants 129
Figure 8 Approximate Age of Online Survey Participants 130
Figure 9 Survey Question #6 Results 133
Figure 10 Survey Question #7 Results 134
Figure 11 Survey Question #8 Results 136
Figure 12 Survey Question #9 Responses 138
Figure 13 Survey Question #10 Results 142
Figure 14 Survey Question #11 Results 143
Figure 15 Survey Question #12 Results 144
Figure 16 Survey Question #13 Results 147
Figure 17 Survey Question #14 Results 149
Figure 18 Survey Question #15 Results 151
Figure 19 Survey Question #16 Results 153
Figure 20 Breakdown of One-on-One Interview Participants' Genders 161
Figure 21 Age of Individual Interview Participants 162
Figure 22 Education Level of Individual Interview Participants 162
Figure 23 Relevant Professional Experiences of Individual Interview Participants 163
Figure 24 Race/Ethnicity of Individual Interview Participants 163

Chapter 1: Introduction

In her paper, Alyssa Sims (2018) explained that the term "drone" is predominantly used to define an Unmanned Aerial Vehicle (UAV) or Remotely Piloted Aircraft (RPA), which operates without an onboard pilot or operator. Officially, the U.S. Federal Aviation Administration (FAA) Modernization and Reform Act of 2012, as defined in U.S. Code: Title 49 Transportation, Chapter 448: Unmanned Aircraft Systems (2018), the FAA's definition of Unmanned Aircraft Systems (UAS) encompasses both the unmanned aircraft and all required equipment for its secure and efficient function. Within this system, the UAV is the key component.

On September 28, 2005, the FAA initially granted an airworthiness certificate for a civilian UAS to the drone manufacturer General Atomics Altair (Timeline of Drone Integration [TDI], 2022). This certification emerged from a collaborative effort between the FAA and General Atomics Altair, aiming to amass technical and operational data to facilitate the formulation of UAS regulatory frameworks (TDI, 2022). Since that initial certificate was issued in September 2005, 790,918 commercial and recreational drones have been registered with the FAA nation-wide in order to ensure compliance with federal regulations and safety standards (Drones by the Numbers, 2023).

In June 2006, the FAA reached an initial agreement with the Air Force to allow the deployment of UASs in civilian airspace during emergencies (TDI, 2022). This decision was influenced by the potential use of UASs like the MQ-9 Reaper and RQ-4 Global Hawk in disaster response, as evidenced by the need for real-time imagery and data during Hurricane Katrina's aftermath. Reaper drones were pivotal in these rescue missions given that they were equipped with thermal imaging cameras capable of detecting human heat signatures from an

altitude of 10,000 feet (TDI, 2022). This agreement marked a significant step in integrating military UAS capabilities into civilian disaster response efforts.

This growing adoption of drones has raised concerns pertaining to the safety and security of facilities and critical infrastructure throughout the United States. Notable incidents over the past decade include a quadcopter drone crash on the White House grounds and another on the White House Ellipse (Department of Homeland Security, 2021). Although these drones were not weaponized and posed no immediate threats, these incidences brought attention to the susceptibility of apparently secure areas to commercially accessible drone technologies.

The potential risks associated with drone technology encompass both safety and privacy concerns (Zwickle et al., 2018). Safety hazards are attributed to the possibility of drones being inadvertently or deliberately crashed into individuals or groups (Kallenborn et al., 2022). Privacy threats extend to private citizens as well as corporate and government entities, considering drones can operate at altitudes varying from ground level to the standard consumer-grade drone altitude limit of 400 feet. These drones often carry advanced imaging technology, with some equipped with cameras boasting 3840x2160 pixel resolution, commonly known as 4K, enabling the capture of highly detailed imagery and videos from previously unconsidered distances and altitudes, which poses significant challenges to infrastructure protection and countermeasures against corporate espionage (Kallenborn et al., 2022; TDI, 2022).

The accessibility of commercial drone technology, coupled with its capacity for modification using readily available materials, presents a significant threat to critical infrastructure. This includes, but is not limited to, power relay stations, where the deployment of small explosive devices via drones could have catastrophic consequences (Lappas et al., 2022). The Islamic State of Iraq and Syria (ISIS), a designated foreign terrorist organization (FTO), has

quickly adopted and militarized this technology, effectively weaponizing commercial quadcopter drones for terroristic purposes (Sims, 2018; U.S. Department of State, 2019). A notable instance occurred during the Battle of Mosul in Mosul, Iraq, where ISIS conducted over 300 drone operations, approximately 100 of which involved armed attacks using modified commercially available drones (Kallenborn et al., 2022).

The appeal of off-the-shelf drones lies in their affordability, ease of modification and operation, and the considerable challenge they pose to defense systems. Even unmodified drones, when maneuvered with malicious intent, pose a significant threat to infrastructure, as these drones can be deliberately flown into targets/structures with the explicit intent to damage (Lappas et al., 2022). Other FTOs, including Ḥarakat al-Muqāwamah al-ʾIslāmiyyah (HAMAS), Hizb'allah, and various non-state actors, have either attempted or succeeded in using drone technology to conduct terroristic activities/attacks. Advancements in drone technology now enable a single pilot to control a swarm of drones, or alternatively, to program drones to follow pre-loaded flight plans autonomously. This technological evolution raises the threat of mass coordinated terrorist attacks on critical infrastructures, such as power plants, water treatment facilities, hospitals, and law enforcement agencies, potentially orchestrated by a minimal number of operators or even a single individual (Department of Homeland Security, 2021).

An instance of such a multi-drone attack within the United States was reported at the Palo Verde Generation Station, the nation's largest nuclear power plant. In September 2019, security personnel documented multiple large drones, equipped with spotlights, operating at altitudes of 200 to 300 feet above ground within secure areas of the plant over two consecutive nights (Rogoway & Trevithich, 2020). The drones loitered in these areas for approximately an hour on the second night. To date, the identity or identities of the perpetrators remain undisclosed to the

public, and it is believed that non-state actors were responsible for this coordinated multi-drone surveillance attack (Rogoway & Trevithich, 2020).

The United States' electrical power grid is divided into three major regions: the Eastern Interconnection, the Western Interconnection, and the Texas Interconnected system. The focus of this study will be the Western Interconnection, which spans from the Pacific Ocean to the Rocky Mountain states and is managed by the Western Electricity Coordinating Council (WECC). The WECC oversees an extensive network comprising more than 1.8 million square miles across 14 states, the Canadian provinces of British Columbia and Alberta, and the northern portion of Baja California in Mexico, serving over 80 million people and businesses (Western Interconnection, 2023).

The WECC's electrical power grid system includes 5,032 power generators of diverse types, transmission lines, substations, natural gas pipelines, and over 136,000 miles of transmission lines servicing to both residential and commercial needs (Western Interconnection, 2023). While this study will primarily focus on these larger infrastructures, it acknowledges the existence of smaller power-related subsystems within the WECC Grid. These subsystems, although not the central focus, play a crucial role in maintaining the overall stability and efficiency of the grid.

Haugstvedt (2023) pointed out that as drone technology continues to evolve, drones will be capable of achieving higher speeds and carrying heavier payloads as well as becoming more accessible and cost-effective. These advancements facilitate the weaponization of drones in both offensive (e.g., illicit surveillance, carrying hazardous payloads, smuggling) and defensive (e.g., security monitoring) capacities. Consequently, even small commercially available drones could

pose a threat to the Western Interconnection electrical power grid and the people, businesses, and corporations reliant on its services (EPA, 2019).

Statement of the Problem

The problem addressed by this study was the threat that current and emerging aerial drone technologies pose to the Western Interconnection electrical power grid, as perceived by subject matter experts (SME) from the U.S. Department of Energy (DOE), the Federal Energy Regulatory Commission (FERC), and the Western Electricity Coordinating Council (WECC). This research study aimed to delineate the perceived risk level of these technologies to the Western Interconnection infrastructure (Franke et al., 2023; Rogers & Kunertova, 2022). The study also assessed the level of concern among these experts and evaluated their perception of the adequacy of current protective measures against potential drone technology attacks.

The Western Interconnection electrical power grid, overseen by the WECC, spans over 1.8 million square miles across 14 states, parts of Canada, and Mexico, supporting over 80 million individuals and businesses (Western Interconnection, 2023). It comprises 5,032 power generators, extensive transmission lines, substations, and natural gas pipelines, serving a wide range of residential and commercial needs (Western Interconnection, 2023). This infrastructure is vital for the daily lives of U.S. residents, powering industries and homes alike (Western Interconnection, 2023; McBride & Siripurapu, 2021).

Since the FAA (2024) issued the first UAV airworthiness certificate on September 28, 2005, drone technology has significantly evolved, expanding its use among private citizens, organizations, and various professional sectors including agriculture, real estate, and infrastructure maintenance. This widespread adoption spans enthusiasts, local governments, and

federal agencies. However, the pace of regulatory adaptation to these rapid advancements has been slow (Alsoliman et al., 2023; Haugstvedt, 2023; Rogers & Kunertova, 2022; FAA, 2022b).

The advancement of drone technology raises potential security concerns for critical infrastructures like the Western Interconnection electrical grid. Federal agencies, including the DOE, FERC, and WECC, are examining these implications to refine protective measures. Research by Franke et al. (2023) as well as Rogers and Kunertova (2022) underscored the need for continuous evaluation in addressing the risks drones pose to the U.S. electrical grid.

Purpose of the Study

The purpose of this descriptive qualitative study was to analyze and identify the severity of risk posed by current and emerging commercial aerial drone technology to America's Western Interconnection Electrical Grid Infrastructure. Due to advancements in drone technology and its increased use by companies and hobbyists, there is a pressing need, as identified by Krichen et al. (2022), to address new security and safety challenges faced by both private and federal agencies in safeguarding the Western Interconnection's geographically vast and technically complex power grid. This study aimed to systematically quantify the associated risks, with a specific focus on assessing the perspectives and defined responsibilities of DOE, FERC, and WECC personnel in addressing potential threats. Additionally, it sought to develop and recommend effective solutions to mitigate these risks.

Utilizing a qualitative research design, this study proactively gathered and analyzed numerical and descriptive data to ascertain the magnitude and severity of perceived risks by key entities, specifically the DOE, the FERC, and the WECC. This was achieved through the implementation of structured surveys, designed to elicit detailed responses on the potential threats posed by drones. The collated data provided insights into the perceived vulnerability of

the Western Interconnection network, encompassing power plants, transmission lines, substations, and distribution centers across 14 states, as seen by these major regulatory and oversight bodies, thereby affecting the security of a network that serves over 80 million people (McBride & Siripurapu, 2021; Western Interconnection, 2023).

Data collection involved formal National University Institutional Review Board (IRB) approval in order to conduct an anonymous online survey targeting professionals from professionally recruited/solicited DOE, FERC, and WECC subject matter experts. The research questionnaire utilized open-ended questions to gather rich, qualitative data. These questions were designed to elicit detailed responses and insights from participants, allowing for an in-depth understanding of their perspectives and experiences. Finally, the survey was followed by interviews of participants willing to participate in follow-up questioning conducted via electronic means (e.g., phone, zoom, Microsoft Teams, etc.).

This qualitative research study was designed to enhance the contemporary academic understanding of both current and prospective risks posed by drones to the Western Interconnection Electrical Grid. Its aim was to inform the creation of effective strategies for mitigating and countering potential drone-induced threats to the electrical infrastructure. The findings of this study were expected to broaden knowledge on safeguarding electrical infrastructures throughout the United States, at the unclassified level, against drone threats.

Introduction to Theoretical Framework

The first two decades of the 21st century have marked a period of significant technological transformations, influencing various facets of personal life, business operations, and global commerce. This research study employed a multi-disciplinary approach to integrate three interrelated concepts: Technology Risk Assessment, Critical Infrastructure Protection

(CIP), and Regulatory Adaptation to Technological Advancements. This evaluatory construct was essential, considering the rapid pace of drone technological advancements and their growing use across the United States, as there are currently there are over 1.1 million recreational drones registered with the FAA (Current Unmanned Aircraft State Law Landscape, 2023). Overall, this research topic confronted a dual challenge by first seeking to quantify the current and future threat levels posed by existing and emerging drone technologies, then forecasting these threats over the next decade, relying on current technological trends and predictive analyses.

University of Virginia Professor R. Edward Freeman's (1984, 2010, 2015) Stakeholder Theory provided the core of this study's research framework; specifically, it emphasized the importance of understanding and aligning the interests of all stakeholders. Within the context of this research study, Stakeholder Theory was applied to drone technology and infrastructure protection. This approach underscored the interconnectedness not just of system components, but of diverse stakeholder perspectives, including technological, human, environmental, and organizational elements that influence and are influenced by one another. By adopting a stakeholder perspective, the study identified the complex interactions and expectations concerning drones and critical infrastructures between stakeholders such as regulators, businesses, local communities, and environmental groups, and highlighted how the actions or changes impacting one group of stakeholders can have cascading effects on the whole system.

Freeman's (1984, 2010, 2015) Stakeholder Theory also supports the development of an integrated approach to risk assessment and management, emphasizing that effective protection of critical infrastructures requires understanding and considering the diverse values and objectives of all stakeholder groups. This approach aids in pinpointing vulnerabilities and interdependencies from a stakeholder impact perspective, which may not be apparent when

examining technological or infrastructural components in isolation. Moreover, it guides the regulatory adaptation process by highlighting the need for comprehensive policies that address the multifaceted impacts of drone technologies across various stakeholder dimensions.

By integrating Stakeholder Theory, this study aimed to devise strategies that enhance the systemic resilience and robustness of critical infrastructures, ensuring they can effectively anticipate, manage, and mitigate disruptions caused by advanced drone technologies. This broader, more inclusive perspective supports the development of more effective governance and management strategies. Such an approach is essential for keeping pace with rapid technological advancements in the drone sector (Rogers & Kunertova, 2022).

The first component of this research study's framework was the concept of Technology Risk Assessment. This involved a thorough analysis of the evolving capabilities of drone technology, including their increased range, payload capacity, and autonomous functions. The assessment construct itself extended to understanding how easily these technologies can be accessed and potentially misused by various entities, ranging from hobbyists to hostile actors (Kalinin et al., 2021; El Marady & Rahouma, 2021). This facet of the framework was vital for evaluating the range and severity of threats drone technologies may pose to critical infrastructures, especially in scenarios where they could be used for surveillance, unauthorized data collection, or even direct sabotage.

The second component of this research study's framework was Critical Infrastructure Protection (CIP). This concept stressed the imperative of safeguarding essential systems and assets, with a specific emphasis on the electrical grid (Barka et al., 2019). Given its criticality to national security and public welfare, the electrical grid's vulnerability to drone-related disruptions or attacks is a major concern (Chowdhury & Gkioulos, 2021). The framework will

delve into existing and innovative strategies and methodologies within CIP, analyzing how they can be tailored to counteract the specific challenges drones present. This includes exploring physical and cybersecurity measures, emergency response protocols, and resilience-building strategies to enhance the grid's defenses against potential drone intrusions or attacks (Calandrillo et al., 2020; Kalinin et al., 2021).

The final component of the research study's framework pertained to Regulatory Adaptation to Technological Advancements. This aspect involved a critical examination of how regulatory bodies, notably the FAA and other pertinent federal agencies, have reacted to the swift development and widespread use of drone technology (Calandrillo et al., 2020), and focused on understanding the evolution of regulatory frameworks, pinpointing current gaps, and identifying the challenges faced by these agencies in keeping pace with technological advancements (Sukamto et al., 2023). This exploration highlighted the necessity for dynamic and flexible regulatory approaches that can promptly adapt to emerging risks, while also fostering the responsible use of drone technology.

This study endeavored to take a crucial step toward ensuring the security and continued functionality of a key component of America's critical infrastructure nation-wide. As drone technology continues to evolve and proliferate, the urgency of understanding and mitigating its potential risks to the Western Interconnection cannot be overstated. The research represented a proactive approach to a growing and dynamic challenge, aiming to contribute significantly to national security and the safety of millions of Americans who rely on the Western Interconnection for their daily energy needs.

Introduction to Research Methodology and Design (Nature of the Study)

This study adopted a qualitative research design to explore the impact of commercially available aerial drones on the physical infrastructure of America's Western Interconnection Electrical Grid. It combined numerical analysis through surveys with in-depth qualitative assessments of SMEs inputs, shared experiences, and recommendations to comprehensively evaluate potential threats (Creswell, 2013; Denzin et al., 2023, pp. 121–141). This study aimed to engage a final sample of 30 participants, who are professional SMEs in their respective fields of functional specialization from. Initial contacts were made with key SMEs from the DOE, the FERC, and the WECC with active employment of professional snowballing techniques as much as possible in order to recruit additional experts, targeting vital areas such as Electrical Engineering and Grid Security, Aerospace and Drone Technology, Cybersecurity and Information Technology, Law Enforcement and Counterterrorism, and Regulatory and Policy expertise, until the target of 30 participants was achieved (Parker et al., 2019).

These fields were crucial for a holistic understanding of the multifaceted threats drones pose to grid security. To ensure a comprehensive overview, these experts represented a diverse range of geographic locations across the Western Interconnection Electrical Grid, including major power hubs in states like California, Oregon, and Washington, as well as rural and remote areas where the grid might be more vulnerable. Additionally, experts from cross-border regions near Canada and Mexico were included to evaluate international implications. The sample population was divided into three distinct groups: representatives from the DOE, the FERC, and WECC, capturing a broad spectrum of perspectives and expertise vital to the assessment of aerial threats to the grid infrastructure.

Research Questions

RQ1:

What is the perceived risk level among Subject Matter Experts (SMEs) from the DOE, FERC, and WECC, regarding the potential of current and near-future aerial drone technologies to cause damage or destruction to key aspects of the Western Interconnection Electrical Grid infrastructure?

RQ2:

What is the quantifiable level of concern among SMEs from the DOE, FERC, and WECC regarding current and near-future aerial drone technologies as a potential threat to the Western Interconnection Electrical Grid infrastructure?

RQ3:

What is the perceived adequacy of the measures taken by the DOE, FERC, and WECC in safeguarding the Western Interconnection Electrical Grid infrastructure from current and near-future aerial drone technology attacks?

Significance of Study

The research presented in this study explored the complex and rapidly evolving domain of UAVs and their significant implications for national security and critical infrastructure protection, with a particular emphasis on the Western Interconnection electrical power grid. This study was motivated by the acknowledgment of drones' transformative impact across civilian and military spectrums, characterized by swift technological advancements and emerging regulatory dilemmas. The importance of this research study stemmed from the urgent need to address the growing proliferation of drone technology that, despite offering substantial benefits for commercial and recreational uses, also presents formidable challenges to critical infrastructure, security, and privacy.

Addressing the core issue of this study, the threat posed by drones to the Western Interconnection, promised several significant benefits. Primarily, it aimed to bolster security measures to protect critical infrastructure against potential UAV intrusions while providing empirical insights to inform the refinement of regulatory frameworks, ensuring they effectively counteract the risks of misuse while accommodating technological progress. By examining the utilization of drones by FTOs, this research also underscored the criticality of devising proactive strategies to mitigate such threats, contributing to a more secure national security landscape.

In essence, this study constituted an in-depth investigation into the nexus between drone technology and infrastructure security. This study purposed to advance a nuanced understanding of the associated risks, regulatory challenges, and countermeasures. By situating this inquiry within the wider discourse on national security and technological advancement, the research aimed to pave the way toward more resilient infrastructure, informed regulatory approaches, and a deeper insight into the profound impact of UAVs on modern society.

Definitions of Key Terms

Air Force

The U.S. Air Force is the air service branch of the United States Armed Forces, providing rapid, flexible, and lethal air and space capability that can deliver forces anywhere in the world within hours (U.S. Department of Defense, 2022).

Airworthiness Certificate

A document issued by the FAA certifying that an aircraft is safe for flight (FAA, 2022a).

Artificial Intelligence (AI)

The simulation of human intelligence by machines, especially computer systems. It involves processes like learning, reasoning, and self-correction to perform tasks that typically

require human intelligence, such as visual perception, speech recognition, decision-making, and language translation (Helm et al., 2020).

Civilian Airspace

Airspace not designated for military or defense purposes, where civilian aircraft operate (FAA, 2020a).

Commercial

Operation of an uncrewed or model aircraft for profit and business activities (FAA, 2020b).

Coordinated Terrorist Attacks

Terrorist acts carried out simultaneously or in a planned sequence, potentially using drones, to maximize impact (Planning Considerations: Complex Coordinated Terrorist Attacks, 2018).

Corporate Espionage

The practice of using drones or other means to illegally acquire trade secrets or sensitive information from competitors (Barka et al., 2019).

Critical Infrastructure Protection (CIP)

Strategies and measures implemented to secure essential services and facilities from threats (Chowdhury & Gkioulos, 2021).

Critical Infrastructures

Essential systems and assets vital to a country's security, economy, and public health and safety, such as power plants and water supply systems (US EPA, 2019).

Department of Energy (DOE)

A cabinet-level department of the United States Government concerned with the United States' policies regarding energy and safety in handling nuclear material (US Department of Energy, 2023).

Drone

A remotely operated or autonomous flying vehicle, often used for surveillance, recreational, and increasingly for commercial purposes (Drones by the Numbers, 2023).

Eastern Interconnection

One of the two major AC power grids in North America, covering the area east of the Rocky Mountains (US Department of Energy, 2023).

Federal Aviation Administration (FAA)

The United States governmental body responsible for regulating all aspects of civil aviation in the U.S. (FAA, 2021).

FAA Modernization and Reform Act of 2012

Legislation aimed at improving the efficiency of the National Airspace System, the safety of aviation, and to modernize the air traffic control system (Mica, 2012).

Federal Energy Regulatory Commission (FERC)

An independent agency that regulates the interstate transmission of electricity, natural gas, and oil in the U.S. (Federal Energy Regulatory Commission, 2022).

Foreign Terrorist Organizations (FTO)

Designated by the U.S. Department of State, these are foreign organizations that engage in, or have the capability and intent to engage in, terrorist activity that threatens the security of U.S. nationals or the national security of the United States (U.S. Department of State, 2019).

General Atomics Altair

A high-altitude, long-endurance unmanned aircraft designed for scientific research and surveillance purposes (Timeline of Drone Integration [TDI], 2022).

Global Hawk Drone

Types of military drones used by the United States for reconnaissance and surveillance (U.S. Air Force, 2014).

Hizb'allah

A Shia Islamist political party and militant group based in Lebanon, also known to utilize drone technology (Rogers & Kunertova, 2022).

Ḥarakat al-Muqāwamah al-ʾIslāmiyyah (HAMAS)

A Palestinian Sunni-Islamic fundamentalist militant organization, known to have explored using drones for its activities (Rogers & Kunertova, 2022).

Islamic State of Iraq and Syria (ISIS)

A militant group known for using drones for surveillance and as weapons in conflict zones (Rogers & Kunertova, 2022).

Machine Learning (ML)

A subset of AI that focuses on developing algorithms that enable computers to learn from and make decisions based on data. Instead of being explicitly programmed, ML models improve their performance on tasks by identifying patterns and making inferences from training data. It includes types like supervised learning, unsupervised learning, and reinforcement learning (Helm et al., 2020).

Natural Gas Pipelines

Infrastructure used to transport natural gas from production sites to consumers and power plants (Western Interconnection, 2023).

Non-state Actors

Individuals or groups not affiliated with any specific nation's government, which may include terrorists, rebels, or private entities (U.S. Department of State, 2019).

Palo Verde Generation Station

The largest nuclear power plant in the U.S., located in Arizona.

Power Generators, Transmission Lines, Substations

Components of the electrical grid that generate, transmit, and distribute electricity to consumers (Western Interconnection, 2023).

Predator Drone

Type of military drone used by the United States as an intelligence-collection asset and secondarily against dynamic execution targets (U.S. Air Force, 2015).

Privacy Threats

Risks related to unauthorized surveillance and data collection by drones, infringing on individuals' privacy (Rogers & Kunertova, 2022).

Remotely Piloted Aircraft (RPA)

An unmanned aircraft that is piloted from a remote location (OLRC Home, 2018).

Recreational Drones

Drones used for personal enjoyment, leisure, or hobby (What Does the FAA Consider as Commercial Drone Use?, 2020).

Technology Risk Assessment

The evaluation of potential risks and vulnerabilities associated with the use or development of technology (Rogers & Kunertova, 2022).

Texas Interconnected System

An electric grid that covers most of Texas, managed by the Electric Reliability Council of Texas (ERCOT) (McBride & Siripurapu, 2021).

Thermal Imaging Cameras

Devices that detect heat and create images from that data, often used in drones for search and rescue operations (U.S. Air Force, 2015).

Unmanned Aerial Vehicle (UAV)

An aircraft piloted by remote control or onboard computers, not requiring a human pilot onboard (OLRC Home, 2018).

Unmanned Aircraft Systems (UAS)

Consists of the unmanned aircraft (the drone itself) and all of the associated support equipment, control station, data links, telemetry, communications and navigation equipment necessary to operate the unmanned aircraft (OLRC Home, 2018).

Weaponization of Drones

The modification of drones to carry and deploy weapons (Department of Homeland Security, 2021).

Western Electricity Coordinating Council (WECC)

A non-profit corporation responsible for coordinating and promoting bulk electric system reliability in the Western Interconnection of the U.S. (Western Electricity Coordinating Council - Overview, News & Similar Companies, 2024).

Summary

The introductory chapter of this research study set a comprehensive framework for examining the implications of drone technology on the security of the Western Interconnection electrical grid. It methodically defined the terminology, reviewed the historical context, and

outlined the regulatory landscape that has shaped the use and management of unmanned aerial vehicles. This section examined the significance of the electrical grid to national and public security, as well as the necessity to address the potential threats drones may pose.

This section also presented the problem statement and purpose of the study, detailing the concerns over safety, privacy, and the security of critical infrastructure in the face of advancing drone technology. Specifically, the defined research questions and hypotheses focused on explored the increasing utilization of drones across various sectors against a backdrop of slowly evolving regulations and raised questions about the effectiveness and vulnerabilities of current safety and privacy measures. By outlining the research methodology, which employed a qualitative approach, this section holistically assessed the perceived risks to the Western Interconnection and the current measures' effectiveness from the perspective of key stakeholders, which included the DOE, FERC, and the WECC among others.

Thus, this section not only identified the research gap but also emphasized the study's potential to contribute to the broader discussion on safeguarding national security and critical infrastructure. It pointed out the need for informed policy-making and strategic solutions to mitigate the risks associated with the proliferation of drone technology, an approach meant to bolster the resilience and security of the Western Interconnection, a critical component of the nation's energy infrastructure that supports the livelihood and economic prosperity of millions. Building on this foundational understanding of the risks posed by drone technology and the protective measures for the Western Interconnection electrical grid, Chapter 2 delves into an extensive review of existing literature which explores theoretical frameworks, historical developments, and contemporary challenges, providing a critical backdrop for the study's investigation into emerging drone threats and infrastructure security.

Chapter 2: Literature Review

The problem to be addressed by this study is the threat that current and emerging aerial drone technologies pose to the Western Interconnection electrical power grid, as perceived by subject matter experts (SME) from the U.S. Department of Energy (DOE), the Federal Energy Regulatory Commission (FERC), and the Western Electricity Coordinating Council (WECC). The purpose of this descriptive qualitative study was to analyze and identify the severity of risk posed by current and emerging commercial aerial drone technology to America's Western Interconnection Electrical Grid Infrastructure. Additionally, the research sought to delineate the risk levels of these technologies to the Western Interconnection infrastructure, drawing on insights from Franke et al. (2023) as well as Rogers and Kunertova (2022).

Analyzing drone threats to the Western Interconnection power infrastructure reveals a number of concerns, including physical security, cybersecurity, regulatory challenges, and socio-economic effects. Researchers such as Grzegorz Wojciech Pietrek (2022) and Yadav et al. (2022) have previously identified a variety of serious security risks posed by drones conducting unauthorized surveillance for various organizations, both public and private. These drones, with their advanced maneuverability and payload capabilities, easily infiltrate restricted areas around critical power infrastructure for illicit reconnaissance (Khawaja et al., 2022). Such activities can expose operational and structural vulnerabilities in power stations and transmission lines, potentially leading to coordinated sabotage efforts that could significantly disrupt power distribution systems (Pietrek, 2022).

Broadly speaking, the contemporary threat landscape frequently encompasses physical attacks where drones equipped with destructive payloads can launch direct assaults on infrastructure components (Khawaja et al., 2022; Yuvaraj & Velliangiri, 2023). These critical

attack vulnerabilities underscore the potential for physical damage and highlight the urgent need for effective detection and neutralization systems to counter airborne threats. Simultaneously, the cybersecurity domain emerges as a crucial area of concern, with drones serving as vectors for cyberattacks targeting control systems and data communication networks within the power infrastructure (Chowdhury & Gkiouls, 2021). This dual-threat scenario demands a significant shift in cybersecurity strategies to incorporate both traditional cyber defenses and drone-specific countermeasures.

Navigating the regulatory and legal environment associated with drone activities also presents distinct challenges. The development of comprehensive laws aimed at mitigating drone-related threats, while simultaneously promoting the beneficial uses of drones in infrastructure maintenance and emergency services, represents a delicate balancing act (FAA, 2022; ICAO 2019). This is further complicated by the rapid technological advancement of drones, which often outpaces the formulation of corresponding regulatory measures.

Addressing the threat of malicious drones, especially across the extensive and diverse electrical infrastructure of the Western Interconnection, introduces significant technical and operational challenges. Implementing anti-drone technologies, ranging from electronic jamming to physical interception systems, requires strategic flexibility and adaptability to meet the evolving drone threat landscape (Yadav et al., 2022). Additionally, the widespread use of surveillance and drone detection measures raises substantial privacy concerns, necessitating the creation of policies that balance the protection of individual freedoms with the security of critical infrastructure (Pietrek, 2022).

Coordinating an effective response to drone threats requires a complex network of stakeholders, including utility providers, regulatory bodies, law enforcement, and defense

agencies. Developing standardized protocols can help facilitate a unified and efficient response to drone-related security incidents (Pietrek, 2022; Yadav et al., 2022). Furthermore, the potential economic impacts of power infrastructure disruptions—whether from direct attacks or the financial burdens of implementing anti-drone strategies—add another layer of complexity to the strategic considerations needed to protect essential energy resources (Khawaja et al., 2022).

The ongoing debate regarding the impact of drone threats on power infrastructure showcases divergent viewpoints on risk assessment, mitigation strategies, regulatory approaches, and privacy concerns (Sands, 2022; Rogers & Kunertova, 2022). Privacy concerns further complicate the debate, indicating the need for a balanced approach that respects both security needs and civil liberties. These concerns effectively illustrate the multi-faceted nature of addressing potential drone threats to power infrastructure, emphasizing the necessity of a holistic strategy that integrates security, technology, regulation, and respect for privacy (Sands, 2022; Rogers & Kunertova, 2022). Such an approach is crucial for effectively countering the evolving drone threats while ensuring the resilience and security of the Western Interconnection's power infrastructure.

This second chapter literature review aimed to present a concise yet comprehensive literature review on this topic by drawing on relevant academic peer-reviewed sources, contemporary mainstream media, and materials from industry-specific professional associations. This researcher's primary goal was to offer a balanced approach that effectively integrates these diverse perspectives. The researcher outlined the theoretical academic framework of Freeman's (1984) Stakeholder Theory, along with its numerous formal revisions, which provides the foundational guidance for this study. Next, the researcher detailed the significant milestones of the historical evolution of drone technology, followed by an examination of the practical aspects

of UAVs, detailing their operational capabilities, communication systems, and payload capacities. Finally, this second chapter concluded with an analysis of challenges, security issues, trends, and regulatory structures, and history involving drone technology and critical infrastructure security.

This literature review was based on information sourced from National University's online library databases. The specific databases used are FBI, DoD, DHS, FAA, Northcentral University Library, Pro-Quest, and Google Scholar. Search queries used the following keywords to conduct the online searches: Drones, Unmanned Aerial Vehicles (UAV), Electrical grid infrastructure, Commercial drones, Drone technology risks, Aerial drones and electrical grids, UAV applications in electrical grids, Commercial drone regulations, Drone surveillance risks, UAV impact on infrastructure security, etc. See Appendix A for a complete list of all search terms, combinations, and categories that are used in the research in this study.

Theoretical Framework

The theoretical framework of this research is firmly anchored in Stakeholder Theory, as presented by University of Virginia Professor R. Edward Freeman (1984, 2010, 2015). Stakeholder Theory is instrumental in comprehending the varied and often competing interests of all stakeholders involved in issues pertaining to drone technology and the protection of critical infrastructure. This understanding is particularly crucial for ensuring the safety and operational continuity of America's critical infrastructure systems, such as the Western Interconnection electrical grid. The research effort employed a multidisciplinary approach that integrated Technology Risk Assessment, CIP, and Regulatory Adaptation to Technological Advancements. This integration is essential given the rapid pace of drone technology advancements and their

extensive use, with over 1.1 million recreational drones currently registered in the United States (Current Unmanned Aircraft State Law Landscape, 2023).

This approach emphasized the interconnectedness of technological, human, environmental, and organizational elements, demonstrating how changes affecting one group can impact the entire system. By applying Freeman's (1984, 2010, 2015) Stakeholder Theory, the study aimed to identify the complex interactions and expectations among the three SME groups from the DOE, FERC, and WECC regarding drones and critical infrastructures. The research focused on evaluating the risks posed by drone technology to the Western Interconnection electrical power grid, a crucial infrastructure covering over 1.8 million square miles across the United States, Canada, and Mexico. A wide array of subject matter experts from the DOE, FERC, and WECC provided insights into potential vulnerabilities and the effectiveness of current protective measures (Western Interconnection, 2023).

These theoretical perspectives provided the foundation for addressing the following research questions: What is the perceived risk level among SMEs from the DOE, FERC, and WECC, regarding the potential of current and near-future aerial drone technologies to cause damage or destruction to key aspects of the Western Interconnection Electrical Grid infrastructure? What is the quantifiable level of concern among SMEs from the DOE, FERC, and WECC regarding current and near-future aerial drone technologies as a potential threat to the Western Interconnection Electrical Grid infrastructure? What is the perceived adequacy of the measures taken by the DOE, FERC, and WECC in safeguarding the Western Interconnection electrical grid infrastructure from current and near-future aerial drone technology attacks?

This research study drew from theories commonly used in homeland security linking leadership, risk management, security, technology, and terrorism. Homeland security is

structured around eleven core topics, each linked to at least one dominant theory (Comiskey, 2018). These core areas include natural and human-made hazards, collaboration, critical thinking, infrastructure, cybersecurity, intelligence, risk management, emergency management, preparedness, strategy, and terrorism (Comiskey, 2018). As outlined by the Department of Homeland Security (2013), American Homeland Security encompasses various professions including law enforcement, emergency management, the military, public health, and others, each with relevant theories applicable to the field. This research aimed to provide a comprehensive framework addressing the complex interplay between drone technology, critical infrastructure protection, and stakeholder interests. The research questions were designed to gain a deeper understanding of the perceived risks, concerns, and adequacy of protective measures related to the use of aerial drone technologies within the Western Interconnection electrical grid, an essential infrastructure spanning the United States, Canada, and Mexico.

By applying Freeman's Stakeholder Theory (1984, 2010, 2015), the framework goes beyond merely considering technological and infrastructural elements; it incorporates human, environmental, and organizational factors that both influence and are influenced by drone technology and critical infrastructure protection. This particular academic approach acknowledges the interconnectedness of various system components and the diverse perspectives of different stakeholders. The framework aims to devise strategies that enhance the systemic resilience and robustness of critical infrastructures. This involves ensuring that these infrastructures can effectively anticipate, manage, and mitigate disruptions caused by advanced drone technologies. By considering the complex interactions between different stakeholder groups, the framework highlights the cascading effects that changes affecting one group can have across the entire system.

Other Considered Theories

Systems Theory

Systems Theory is an interdisciplinary framework that examines complex entities as cohesive systems with interconnected and interdependent components (Bertalanffy, 1968; Boss et al., 2008). Originating from the work of biologist Ludwig von Bertalanffy in the 1940s, Systems Theory has been widely adopted across disciplines such as biology, engineering, social sciences, and management studies (Boss et al., 2008). At its core, Systems Theory emphasizes interconnectedness, positing that changes or actions in one part of the system inevitably affect other parts.

This holistic perspective is crucial for understanding how individual elements function together within the whole system. The theory also highlights dynamic interactions, recognizing that systems are not static but constantly evolving and adapting to internal and external influences (Bertalanffy, 1968; Boss et al., 2008). Because it has been commonly used in research studies that require a comprehensive analysis of complex interactions, contemporary Systems Theory often incorporates frameworks such as cybernetics, which focuses on regulatory and control mechanisms, and chaos theory, which examines how small changes can lead to significant impacts within a system (Boss et al., 2008). This approach facilitates a deeper understanding of the intricacies of relationships and dependencies that characterize complex systems.

Systems Theory was originally considered for this research study because of its potential holistic approach to analyzing the interconnectedness of various elements within the Western Interconnection electrical grid. By viewing the grid as a whole system, Systems Theory would facilitate an examination of how drone technology impacts different components and their

interdependencies. Additionally, its focus on dynamic interactions would help explore how potential drone threats might influence various facets of the electrical grid, thereby providing a comprehensive understanding of the system's vulnerabilities and resilience.

However, this researcher ultimately determined that Systems Theory's broad focus, which may not adequately address the specific interests and perspectives of individual stakeholders involved in critical infrastructure protection, led to the determination that it was not suitable for this study. Unlike Stakeholder Theory, which emphasizes the importance of considering the varied and often competing interests of different stakeholders, Systems Theory may overlook the nuanced interactions and expectations between key groups such as regulators, businesses, local communities, and environmental organizations (Freeman et al., 1984, 2010,2015; Boss et al., 2008). Consequently, while Systems Theory provides valuable insights into the overall functioning of complex systems, Stakeholder Theory offers a more targeted approach for understanding and aligning the diverse interests that are crucial for developing effective strategies to protect critical infrastructure from drone technology threats.

Risk Management Theory

Risk Management Theory is a comprehensive framework that focuses on systematically identifying, assessing, and prioritizing risks, followed by coordinated efforts to minimize, monitor, and control the likelihood or impact of adverse events (Giambona et al., 2018). Widely applied across fields such as finance, engineering, healthcare, and security, the primary objective of Risk Management Theory is to ensure that organizations can achieve their goals and maintain operational continuity despite potential threats. The primary principles of this theory include risk identification, risk assessment, risk prioritization, and risk mitigation (Giambona et al., 2018).

Risk identification involves recognizing potential risks that could affect the objectives of an organization or system, serving as the initial step in the risk management process. Following this, risk assessment quantifies the likelihood and potential impact of identified risks, providing a basis for understanding their significance. Risk prioritization helps in determining which risks require immediate attention and resources, ensuring that efforts are focused on the most critical threats. Finally, risk mitigation involves developing and implementing strategies to reduce the probability or impact of these risks.

Applying Risk Management Theory to this study could have been beneficial due to its structured approach to handling threats posed by drone technology to the Western Interconnection electrical grid. By identifying and assessing the risks associated with drone technology, this theory would facilitate a detailed analysis of potential vulnerabilities within the grid. Moreover, the prioritization process would help in allocating resources to mitigate the most critical risks, ensuring a focused and efficient response to drone-related threats.

Risk Management Theory provides a robust framework for handling threats; however, it may not have fully captured the diverse interests and perspectives of individual stakeholders involved in critical infrastructure protection. Unlike Stakeholder Theory, which focuses on the importance of considering the varied and often competing interests of different stakeholders, Risk Management Theory primarily focuses on the technical aspects of risk without necessarily addressing the broader social, environmental, and organizational contexts (Giambona et al., 2018). As a result, Risk Management Theory may overlook the subtle interactions and expectations between key groups such as regulators, businesses, local communities, and environmental organizations. While Risk Management Theory offers valuable insights into the technical aspects of risk mitigation, Stakeholder Theory provides a more comprehensive

approach for understanding and aligning the diverse interests crucial for developing effective strategies to protect critical infrastructure from drone technology threats.

Resilience Theory

The Resilience Theory framework emphasizes the capacity of systems, organizations, or individuals to endure, adapt to, and recover from disruptions and adversities (Holling, 1973; Bertsia & Poulou, 2023). Originally developed in the fields of ecology and psychology by ecologist C.S. Holling (1973), this theory has been broadly applied in disciplines such as engineering, disaster management, and organizational studies. The core principles of Resilience Theory include robustness, adaptability, and transformability.

The robustness principle refers to the strength of a system to withstand shocks without significant loss of function, ensuring that essential operations continue during disruptions (Holling, 1973). Adaptability refers to the system's ability to modify its structures and processes in response to changing conditions and new information, facilitating ongoing functionality amid evolving threats (Holling, 1973). Finally, the transformability principle involves the capacity of a system to undergo fundamental changes when existing structures become untenable, thereby enabling the emergence of new, more resilient configurations (Holling, 1973).

Resilience Theory is commonly used in studies that focus on understanding and enhancing the ability of systems to cope with and recover from adverse events. Its structured approach often includes frameworks such as Socio-Ecological Systems (SES) theory, which examines the interactions between human and environmental systems, and adaptive management, which emphasizes learning and flexibility in managing complex systems (Ledesma, 2014). Additionally, resilience assessment methodologies typically involve

qualitative and quantitative analyses to evaluate the vulnerabilities, strengths, and adaptive capacities of the system in question.

Applying Resilience Theory within this study could have provided significant insights into how the Western Interconnection electrical grid might maintain its functionality and recover from potential disruptions caused by drone technologies. This approach would facilitate an in-depth exploration of the grid's capacity to adapt to and recover from threats, thereby ensuring continuous operation. Resilience Theory could have potentially supported an assessment of the system's vulnerabilities and strengths, pinpointing areas that needed enhancements to boost overall resilience.

Resilience Theory offers valuable perspectives on system robustness and recovery, but it may not fully address the varied interests and perspectives of individual stakeholders involved in critical infrastructure protection. Unlike Stakeholder Theory, which zeroes in on the diverse and sometimes conflicting interests of different stakeholders, Resilience Theory primarily focuses on system resilience (Freeman et al., 1984, 2010,2015; Holling, 1973). This approach might overlook the complex interactions and expectations among key groups such as regulators, businesses, local communities, and environmental organizations. Although Resilience Theory provides important insights into strengthening system resilience, Stakeholder Theory offers a more encompassing approach for understanding and aligning the diverse interests essential for developing effective strategies to protect critical infrastructure against drone technology threats.

Stakeholder Theory

As discussed earlier in this literature review, Freeman's Stakeholder Theory (1984, 2010, 2015) serves as the theoretical foundation for this academic research, chosen for its comprehensive approach to understanding the varied interests and perspectives of all

stakeholders involved in protecting the Western Interconnection electrical grid from drone technology threats. This theory offers a holistic perspective by considering the viewpoints of each stakeholder, crucial for safeguarding the grid. The research framework, grounded in Freeman's theory, stresses the alignment of stakeholder interests and applies these principles to the realms of drone technology and infrastructure protection. It explores the interconnectedness of technological, human, environmental, and organizational elements, allowing for the identification of complex stakeholder interactions and guiding the formulation of resilient strategies to manage and mitigate disruptions posed by advanced drone technologies (Goel, 2020).

Dr. Freeman introduced Stakeholder Theory in his seminal work, "Strategic Management: A Stakeholder Approach" (1984), during his tenure at the University of Virginia's Darden School of Business. His theory conceptually redefined corporate responsibilities, shifting focus from shareholders to a broader array of stakeholders including employees, customers, suppliers, and the community, thereby emphasizing the interconnectedness of these groups and the importance of managing relationships to achieve sustainable success. Freeman's broad definition of stakeholders as "any group or individual who can affect or is affected by the achievement of the organization's objectives" (Freeman, 1984, p. 46) encompasses a wide range of entities with vested interests in an organization's outcomes.

The ethical principles highlighted in Freeman's theory (1984, 2010, 2015) include corporate responsibility to all stakeholders, fairness, transparency, advocating for equitable treatment, and open communication to foster trust and accountability. Since its introduction, this theory has shifted business ethics from focusing solely on shareholder primacy to considering a broader range of stakeholder interests, promoting socially responsible and sustainable practices.

However, the sustainability of this theory is challenged by the need to balance conflicting interests, manage short-term pressures, and sustain increased operational costs while maintaining transparency and accountability. Scholars such as Barney (2018), Bosse & Phillips (2016), as well as Van Lange et al. (2013) argued for a supportive regulatory environment to help businesses achieve their objectives sustainably amidst these complex social, environmental, and economic impacts.

In their July 2007 work on Stakeholder Capitalism, Freeman et al. expanded on the 1984 principles, weaving stakeholder relationships into the fabric of capitalist practice and advocating for a stakeholder-centric model of capitalism that promotes economic efficiency, moral integrity, and social responsibility. The April 2010 refinement by Freeman et al. integrated group-level social roles and collective value creation, highlighting the tension between individual self-interests and collective goals. This discourse enhances understanding of stakeholder interactions and the need to resolve these tensions effectively.

In July 2015, Freeman et al. introduced the Hub-and-Spoke Model in Stakeholder Theory, depicting dynamic interactions between stakeholder groups and central decision-makers. This model has sparked debate among scholars like Bridoux and Stolehorst (2022), who question its effectiveness in governing stakeholder interactions and facilitating joint value creation. Bridoux and Stolehorst (2022) suggested that in today's data-driven capitalist economies, successful joint value creation depends heavily on a broad spectrum of stakeholders extending beyond traditional business contexts.

The on-going evolution of Stakeholder Theory, as discussed by Freeman et al. (2010) and in subsequent revisions, recognizes the diversity within stakeholder groups and the importance of leadership in balancing varied interests and motivations to align stakeholders effectively. This

leadership role is crucial for ensuring productive collaboration despite differences. Moreover, the emphasis on managing internal conflicts and maintaining regular stakeholder interactions, as stressed by both Bosse and Phillips (2016) as well as Van Lange et al. (2013), is vital for effective governance and decision-making.

Ostrom (2010) contributed to this discussion by highlighting the urgency of addressing conflicts swiftly to keep the group focused on cooperative behavior. This was crucial to prevent conflicts from spreading and harming the group's collective goals. Bridoux and Stolehorst (2022) also noted the significance of shared governance within groups, where no single stakeholder had ultimate authority to resolve disputes. This situation called for proactive cooperative efforts, as illustrated by Van Hille et al. (2019), to resolve individual conflicts and motivate the group to work together harmoniously. Overall, the narrative indicates a shift in Stakeholder Theory towards a more dynamic understanding of how to manage the intricate interplay of individual and collective interests within groups. This ongoing scholarly discussion illustrates the evolving nature of stakeholder theory and its implications for both theory and practice in a globalized economic landscape.

Stakeholder Theory is especially advantageous for this study as it presents a comprehensive understanding of the interests and perspectives of all relevant parties involved in the protection of the Western Interconnection electrical grid infrastructure from drone technology threats. This theory facilitates a holistic approach by considering the varied and often competing interests of different stakeholders, including regulators, businesses, local communities, and environmental groups. It underscores the interconnectedness of technological, human, environmental, and organizational elements, providing a nuanced view of how changes affecting one group can impact the entire system.

This focus on stakeholder interactions and expectations is crucial for developing effective strategies that address the complexities of drone technology and its implications for critical infrastructure. Furthermore, Stakeholder Theory supports the integration of Technology Risk Assessment, Critical Infrastructure Protection (CIP), and Regulatory Adaptation, ensuring that the diverse values and objectives of all stakeholder groups are considered. This inclusive approach fosters more robust and resilient solutions, making Stakeholder Theory a more beneficial framework for this study compared to other theoretical alternatives.

Technology Risk Assessment

Technology Risk Assessment in the field of Homeland Security is a crucial process aimed at identifying and evaluating the risks associated with using technology to protect national security (DHS, 2013). This process involves pinpointing potential threats such as cyber-attacks, hardware malfunctions, and data breaches, as well as assessing vulnerabilities in current technology systems. It also examines the likelihood of these risks occurring and their possible impact on national security operations. By prioritizing the most significant risks, Homeland Security can allocate resources effectively to mitigate them (DHS, 2013). This involves implementing technical controls like encryption and firewalls, establishing robust policies and procedures, and conducting regular training for personnel (DHS, 2013). Continuous monitoring and regular audits are essential to ensure these measures remain effective and up-to-date. Ultimately, the goal is to ensure that all technologies used in Homeland Security are secure, reliable, and capable of withstanding evolving threats (DHS, 2013).

This comprehensive framework begins with Technology Risk Assessment, a critical component that involves a thorough analysis of the evolving capabilities of drone technologies. This includes examining advancements such as increased range, payload capacity, and

autonomous functionalities. The assessment evaluates how these technologies can be accessed and potentially misused by various actors, ranging from hobbyists to hostile entities. This spectrum of threats posed includes unauthorized surveillance, data breaches, and direct sabotage of critical infrastructure.

This component also involves developing detailed risk scenarios to anticipate potential misuse of drone technologies. These scenarios serve as a foundation for understanding the range and severity of threats and for devising strategies to mitigate these risks effectively. By considering various misuse cases, from recreational accidents to intentional attacks, the assessment provides a holistic view of the potential dangers associated with drone technology.

Origin and Application of Technology Risk Assessment

The origin of Technology Risk Assessment can be traced back to the broader discipline of risk theory, which itself has evolved over centuries from the fields of mathematics, statistics, and economics, focusing initially on the quantification and management of financial risk (Technology Risk Assessment, 2024). Over time, the concept expanded beyond these confines, incorporating insights from psychology, sociology, and environmental science to address a wide array of risks. In the late 20th century, the emergence of complex technologies and the recognition of their potential societal impacts necessitated the development of specific methodologies to assess and mitigate technological risks (Technology Risk Assessment, 2024). This evolution reflects an ongoing effort to understand and manage the uncertainties and potential adverse consequences associated with technological advancements.

Historically, this framework was applied primarily to industrial and engineering contexts, where the focus was on quantifying the potential hazards associated with the use of machinery, chemicals, and other technologies in terms of their likelihood and potential impact on human

health, safety, and the environment (Kalinin et al., 2021). The methodology involved a systematic process of hazard identification, risk analysis, and risk evaluation, followed by the implementation of risk control measures to mitigate identified risks to acceptable levels. Originally, the framework's application was centered around ensuring workplace safety and environmental protection, particularly in high-risk industries such as chemical manufacturing, nuclear power, and aerospace (El Marady & Rahouma, 2021). It provided a structured approach for assessing the potential adverse consequences of technological processes and systems, leading to the development of safety standards, emergency response strategies, and regulatory policies designed to prevent accidents and mitigate their impacts (Technology Risk, 2024).

In current studies, the Technology Risk Assessment framework has been adapted and expanded to address the complexities of emerging technologies, including digital and information technologies, biotechnology, and, notably, drone technology (Kalinin et al., 2021; El Marady & Rahouma, 2021). The framework's application has broadened beyond traditional industrial settings to include public health, cybersecurity, privacy, and societal impacts. This evolution reflects the changing landscape of technological risks in the 21st century, characterized by the rapid development and widespread adoption of new technologies that pose unique challenges in terms of surveillance, data security, and ethical considerations (Kalinin et al., 2021; El Marady & Rahouma, 2021).

The application of the Technology Risk Assessment framework in current studies involves a more nuanced analysis of risks, incorporating interdisciplinary insights from fields such as computer science, ethics, and social sciences (Technology Risk Assessment, 2024). For instance, in the context of drone technology, risk assessments now consider not only the physical safety risks associated with drone operations, such as collisions and accidents, but also privacy

risks, cybersecurity vulnerabilities, and the potential for misuse in unauthorized surveillance or hostile actions (Kalinin et al., 2021; El Marady & Rahouma, 2021). Current applications of the framework also emphasize stakeholder involvement and public engagement in the risk assessment process, recognizing the importance of addressing societal concerns and ethical implications of technology deployment.

Moreover, contemporary studies leverage advanced methodologies, including simulation modeling, scenario analysis, and big data analytics, to predict and analyze risks associated with technological innovations (Kalinin et al., 2021). This contemporary line of thinking reflects a shift toward more dynamic and predictive approaches to risk assessment, aimed at anticipating future challenges and informing the development of resilient and adaptive risk management strategies. While the original use of the Technology Risk Assessment framework was primarily focused on industrial safety and environmental protection, its application in current studies has evolved to encompass a broader range of risks associated with a wide array of emerging technologies. This evolution illustrates the framework's adaptability and its critical role in guiding the responsible development, deployment, and governance of new technologies in a rapidly changing world.

Historical Evolution of Drones

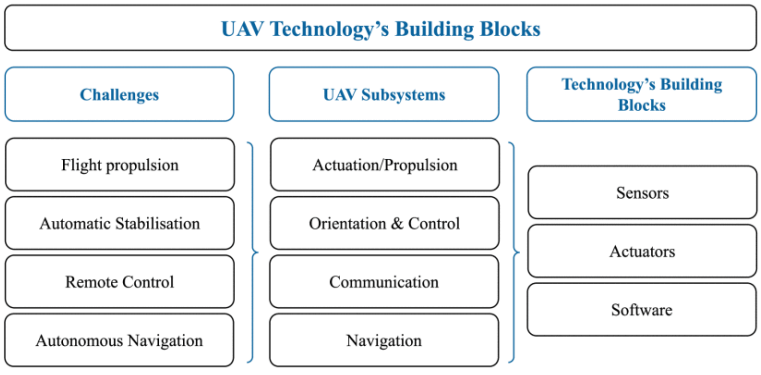
The history of drone technology represents a remarkable journey of innovation and adaptation, evolving from rudimentary mechanical flyers into sophisticated systems integral to various modern applications; see Appendix B for a more complete timeline of drone technology development. The concept of UAVs can be traced back to as early as the late 18th century. In 1783, Joseph-Michel and Jacques-Étienne Montgolfier, two pioneering brothers from France, demonstrated the first public display of an unmanned aircraft with their hot-air balloon in

Annonay, France (Miličević & Bojković, 2021; Newcome, 2004). This event was a milestone in aviation history, capturing the imagination of the public and scientists alike. These hot-air balloons were the first aircraft to operate without a human pilot on board, utilizing the principles of buoyancy and controlled heat to achieve flight (Miličević & Bojković, 2021).

This innovation laid the foundational groundwork for future developments in UAV technology by showcasing the potential for human-made machines to navigate the skies autonomously (Moschetta & Namuduri, 2017). The Montgolfier brothers' demonstration was not only a technical achievement but also a cultural phenomenon that inspired subsequent generations of inventors and engineers to explore the possibilities of unmanned flight (Moschetta & Namuduri, 2017). This initial success in creating a functional unmanned aerial vehicle set the stage for a series of technological advancements that would eventually lead to the sophisticated drones we see today, capable of performing complex tasks across a multitude of industries. See Figure 2.1 for a graphical depiction of challenges, subsystems, and technology building blocks in UAV development.

Figure 1

Key UAV Technology Building Blocks



Note. This model summarizes UAV technology's key to the development and evolution of drone technology. From The Rise of Drones in Internet of Things: A Survey on the Evolution,

Prospects and Challenges of Unmanned Aerial Vehicles, by Labib et al., 2021, IEEE Access, 9, p. 115466–115487. .

The military potential of UAVs was first explored in 1849 when Austrian artillery lieutenant Franz von Uchatius invented the balloon bomb, an innovative yet rudimentary form of aerial warfare (Miličević & Bojković, 2021; Newcome, 2004). Field Marshal von Radetsky utilized these balloons in an attempt to attack the city of Venice during the Austrian siege (Miličević & Bojković, 2021). These balloon bombs were designed to carry explosive devices over enemy positions; however, they proved largely ineffective due to their inability to be accurately guided, often resulting in the bombs being blown off course by the wind (Miličević & Bojković, 2021; Newcome, 2004). Despite their lack of success, this early experimentation highlighted the potential for UAVs to be used in military applications, setting a precedent for future developments.

This period of early UAV exploration continued in 1858 with the pioneering efforts of Gasper Felix Tournachon, a French photographer also known as Nadar (Advanced Air Mobility, 2019; Newcome, 2004; Miličević & Bojković, 2021). Tournachon achieved a significant milestone in aerial reconnaissance by taking the first aerial photograph from a hot-air balloon over Paris (Miličević & Bojković, 2021; Newcome, 2004). Although the photograph itself has been lost to history, the endeavor marked a crucial step in utilizing UAVs for intelligence purposes, demonstrating how aerial perspectives could provide valuable information about enemy positions and landscapes (Newcome, 2004). This innovation and the strategic advantages of aerial photography laid the groundwork for more advanced surveillance techniques.

Further advancements in UAV technology were made April 26, 1897, by Alfred Nobel, the inventor of dynamite and a prominent figure in scientific innovation (Reichhardt, 2009).

Nobel launched a rocket equipped with a camera, marking the first integration of photographic equipment into an unmanned system (Miličević & Bojković, 2021). The ability to remotely gather visual intelligence without risking human lives significantly broadened the scope of UAV usage, paving the way for future developments in both military and civilian contexts.

In September 1898, the pioneering work of Nikola Tesla demonstrated the potential for remote control with his radio-controlled boat at Madison Square Garden, a significant technological breakthrough of the era (Advanced Air Mobility, 2019; Newcome, 2004). Tesla's invention was a small boat equipped with a radio receiver and controlled remotely by signals transmitted from Tesla's device. This boat responded to directional signals and flashed lights on command, captivating the audience and demonstrating the possibilities of remote-operated technology (Newcome, 2004; Moschetta & Namuduri, 2017). Some spectators were so amazed by the demonstration that they believed it was a feat of magic or telekinesis, reflecting the novelty and futuristic nature of Tesla's work (Newcome, 2004). This innovation was an early precursor to modern UAVs, promoting the feasibility of controlling machines wirelessly and paving the way for subsequent developments in remote-operated vehicles.

Tesla's groundbreaking demonstration laid the foundation for more advanced applications of remote-control technology in military operations. This potential was realized during World War I, particularly in the Battle of Neuve Chapelle in 1915, March 10 through March 13 (Advanced Air Mobility, 2019). British forces utilized aerial reconnaissance techniques, employing aircraft to capture photographs of the German front lines (Miličević & Bojković, 2021; Moschetta & Namuduri, 2017). These aerial photographs were then analyzed to create detailed maps of enemy positions, providing a significant tactical advantage. This use of aerial photography marked an early example of sophisticated UAV reconnaissance, introducing

the concept of leveraging unmanned systems for intelligence-gathering purposes. The success of these reconnaissance missions highlighted the critical role that UAVs could play in military strategy, foreshadowing their increasing importance in future conflicts (Miličević & Bojković, 2021).

The first UAV specifically designed as a weapon was the Kettering Bug, developed by the American engineer Charles Kettering, with its first successful test flight on October, 1918 (National Museum of the United States Air Force, 2015; Advanced Air Mobility, 2019). This innovative aerial torpedo, created during World War I, was designed to carry 180 pounds of explosives and use pre-set controls for navigation (National Museum of the United States Air Force, 2015). The Bug operated on a simple guidance system that included a predetermined number of engine revolutions to determine its range. Once the specified distance was reached, the engine would shut off, and the wings would detach, causing the explosive-laden fuselage to fall onto the target (National Museum of the United States Air Force, 2015). Although it saw limited use and was never deployed in combat, the Kettering Bug represented a significant leap forward in drone technology, showcasing the potential for UAVs in offensive military roles and laying the groundwork for future developments in unmanned aerial weaponry.

By early 1935, advancements in UAV technology continued with the Royal Air Force's development of the De Havilland DH.82B Queen Bee (Advanced Air Mobility, 2019). This aircraft was a low-cost, radio-controlled drone used for aerial target practice, designed to train anti-aircraft gunners. The Queen Bee was essentially a modified version of the manned De Havilland Tiger Moth biplane, fitted with a radio control system that allowed it to be flown remotely (Miličević & Bojković, 2021). Its ability to be controlled from a distance and reused multiple times made it an efficient and practical tool for military training. The Queen Bee is

considered to be the first modern drone due to its sophisticated control systems and practical applications (Miličević & Bojković, 2021; Moschetta & Namuduri, 2017).

Inspired by the success of the Queen Bee, the U.S. Navy initiated a similar program in early 1936, recognizing the strategic advantages of remote-controlled target drones. This led to the development of the Curtiss N2C-2, the first radio-controlled UAV torpedo, in 1937 (Advanced Air Mobility, 2019; Miličević & Bojković, 2021). The N2C-2 was an adaptation of the Curtiss N2C Fledgling biplane, modified to be controlled remotely. It received commands from an operator in a nearby aircraft, who could guide the drone during flight and target practice exercises. While the N2C-2 had limitations, such as its dependence on the operator's proximity, it marked a significant step forward in the evolution of UAV technology (Miličević & Bojković, 2021). This period of innovation laid the foundation for the more advanced and autonomous drones that would follow.

Innovation in drone technology continued during World War II with actor Reginald Denny's invention of the Radio Plane, a radio-controlled target plane (Advanced Air Mobility, 2019). Denny, leveraging his passion for aviation and his Hollywood connections, founded the Radioplane Company, which produced these drones primarily for military training purposes (Miličević & Bojković, 2021). The Radio Plane served as a target for anti-aircraft gunnery practice, allowing soldiers to improve their accuracy and effectiveness. This development marked a pivotal advancement in drone technology, demonstrating the practical applications of radio-controlled aircraft.

By July 1944, the U.S. Air Force and Boeing had developed the BQ-7, an ambitious project aimed at achieving first-person view (FPV) flight (Blom, 2010). The BQ-7, also known as the Aphrodite drone, involved converting old bombers into remotely piloted explosive-laden

aircraft (Blom, 2010). These drones were equipped with rudimentary television cameras to provide a live feed to the operator, who would guide the aircraft towards its target. Although the BQ-7 missions were largely ineffective and posed significant risks to the pilots who had to bail out before the drone was remotely controlled, the project represented an important step in the evolution of drone technology (Blom, 2010). It established the potential for UAVs to be used in direct combat roles, paving the way for more advanced and safer FPV systems in the future.

From the early 1970s to the late 1980s, marked a significant leap in drone capabilities with Israel's development of the Mastiff and IAA Scout series (Blom, 2010; Miličević & Bojković, 2021). These UAVs were designed to enhance military situational awareness and provide real-time intelligence to commanders. The Mastiff, introduced in the early 1970s, was one of the first UAVs to be used extensively for battlefield surveillance (Blom, 2010; Miličević & Bojković, 2021). It was followed by the more advanced IAA Scout, which featured improved sensors and communication systems (Onohwakpor et al., 2020). These Israeli drones demonstrated the strategic advantages of UAVs in modern warfare, allowing for continuous monitoring of enemy movements and rapid response to changing battlefield conditions. The success of the Mastiff and Scout series had a pivotal impact on the use of UAV technology in military operations.

The effectiveness of drones in combat was explicitly demonstrated during the Battle of Jezzine in 1982, June 13 through June 14, a significant engagement during the Lebanon War, where Israel used UAVs to outmaneuver the Syrian Air Force (Cohen-Almagor, 2022). Israeli forces deployed UAVs for real-time surveillance and electronic warfare, enabling them to gather critical intelligence and coordinate their operations with unprecedented precision (Cohen-

Almagor, 2022). The success of these drones in disrupting Syrian air defenses and providing tactical advantages contributed to the growing role of UAVs in modern warfare.

In response to Israel's demonstrated success, the United States began to significantly scale up its drone program by 1985, recognizing the transformative potential of UAVs in military operations (Blom, 2010; Cohen-Almagor, 2022). This led to a collaborative effort between the United States and Israel, resulting in the joint development of the RQ-2 Pioneer drone in December of 1985 (Miličević & Bojković, 2021). The RQ-2 Pioneer was designed for reconnaissance and surveillance missions, featuring advanced imaging systems and real-time data transmission capabilities.

The RQ-2 Pioneer saw significant use during the Gulf War on August 2, 1990 to February 28, 1991, where it played a crucial role in coalition forces' operations (Miličević & Bojković, 2021). For the first time in a major conflict, drones were flown continuously throughout the war, providing persistent surveillance and intelligence support. The Pioneer's ability to operate around the clock marked a new era of 24/7 UAV operations, revolutionizing how military intelligence was gathered and utilized (Blom, 2010; Miličević & Bojković, 2021). The continuous use of drones during the Gulf War solidified their place in modern military strategy, demonstrating their indispensable role in enhancing situational awareness, guiding precision strikes, and reducing risks to human pilots. This period marked a significant turning point in the evolution of military drones, showcasing their potential to fundamentally change the dynamics of modern warfare and setting the stage for future advancements in UAV capabilities (Newcome, 2004).

The development of the Predator drone in January 1994 marked a pivotal moment in the evolution of UAV technology, bringing weaponized drones to the forefront of modern warfare

(Timeline of Drone Integration | Federal Aviation Administration, 2022). This platform, officially designated as the MQ-1 Predator, was developed by General Atomics with significant input from UAV pioneers like Abraham Karem. Karem's innovative designs and engineering expertise were instrumental in creating a drone that combined long-endurance capabilities with advanced surveillance and strike functionalities (Blom, 2010; Miličević & Bojković, 2021). The Predator was equipped with sophisticated sensors, cameras, and laser-guided missiles, allowing it to perform both reconnaissance and targeted strike missions with high precision (Miličević & Bojković, 2021). This dual capability redefined the public image of UAVs, showing them to be precise, remotely operated weapons capable of conducting complex military operations with minimal risk to human operators (Blom, 2010; Miličević & Bojković, 2021).

The groundbreaking potential of UAV technology extended beyond military applications, particularly evident in the aftermath of Hurricane Katrina in August 2005. The devastation caused by the hurricane prompted the FAA to allow UAVs to operate in civilian airspace for the first time in the United States (Timeline of Drone Integration | Federal Aviation Administration, 2022). On May 18, 2006, UAVs were deployed for search and rescue missions, damage assessment, and disaster relief operations (Department of Defense, 2015). Equipped with thermal cameras and real-time video feeds, these drones provided critical support to emergency responders, helping to locate survivors and assess the extent of the damage caused by this catastrophic natural disaster.

This milestone marked the beginning of significant civilian and commercial applications for drone technology. The successful deployment of UAVs in disaster relief demonstrated their versatility and effectiveness in addressing real-world challenges. It opened the door for further exploration of UAV capabilities in various civilian sectors, including agriculture, environmental

monitoring, infrastructure inspection, and public safety (Labib et al., 2021). The regulatory changes following Hurricane Katrina paved the way for the integration of drones into civilian airspace, leading to the rapid growth of the commercial drone industry and the development of a wide range of applications that continue to expand today (Labib et al., 2021).

In the early part of the 2010s, the consumer drone market began to emerge, driven by efforts to adapt military UAV technology for civilian use (Timeline of Drone Integration | Federal Aviation Administration, 2022). Innovators recognized the potential for drones to become mainstream consumer products, offering diverse applications beyond their initial military purposes. A significant innovation was the introduction of a quadcopter in 2010, controllable via a smartphone or tablet (Miličević & Bojković, 2021). This development made drone technology accessible to the general public, featuring an intuitive interface and an affordable price point. Innovations like these lowered the barriers to entry for consumers and hobbyists interested in aerial technology, marking a pivotal shift in the perception of drones from specialized military tools to versatile gadgets suitable for both recreational and practical use.

By December 2013, major companies such as FedEx, UPS, Amazon, Google, and Uber recognized the immense potential of drones for delivery services and began exploring and testing various concepts to integrate UAV technology into their logistics operations (Timeline of Drone Integration | Federal Aviation Administration, 2022; El-Adle et al., 2023). These companies envisioned a future where drones could revolutionize last-mile delivery, offering faster, more efficient, and cost-effective solutions for transporting packages directly to customers' doorsteps. The initial experiments focused on overcoming technical and regulatory challenges, such as ensuring safe and reliable flight paths, managing air traffic, and complying with aviation regulations (El-Adle et al., 2023). These efforts marked the beginning of a transformative shift

in the logistics and delivery industry, driven by the promise of drone technology to enhance service delivery and customer satisfaction.

Later in 2013, technology advancements further revolutionized the consumer drone market with drones featuring user-friendly designs, integrated high-definition cameras, and advanced flight capabilities, setting a new benchmark for consumer drones (FAA, 2024). Equipped with GPS stabilization, automatic flight modes, and high-quality camera systems, these drones enabled users to capture stunning aerial photographs and videos effortlessly (FAA, 2024). The accessibility of high-quality aerial photography attracted not only hobbyists, but also professionals in fields such as real estate, filmmaking, and environmental monitoring, spurring significant growth in the consumer drone industry.

Since these technological advancements, the capabilities and applications of UAVs have continued to expand rapidly across multiple sectors (Miličević & Bojković, 2021). Technological advancements in battery life, payload capacity, navigation systems, and autonomous flight have significantly enhanced the performance and reliability of drones. These improvements have broadened the scope of UAV applications, extending beyond delivery services to include agriculture, infrastructure inspection, environmental monitoring, and emergency response (Schulzke, 2018). The growing versatility and utility of drones have fueled a burgeoning market, with industry analysts projecting the global UAV market to be worth $92 billion by 2030 (Onag, 2020). This rapid growth underscores the increasing importance of drones in both commercial and consumer markets, driven by ongoing innovation and expanding use cases.

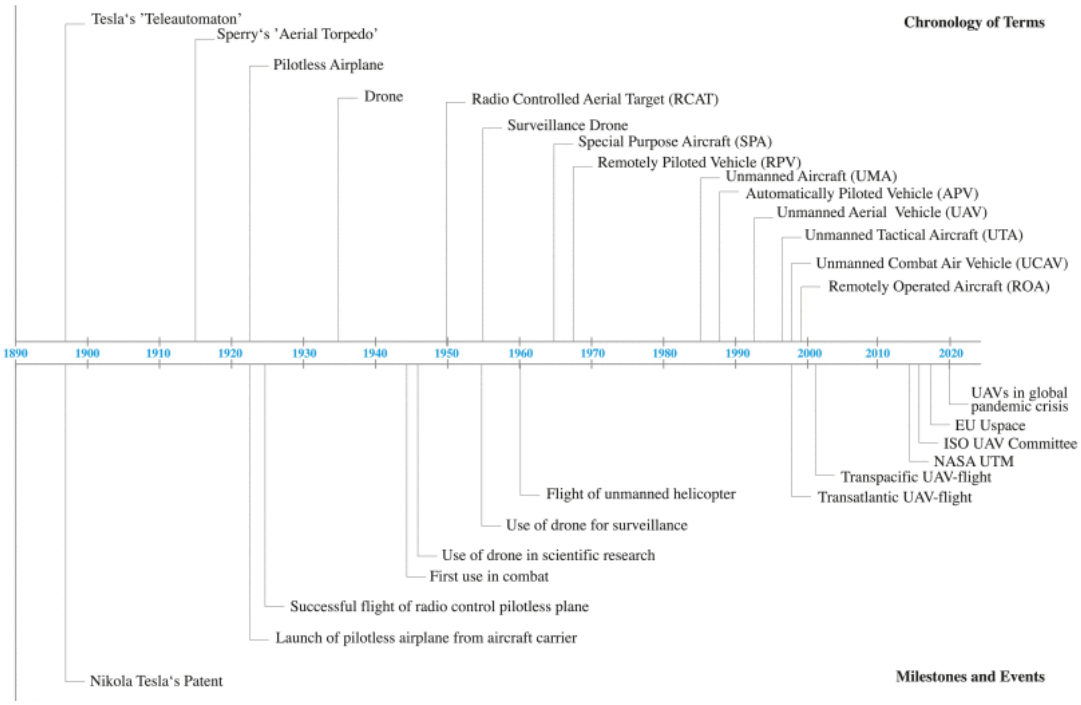
The COVID-19 Pandemic further redefined the critical role that drones can play in addressing global challenges and managing crises. During the pandemic, drones were deployed

for various tasks, including quarantine enforcement, mass disinfection of public spaces, and the delivery of medical supplies to hard-to-reach areas (Mohsan et al., 2022). In cities around the world, drones equipped with loudspeakers and cameras were used to monitor compliance with social distancing measures and communicate public health messages (Mohsan et al., 2022). Additionally, UAVs played a vital role in transporting essential medical supplies, such as personal protective equipment (PPE) and medications, to remote or isolated communities, ensuring timely delivery without risking human contact (Mohsan et al., 2022; Fink et al., 2023).

The progression of drone technology from its early military applications to its widespread use in fields such as cinema, agriculture, and beyond has significantly influenced both technological and societal landscapes. The potential advancements in drone technology promises not only continued innovations, but also to introduce new challenges and opportunities in areas such as regulation, ethics, and societal integration. The evolution of drone technology demonstrates how continuous advancements can drive substantial changes across multiple domains, fundamentally reshaping our interactions with technology and its applications for diverse purposes. See Figure 2.2 for a chronological timeline of drone technology terms.

Figure 2

Overview of Chronology of Drone Technology Terms



Note. This model summarizes the chronology of terms in the evolution of drone technology. From "The Rise of Drones in Internet of Things: A Survey on the Evolution, Prospects and Challenges of Unmanned Aerial Vehicles," by Labib et al., 2021, IEEE Access, 9, p. 115466–115487. https://doi.org/10.1109/access.2021.3104963 and "Unmanned Aviation: A Brief History of Unmanned Aerial Vehicles," by Newcome, 2004, USA: American Institute of Aeronautics and Astronautics.

Technical Capabilities

The technical capability analysis of current and emerging drone technologies requires a comprehensive examination of several key factors, particularly range, payload capacity, and autonomy, to understand their operational capabilities and associated risks. Range, a critical determinant of a drone's operational envelope, varies significantly across different types of drones. Short-range models, defined by Public Law 112–95 (2012) as unmanned aircraft weighing less than 55 pounds, typically cover a few miles and are often used in recreational activities. In contrast, long-range drones, capable of traversing hundreds of miles, are primarily

employed in military and expansive commercial operations. Advances in battery technology, communication systems, and propulsion efficiency have significantly extended the operational range of drones. Xiao et al. (2023) highlighted improvements in lithium-ion batteries that enhance drone endurance.

Initially defined by the FAA in February, 2012, UAVs have evolved from simple aircraft operating without direct human intervention to complex systems known as UASs (Public Law 112-95, 2012). This shift, recognized by the FAA (2022), encompasses not only the aircraft but also the ground-based controllers and the communication links between them. At the heart of UAV technology is the ability to fly autonomously or under remote control. Autonomous UAVs, powered by advancements in artificial intelligence (AI) and machine learning, navigate through pre-programmed flight plans or make real-time decisions independently (FAA, 2022b). Conversely, remotely piloted UAVs are controlled by operators from ground stations through a blend of human skill and technological prowess (FAA, 2022b).

This duality of operation modes opens up a plethora of applications, ranging from military operations, where they offer a safer alternative for reconnaissance and surveillance, to agriculture, where they enable precision farming practices (Barka, 2019). UAVs also play critical roles in search and rescue operations, environmental monitoring, and even commercial ventures like aerial photography and delivery services (Barka, 2019). As UAV technology continues to advance, its integration into various sectors promises to bring new opportunities and challenges, particularly in terms of regulation, ethical considerations, and seamless integration into national airspace systems (FAA, 2022b). The evolution of UAVs from simple unmanned aircraft to integral components of sophisticated UAS reflects a growing appreciation of their potential to revolutionize industries and practices worldwide.

In contrast to UAVs, the term RPA emphasizes the role of a human pilot in controlling the aircraft from a remote location (FAA, 2002). Unlike autonomous UAVs, RPAs are directly controlled by human operators. This definition aligns with the International Civil Aviation Organization's (ICAO) terminology, reflecting a global consensus on the importance of distinguishing between fully autonomous systems and those under direct human control. Commercial and recreational UAS operations typically involve a single pilot; however, more sophisticated systems, such as those used in military operations, may incorporate an additional operator to manage ancillary systems like sensors and communication devices not directly related to flight (FAA, 2022b). Within a UAS framework, neither pilots nor operators are situated within the aircraft, operating instead from a location often remote from the aircraft's operational zone.

Payload capacity, another crucial aspect, defines the maximum weight a drone can carry, directly impacting its utility across various applications. For instance, in agriculture, drones equipped with advanced sensors and spraying mechanisms require substantial payload capacities to be effective. Consumer drones typically have a payload capacity ranging from 0.5 to 5 pounds, while commercial drones, such as the DJI Matrice 600 Pro, can carry up to 13 pounds, making them suitable for heavy cameras or agricultural spraying equipment (FAA, 2022; Support for Matrice 600 Pro, 2024). Some industrial drones can carry payloads exceeding 500 pounds in addition to the aircraft's own weight, enabling the transport of significant equipment and supplies (Hecken et al., 2021).

Military drones, such as the MQ-9 Reaper, boast payload capacities of approximately 3,750 pounds, including armaments and sensor packages (FAA, 2022b). Recent research highlights the development of lightweight yet robust materials and innovative design techniques

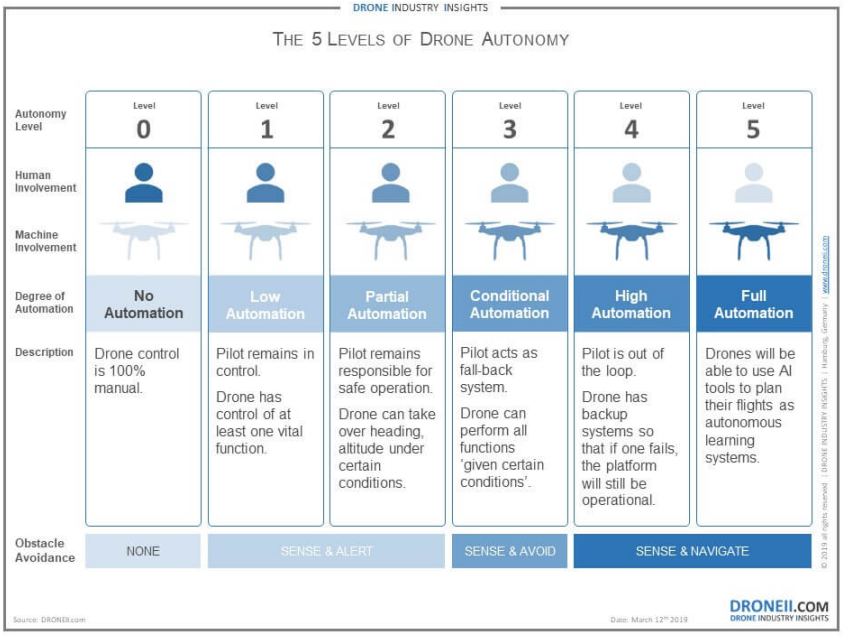
to maximize payload efficiency without compromising flight performance (Arun et al., 2023; García-Gascón et al., 2022). Additionally, the integration of modular payload systems has allowed for greater flexibility, enabling drones to switch between different operational roles seamlessly.

Autonomy, defined as the ability of drones to operate without human intervention, has seen remarkable advancements with the incorporation of artificial intelligence (AI) and machine learning (ML) (Tech Talk: Identify Drone Autonomy - Drone Industry Insights, 2019). Autonomous drones equipped with advanced navigation systems, real-time data processing capabilities, and adaptive algorithms can perform complex tasks such as real-time surveillance, search and rescue missions, and precision agriculture with minimal human oversight. The five levels of autonomy range from basic assisted flight, such as altitude hold and GPS-based navigation seen in commercial and consumer drones, to high autonomy, where drones can perform entire missions without human intervention (Tech Talk: Identify Drone Autonomy - Drone Industry Insights, 2019).

For example, the Skydio 2 drone, manufactured by the United States-based company Skydio, can navigate complex environments autonomously with advanced obstacle avoidance and AI, while research is pushing towards full autonomy where drones can handle complex situations without human input (Skydio Inc., 2024). Research conducted by Nouacer et al. (2020) and Hussein et al. (2021) delved into the development of robust autonomy frameworks that ensure operational safety and reliability, addressing challenges related to obstacle avoidance, dynamic decision-making, and environmental adaptability. These advancements reflect the potential and complexity of integrating highly autonomous drones into various sectors. See Figure 2.3 for a graphical depiction of the five levels of drone autonomy.

Figure 3

Overview of the 5 Levels of Drone Autonomy



Note. This model summarizes the five levels of drone autonomy. From Tech Talk: Identify Drone Autonomy - Drone Industry Insights, by Tech Talk, March 7, 2019, https://droneii.com/drone-autonomy

Understanding these technical capabilities is pivotal in identifying potential risks and vulnerabilities associated with drone operations. The increasing range and payload capacities potentially pose significant challenges in terms of airspace management, privacy concerns, and security threats. Autonomous operations, while enhancing efficiency, also raise critical issues regarding accountability, control, and the potential for misuse.

UAS Communication Links

The communication links that facilitate interaction between the drone and the control station are critical technological conduits ensuring the seamless operation of UASs worldwide. These links comprise a sophisticated array of hardware and software designed to transmit control

signals, navigational commands, and real-time data between the remotely located pilot and the UAV's actual operating location. Utilizing a combination of radio frequencies, satellite communications, and sometimes cellular networks, these communication systems allow for the transmission of vital operational parameters, including altitude, speed, and GPS positioning, as well as sensor and camera feeds from the UAV to the control station. This enables the remote pilot in command to monitor the UAV's status, make informed decisions, and steer the aircraft with precision. Furthermore, the integrity and security of these links are paramount, as they must prevent unauthorized access and ensure reliable control under varying environmental conditions and potential electronic interference, thereby safeguarding the operational efficacy and safety of the UAS missions.

Radio Frequency Links

Radio Frequency (RF) links represent a foundational technology in the realm of UAS operations, primarily facilitating communication for short to medium range flights. The Federal Communications Commission (FCC), as of 2023, noted that UAS RF links utilize a spectrum of frequency bands, prominently including the 900 MHz, 2.4 GHz, and 5.8 GHz bands. These frequencies are particularly favored within the industry due to their optimal balance between transmission range and data bandwidth capacity, making them suitable for a variety of UAS applications (ICAO, 2019).

The selection of a specific frequency band for UAS operations is influenced by several critical factors. Regulatory restrictions play a significant role, as different regions may have specific guidelines and limitations regarding the use of certain frequency bands for aerial communication. This necessitates thorough knowledge and compliance with local and international regulations to ensure legal UAS operations.

Interference potential is another decisive consideration. The chosen frequency band must minimize the risk of signal disruption, which can be caused by the presence of other electronic devices operating on similar frequencies. This is particularly crucial in densely populated or highly industrialized areas, where the spectrum can become crowded, leading to potential signal interference. The 2.4 GHz band, for example, is commonly used for Wi-Fi, Bluetooth, and other wireless communications, making it susceptible to interference in urban environments (FCC, 2023). Conversely, the 900 MHz and 5.8 GHz bands might offer less crowded alternatives, albeit with their own limitations and considerations (FCC, 2023).

Non-line-of-sight operations also influence the choice of frequency band. Certain UAS missions require the capability to communicate effectively even when the UAV is not directly visible to the control station, necessitating signals that can propagate over longer distances or penetrate obstacles (FCC, 2023). Lower frequency bands, such as 900 MHz, are generally better at navigating through or around obstructions compared to higher frequencies, which may be more suitable for line-of-sight operations but offer higher data rates (FCC, 2023). This dynamic interplay between technology, regulation, and operational needs underscores the complex nature of UAS operations.

Satellite Communications Links

For long-range UAS operations that extend beyond the visual range of the control station, satellite communications (satcom) emerge as the primary mechanism for command and control. This is exemplified by the operations of RPA like the USAF RQ-4 Global Hawk, a high-altitude, long-endurance UAS designed for global reconnaissance missions (Secretary of Defense, 2018). According to the Secretary of Defense in 2018, satcom links are indispensable for controlling these RPAs over extensive distances, encompassing international waters and isolated regions.

The utility of satcom in such contexts emphasizes its critical role in enhancing the operational reach and flexibility of long-range UAS missions.

Satcom links offer several unique advantages, chief among them being the ability to provide global coverage (ICAO, 2019). This is particularly vital for missions requiring operational capabilities over geographically dispersed areas or in environments where traditional communication systems are impractical or unavailable. By leveraging satellite technology, control stations can maintain continuous communication with RPAs, regardless of their geographical location (Secretary of Defense, 2018). This global connectivity facilitates a wide range of applications, from surveillance and reconnaissance to disaster response and environmental monitoring, enabling UAS to operate in areas that are otherwise inaccessible (FCC, 2023).

However, the use of satcom links in UAS operations is not without its challenges. One significant drawback is the introduction of higher latency in the command-and-control loop compared to RF links (Department of Defense, 2015). This delay is attributed to the time it takes for signals to travel to the satellite and back to Earth, which can impact the timeliness of command execution and data receipt (Department of Defense, 2015). Such latency can be particularly critical in scenarios requiring real-time decision-making or rapid response to changing conditions (FCC, 2023).

Additionally, satcom requires a clear line of sight to the satellite to establish and maintain a stable connection. This requirement can pose operational limitations, especially in environments where physical obstacles or atmospheric conditions may obstruct the satellite's visibility (Rogers & Kunertova, 2022). Furthermore, the need for specialized equipment, such as

satellite dishes and transceivers capable of establishing and sustaining satellite links, adds to the complexity and cost of satcom-enabled UAS operations.

Despite these challenges, the strategic value of satcom for extending the operational capabilities of UAS, especially in long-range and international missions, is undeniable. As technology advances, ongoing innovations in satellite communication are expected to reduce latency, enhance signal reliability, and expand the bandwidth available for UAS operations (FCC, 2023). These developments will likely further solidify satcom's role as a critical enabler of global UAS activities, as it can potentially provide a robust and versatile communication backbone that supports a wide array of civilian and military applications.

Cellular Networks

The integration of existing cellular networks for command-and-control communications in commercial and recreational Unmanned Aircraft Systems (UAS) is becoming increasingly prevalent, as noted by the FAA (2022). This trend capitalizes on the widespread availability and robust infrastructure of cellular networks, which are particularly dense and reliable in urban and suburban areas. The utilization of these networks for UAS operations introduces a significant advantage in terms of coverage, enabling drones to operate efficiently over larger areas without the need for bespoke communication systems (FCC, 2023).

One of the most compelling aspects of leveraging cellular networks for UAS operations is the support for data-intensive applications. Given the high bandwidth characteristic of modern cellular networks, UAS can transmit large volumes of data in real time (FAA, 2022; FCC, 2023). This capability is crucial for a wide range of applications, from high-resolution video streaming for surveillance purposes to the rapid transfer of environmental data for research and monitoring

projects. The ability to handle such data-intensive tasks with ease opens new possibilities for UAS technology, enhancing their utility and effectiveness across various sectors (Sands, 2022).

The advent of advanced cellular technologies, such as Long-Term Evolution (LTE) and 5G networks, further augments the potential of UAS operations. These technologies offer significantly lower latency compared to previous generations, facilitating near-real-time command and control, which is essential for precise, responsive UAS maneuvering (FCC, 2023). Additionally, LTE and 5G networks are designed to support a large number of devices simultaneously, addressing one of the critical challenges in densely populated areas where network congestion could otherwise impair communication reliability (FCC, 2023).

The promise of LTE and 5G technologies for UAS operations extends beyond improved performance metrics. These networks also introduce the capacity for more complex and autonomous operations, enabling drones to make data-driven decisions on the fly based on vast amounts of information processed in real time (Sands, 2022). This capability paves the way for more sophisticated applications, including autonomous delivery services, advanced agricultural monitoring, and dynamic traffic management systems (Secretary of Defense, 2018).

The FAA's recognition of the potential for cellular networks to revolutionize UAS command-and-control communications underscores a significant shift towards more integrated, efficient, and sophisticated drone operations (FAA, 2022b). As cellular technology continues to evolve, with ongoing improvements in speed, latency, and connectivity, the scope for UAS applications is set to expand dramatically. These advancements are set to herald in a new era of innovation and utility in the drone industry.

Optical Communication Links

Optical communication links, encompassing technologies such as laser and infrared, represent a specialized yet less frequently utilized method for secure, high-bandwidth communication over short distances (Carrasco-Casado & Mata-Calvo, 2020). As noted by the Secretary of Defense in 2018, these systems are distinguished by their capacity to deliver exceptionally high data rates. This feature is particularly beneficial for applications that demand the transmission of high-definition video or substantial volumes of sensor data, as highlighted by researchers Carrasco-Casado and Mata-Calvo (2020). The ability to rapidly transfer large datasets or stream high-quality video in real time offers significant advantages for a variety of UAS applications, from surveillance and security operations to environmental monitoring and disaster assessment.

The primary strength of optical communication lies in its provision of highly secure and interference-free channels. Unlike RF or cellular communications, which can be susceptible to interception or jamming, optical links utilize light to transmit data, making unauthorized access or disruption considerably more challenging (Al-Nahhal et al., 2022). This aspect of optical communication is particularly appealing for military, government, and other sensitive operations where security is paramount.

However, the deployment of optical communication links in UAS operations is subject to certain limitations. A critical requirement for establishing a successful optical link is the necessity for a direct line of sight between the transmitter and receiver. This constraint implies that any physical obstruction, whether buildings, terrain, or even moving objects, can disrupt the communication link, thereby restricting the operational flexibility of UAS relying on this technology (Al-Nahhal et al., 2022). Furthermore, optical communications are vulnerable to atmospheric conditions (Carrasco-Casado & Mata-Calvo, 2020). Factors such as fog, rain, or

dust can significantly attenuate the light signal, impacting the reliability and quality of the transmitted data. These environmental sensitivities necessitate careful consideration of operational environments and may limit the applicability of optical links to specific conditions and contexts.

Despite these challenges, the development and integration of optical communication technologies into UAS operations continue to advance. Innovations aimed at increasing the robustness of optical links against atmospheric disturbances and enhancing alignment technologies to maintain line of sight are gradually overcoming historical limitations (Al-Nahhal et al., 2022). The ongoing research and development in this field promise to expand the utility of optical communication, making it a more viable option for a broader range of UAS applications (Al-Nahhal et al., 2022).

While optical communication links currently occupy a niche within UAS communication strategies due to their specific requirements and limitations, their potential for secure, high-bandwidth data transmission positions them as a strong potential technology for future advancements within the UAS ecosystem. As technical improvements are made, optical links may offer compelling solutions for scenarios demanding high data throughput and unparalleled security. This would be a complementing technology to existing RF and cellular communication methods in the diverse ecosystem of UAS operations (Carrasco-Casado & Mata-Calvo, 2020).

Critical Infrastructure Protection (CIP)

Following the risk assessment, the framework emphasizes Critical Infrastructure Protection (CIP). This aspect focuses on safeguarding essential systems, particularly the electrical grid, from disruptions or attacks facilitated by drone technologies. The CIP component entails identifying specific vulnerabilities within critical infrastructure that could be exploited by

drone technologies. This includes physical vulnerabilities, such as the susceptibility of power lines and substations to drone strikes, as well as cybersecurity vulnerabilities, such as the potential for drones to be used as vectors for cyber-attacks.

Developing protective measures is a key part of this component. This involves both preventive and responsive strategies, such as deploying anti-drone technologies, enhancing physical security around critical assets, and implementing advanced cybersecurity protocols. Additionally, establishing robust emergency response protocols is crucial to ensure that responses to drone-related incidents are swift and effective, minimizing the impact on critical infrastructure.

Origin and Application of CIP

The CIP framework originated in the context of national security and public policy, aimed at safeguarding essential systems and assets that are crucial for the functioning of a society and economy (Rigaud et al., 2024). Originally, the focus of CIP was primarily on physical security measures designed to protect critical infrastructure components, such as power plants, water treatment facilities, and transportation systems, from threats like terrorism, sabotage, and natural disasters (Department of Homeland Security [DHS], 2013; Dawson et al., 2021). This initial application was driven by the recognition that the disruption or destruction of any of these components could have severe consequences for national security, public health and safety, economic stability, and the overall well-being of a nation (DHS, 2013; Dawson et al., 2021).

The origin of formal CIP efforts can be traced back to the latter part of the 20th century, particularly in the United States, with the issuance of Presidential directives and the establishment of national programs aimed at identifying critical infrastructures and developing

strategies to protect them (DHS, 2013; Dawson et al., 2021). These early initiatives laid the groundwork for a coordinated approach to CIP. It emphasized the importance of collaboration between government agencies, the private sector, and other stakeholders responsible for the management and protection of critical infrastructure.

In current studies and applications, the CIP framework has evolved to address the complexities introduced by technological advancements, particularly the increasing digitization of critical infrastructure systems and the growing threat of cyber-attacks (Chowdhury & Gkioulos, 2021). Today, CIP not only encompasses physical security measures but also cyber security, information security, and the resilience of critical infrastructure systems (Chowdhury & Gkioulos, 2021). This broader approach recognizes that critical infrastructures are increasingly interconnected and reliant on information and communication technologies, making them vulnerable to a wider range of threats that can cross traditional physical boundaries.

Modern CIP strategies involve a comprehensive risk management approach that includes threat identification, vulnerability assessment, risk analysis, and the implementation of protective measures to mitigate both physical and cyber risks. This includes the development of standards and guidelines for cybersecurity, the adoption of best practices for resilience and redundancy, and the establishment of incident response and recovery plans to ensure the continuity of critical services in the event of a disruption or attack (Rigaud et al., 2024). Furthermore, current applications of the CIP framework emphasize the importance of information sharing and collaboration among stakeholders across sectors and national borders. The recognition that critical infrastructure systems often span multiple jurisdictions and sectors has led to the development of information sharing and analysis centers (ISACs) and public-private partnerships

to facilitate the exchange of threat intelligence and best practices for infrastructure protection (Rigaud et al., 2024).

The evolution of the CIP framework from its original focus on physical security to its current comprehensive approach reflects the changing landscape of threats and the increasing recognition of the importance of protecting the critical infrastructures that underpin modern society. This evolution demonstrates an adaptive response to emerging challenges. This evolution ensures that the framework remains relevant and effective in safeguarding essential services against both traditional and novel threats (Chowdhury & Gkioulos, 2021).

CIP and National Security

According to the U.S. Department of Homeland Security (2023), CIP is a cornerstone of national security, emphasizing the need to safeguard essential systems and assets that underpin society's functioning, economic stability, and public safety. In recent years, the rise of drone technology has presented both revolutionary advantages and significant security challenges (Ivanović & Baić, 2020). The potential for drones to conduct surveillance, monitor infrastructure, and respond to emergencies grows each year with advances in drone, communication, and imaging technology. However, real-world incidents of drone incursions and attacks underscore the urgent need to protect critical infrastructure, such as the Western Interconnection electrical grid, from potentially evolving drone threats (Critical Infrastructure | Homeland Security, 2023).

One such incident occurred in December 2018 at Gatwick Airport in the United Kingdom, where drone sightings caused the airport to shut down for 36 hours, affecting over 140,000 passengers and disrupting 1,000 flights (Mezzofiore, 2018). This incident highlighted the vulnerability of critical infrastructure to relatively simple yet highly disruptive drone

incursions. The inability to quickly identify and neutralize the drones identified significant gaps in the security framework, leading to widespread economic and operational repercussions.

Another alarming example is the September 2019 drone attack on Saudi Arabia's Abqaiq oil processing facility and Khurais oil field. The drones caused extensive damage, temporarily halting half of the country's oil production, which equated to about 5% of global daily oil supply (Attacks on Saudi Oil Facilities: Effects and Responses, 2019). This attack demonstrated the capacity of drones to inflict substantial harm on critical energy infrastructure, with far-reaching implications for global markets and geopolitical stability.

On April 22, 2015, a drone carrying radioactive material was found on the roof of the Japanese Prime Minister's office, raising concerns about the potential for drones to be used in acts of terrorism (Ripley, 2015). Although no one was harmed, the incident underscored the threat posed by drones to national leaders and government buildings. This incident also exposed drones' potential use in targeted attacks on high-value infrastructure.

Non-State Actors. Over the last decade, the proliferation and utilization of UAVs by non-state actors have emerged as a significant and troubling phenomenon (Kallenborn et al., 2022; Krichen et al., 2022; Haugstvedt, 2023). This development, particularly evident over the last five years, has seen various violent non-state groups, including FTOs, insurgents, and criminal cartels, acquiring and deploying these sophisticated technologies to further their strategic objectives (Kallenborn et al., 2022; Haugstvedt, 2023). The use of armed UAVs has been predominantly concentrated in conflict zones within the Middle East and Central Asia, with notable incidents reported in Iraq, Syria, Yemen, and Afghanistan (Haugstvedt, 2023). However, the geographical scope of this threat is expanding, with evidence of UAV usage by non-state actors in Ukraine, Myanmar, Mexico, and Ecuador (Haugstvedt, 2023).

Hezbollah and Hamas are among the earliest adopters of armed UAVs, largely due to support from Iran (Kallenborn et al., 2022; Haugstvedt, 2023). These groups pioneered the use of drones for reconnaissance and combat, setting a precedent that has been followed by other entities such as ISIS and Hayat Tahrir al-Sham, who have used UAVs extensively in their operations in Iraq and Syria (Zimmerman, 2023). The Houthis in Yemen have also leveraged UAV technology to conduct attacks against both Yemeni government forces and the Saudi-led coalition. The Taliban's use of drones, primarily for surveillance, has evolved to include armed attacks, reflecting similar tactics used by ISIS (Haugstvedt, 2023). Additionally, criminal organizations, particularly Mexican cartels, have adapted these methods to their context, using drones to carry out attacks against law enforcement and rival groups (Kallenborn et al., 2022; Haugstvedt, 2023; Zimmerman, 2023).

The timeline of UAV usage by non-state actors indicates a significant increase in incidents from January 2016 onwards, with ISIS playing a pivotal role in this surge (Haugstvedt, 2023). ISIS's innovative use of commercial quadcopters modified to drop grenades has inspired other groups, including the Taliban and Mexican cartels, to adopt similar tactics (Kallenborn et al., 2022; Haugstvedt, 2023). Other non-state actors in Myanmar and Ukraine have been documented using armed drones in their respective conflicts (Haugstvedt, 2023). The dual-use nature of UAVs, capable of both surveillance and direct attack, has made them a versatile tool in the arsenals of these groups.

The procurement of UAVs by non-state actors varies but generally includes direct support from state sponsors, as seen with Iran's backing of Hezbollah and Hamas, and the modification of commercially available drones (Haugstvedt, 2023). The rise of 3D printing technology has contributed to the creation and enhancement of UAV components and weaponry,

potentially enabling more sophisticated and autonomous capabilities in the future (Kallenborn et al., 2022; Krichen et al., 2022; Haugstvedt, 2023). This technological advancement poses a significant challenge for counter-terrorism and security efforts globally.

The adaptation cycle between state and non-state actors is particularly noteworthy. Non-state actors have been observed to learn from and mimic state military tactics, while state actors, in turn, adopt innovations developed by non-state actors (Haugstvedt, 2023). This phenomenon has been prominently displayed in the Ukraine conflict, where Ukrainian forces have employed commercially available drones in a manner reminiscent of non-state actors' tactics in other conflict zones (Haugstvedt, 2023). This cyclic adaptation reflects the dynamic nature of modern warfare, where both state and non-state actors continually evolve their strategies and technologies based on observed successes and failures.

In a recent example of a traditional attack plan, Sarah Beth Clendaniel, a 36-year-old woman from Catonsville, Maryland, was sentenced to 18 years in prison with lifetime supervision for plotting to attack power stations around Baltimore as part of a White supremacist-inspired domestic terrorism/anti-government plan (U.S. Department of Justice Office of Public Affairs, 2024). The foiled plot, masterminded by co-conspirator Brandon Russell, aimed to destabilize the government and could have caused $75 million in damages and widespread power outages and led to Clendaniel's arrest in Month 2023 (MWSCDBRPG, 2024). This attack plan demonstrates how traditional defense systems are ill-equipped to handle the unique challenges posed by drones' rapid deployment, remote control capabilities, and stealth characteristics (Kallenborn et al., 2022; Lappas et al., 2022).

The increasing acquisition and use of armed UAVs by non-state actors present a multifaceted and evolving threat. These groups have demonstrated considerable ingenuity in

adapting commercially available technologies for their purposes, posing significant challenges to national and international security frameworks. Understanding the dynamics of non-state actors' use of UAVs and their potential future developments is essential for developing robust and effective countermeasures.

Mini-Drone Swarm Technology. Mini-drone swarms, a burgeoning area within UAV technology, present a myriad of practical applications, intricate challenges, future possibilities, and security risks. A mini-drone swarm is an innovative and advanced configuration of small, lightweight unmanned aerial vehicles (UAVs) designed to operate cohesively as a unit (Lehto & Hutchinson, 2020). These swarms are characterized by their sophisticated coordination and communication capabilities, which are facilitated by cutting-edge technologies in artificial intelligence (AI) and machine learning. Each mini-drone within the swarm is equipped with sensors, GPS, and communication systems that enable real-time data sharing and synchronized movements (Lehto & Hutchinson, 2020). The collective behavior of these drones allows them to execute complex tasks with remarkable efficiency and precision, often surpassing the capabilities of individual drones.

This technology draws inspiration from natural swarming behaviors observed in birds, fish, and insects, translating these biological phenomena into autonomous, artificial systems. Mini-drone swarms have significant applications across various domains, including military and defense for surveillance and reconnaissance missions, disaster management for search and rescue operations, agriculture for precision farming, environmental monitoring for tracking wildlife and assessing ecological damage, and commercial activities such as aerial photography, infrastructure inspection, and package delivery (Lee & Shim, 2018). Despite their promising capabilities, the deployment of mini-drone swarms faces challenges related to regulatory

compliance, technological limitations, safety, and security concerns, all of which necessitate ongoing research and development to fully realize their potential (Lee & Shim, 2018). As such, mini-drone swarms represent a critical area of study in the field of UAV technology, with the potential for significant impacts on a wide array of industries and applications.

The operational efficacy of these UAV swarms hinges on robust communication systems, enabling seamless coordination and execution of complex tasks with minimal human intervention, assisted by advancements in AI and machine learning. In the realm of military and defense, mini-drone swarms offer strategic advantages through enhanced surveillance, reconnaissance, and precision strikes, covering extensive areas swiftly and efficiently (Lehto & Hutchinson, 2020). Their utility extends to disaster management, where they can conduct rapid surveys of affected regions, provide real-time data, and aid in locating survivors (Munawar et al., 2022). In agriculture, mini-drones assist in precision farming by monitoring crop health, applying pesticides accurately, and optimizing resource utilization (Lachow, 2017). Environmental monitoring benefits from their deployment in tracking wildlife, assessing ecological damage, and conducting scientific research in remote or hazardous areas (Lachow, 2017).

Commercially, these swarms can be employed for infrastructure inspection, aerial photography, and logistics, including last-mile delivery services, thus enhancing efficiency and reducing operational costs (Lehto & Hutchinson, 2020; El-Adle et al., 2023). However, the widespread adoption of mini-drone swarms is impeded by several challenges. Regulatory frameworks are still evolving, requiring coordination across different jurisdictions to facilitate broader deployment (Lehto & Hutchinson, 2020; Munawar et al., 2022; El-Adle et al., 2023; Lachow, 2017).

Technological limitations, such as battery life, communication range, and payload capacity, constrain their operational capabilities. Ensuring the safety and reliability of swarm operations, particularly in densely populated areas, remains a significant concern, necessitating advancements in safety protocols and real-time data processing algorithms for effective swarm coordination (Lehto & Hutchinson, 2020). Security issues, particularly cybersecurity threats, pose substantial risks as mini-drone swarms are vulnerable to hacking and malicious attacks, which could have dire consequences for public safety and national security (Lehto & Hutchinson, 2020; Schulzke, 2018).

These incidences of drone incursions and the use of drones as weapons of war/attack, highlight the need for robust counter-drone measures to be investigated and potentially integrated into CIP strategies. Effective counter-drone systems should encompass a multi-layered approach, combining detection, identification, tracking, and neutralization technologies (Kallenborn et al., 2022; Labib et al., 2021). While drone technology offers substantial benefits for enhancing the resilience and operational efficiency of critical infrastructure, real-world incidents, like those previously discussed, have demonstrated the high-risk drones pose to life and infrastructure if used in an offensive/hostile manner. Safeguarding essential systems and assets from drone-related threats requires an integrated approach that combines advanced technological solutions with stringent regulatory measures (Kallenborn et al., 2022; Labib et al., 2021; Zimmerman, 2023). By learning from historical incidents and continuously evolving CIP strategies, stakeholders can effectively mitigate risks, ensuring the secure and uninterrupted operation of critical infrastructure crucial to national security and public welfare.

Regulatory Adaptation to Technological Advancements

The final component of the framework is Regulatory Adaptation to Technological Advancements. This involves a critical examination of how regulatory bodies, particularly the Federal Aviation Administration (FAA), have responded to the rapid development and widespread deployment of drone technologies. The analysis includes a historical overview of regulatory changes, identifying gaps in the current regulatory frameworks, and proposing dynamic, flexible regulatory approaches that can quickly adapt to new technological realities and emerging risks.

This component underscores the necessity for regulatory bodies to be proactive rather than reactive. By anticipating future developments in drone technology and understanding their potential implications, regulatory agencies can develop forward-thinking policies that both mitigate risks and support technological innovation. This includes creating agile regulatory processes, pilot programs to test new regulatory approaches, and fostering public-private partnerships to enhance regulatory efficacy.

Origin and Application of Regulatory Adaptation to Technological Advancements

The Regulatory Adaptation to Technological Advancements framework originates from the broader field of regulatory theory, which examines how laws and regulations evolve in response to changes in society, including technological innovation (Calandrillo et al., 2020). Originally, this framework was applied in a reactive manner, with regulations often being developed or amended after a new technology had already become widespread and its impacts—both positive and negative—had become apparent (Rigaud et al., 2024). This approach was partly due to the slower pace of technological change in the past and the time it took for the full implications of new technologies to be understood. For example, early regulations in the

automotive industry focused on safety and manufacturing standards only after cars became a common feature of urban landscapes (Alsoliman et al., 2023).

In these initial applications, the regulatory framework aimed to balance the promotion of technological innovation and its economic benefits with the protection of public health, safety, and the environment. Regulations were often sector-specific, addressing the particular risks and challenges associated with specific technologies or industries (Caparini & Gogolewska, 2021). This approach resulted in the development of a patchwork of regulations that could be rigid and slow to adapt to new technological developments.

In current studies and applications, the framework for Regulatory Adaptation to Technological Advancements has evolved to be more proactive and dynamic, reflecting the accelerated pace of technological change and the complex, interconnected nature of modern technologies (Caparini & Gogolewska, 2021). There is an increased emphasis on anticipatory governance, which seeks to foresee and address potential regulatory challenges before they arise. This involves ongoing monitoring of technological trends, stakeholder engagement, and the development of flexible regulatory mechanisms that can be quickly adjusted as new information becomes available or as technologies evolve.

Furthermore, current applications of the framework often employ a multi-stakeholder approach, involving collaboration between governments, industry, academia, and civil society to develop regulations that are both effective and socially acceptable (Calandrillo et al., 2020). This approach acknowledges that regulatory bodies alone may not have the necessary expertise to fully understand the implications of complex technologies, such as artificial intelligence, biotechnology, and cybersecurity. By engaging a broader range of perspectives, regulators aim to create more informed, balanced, and agile regulatory responses.

Additionally, there is a growing recognition of the need for international cooperation in regulatory adaptation, as many technological advancements, particularly in the digital domain, transcend national borders (Caparini & Gogolewska, 2021). This has led to efforts to harmonize regulations across jurisdictions and to develop international standards and guidelines for emerging technologies. While the original use of the Regulatory Adaptation to Technological Advancements framework was more reactive and sector-specific, its application in current studies has become more proactive, inclusive, and geared towards fostering international collaboration. This evolution aims to better balance the promotion of innovation with the need to address the ethical, social, and security challenges posed by rapid technological change.

Federal Aviation Administration

Established by the Federal Aviation Act of 1958, the FAA serves as a pivotal agency within the United States Department of Transportation, tasked with the comprehensive regulation and oversight of civil aviation across the U.S (FAA, 2021; Federal Register, 2024). This establishment was driven by a growing concern for aviation safety, prompting the need for a dedicated body to oversee the burgeoning sector. The FAA's primary mission is to ensure the safety and efficiency of the nation's aerospace system, a commitment that encompasses a wide range of responsibilities (FAA, 2021). Among these duties are the regulation of air transportation, which involves setting and enforcing rules for all facets of civil aviation, certifying pilots and aviation professionals, registering aircraft, and overseeing the construction and operation of airports (FAA, 2021). The agency plays a critical role in maintaining the aviation standards making it an indispensable component of the United States transportation infrastructure.

International Civil Aviation Organization UAS Regulations Development

The International Civil Aviation Organization (ICAO) has adopted a comprehensive and methodical approach to crafting standards for UASs, in response to their rapid advancement and increasing presence in global airspace. This strategy is characterized by extensive collaboration with member states, industry stakeholders, and international aviation organizations, aimed at ensuring the safe, secure, and sustainable integration of UAS operations worldwide. Through this collaborative effort, ICAO (2018) sought to establish a coherent regulatory framework that addresses a wide array of concerns, ranging from safety and security to privacy and environmental impact.

The ICAO's contributions to this field encompass the development of standards and recommended practices (SARPs), alongside guidance materials and tools specifically designed for UAS operations, taking into account their distinctive characteristics and operational requirements (ICAO, 2019). The organization also plays a crucial role in coordinating international efforts to tackle challenges associated with airspace management, pilot licensing, and UAS traffic management systems. By adopting a proactive and inclusive approach, ICAO aims to support the UAS sector's burgeoning growth, ensuring its seamless and safe incorporation into the global aviation system (ICAO, 2019).

The regulatory framework for UAS operations, as structured by ICAO, is categorized into three primary risk-based groups, each outlining specific operational constraints and authorization requirements to maintain safety and compliance within the expansive aviation ecosystem. The "Low Risk" category permits UAS operations without prior regulatory approval, subject to adherence to predefined parameters like visual line of sight operation, maintaining safe distances from people, buildings, and aerodromes, and not exceeding certain altitudes (ICAO, 2019).

These operations, typically conducted in favorable weather conditions and within uncontrolled airspace, are restricted by aircraft specifications regarding weight and speed to mitigate risks.

The “Regulated Minimal Risk” category requires operational authorization from aviation authorities, based on a comprehensive safety risk assessment of the proposed operation (ICAO, 2019). This category encompasses operations with a slightly higher risk level. Flights with a closer proximity to populated areas or shared airspace with manned aircraft introduce risks and requirements for remote pilots to possess a basic understanding of aviation principles and for the UAS to adhere to elementary identification and reporting standards (ICAO, 2019).

The “Regulated Acceptable Risk” category imposes traditional aviation regulatory practices on UAS operations deemed to carry significant risk, possibly including flights beyond visual line of sight (ICAO, 2019). This highest tier of risk entails stringent operational limitations, pilot licensing, aircraft certification, and safety mitigations (ICAO, 2019). This category reflects the increased likelihood of interactions with manned aircraft and operations within densely populated or sensitive areas.

Summary

Overall, UAVs have undergone a profound transformation, evolving from rudimentary military tools into sophisticated systems that are now indispensable across various civilian sectors. These sectors include agriculture, where drones assist in precision farming by monitoring crop health and optimizing resource use; environmental monitoring, where they track changes in ecosystems and wildlife populations; disaster management, where they aid in search and rescue operations and damage assessments; and commercial enterprises, such as infrastructure inspection and aerial photography, where they provide efficient and cost-effective solutions. This technological evolution is primarily driven by advancements in UAV

capabilities, particularly in terms of range, payload capacity, and autonomy. Modern UAVs can cover extensive distances, carry significant loads, and operate autonomously, making them highly versatile and effective tools.

Despite these advancements, the proliferation of UAVs has introduced several significant challenges, especially in terms of security and regulation. UAVs have the potential to threaten critical infrastructure, such as the Western Interconnection electrical grid, through unauthorized surveillance, cyberattacks, and direct physical attacks. The advanced maneuverability and payload capabilities of drones enable them to infiltrate restricted areas, conduct illicit reconnaissance, and launch destructive payloads, posing serious risks to the security and stability of vital infrastructure. These threats necessitate the development of comprehensive security strategies that include advanced detection and neutralization technologies to counter airborne threats, robust cybersecurity measures to protect against cyber intrusions, and well-defined regulatory frameworks to govern the use and operation of UAVs.

The rapid pace of UAV technological advancements often outpaces the development of corresponding regulatory measures, creating a dynamic and challenging environment for policymakers. Balancing the need to mitigate security risks with the promotion of beneficial uses of UAVs requires a nuanced and adaptive regulatory approach. This includes the formulation of laws and guidelines that address the unique challenges posed by drones while encouraging innovation and the positive applications of UAV technology.

Effective coordination among various stakeholders is crucial for developing and implementing these strategies. Utility providers, regulatory bodies, law enforcement agencies, and defense organizations must collaborate to establish standardized protocols and ensure a

unified and efficient response to drone-related security incidents. This collaborative effort is essential for addressing the complex and evolving threat landscape posed by UAVs.

Additionally, the widespread use of surveillance and drone detection measures raises substantial privacy concerns. Policies must be crafted to balance the protection of individual freedoms with the need to secure critical infrastructure. Privacy considerations are integral to gaining public trust and ensuring that security measures do not infringe on civil liberties.

As UAV technology continues to advance, it presents both significant opportunities and formidable challenges. The potential benefits of drones in various applications are immense, but so are the risks associated with their misuse. To harness the potential of UAVs while safeguarding essential services and infrastructure, continuous innovation in security technologies, adaptive regulatory strategies, and effective stakeholder collaboration are essential. The evolving landscape of UAV technology necessitates a holistic approach that integrates security, technology, regulation, and respect for privacy to ensure the resilience and security of critical infrastructure. Building on this understanding, Chapter 3 outlines the research methodology, detailing the qualitative approach, data collection methods, and analytical strategies designed to explore SMEs' perspectives on drone threats to the Western Interconnection electrical grid.

Chapter 3: Research Method

The problem addressed by this study is the threat that current and emerging aerial drone technologies pose to the Western Interconnection electrical power grid, as perceived by subject matter experts (SME) from the U.S. Department of Energy (DOE), the Federal Energy Regulatory Commission (FERC), and the Western Electricity Coordinating Council (WECC). The purpose of this descriptive qualitative study was to analyze and identify the severity of risk posed by current and emerging commercial aerial drone technology to America's Western Interconnection Electrical Grid Infrastructure. The research involved a systematic evaluation of potential vulnerabilities that drones could exploit within the Western Interconnection Electrical Grid Infrastructure. Findings from the study were intended to guide policymakers and industry leaders in implementing strategies to mitigate these risks.

The arrival of drone technology marked the beginning of a new phase of security concerns that extends far beyond individual privacy, encompassing the safety and integrity of critical national infrastructure. As stated in Chapter 1, Zwickle et al. (2018) discussed how drone technology presents considerable concern not only for individual citizens' privacy and safety but also the protection and operation of a nation's critical infrastructure. The advanced and sophisticated capabilities of drones, many of which can be equipped with technologically advanced surveillance tools (i.e., high-resolution cameras, thermal sensors, etc.), enable the collection of personal data without consent, potentially facilitating unauthorized surveillance, corporate espionage, and data breaches (Kindervater, 2016; Labib et al., 2021).

A coordinated effort from national security stakeholders is essential to address the growing threat that drone technology poses to critical infrastructure, specifically the Western Interconnection Electrical Power Grid. This research sought to identify and highlight critical

weaknesses and points of failure vulnerable to drone attack in an effort to help equip organizations responsible for securing and maintaining these infrastructures with the knowledge and tools necessary to defend against potential drone attacks and sabotage. Additionally, this research sought to identify improvements and/or upgrades needed to the Western Interconnection electrical power grid to combat drone threats as perceived by SMEs familiar with this specific electrical infrastructure.

The implications of this research were expected to potentially lead to enhanced security protocols, improved infrastructure resilience, and the development of targeted countermeasures necessary to safeguard the Western Interconnection Electrical Power Grid from emerging drone-related threats as identified by subject matter experts. Furthermore, the insights and recommendations from this study could be applied on a national scale, helping to inform policies and strategies aimed at securing other critical infrastructures across the country. By addressing vulnerabilities within the Western Interconnection, this research could serve as a model for enhancing the security of power grids and other vital systems nationwide.

This research study built upon previous studies by expanding the understanding of the risks posed by drone technology to critical infrastructure. Prior research has explored the safety, privacy, and security threats posed by drones, including their use in surveillance, sabotage, and even terrorism (Zwickle et al., 2018; Kallenborn et al., 2022). This study specifically focused on a critical segment of the United States' regional electrical power grid systems (i.e., Western Interconnection), offering a more detailed analysis on how emerging drone technologies can exploit vulnerabilities in a system that serves over 80 million people and businesses (Western Interconnection, 2023). It considered foundational knowledge about drone weaponization and

unauthorized use, but added a unique layer by homing in on SMEs' perspectives from key regulatory and security agencies.

This research study was unique in its application of a qualitative research approach, which involves gathering detailed insights from those directly responsible for servicing, operating, and protecting the critical power grid. This contrasts with previous quantitative or theoretical studies, offering a more practical, in-depth understanding of how drone technology impacts this specific critical infrastructure. By doing so, the study provided actionable insights that went beyond the general concerns about drones, targeting specific vulnerabilities and suggesting tailored protective measures for the Western Interconnection, which could also inform national strategies.

Research Methodology and Design (Nature of the Study)

Qualitative Research Fundamentals

For researchers focusing on the exploration of complex phenomena, qualitative research methodology is a foundational approach through the use of detailed, contextual, and interpretive analysis (Jensen & Laurie, 2017). Unlike quantitative methods, which prioritize measurable data and statistical outcomes, qualitative research methodology is concerned with understanding the deeper meanings, experiences, and interactions within a given context (Foerstle et al., 2016; Jensen & Laurie, 2017).

Qualitative methodology's primary strength lies in its ability to delve into the "why" and "how" of human behavior, making it particularly valuable in areas where variables are not easily quantified or when the research aims to explore subjective experiences, attitudes, and motivations (Foerstle et al., 2016). The versatility of qualitative research extends across a wide range of disciplines, including but not limited to social sciences, healthcare, education, and

organizational studies, where capturing the intricacies of human experiences and social dynamics is vital (Jensen & Laurie, 2017).

Qualitative research methodology, with its broad applications across social sciences, healthcare, education, organizational studies, and other fields of study, offers a unique approach to capturing the complexity of real-world situations. This methodology prioritizes participants' perspectives, allowing researchers to explore attitudes, beliefs, and perceptions that provide nuanced insights into how individuals and groups experience their environments. According to Corbin and Strauss (2008), the qualitative toolkit, comprising of in-depth interviews, focus groups, participant observations, and case studies, enables the collection of additional insights and/or context through narrative data (i.e., actions, interactions, etc.) that quantitative methods may overlook.

As Mills (2019) highlighted, a distinguishing feature of qualitative research is its adaptability to identify emergent data, making it particularly valuable for studies in areas with limited prior research or when examining complex social phenomena and/or events. This flexibility facilitates the generation and refinement of theories, as researchers can iteratively develop conceptual frameworks based on their findings (Mills, 2019). The depth and richness of qualitative data contribute significantly to theory development and offer context-rich insights that inform policy, practice, and further research. By capturing cultural, social, and emotional dimensions, qualitative research provides a holistic understanding of how various factors interact within social and cultural contexts (Corbin & Strauss, 2008; Mills, 2019). This approach stands as a rigorous and valuable methodology in its own right, complementing quantitative methods while offering unique insights into the complexities of human experience and social dynamics (Corbin & Strauss, 2008; Mills, 2019).

Transferability of Study

The concept of transferability significantly enhances the potential impact and broader applicability of qualitative research studies (Mills, 2019). By utilizing clear assumptions about the relevance of participants' perspectives and the significance of the phenomena under study, researchers can draw contextual inferences about how findings might apply to other similar settings or situations (Mills, 2019). The analysis of contextual data provides specific meanings within the studied context, while the evaluation of applicability gauges how these findings can inform understanding or practices in comparable contexts (Corbin and Strauss, 2008; Mills, 2019).

This methodological research approach allows studies to surpass their specific settings, offering models or insights that could be adapted for similar situations and/or systems (Corbin & Strauss, 2008; Mills, 2019). The qualitative methodology, often focusing on in-depth perspectives from SMEs, often produces detailed and nuanced data that can be extrapolated for its potential relevance in a diverse group of settings and/or situations (Corbin & Strauss, 2008). Well-executed qualitative studies not only address the immediate concerns within their specific contexts, but also contribute to a broader theoretical understanding and practical applications in related fields, boosting their potential impact on knowledge development and practice (Corbin & Strauss, 2008; Mills, 2019).

Research Confirmability

In qualitative research, assessing the reliability and trustworthiness of data requires a focus on both methodological consistency and interpretative objectivity. Merriam and Tisdell (2016) emphasized the importance of clear and consistent data collection, which enhances the dependability of findings and safeguards against procedural variations across participants and

settings. This approach, as outlined by Jensen and Laurie (2017), theoretically allowed for study replication with similar results, further reinforcing dependability in qualitative research. Confirmability in qualitative studies is typically established through neutral methodological frameworks that allow the data to speak for itself without researcher bias.

To achieve this research objective, qualitative researchers often employ several strategies: maintaining comprehensive audit trails, engaging in reflexive practices, utilizing data triangulation, conducting member checks, and providing holistic descriptions of research contexts and procedures. Merriam and Tisdell (2016) advanced that these particular methodological approaches collectively strengthen qualitative data's dependability by demonstrating methodological consistency, while simultaneously bolstering confirmability by showing that results emerge from participants' experiences rather than researcher bias. The careful application of these strategies establishes a robust, verifiable research process amenable to external scrutiny in qualitative studies. By ensuring that results stem from participants' experiences rather than researcher preconceptions, confirmability underpins the credibility of qualitative research, enabling meaningful insights into complex social phenomena and contributing to the generation of authentic knowledge across various fields (Jensen & Laurie, 2017; Merriam & Tisdell, 2016).

Data Triangulation

Data triangulation in qualitative research serves as a methodological strategy to enhance the validity, comprehensiveness, and depth of findings through the integration of multiple data sources and perspectives. As developed by Carter et al. (2014), this approach involved the utilization of diverse data collection methods or the acquisition of information from varied sources, thereby constructing a multifaceted understanding of the phenomenon under

investigation. Patton (1999) argued this methodological approach facilitated a more nuanced and scholarly comprehension of complex social realities.

In empirical application, researchers employ various triangulation strategies in order to enhance the credibility and validity of their qualitative findings (Bans-Akutey & Tiimub, 2021). Method Triangulation, as described by Carter et al. (2014), involves the convergence of multiple data collection techniques, such as in-depth interviews, participant observations, and document analysis. This approach allowed for a comprehensive examination of the research subject from diverse methodological angles. Data Source Triangulation, another critical strategy, entails the collection of data across different temporal and spatial dimensions, enabling researchers to discern potential variations or consistencies in the phenomenon across these contexts (Carter et al., 2014).

The process of data triangulation extends beyond mere data collection to encompass rigorous analytical procedures. Bans-Akutey & Tiimub (2021) illustrated how researchers engage in comparative analysis of data derived from various sources, identifying patterns, convergences, and divergences. This analytical process, as previously articulated by Denzin (1978) and Patton (1999), serves to validate findings through the corroboration of evidence from multiple sources, thereby enhancing the credibility and robustness of the research conclusions.

Furthermore, the implementation of Investigator Triangulation, as described by Carter et al. (2014), involved the engagement of multiple researchers in the study of a singular phenomenon, followed by a collaborative synthesis of their individual findings. This approach mitigates potential researcher bias and enriches the interpretative depth of the study. Complementarily, Theory Triangulation, as elucidated by Polit and Beck (2012), involved the

application of diverse theoretical frameworks to the interpretation of data, facilitating a more comprehensive and multifaceted understanding of the research subject.

The integration of these varied triangulation techniques culminated in a research methodology that significantly enhances the validity, reliability, and depth of qualitative findings. As posited by Corbin and Strauss (2008), this approach contributed substantially to the scientific rigor and dependability of qualitative research. Ultimately, data triangulation enables researchers to construct a more holistic, nuanced, and empirically grounded understanding of complex social phenomena, thereby augmenting the scholarly contribution and practical applicability of qualitative research findings (Bans-Akutey & Tiimub, 2021).

Applying Qualitative Research Methodologies

This study employed a qualitative research methodological framework to build upon existing literature while focusing specifically on the Western Interconnection electrical power grid. The research drew from published academic works, including those of Calandrillo et al. (2020), Rogers and Kunertova (2022), Rogoway and Trevithich (2020), Schulzke (2018), Sims (2018), Zimmerman (2023), and Zwickle et al. (2018). Moreover, this research study was deliberately developed in such a way as to actively pursue and elicit expert insights, recommendations, and shared perspectives from individual SMEs charged with overseeing the maintenance, security, and operation of their respective portions and specific systems within the Western Interconnection electrical power grid.

The primary focus of this research was to obtain specific inputs identifying and highlighting the significance and severity of perceived risks posed by drone technology to the Western Interconnection Electrical Power Grid. Additionally, the study sought to determine necessary steps for safeguarding this critical system against future drone threats. This research

topic was pursued with the aim of strengthening and protecting critical infrastructure from evolving technological threats that are both easily weaponized and widely available to the general public. Ultimately, this research study aimed to identify key weaknesses in the Western Interconnection electrical power grid infrastructure, with the goal of driving advancements in regulatory reforms to better mitigate these perceived threats to national security.

Weighing Other Methodological Frameworks

The present study examined the emerging threat of UAS's to the Western Interconnection Electrical Power Grid, a critical component of national infrastructure security. While a qualitative methodology was ultimately employed, the selection of an appropriate research framework required careful consideration of various approaches, each presenting distinct advantages and limitations in addressing the multifaceted nature of this security challenge. This methodological deliberation was crucial, as it significantly influenced this research study's capacity to generate meaningful insights and inform policy decisions. The following discussion explores alternative methodological frameworks that were considered, analyzing their potential applications, strengths, and weaknesses in the context of investigating UAS threats to electrical grid infrastructure.

Mixed Methods. A mixed methods approach stood out as a potentially powerful tool for comprehensively examining drone threats. This methodology could have seamlessly integrated qualitative insights from SMEs at organizations like the FERC, and WECC with quantitative analysis of drone incident data or simulated threat scenarios (Jason & Glenwick, 2016). For instance, the researcher could have conducted in-depth interviews with grid security experts to understand their perceptions and experiences, while simultaneously analyzing statistical data on drone sightings near critical infrastructure or patterns in reported security breaches. This dual

approach could have provided a nuanced understanding of both the human and technical dimensions of the threat landscape.

The strength of mixed methods is its ability to triangulate findings, potentially enhancing the validity and reliability of the research (Jason & Glenwick, 2016). By addressing both the "why" and "how" questions through qualitative inquiry and the "how many" and "how often" questions via quantitative analysis, this approach could have offered a more holistic view of the drone threat (Jason & Glenwick, 2016). For example, it might have revealed not only the frequency of drone incursions near power facilities but also the underlying motivations and challenges in detecting and deterring such incidents.

That being said, this approach is certainly not without its own unique set of challenges. The complexity of integrating qualitative and quantitative data may have required advanced expertise and additional time, funding, and resources (Jason & Glenwick, 2016). Moreover, in the context of emerging threats like drones, the scarcity of robust quantitative data could have potentially limited the effectiveness of the quantitative component.

Case Study. Alternatively, a case study methodology could have provided deep, contextual insights into specific drone threat incidents or scenarios. This approach would have involved selecting and thoroughly examining particular cases, such as the widely reported drone sightings at the Palo Verde Nuclear Power Plant or other documented incidents involving the Western Interconnection Grid (Denzin et al., 2023, pp. 121–141). The researcher could have dissected these events, analyzing the nature of the threat, the effectiveness of response measures, and the subsequent impacts on security protocols and policies.

The case study method excelled in revealing the intricate interplay between various factors - technological capabilities, human decision-making, regulatory frameworks, and

environmental conditions (Denzin et al., 2023, pp. 121–141). It could have uncovered specific vulnerabilities in grid security and highlighted effective countermeasures through the lens of real-world events. For instance, a detailed examination of a thwarted drone incursion might have revealed critical gaps in early warning systems or showcased successful inter-agency coordination in threat response.

Further, it should be noted that the primary limitation of this approach is its potential lack of generalizability. The insights gained from a handful of cases, while valuable, might not have been representative of the broader threat landscape. Additionally, given the relatively recent emergence of drone threats to critical infrastructure, well-documented cases might have been scarce, potentially limiting the scope of analysis.

Quantitative Risk Assessment. A third methodological avenue, quantitative risk assessment, offered a data-driven approach to understanding and quantifying drone-related risks to the electrical grid. This method would have involved developing sophisticated mathematical models to assess the likelihood and potential impact of drone-based attacks on various components of the Western Interconnection (Aven, 2011, pp. 2–6). Researchers could have created probabilistic models that factored in drone capabilities, grid vulnerabilities, and potential cascading effects of targeted attacks.

The strength of quantitative risk assessment is its ability to provide objective, measurable risk metrics, which could have been invaluable for prioritizing security efforts and resource allocation (Aven, 2011, pp. 2–6). This approach would have enabled scenario modeling and "what-if" analyses, allowing stakeholders to explore the potential outcomes of different threat levels or countermeasures (Aven, 2011, pp. 2–6). For example, it could have helped quantify the risk reduction achieved by implementing various drone detection technologies at key grid

locations. However, the effectiveness of this method heavily depended on the quality and availability of input data. Given the evolving nature of drone technology and the limited historical data on drone attacks on power infrastructure, developing accurate risk models could have been challenging in regard to time and financial constraints. There was also a risk of oversimplification, as complex, dynamic threats might have been reduced to numerical values that failed to capture important qualitative aspects of the risk landscape.

Each of these methodologies offered a unique lens through which to examine the drone threat to electrical infrastructure. The mixed methods approach provided a balanced view, combining the richness of expert insights with the objectivity of numerical data. The case study methodology offered an opportunity for deep, nuanced exploration of specific incidents, potentially uncovering critical insights that might have been overlooked in broader analyses. The quantitative risk assessment approach provided a structured, data-driven foundation for decision-making in grid security efforts.

However, the selection of an appropriate methodology had to be guided by careful consideration of the specific research objectives, available resources, and the nature of accessible data. In the context of studying emerging threats like drones to critical infrastructure, each methodology presented both opportunities and challenges. The mixed methods approach, while comprehensive, required significant expertise and resources to effectively integrate diverse data types. The case study methodology, though rich in detail, might have struggled with broader applicability. The quantitative risk assessment, while offering objective measures, was challenged by the limited historical data and the rapidly evolving nature of drone technology.

Ultimately, the choice of methodology significantly influenced the nature of insights generated and their applicability to enhancing grid security. The researcher had to carefully

weigh the strengths and limitations of each approach against their specific research goals and the practical constraints of studying an emerging and dynamic threat landscape. This methodological decision was crucial not only for the academic rigor of the study but also for its potential to inform effective policy and security measures to protect critical electrical infrastructure from evolving drone threats.

Population and Sample

The target population for this research study consisted of individual SMEs from various fields of specialization, including electrical engineering and grid security, aerospace and drone technology, cybersecurity and information technology, law enforcement and counterterrorism, as well as regulatory and policy expertise. With regard to quantifying the total potential population sample, this researcher drew representative from three key organizations—DOE, FERC, and WECC—that play critical roles in overseeing, regulating, and managing the Western Interconnection electrical power grid. This approach ensured that the population had direct, relevant experience with the subject matter, while the diversity of expertise contributed to a comprehensive understanding of the complex issues surrounding drone technology and electrical grid security.

The DOE, as a federal executive department, plays a crucial role in overseeing national energy policy and security. Its broad mandate encompasses research and development in energy technologies, nuclear security, and the resilience of critical energy infrastructure. In the context of this study, the DOE's expertise is invaluable for understanding the overarching national security implications of drone threats to the power grid. Their involvement in cutting-edge research and policy formulation positions them uniquely to provide insights into emerging vulnerabilities and potential technological solutions.

The FERC, an independent agency, regulates the interstate transmission of electricity, natural gas, and oil. Its role in this study is pivotal, as it brings a regulatory perspective to the issue of drone threats. FERC's expertise was crucial for understanding how current regulations might address or fall short in mitigating drone-related risks to the power grid. Moreover, their insights could shed light on the challenges and opportunities in developing new regulatory frameworks to enhance grid protection against evolving technological threats.

The WECC, responsible for coordinating and promoting bulk electric system reliability in the Western Interconnection, brings practical, on-the-ground expertise in grid operations and security. Their regional focus was particularly relevant, as they deal with the day-to-day realities of maintaining grid stability and security across a vast and diverse geographical area. WECC's involvement ensured that the study benefits from hands-on operational knowledge and region-specific insights that might not be captured at the federal level.

The SMEs within this population were expected to possess a diverse range of expertise crucial for understanding the complex interplay between drone technology and electrical grid security. This includes specialists in Electrical Engineering and Grid Security, who could provide detailed knowledge about the technical aspects of grid infrastructure and its vulnerabilities. Aerospace and Drone Technology experts brought critical insights into the capabilities and limitations of drone systems, both current and emerging. Cybersecurity and Information Technology specialists were essential for addressing the digital aspects of grid security, particularly as drones become more sophisticated and potentially serve as vectors for cyber-attacks.

Law Enforcement and Counterterrorism experts contribute vital perspectives on threat assessment, incident response, and preventive strategies. Their expertise were crucial for

understanding how drone threats might manifest in real-world scenarios and how to effectively counter them. Regulatory and Policy specialists provide insights into the legal and governance frameworks surrounding both grid operations and drone use. Their knowledge was indispensable for navigating the complex regulatory landscape and identifying potential gaps or areas for policy intervention. This multidisciplinary approach allowed for a comprehensive examination of technical vulnerabilities, regulatory challenges, operational constraints, and emerging technological trends.

Sample Design and Justification

This research study aimed to actively solicit a sample of 30 well-qualified volunteer participants, equally divided among the DOE, FERC, and WECC. This sample size was determined after careful consideration of both methodological best practices and the practical constraints of qualitative research. In qualitative studies involving expert interviews, sample sizes typically range from 20 to 50 participants, with 30 often cited as a point where theoretical saturation is likely to occur (Guest et al., 2006; Mason, 2010). Theoretical saturation refers to the point at which additional data collection does not yield substantially new insights or themes, ensuring that the study captures a comprehensive range of perspectives without unnecessary redundancy (Guest et al., 2006; Mason, 2010).

The choice of 30 participants balances the need for depth of insight with the practicalities of data collection and analysis in qualitative research. This number allowed for a robust representation from each of the three key organizations while remaining manageable for an in-depth qualitative analysis. The equal distribution, 10 participants each from DOE, FERC, and WECC, ensured that perspectives from national policy, regulatory, and regional operational levels were adequately represented.

The appropriateness of this sample was underscored by several crucial factors. Firstly, the SMEs have direct involvement in grid maintenance, security, and operations, providing a nuanced understanding of vulnerabilities and challenges that would be difficult to obtain from theoretical research alone. Their day-to-day engagement with the realities of grid security and drone technology ensured that the insights gathered are grounded in practical experience and current realities.

Secondly, the diverse expertise of the sample aligned closely with the complex, interdisciplinary nature of the research problem. Drone threats to electrical infrastructure span technical, regulatory, and operational domains, necessitating a multifaceted approach to their study. The inclusion of experts from various specializations ensured that all relevant aspects of the issue are adequately explored and understood.

Furthermore, the combination of DOE, FERC, and WECC experts offers both broad national perspectives and specific regional knowledge. This dual perspective is crucial for understanding how national policies and regional practices intersect in addressing emerging security challenges. It allowed the study to contextualize drone threats within both national security concerns and the specific operational realities of the Western Interconnection.

The sample's composition also bridged the gap between policy formulation and practical implementation. Many of the selected SMEs were likely to be involved in both shaping policies and executing protective measures. This dual role was expected to supplement individual perspectives, allowing them to speak to both the theoretical underpinnings of grid security and the practical challenges of implementing protective measures against drone threats.

Geographical diversity within the sample is another key strength. By including experts from various regions served by the Western Interconnection, the study captured a wide array of

contextual factors and challenges. This diversity was crucial as it allowed for the consideration of how topographical variations (e.g., mountainous regions versus plains) might influence both drone operations and grid vulnerabilities. It also enabled the study to explore how different population densities and land-use patterns across the Western Interconnection might affect the nature and severity of drone threats.

Moreover, this geographical spread provides insights into how regional variations in regulations, resources, and response capabilities might impact the overall security posture against drone threats. Urban areas, for instance, might face challenges related to high-density infrastructure and limited drone operation spaces, while rural areas might grapple with issues of vast, difficult-to-monitor territories. By capturing these diverse perspectives, the study developed a more nuanced understanding of the varied challenges faced across the Western Interconnection's extensive network.

Sampling Strategy and Data Collection

The study employed purposive sampling, specifically expert sampling, which aligns with the qualitative methodology and the specialized nature of the research topic. This sampling strategy allowed for the deliberate selection of participants based on their specific expertise and relevance to the research questions. By targeting SMEs in fields directly related to electrical grid security and drone technology, the study aimed to gather rich, informed insights that directly address the complex issues at hand.

To enhance the sample's comprehensiveness and ensure a wide range of perspectives, professional snowballing techniques were used. This method leveraged the professional networks of initial participants to identify and recruit additional experts who could bring valuable perspectives to the study. The snowballing technique was particularly useful in this

context, as it could help uncover experts who might not be immediately visible through organizational structures, but who possess valuable insights into the research topic.

The data collection process, after receiving formal approval from the National University IRB, occurred in two distinct but complementary phases. The first phase involved an anonymous online survey administered through *SurveyMonkey.com*, a publicly available and widely recognized platform in academic and professional research circles. *SurveyMonkey.com's* reputation for data security, user-friendly interface, and compliance with research ethics standards made it an ideal choice for this research study (Rea et al., 2021).

This researcher's survey was intentionally designed with open-ended questions crafted to elicit rich, qualitative responses from participants. These questions were carefully formulated to explore various aspects of drone threats to the electrical grid, including technical vulnerabilities, regulatory challenges, operational concerns, and potential mitigation strategies. The use of *SurveyMonkey.com* not only ensured a user-friendly experience for participants but also provided a robust and credible foundation for data collection, aligning with the ethical standards set forth by the NU IRB Staff.

This approach leveraged the platform's anonymity features, potentially encouraging more candid responses on sensitive topics related to grid security, while maintaining the highest standards of research integrity. This approach allowed participants to provide insights they otherwise may have hesitated to share in a more formal, identifiable setting, particularly given the sensitive nature of grid security. The survey format also allowed participants to thoughtfully consider their responses and provide detailed information at their own pace.

Following the survey, the second phase consisted of follow-up interviews with participants who indicated willingness to engage in further discussion. These interviews were

conducted via electronic means, such as telephone calls, Zoom video conferences, or Microsoft Teams meetings. This flexibility in interview format was designed to accommodate the potentially busy schedules of the SMEs and to allow for participation from geographically dispersed experts.

The interviews were intended to serve several important purposes. They allowed for more nuanced exploration of key points raised in the survey responses, providing an opportunity to delve deeper into complex issues or clarify ambiguous responses. The interactive nature of interviews also permitted the researcher to ask follow-up questions, explore unexpected themes that may have emerged from the survey data, and capture the contextual nuances that might be missed in written responses.

This dual-method approach to data collection was designed to capture both broad themes across the sample and in-depth individual perspectives, enhancing the richness and validity of the data gathered. The combination of anonymous surveys and personalized interviews allowed for a comprehensive exploration of the research questions. The result was a balance between the need for candid, unrestricted responses and the depth and clarity achievable through direct interaction.

The proposed population and sample parameters of this research study were intentionally designed to be of a balanced size, explore diverse expertise, and cover broad geographical representation, and was well-suited to provide a comprehensive, in-depth exploration of drone threats to the Western Interconnection Electrical Grid. This thoughtful approach enhanced the study's potential to generate findings that are both academically robust and practically relevant and aligned with best practices in qualitative research methodology while addressing the unique demands of studying emerging technological threats to critical infrastructure. By incorporating

this breadth of expertise and geographical representation, the sample was structured to provide a nuanced, multi-faceted understanding of the complex interplay between drone technology and electrical grid security.

Instrumentation

In modern qualitative research designs, studies are built upon a foundation of constructivist and interpretivist models, which emphasize that reality is subjective and socially constructed through individual or group experiences (Mills, 2019; Racine et al., 2020). These designs focus on understanding the meaning that participants assign to their experiences and the contextual factors influencing these perceptions. A key element in many of these designs, as advanced by Mills (2019) and Racine et al. (2020), was the use of one-on-one interviews between the researcher and carefully screened participants who voluntarily engage in the research efforts at-hand. These interviews, conducted in-person, over the telephone, or via online video communication platforms, allow for a deep exploration of complex phenomena and help generate rich, detailed data. Additionally, qualitative researchers typically employ flexible and adaptive methods that support data collection and analysis (Yin, 2015).

This study employed two primary data collection methods: an anonymous online survey and follow-up semi-structured interviews. These instruments were specifically developed for the research and approved by the NU IRB Office, ensuring adherence to ethical standards and methodological rigor. The anonymous online survey, conducted via *SurveyMonkey.com*, was designed to gather detailed and candid responses from the SME participants. The *SurveyMonkey.com* web-based platform was chosen for its secure, user-friendly platform, ensuring the anonymity of participants, which was crucial given the sensitive nature of the study's focus on critical infrastructure vulnerabilities. The survey employed open-ended

questions to explore technical vulnerabilities, regulatory challenges, operational concerns, and mitigation strategies related to drone threats. This open-ended format was specifically selected to allow participants the freedom to provide in-depth, nuanced responses, facilitating a comprehensive understanding of the complex risks posed by drone technologies.

The survey's design was informed by an extensive review of relevant literature, including key studies by Zwickle et al. (2018) and Kallenborn et al. (2022), to ensure the current research effort specifically addressed the most pressing issues in the field. The questions were structured to guide participants from broader inquiries to more specific topics, allowing for progressive immersion in the subject matter and encouraging deeper reflection as participants worked through the survey. This structure helped ensure the data captured both high-level strategic concerns and detailed operational insights regarding the impact of drone technology on grid security.

Following the survey, semi-structured interviews were conducted with participants who volunteered for further engagement. These interviews, conducted through secure platforms such as Zoom or Microsoft Teams, were intended to expand on key insights from the survey, clarify any ambiguities, and explore emerging themes in greater depth. The semi-structured format provided consistency in questioning across participants while maintaining flexibility to probe specific areas of interest that emerged during the conversations. This method allowed for a deeper understanding of complex issues and encouraged the discussion of new insights that might not have been fully addressed in the survey responses.

The design and implementation of these data collection methods were informed by Freeman's Stakeholder Theory (1984), which emphasizes the importance of considering the diverse interests of all stakeholders affected by a particular issue. This framework ensured that

the study captured not only the perspectives of individual experts but also a holistic understanding of how various stakeholders—such as regulatory bodies, operational personnel, and technology specialists—interact with and influence the security of critical infrastructure. By grounding the research instruments in Stakeholder Theory, the study aimed to reveal areas of alignment and conflict among stakeholders, ultimately contributing to a more comprehensive understanding of how drone technology impacts the security of the Western Interconnection.

This dual-method approach, combining the breadth of the survey with the depth of the interviews, reflected the strengths of qualitative research in capturing both the wide range of expert opinions and the detailed insights necessary to understand complex phenomena. The anonymous survey allowed participants to provide unfiltered responses on sensitive topics, while the semi-structured interviews offered the opportunity to explore those responses further and gain additional insights. Together, these methods enabled the researcher to triangulate findings, enhancing the overall validity of the study and ensuring that the research could adapt to emerging themes and insights throughout the data collection process.

To ensure reliability and validity, several measures were implemented. The survey instrument was pre-tested with a small group of experts to assess clarity and relevance, and SurveyMonkey's data validation features were utilized to ensure data integrity. For the interviews, a standardized interview guide was used to ensure consistency, while member-checking procedures were employed to allow participants to review their interview transcripts, ensuring the accuracy of their contributions. Additionally, peer debriefing sessions were conducted, where the researcher discussed emerging themes and potential biases with colleagues not directly involved in the study, further enhancing the reliability of the findings.

Since the survey and interview protocols were developed specifically for this study, no external permissions were required; however, if standardized measures had been incorporated, appropriate permissions would have been sought and documented in the appendix. This comprehensive approach to instrumentation, combining the anonymous survey with in-depth follow-up interviews, provided a robust, multi-layered dataset, grounded in the lived experiences and professional knowledge of SMEs directly responsible for the security of the Western Interconnection. The combination of these methods allowed the study to deliver a nuanced understanding of the vulnerabilities posed by drones and informed recommendations for mitigating these emerging threats through strategic insights and detailed technical knowledge.

Study Procedures

The study procedures involved data collection through online surveys and one-on-one interviews, followed by data analysis. Inferences were then developed based on the analysis to draw conclusions and provide recommendations at the conclusion of the study (Yin, 2015). The data collected and analyzed in this study aimed to document similarities and/or differences, key themes, and apparent trends (Castillo-Montoya, 2016; Yin, 2015).

Freeman et al.'s (2010) Stakeholder Theory provided the foundation for this research study's data analysis procedures. The core ideas of the theory emphasized the importance of understanding the perspectives of various stakeholders, such as regulatory bodies, operational personnel, and cybersecurity experts, and how their concerns and interests intersected. Open coding was used to identify themes related to stakeholder concerns, such as grid vulnerabilities and regulatory challenges.

As noted by Scott and Medaugh (2017), axial coding helped explore connections between these themes, examining how different stakeholder views were interrelated. Finally, selective

coding was employed to develop a cohesive framework that captured the alignment or divergence of stakeholder perspectives on drone-related risks to the Western Interconnection grid. These coding techniques, guided by Freeman et al.'s (2010) Stakeholder Theory, enabled a comprehensive analysis that reflected the diverse viewpoints of those responsible for grid security.

This research study sought to leverage primary data sources in its data collection as it proved essential in evaluating the perceived risks that drone technology poses to the Western Interconnection electrical grid. This data was collected directly from SMEs via two methods: an anonymous online survey and semi-structured one-on-one interviews. The online survey was used to gather initial insights from SMEs on grid vulnerabilities, regulatory challenges, and the potential impacts of drone technology, while the semi-structured interviews provided an opportunity for the researcher to explore these topics in greater depth. By analyzing this data using open, axial, and selective coding, this research endeavor was able to build a qualitatively holistic understanding of the complex interactions between drone technology and grid security, grounded in the lived experiences of key stakeholders.

Data Analysis

This study focused on examining and identifying the severity of risks, as seen by the sample population, posed by current and emerging commercial drone technology to the Western Interconnection electrical grid. This researcher's data collection and analysis leveraged focused sampling meant to garner specific inputs from SMEs to highlight perceived risks and recommend necessary safeguarding measures against future drone threats. The researcher used a secure Excel spreadsheet to maintain data integrity/security to include study participants contact information and to document all follow-up communications during the data collection process.

This researcher specifically focused on the use of open-ended, in-depth, non-leading questions in their online survey to gather detailed insights from SMEs about the risks posed by drone technology to the Western Interconnection Electrical Grid. The questions were carefully worded to avoid leading participants toward any specific conclusions, ensuring that their responses reflected their own expertise and experiences. By using open-ended questions, the researcher encouraged participants to provide more thoughtful and comprehensive answers, which allowed for a broader range of perspectives on issues like grid vulnerabilities, regulatory challenges, and operational risks (Mills, 2019).

After receiving formal approval from the NU IRB Office for the research plan, the recruitment of participants through strategic, purposeful sampling began. This approach required thorough and transparent documentation to ensure accurate representation of the SMEs and geographic diversity among the selected participants. This strategic approach was meant to ensure that responses were not constrained by predefined options, giving SMEs the opportunity to elaborate on key concerns and provide detailed explanations. The in-depth nature of the questions was essential for capturing the complexity of drone-related threats, as well as the varied and specialized knowledge of the participants.

After receiving formal IRB approval, the questionnaire was distributed via *SurveyMonkey.com*, a secure online platform. To achieve a sufficient sample size for this study, invitations were sent to participants through their official organizational email addresses, ensuring that only authorized SMEs from the DOE, FERC, and WECC received the survey. Participants were required to review and agree to informed consent at the beginning of the survey. Due to the use of purposeful sampling, responses were collected anonymously, and all data was securely archived on the researcher's password-protected personal computer to

maintain confidentiality. The raw data was accessible only to the researcher, with identifiable information coded to protect participant privacy.

In addition to this initial sampling strategy, the snowball method was employed to expand the pool of participants. After the initial group of SMEs was recruited, these participants were asked to refer additional experts who could offer valuable insights into the study. This approach allowed the researcher to reach a broader and more diverse population of SMEs, ensuring a more comprehensive understanding of the risks posed by drone technology to the grid. By utilizing the snowball method, the study was able to increase its sample size efficiently while maintaining the depth and relevance of the data collected (Parker et al., 2019).

The combination of purposeful and snowball sampling ensured that the study captured a well-rounded view of the risks. It also ensured the representation from various geographic regions and areas of expertise within the grid's operational and regulatory structure. This method also contributed to achieving data saturation, as the growing participant pool offered increasingly overlapping themes and insights.

For the one-on-one interviews, a semi-structured format was developed, providing a consistent set of questions while allowing flexibility to explore specific areas in more depth based on participants' responses. The interview guide was also approved by the NU IRB Office. Interviews were scheduled via email, and participants had the option to conduct them via secure Zoom video calls or by traditional one-on-one phone calls. Informed consent, in the form of written consent, was required prior to each interview, with the consent forms securely stored on the researcher's password-protected computer.

The interview questions were designed using open-ended formats, following the professional research interview protocols established by Jacob and Furgerson (2012). This

approach, combined with the use of online Zoom interviews or traditional phone calls, allowed for the exploration of each participant's experiences and attitudes. It provided flexibility to understand and analyze the shared opinions and perceptions of the interviewees, contributing to a deeper, more nuanced understanding of the risks posed by drone technology to the Western Interconnection electrical grid.

Any PII-related (e.g., names, contact information, etc.) information relating to participants surveys and/or interviews will also be securely stored on the researcher's personal password-protected computer. Further, all PII associated with recordings and transcriptions will be protected by data safeguards to include password protected folders, etc. These steps were taken to ensure that the privacy of participants was maintained throughout the study, while still allowing PII to be used for research purposes.

Informed consent was built directly into the *SurveyMonkey.com* web-hosted online survey, requiring participants to review the consent form and agree to the terms before they could proceed with answering any questions. This ensured that all participants were fully informed about the study's purpose, procedures, and confidentiality measures before providing their responses. For the one-on-one interviews, separate informed consent forms were sent to participants via their personal or work email addresses. These forms were required to be signed and returned prior to scheduling the interviews, ensuring that consent was explicitly documented for both phases of the research.

Following the survey phase, the researcher personally contacted each participant who agreed to participate in the one-on-one interviews to coordinate the logistics. This included confirming a mutually convenient date and time, as well as the preferred communication method—either through secure individual Zoom video calls or phone calls. The interviews were

expected to last between 30 and 60 minutes, depending on the depth of the participants' responses and the complexity of the topics discussed. The researcher remained flexible in scheduling to accommodate participants' availability and preferences, ensuring a smooth process for transitioning from the survey to the in-depth interview phase.

If the interviewee provided consent to record, interviews were recorded and the recordings were then securely archived using file protection/encryption to prevent unauthorized access (Mills, 2019; Salkind, 2012). Transcriptions were stored in encrypted files, and any personally identifiable information was anonymized during transcription. Strict confidentiality protocols were followed throughout the study, ensuring that all data remained secure and accessible only for analysis purposes. These measures were essential for protecting the privacy and integrity of the data collected during both the questionnaire and interview phases of the research.

Thematic coding was derived from each interview transcript through a systematic review process. The researcher carefully analyzed the responses, identifying recurring concepts, ideas, and patterns that emerged from the SMEs' insights (Yin, 2015). These initial codes were tracked and organized within the before mentioned Microsoft Excel spreadsheet, allowing for easy categorization, and cross-referencing of themes across multiple interviews. This method facilitated a comprehensive overview of the diverse perspectives shared by the participants.

Following the initial thematic coding, axial coding was employed to examine potentially matching codes for comparison (Yin, 2015). This process involved identifying relationships, connections, and hierarchies among the themes that emerged during the initial coding phase. The researcher used the Excel spreadsheet to group related codes, exploring how different

aspects of drone-related risks, such as technical vulnerabilities, regulatory challenges, and operational concerns, intersected or influenced each other.

In addition to using Microsoft Excel for initial data organization, the researcher utilized NVivo 15, a specialized qualitative data analysis software, to enhance the rigor of the coding process. NVivo's academic oriented functions facilitated more complex thematic and axial coding operations. The software allowed for efficient management of the large volume of qualitative data gathered from the interviews and open-ended survey responses.

During the thematic coding phase, NVivo's node system was employed to categorize and organize emerging themes, enabling the researcher to easily track the frequency and context of specific concepts across multiple data sources. For axial coding, NVivo's relationship mapping tools were instrumental in visualizing and analyzing the connections between different themes. This software-assisted approach enhanced the researcher's ability to identify intricate patterns and relationships within the data, particularly in understanding how various aspects of drone-related risks to the Western Interconnection electrical grid interrelated and influenced each other. The use of NVivo in conjunction with Excel spreadsheets provided a strong framework for managing, analyzing, and synthesizing the complex qualitative data, ensuring a thorough and systematic approach to deriving insights from the SMEs' responses.

Assumptions

In academic research studies, identified assumptions serve as a foundation that frames the design, data collection, and analysis processes (Yin, 2015). Assumptions are the underlying premises that the researcher accepts as valid, often without direct empirical evidence, but are necessary for advancing the study (Salkind, 2012; Yin, 2015). These assumptions help shape the

scope of the research, inform the selection of methods, and influence how the results are interpreted (Salkind, 2012).

In qualitative research, assumptions often concern participant expertise, theoretical frameworks, or the reliability of data collection methods (Salkind, 2012; Yin, 2015). Acknowledging these assumptions helps the researcher make informed decisions and gather relevant evidence (Yin, 2015). Articulating assumptions clarifies the study's limitations, as their validity may not be universal (Salkind, 2012; Yin, 2015). This process is important for maintaining transparency, rigor, and credibility (Yin, 2015). Clearly stating assumptions provides insight into the research context, aligns the study's design with its objectives, and enables more precise evaluation of the findings and their validity (Salkind, 2012; Yin, 2015).

The researcher's decision to use Freeman's (1984, 2010, 2015) Stakeholder Theory as the framework for examining the potential risks drone technology poses to the Western Interconnection Electrical Grid was rooted in several interconnected assumptions about the nature of the problem and the most effective approach to studying it. First and foremost, the researcher assumed that the challenge of protecting the electrical grid from drone threats is a multifaceted issue that extends beyond just technical considerations. This assumption reflects an idea that, while technological aspects are crucial, they are inseparable from the social, economic, and regulatory contexts in which they exist. By adopting Freeman's (1984, 2010, 2015) Stakeholder Theory, the researcher acknowledges that the grid's vulnerability to drones is not just a matter of physical infrastructure or cybersecurity, but also involves complex human systems and decision-making processes.

The application of this theory also assumed that a wide range of stakeholders have valid and important perspectives on the issue. These stakeholders include, but are not limited to,

federal regulators like the DOE and FERC, regional entities like WECC, local utility companies, drone manufacturers, privacy advocates, environmental groups, and communities served by the grid. The researcher determined, through the evaluation of each agencies mission statements and charters, that each of these groups has unique insights, concerns, and potential solutions that are vital to understanding the full scope of the problem (*Energy Security*, 2024; *Office of CESE*, 2023; *OEIS & FERC*, 2024; *WECC*, 2024). This assumption challenges more traditional, top-down approaches to infrastructure security by suggesting that valuable knowledge is distributed across various stakeholder groups rather than concentrated in a single expert body.

This researcher also assumed that the stakeholder perspectives, while diverse and potentially conflicting, could be synthesized into a more comprehensive understanding of the risks and potential solutions. This reflects an optimistic view that collaborative approaches, which consider multiple viewpoints, can lead to more robust and effective security strategies than those developed in isolation by any single group (Salkand, 2012). The use of Freeman's (1984, 2010, 2015) Stakeholder Theory also implies an assumption about the nature of risk and security in complex systems.

Vulnerabilities within America's regionally based electrical power grid systems are not only technical weaknesses, but can arise from misalignments between different stakeholders' priorities or from gaps in communication and coordination (Chowdhury & Gkioulos, 2021; Freeman, 1984). Through the use of surveys, one-on-one interviews, and the mapping out of responses of stakeholders, their relationships, and points of interest, this researcher assumed that they could identify potential weak points in the system that might not be apparent from a purely technical analysis. Furthermore, this approach assumed that affective solutions to drone-related threats should be holistic in their integration. It was understood that sustainable security

measures could not be implemented in isolation but must account for the broader ecosystem of stakeholder interests and interactions (Unger et al., 2023). For example, technological countermeasures against drones would need to be developed alongside regulatory frameworks, industry education initiatives, and strategies for stakeholder engagement.

This researcher also made an implicit assumption about the nature of knowledge and expertise in this domain. By valuing the perspectives of diverse stakeholders, they assumed that crucial insights about grid security and drone threats might come from unexpected sources – not just from traditional experts in energy infrastructure or aviation technology. This reflects a more democratic and inclusive approach to knowledge production in the field of critical infrastructure protection (Barka et al., 2019; Department of Homeland Security, 2013; Kalinin et al., 2021). The use of Freeman's (1984, 2010, 2015) Stakeholder Theory reflects a set of assumptions about the nature of technological risk, the distribution of knowledge and expertise, and the most effective pathways to enhancing the security and resilience of critical infrastructure systems like the Western Interconnection electrical grid.

Limitations

Within this qualitative study, which was designed to provide in-depth insights into drone-related risks to the Western Interconnection electrical grid, several inherent limitations typical of qualitative research methodologies were encountered (Creswell, 2013). One primary concern was the potential for subjectivity and researcher bias, as the researcher's personal experiences and preconceptions about drone technology and grid security—stemming from a USAF RPA Pilot career—may have inadvertently influenced data collection, analysis, and interpretation. To mitigate this, the researcher engaged in reflexivity throughout the research process, critically examining biases and assumptions (Creswell, 2013). Additionally, triangulation was employed

by consulting multiple data sources and seeking peer debriefing to enhance the credibility of the findings (Carter et al., 2014).

This research study encountered several limitations inherent to qualitative research methodologies. The sample size of 30 SMEs from the DOE, FERC, and WECC potentially constrained the breadth of perspectives captured on drone-related risks to the Western Interconnection electrical grid (Creswell, 2013). The focus on expert opinions, while valuable, precluded insights from other stakeholders such as local communities or drone operators. Geographic representation, though diverse, may not have fully encompassed all areas within the extensive Western Interconnection Network. Also, the rapid evolution of drone technology presented a challenge, as insights gathered risked becoming quickly outdated. Additionally, the qualitative nature of the data collected posed difficulties in quantifying risks or providing precise metrics for decision-makers (Haugstvedt, 2023).

To mitigate these limitations, the study implemented several measures. Firstly, a combination of purposive sampling and professional snowballing techniques was employed to recruit experts from various relevant fields and geographic locations within the Western Interconnection Grid. The data collection process utilized both an anonymous online survey via *SurveyMonkey.com* and follow-up interviews conducted through electronic means, enabling a more comprehensive gathering of insights. The iterative data analysis process, involving systematic coding and thematic analysis, allowed for the emergence of new themes and deeper understanding of participants' perspectives.

Efforts were also made to include experts from major power hubs, rural areas, and cross-border regions near Canada and Mexico to capture a broad range of perspectives. This research study diligently sought to ensure confidentiality and anonymity for all participants, potentially

encouraging more candid responses, particularly regarding sensitive security information. Open-ended questions were utilized in both the survey and interviews to elicit in-depth, detailed responses that could capture the complexity of the issues being studied.

Delimitations

As Hennink and Kaiser (2022) explained, delimitations are intentional boundaries set by researchers to define a study's scope, enhancing focus and manageability while providing context for interpreting results. These delimitations, or self-imposed constraints, enhance the focus, clarity, and manageability while optimizing resources and ensuring methodological consistency. They provide context for interpreting results, address ethical considerations, and align research with specific theoretical frameworks (Hennink and Kaiser, 2022). By articulating these boundaries, researchers established a clear framework for understanding the study's scope, applicability, and limitations, thereby enhancing its overall rigor and utility. In this specific qualitative study, three specific delimiting factors have been identified for consideration: (a) specific organizations (DOE, FERC, WECC), (b) a specific geographical area (Western Interconnection), and (c) aerial drones as the threat type.

This research study's delimitations were established to focus the research on the specific threat of drone technology to the Western Interconnection electrical grid. The primary delimitation was the selection of SMEs exclusively from the DOE, the FERC, and the WECC. This decision was rooted in the critical roles these organizations play in overseeing, regulating, and managing the Western Interconnection Electrical Power Grid. The study targeted a sample of 30 participants, equally divided among these three organizations, to ensure a balanced representation of perspectives from national policy, regulatory, and regional operational levels.

Another significant delimitation was the geographical focus on the Western Interconnection, which spans over 1.8 million square miles across 14 states, parts of Canada, and Mexico (*Western Interconnection*, 2023). This specific focus allowed for an in-depth examination of a crucial component of the U.S. electrical infrastructure that serves over 80 million people and businesses (*Western Interconnection*, 2023). The study's scope was further narrowed to examine only aerial drone technologies, excluding other potential threats to the electrical grid.

These delimitations aligned closely with the study's theoretical framework, which was based on Freeman's (1984, 2010, 2015) Stakeholder Theory. This theory emphasizes the importance of understanding and aligning the interests of all stakeholders in a system. By focusing on key regulatory and operational entities, the study sought to capture the perspectives of primary stakeholders in the Western Interconnection's security and operation.

The chosen delimitations directly addressed the problem statement, which centered on the threat posed by current and emerging aerial drone technologies to the Western Interconnection electrical power grid. By concentrating on SMEs from organizations with direct responsibility for the grid's security and operation, the study aimed to gather the most relevant and informed perspectives on this specific threat. These research decisions also supported the purpose statement, which aimed to analyze and identify the severity of risk posed by commercial aerial drone technology to the Western Interconnection Electrical Grid Infrastructure. The focus on SMEs from DOE, FERC, and WECC ensured that the study gathered insights from those most closely involved in assessing and mitigating such risks.

Finally, the delimitations aligned with the research questions, which sought to ascertain the perceived risk level, quantifiable level of concern, and perceived adequacy of protective

measures against drone threats among SMEs from these specific organizations. By restricting the study to these parameters, the research maintained a sharp focus on gathering data directly relevant to these questions, facilitating a deeper and more nuanced understanding of the complex interplay between drone technology and electrical grid security within the Western Interconnection.

Ethical Assurances

Ethical assurances are crucial in qualitative research because of the profound engagement with participants, which often involves exploring personal experiences, perceptions, and sensitive topics (Richards and Schwartz, 2002). This depth of interaction necessitates heightened ethical considerations to protect participants and ensure the integrity of the research. By implementing ethical measures—such as safeguarding participants' rights and welfare, maintaining confidentiality and anonymity, building trust and rapport, demonstrating cultural sensitivity, and upholding data integrity—researchers not only protect those involved but also enhance the quality and credibility of their findings (Richards and Schwartz, 2002). Rigorous adherence to ethical principles helps ensure that the research is conducted responsibly and respectfully, ultimately contributing to the advancement of knowledge while honoring the dignity and rights of all participants (Creswell, 2003; Yin, 2015).

Proper data management and reporting practices further protect participants' privacy. In this study, ethical assurances were crucial given the sensitive nature of infrastructure security information, and to facilitate more candid responses from subject matter experts. Ultimately, these ethical considerations contribute to the broader integrity of scientific inquiry, maintaining public trust in research institutions and processes (Richards and Schwartz, 2002). By underpinning the validity, reliability, and societal value of qualitative research, ethical assurances

are not merely procedural requirements but fundamental components of meaningful and responsible scholarship (Richards and Schwartz, 2002).

This study received formal approval from the NU IRB Office prior to data collection. The approval process involved a thorough review of the research protocol, including the proposed methodology, data collection instruments, and participant protection measures. The IRB's approval ensured that the study adhered to ethical standards and federal regulations governing the use of human beings as subjects of academic research.

The researcher implemented stringent measures to ensure participant confidentiality and anonymity throughout this research study. All survey responses were collected anonymously through *SurveyMonkey.com*, a secure online platform. For the follow-up interviews, participants were assigned unique identifiers, and any potentially identifying information was removed during the transcription process. This researcher maintained a separate, encrypted file linking participant identifiers to their contact information, accessible only for the purpose of conducting follow-up interviews.

Data security was a primary concern throughout the research process. All collected data, including survey responses, interview transcripts, and analysis files, were securely stored on the researcher's password-protected personal computer. Access to this data was restricted solely to the researcher. Regular backups were performed and stored in an encrypted format on a separate, secure device. In accordance with IRB requirements, all research data will be retained for a specified period after the study's completion, after which it will be securely destroyed.

This researcher, a current USAF RPA Pilot, acknowledged potential biases stemming from personal and professional experiences with drone technology. This background provided valuable insights into the technical aspects of drone operations but also posed a risk of

preconceived notions about drone capabilities and threats. To mitigate these biases, the researcher engaged in ongoing reflexive practices throughout the study. This involved maintaining a reflective journal to critically examine assumptions, interpretations, and decision-making processes.

To further enhance the credibility of the findings and minimize bias, the researcher employed data triangulation methods. This involved cross-referencing data from multiple sources, including survey responses, interview transcripts, and relevant literature. This researcher also sought peer debriefing from colleagues not directly involved in the study, providing an external perspective on the analysis and interpretations.

The research study's design incorporated several features to minimize the influence of researcher bias. Open-ended questions in both the survey and interviews allowed participants to express their views freely, without being led by the researcher's preconceptions. The semi-structured interview format provided a consistent framework while allowing flexibility to explore topics raised by participants, ensuring that the data collection was not overly constrained by this researcher's prior knowledge or assumptions.

Throughout the data analysis process, the researcher maintained a focus on the participants' perspectives, using in-vivo coding techniques to preserve the participants' language and meanings. The iterative nature of the analysis, involving multiple rounds of coding and theme development, allowed for continuous questioning of interpretations and consideration of alternative explanations. By implementing these comprehensive measures for ethical conduct, data protection, and bias mitigation, the researcher strived to ensure the integrity and credibility of the study's findings, providing a reliable foundation for understanding the complex interplay between drone technology and electrical grid security within the Western Interconnection.

Summary

This qualitative study aimed to analyze and identify the severity of risks posed by current and emerging drone technologies to the Western Interconnection electrical power grid in the United States. By gathering insights from SMEs within the DOE, FERC, and WECC through anonymous surveys and semi-structured interviews, the research sought to understand how drones' advanced capabilities present new security challenges to critical infrastructure. Grounded in Freeman's (1984, 2010, 2015) Stakeholder Theory, the study focused on identifying critical vulnerabilities and recommending improvements to safeguard against drone-related threats. The research underscored the importance of proactive measures and coordinated efforts among stakeholders to enhance infrastructure resilience, develop targeted countermeasures, and inform policy decisions. As Chapter 3 has detailed the research methodology of this study, Chapter 4 shifts to presenting findings from the data, highlighting key themes and patterns related to perceived risks and protective measures.

Chapter 4: Findings

The problem to be addressed by this study was the threat that current and emerging aerial drone technologies pose to the Western Interconnection electrical power grid, as perceived by subject matter experts (SME) from the U.S. Department of Energy (DOE), the Federal Energy Regulatory Commission (FERC), and the Western Electricity Coordinating Council (WECC). The purpose of this descriptive qualitative study was to analyze and identify the severity of risk posed by current and emerging commercial aerial drone technology to America's Western Interconnection Electrical Grid Infrastructure. The research aimed to assess the severity of drone-related risks, identify infrastructure vulnerabilities, and evaluate the adequacy of existing protective measures. It also sought to inform interagency coordination, guide policy, and contribute to the broader academic understanding of unmanned aerial system (UAS) risks to critical infrastructure.

Framed by Freeman's (1984) Stakeholder Theory and grounded in modern risk-assessment models, the study addressed three interrelated research questions. First, how likely are current and near-term UAS technologies to disrupt grid operations? Second, what operational, economic, and reputational consequences might such disruptions cause? Third, how effective are existing physical, cyber, procedural, and regulatory safeguards? These questions captured both perceived risk levels and the underlying concerns shaping policy and investment decisions.

The study was prompted by the widening gap between rapidly evolving drone capabilities and slower-moving security policies. Drone use in the Ukraine–Russia conflict has demonstrated how low-cost UAS can scout, jam, or damage critical assets. Yet little systematic evidence exists on how U.S. grid regulators and operators assess these risks (Mittal & Goetz,

2025). This research addressed that gap by examining SME perspectives within DOE, FERC, and WECC jurisdictions.

Survey data from 24 SMEs underscored the urgency: 96% rated the drone threat as "High" or "Critical," and the same proportion viewed new countermeasures as "Very" or "Extremely" urgent. Only 8% judged current protections as even "Moderately Effective"; none rated them "Very" or "Highly Effective." Respondents cited uneven detection capabilities, legal restrictions on jamming or kinetic takedowns, and the rise of autonomous or swarm-capable drones. Examples included a July 2020 drone incursion at a Pennsylvania substation, coordinated sightings near U.S. nuclear facilities in December 2024, and drone tactics in the on-going Ukraine–Russia war that inflicted outsized damage on power assets.

Beyond technical gaps, 92% (22/24) of research participants also highlighted structural and cultural barriers. Half described interagency coordination as minimal, and many were unclear on counter-UAS protocols, exposing knowledge gaps that hinder rapid response. The threat, which all 24 of these 24 SMEs universally noted, is largely compounded by fragmented governance, inconsistent authorities, and organizational cultures still focused on conventional risks like severe weather or cyberattacks (Sims, 2018). This research filled a critical evidence gap and identified where policy, investment, and training must converge to close the protection deficit.

To reach qualified participants, the study used a snowball (chain-referral) recruitment strategy, enabling access to SMEs embedded in security-sensitive roles across the vast Western Interconnection. Initial "seed" participants were drawn from DOE headquarters, WECC's Enforcement and Risk Analysis offices, and FERC's Legal and Enforcement branches. Their diverse networks spanned functional areas and geographic regions.

The referral process served two goals: enhancing demographic and professional diversity by encouraging referrals across different roles and tenures and enabling real-time tracking of participant attributes to steer recruitment toward underrepresented groups. By the third wave, the sample provided sufficient contextual breadth for robust cross-case analysis. While not statistically representative, the snowball method was well-suited to this specialized and geographically dispersed domain. Purposeful seeding and guided referrals yielded a varied, operationally credible sample. The diversity of perspectives supported thematic data saturation and enabled trustworthy, transferable insights into how Western Interconnection stakeholders perceive and prioritize drone-related risks.

Trustworthiness of the Data

For qualitative findings to be accepted as sound and trustworthy, both Barnes (2015) and Lowe et al. (2018) underscored the need for researchers to show that data collection and analysis were carried out with precision and consistency. Doing so meant working from verifiable recordings, applying a systematic coding process, and openly explaining each analytic decision so that peers could trace how raw evidence led to final interpretations. By supplying this level of procedural detail, the present study allows other scholars and SMEs to judge the credibility of its methods and confirm that additional data would have added little new insight, thereby aligning with the standards laid out by Barnes (2015) and Lowe et al (2018).

Credibility

Credibility, the first pillar of qualitative trustworthiness, was pursued through a deliberate combination of triangulation, participant validation, reflexivity, and peer oversight. Following Noble and Heale's (2019) guidance that trustworthy findings must converge from several independent angles, this investigation compared patterns from anonymous online-survey

responses with narrative details captured in two verbatim interview transcripts. The researcher then weighed both sets of evidence against up-to-date, peer-reviewed literature on grid security. Where these evidence streams aligned, for example, in the shared concern that commercially available drones outpace current detection measures, the study accepted the theme as credible. First framed by Lincoln and Guba (1985) as the most critical technique in establishing credibility, member checking was another way the researcher limited potential research biases.

Any discrepancies were recorded, examined, and member checked to limit the influence of potential researcher personal bias (Birt et al., 2016). Consistent with the participant-verification protocol outlined by Birt et al. (2016), each interviewee reviewed an encrypted transcript within forty-eight hours, confirmed technical terminology, clarified intent, and signed off on preliminary codes before further analysis proceeded. Every methodological step, from the first recruitment emails to the final coding revisions, was logged in a detailed audit trail.

This record gives outside scholars and grid-security SMEs a transparent chain of evidence they can review, replicate, or challenge. The combined use of triangulation, member checks, reflexive journaling, and peer debriefs meets the credibility standards set by Noble and Heale (2019) and Birt et al. (2016). These safeguards give other experts a solid basis to trust this research study's conclusions (Noble, 2019; Birt et al., 2016).

Transferability

Daniel (2018) argued that qualitative findings become transferable when researchers offer clear, evidence-based details showing how their data could inform comparable questions in other settings. Birt et al. (2016) added that such transferability rests on the logical expectation that scientifically gathered results from one group of participants and conditions will hold relevance for people and circumstances that share essential features. Extending that view, Noble and Heale

(2019) and Barnes (2015) noted that thick contextual description, covering research setting, sampling logic, and participant roles, allows readers to judge whether conclusions are likely to apply elsewhere. Following these guidelines, the present study documented its purposeful snowball sampling of 24 survey respondents and two participants that volunteered to participate in follow-up interviews and detailed the drone-threat scenarios they evaluated. Combined with a transparent record of data-collection timing, instruments, and analytic procedures, this context enables future scholars and grid-security SMEs to determine when and under what conditions the study's insights may apply to other critical-infrastructure environments.

Dependability

According to Faulkner and Faulkner (2019), qualitative inquiry draws its descriptive power from eliciting detailed participant narratives, often through structured or semi-structured interviews and submitting those accounts to rigorous, systematic analysis. Yet Jensen and Laurie (2017) warned that narrative data can become unmanageable when researchers lack a clear system for organizing large volumes of text, making it difficult to isolate individual viewpoints from ambient noise. Barnes (2015) proposed that dependability is secured when every procedural choice sampling, recording, coding, and interpretation is documented so another scholar can follow each step precisely.

When such documentation is paired with consistent analytic routines, subsequent investigators can replicate the work with reasonable confidence of producing comparable results (Hennink & Kaiser, 2022). Guided by those standards, each interview was audio-recorded, timestamped, and transcribed verbatim; the transcripts and survey datasets were stored in a secure, version-controlled repository. By coupling thorough record-keeping with a transparent, replicable analytic framework, the study addressed the dependability criteria advanced by

Faulkner and Faulkner (2019), Jensen and Laurie (2017), Barnes (2015), and Hennink and Kaiser (2022), enabling future scholars or grid-security SMEs to reproduce the investigation and expect comparable insights.

Confirmability

Confirmability is the trustworthiness standard that asks: Can another qualified person trace each finding back to its evidentiary roots and see that it emerged from the participants' voices rather than the researcher's pre-conceptions (Noble and Heale, 2019)? In the classic framework proposed by Lincoln and Guba (1985), confirmability occupied the same conceptual space that objectivity does in quantitative work, but it is achieved through transparency rather than statistical controls. Yin (2013) therefore urged qualitative scholars to preserve a complete chain of evidence field notes, recordings, transcripts, analytic memos, and decision logs, so an external reviewer can audit how raw statements were transformed into codes and then into themes. Noble and Heale (2019) added that triangulating multiple data sources, investigators, or theories provides an additional safeguard. When the same pattern surfaces independently in more than one strand of evidence, the likelihood that it is an artifact of personal bias diminishes (Noble & Heale, 2019).

The practical importance of confirmability is two-fold. First, it protects the integrity of qualitative insights by making the researcher's interpretive process visible and therefore contestable; peers can spot selective attention, challenge ambiguous coding choices, or offer alternative explanations (Yin, 2013). Second, it supports cumulative scholarship. As Jensen and Laurie (2025) noted, a well-maintained audit trail allows future investigators to replicate the analytic procedures on new data sets or to reanalyze the original material with a different theoretical lens without having to re-invent the entire workflow. In fields such as critical-

infrastructure security, where policy recommendations may hinge on a small number of expert accounts, this level of transparency is essential for persuading other SMEs, regulators, and practitioners that the conclusions rest on solid ground rather than personal intuition.

Of this research study's targeted sample of 30 participants, to ensure a balanced representation of perspectives from national policy, regulatory, and regional operational levels, the study received 24 responses (80%) to the online survey. In addition to the 24 online survey participants, two out of the 24 respondent SMEs volunteered to participate in the follow-on one-on-one structured interviews. Data saturation was achieved at two closely linked points in this study.

First, while coding the open-ended comments from the *SurveyMonkey.com* questionnaire, the researcher found that 90% of all first-cycle codes appeared within the initial 18 of the 24 complete responses. The final six surveys introduced no new categories, indicating that data saturation of questionnaire themes had been reached. Second, the two follow-up interviews were analyzed using the same codebook, and neither interview generated a novel code beyond those already established from the survey data. Because the proportion of new codes had fallen below the 5% threshold recommended by Lowe et al. (2018) for determining data saturation, the researcher concluded that additional data collection was unlikely to yield fresh insights.

Research Question 1:

What is the perceived risk level among Subject Matter Experts (SMEs) from the DOE, FERC, and WECC, regarding the potential of current and near-future aerial drone technologies to cause damage or destruction to key aspects of the Western Interconnection Electrical Grid infrastructure?

Research Question 2:

What is the quantifiable level of concern among SMEs from the DOE, FERC, and WECC regarding current and near-future aerial drone technologies as a potential threat to the Western Interconnection Electrical Grid infrastructure?

Research Question 3:

What is the perceived adequacy of the measures taken by the DOE, FERC, and WECC in safeguarding the Western Interconnection Electrical Grid infrastructure from current and near-future aerial drone technology attacks?

Results

Building on a body of literature that has traced UAS threats to airports, prisons, and East-Coast substations yet has paid limited attention to the sprawling Western Interconnection, the present inquiry applied Freeman's (1984) Stakeholder Theory to map how the region's key decision makers perceive and rank drone-related risks across regulatory, operational, and technical lines of responsibility. Guided by that, a first-wave online survey was distributed through *SurveyMonkey.com* to a targeted sample of 30 participant SMEs drawn from the DOE, the FERC, and the WECC. Twenty-four participants representing an 80 percent response rate completed the instrument. Purposeful snowball sampling was used to secure a professionally credible mix of roles, including control-room operators, transmission planners, cybersecurity leads, and federal reliability regulators, and to ensure that distinct sub-entities within the Western Interconnection (e.g., balancing authorities, investor-owned utilities, rural cooperatives) were present in the data set (Hennink & Kaiser, 2022; Mills, 2019; Yin, 2013).

The NU IRB-approved survey combined eleven five-point Likert items with open-ended prompts to elicit nuanced commentary on three focal areas: the current and near-term likelihood of drone incursions against grid assets, the intensity of respondent concern about those

incursions, and the perceived adequacy of existing detection and mitigation measures. Likert items provided a profile of perceived risk severity, while the free-text boxes captured context that might explain rating patterns, such as gaps in radio-frequency monitoring near remote substations or challenges in securing waivers for counter-UAS technologies. Collectively, these design choices aligned with stakeholder-theory principles by giving each participant a structured yet flexible platform to articulate how their specific vantage point shapes their view of the drone threat landscape.

The study's second-wave qualitative element consisted of two semi-structured interviews with survey respondents who had volunteered their contact information at the close of the questionnaire. Each session followed an NU IRB–approved interview guide that mirrored the survey's three focal areas—current threat level, degree of concern, and effectiveness of counter-UAS measures—and incorporated open prompts and clarifying probes to encourage participants to expand on their earlier responses. Although all eligible SMEs were contacted by both email and phone, only two agreed to participate in the follow-on interviews.

The limited participation was not a reflection of disinterest in the research but rather a consequence of the highly sensitive nature of the subject matter. Of the 10 initial representatives from the DOE, FERC, and WECC the researcher contacted during the first wave survey solicitation, 8 SMEs expressed concerns regarding classification, operational security, and the potential disclosure of vulnerabilities in the Western Interconnection electrical grid. These factors likely discouraged some SMEs from participating in the second-wave interviews. These constraints underscore the difficulty of conducting research in critical-infrastructure security domains, where expert perspectives are vital, but access is often constrained by regulatory and

protective barriers. Conversations were recorded (with permission) and transcribed verbatim for analysis.

When the transcripts were coded with the same framework developed from the survey's open-ended responses, every passage fit within existing categories and no additional codes were needed. This indicated that the interviews introduced no new themes beyond those already captured in the questionnaire. This outcome confirmed that data saturation had been reached, while the dual-phase design still provided valuable narrative context to support and reinforce the breadth of the survey findings. See Table 1 one for a breakdown of SME non-identifiable demographics for reference.

Table 1

Listing of SME non-identifiable demographics

SME ID	***Age***	***Years of Expertise***	***Degree Level***
SME #1	41 – 50	16 – 20	Master's degree
SME #2	31 – 40	11 – 15	Bachelor's degree
SME #3	41 – 50	6 – 10	Bachelor's degree
SME #4	31 – 40	11 – 15	Master's degree
SME #5	31 – 40	6 – 10	Master's degree
SME #6	31 – 40	11 – 15	Bachelor's degree
SME #7	18 – 30	6 – 10	Bachelor's degree
SME #8	31 – 40	6 – 10	Bachelor's degree
SME #9	51 – 60	11 – 15	Master's degree
SME #10	51 – 60	16 – 20	Master's degree
SME #11	41 – 50	11 – 15	Master's degree
SME #12	41 – 50	0 – 5	Bachelor's degree
SME #13	51 – 60	16 – 20	Bachelor's degree
SME #14	31 – 40	0 – 5	Bachelor's degree
SME #15	31 – 40	6 – 10	Master's degree
SME #16	41 – 50	11 – 15	Bachelor's degree
SME #17	61 – 70	21 – 25	Master's degree
SME #18	51 – 60	16 – 20	Bachelor's degree
SME #19	41 – 50	6 – 10	Bachelor's degree
SME #20	18 – 30	0 – 5	Associate degree
SME #21	18 – 30	6 – 10	Associate degree
SME #22	51 – 60	21 – 25	Bachelor's degree
SME #23	41 – 50	21 – 25	Bachelor's degree
SME #24	31 – 40	11 – 15	Associate degree

Note. Werner, J. (2025). Listing of SME non-identifiable demographics. Table generated via Microsoft Excel (post-NVivo analysis).

Participant Demographics

A summary of the demographic data reported individually by the 24 participants through the anonymous online survey has been provided below. The initial recruitment activities targeting SMEs from the DOE, FERC, and WECC produced a participation rate of approximately 15.4%, resulting in the final group of 24 respondents. Demographic details specific to the two voluntary one-on-one interviewees will be presented separately.

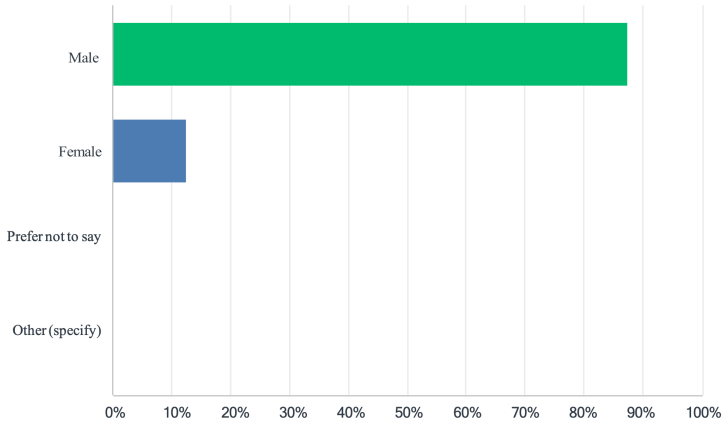
Gender. The self-reported gender breakdown of all 24 online survey participants was 21 males and 3 females (~87.5% and ~12.5%) and displayed below in Figure 4. Of the 24 online surveys taken, 2 participants, approximately 8.33%, volunteered to participate in a follow-up one-on-one online or telephone interview. Both participants in this sub-group where male (100%).

Figure 4

Gender of Online Survey Participants

(1) What is your gender?

Answered: 24 Skipped: 0



ANSWER CHOICES	RESPONSES	
Male	87.50%	21
Female	12.50%	3
Prefer not to say	0.00%	0
Other (specify)	0.00%	0
Total Respondents: 24		

Note. Werner, J. (2025). Survey Question #1 Results. Graphic generated via SurveyMonkey.com data presentation tool.

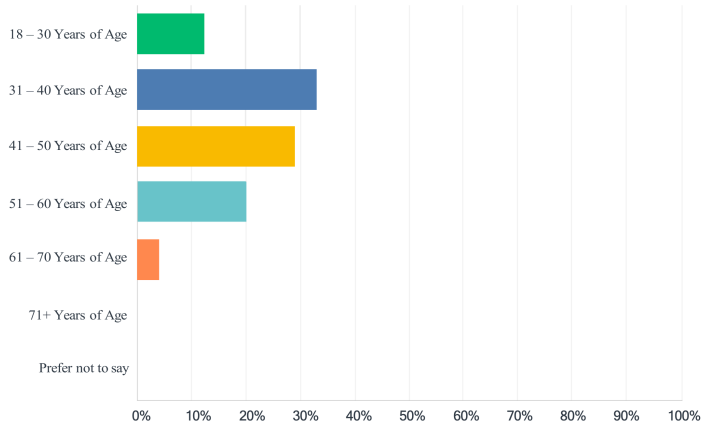
Age of Participants. Participant age demographics indicated a well-distributed range among the 24 respondents self-reporting on their own age based on approximate age categories displayed in Figure 5. The largest group, comprising eight individuals (~33%), reported being between 31 and 40 years old, followed closely by seven respondents (~29%) in the 41–50 age category. Participants aged 51–60 represented five responses (~20%), and three individuals (~12%) indicated they were between 18 and 30 years old. Only one respondent (~4%) fell within the 61–70 age bracket. No participants reported being over 70 years of age, nor did any respondents select the option "Prefer not to say."

Figure 5

Age of Online Survey Participants

(2) What is your approximate age?

Answered: 24 Skipped: 0



ANSWER CHOICES	RESPONSES	
18 – 30 Years of Age	12.50%	3
31 – 40 Years of Age	33.33%	8
41 – 50 Years of Age	29.17%	7
51 – 60 Years of Age	20.83%	5
61 – 70 Years of Age	4.17%	1
71+ Years of Age	0.00%	0
Prefer not to say	0.00%	0
Total Respondents: 24		

Note. Werner, J. (2025). Survey Question #2 Results. Graphic generated via SurveyMonkey.com data presentation tool.

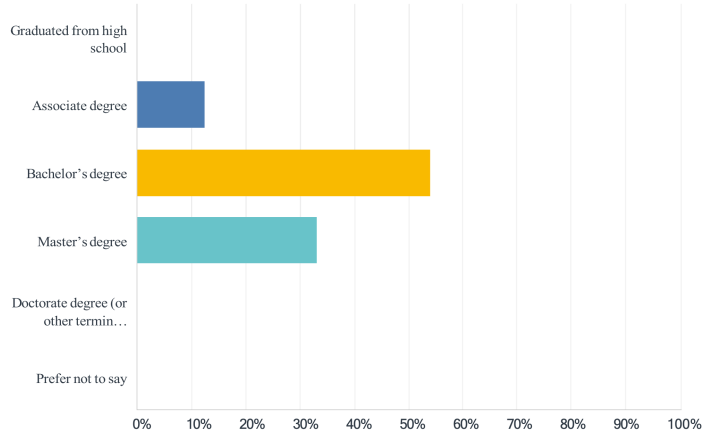
Education Level. Educational attainment among the 24 respondents, displayed in Figure 6, was strongly weighted toward four-year and graduate qualifications. Thirteen participants (~54%) held a bachelor's degree, eight (~33%) had completed a master's program, and three (~13%) reported an associate degree. No participant identified a high-school diploma as their highest credential, reported a doctorate or other terminal degree, or chose to withhold their education level.

Figure 6

Education Level of Online Survey Participants

(3) What is the highest level of education you have completed?

Answered: 24 Skipped: 0



ANSWER CHOICES	RESPONSES	
Graduated from high school	0.00%	0
Associate degree	12.50%	3
Bachelor's degree	54.17%	13
Master's degree	33.33%	8
Doctorate degree (or other terminal post-graduate degree)	0.00%	0
Prefer not to say	0.00%	0
Total Respondents: 24		

Note. Werner, J. (2025). Survey Question #3 Results. Graphic generated via SurveyMonkey.com data presentation tool.

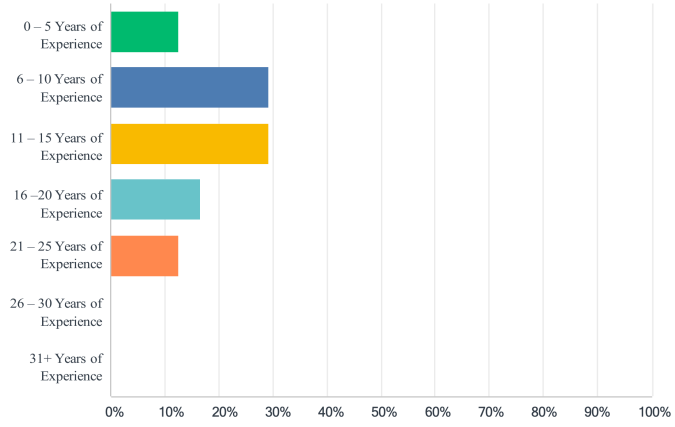
Relevant Professional Experience of Survey Participants. All survey respondents were asked to select the range that best reflected their years of relevant professional experience in grid security, drone technology, and/or related domains. Three participants (~12%) reported 0–5 years in their field. The largest group of respondents were those with 6–10 years and 11–15 years of experience, each represented by seven individuals (~29% apiece). Four respondents (~17%) had accumulated 16–20 years, and another three (~12%) reported 21–25 years. No participant indicated more than 25 years of experience.

Figure 7

Relevant Professional Experience of Online Survey Participants

(4) How many total years of relevant professional experience do you currently possess?

Answered: 24 Skipped: 0



ANSWER CHOICES	RESPONSES	
0 – 5 Years of Experience	12.50%	3
6 – 10 Years of Experience	29.17%	7
11 – 15 Years of Experience	29.17%	7
16 – 20 Years of Experience	16.67%	4
21 – 25 Years of Experience	12.50%	3
26 – 30 Years of Experience	0.00%	0
31+ Years of Experience	0.00%	0
Total Respondents: 24		

Note. Werner, J. (2025). Survey Question #4 Results. Graphic generated via SurveyMonkey.com data presentation tool.

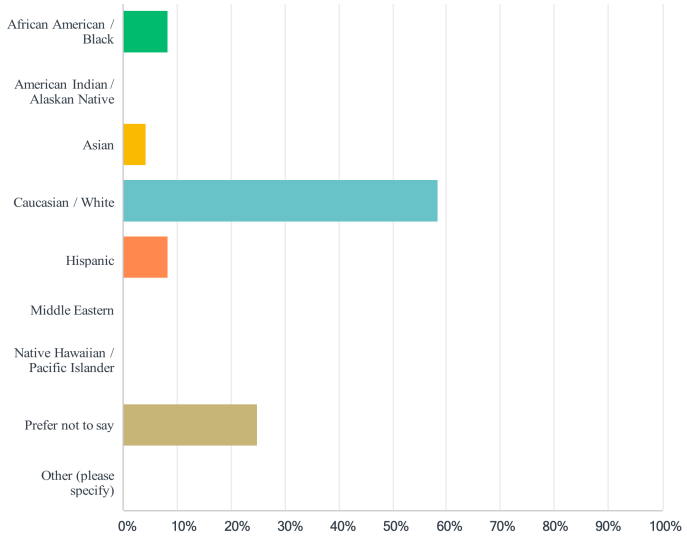
Race/Ethnicity. Finally, online survey participants were asked to indicate the racial or ethnic category that best represented them. Of the 24 respondents, fourteen (~58%) identified as Caucasian/White, two (~8%) as African American/Black, and two (~8%) as Hispanic. One respondent (~4%) selected Asian, while six (~25%) preferred not to disclose their race or ethnicity. No participants identified as American Indian/Alaskan Native, Middle Eastern, Native Hawaiian/Pacific Islander, or chose "Other."

Figure 8

Approximate Age of Online Survey Participants

(5) What is your approximate age?

Answered: 24 Skipped: 0



ANSWER CHOICES	RESPONSES	
African American / Black	8.33%	2
American Indian / Alaskan Native	0.00%	0
Asian	4.17%	1
Caucasian / White	58.33%	14
Hispanic	8.33%	2
Middle Eastern	0.00%	0
Native Hawaiian / Pacific Islander	0.00%	0
Prefer not to say	25.00%	6
Other (please specify)	0.00%	0
Total Respondents: 24		

Note. Werner, J. (2025). Survey Question #5 Results. Graphic generated via SurveyMonkey.com data presentation tool.

Survey Question Responses

Beyond the demographic section, the questionnaire included eleven applicable items that gauged participants' perceptions of drone-related risks, grid vulnerabilities, and the adequacy of existing countermeasures. A separately labeled twelfth item, marked as voluntary, invited each respondent to indicate whether they were willing to participate in a one-on-one follow-up interview to discuss their answers and professional insights in greater depth. The aggregated results for all twelve items are documented below.

Survey Question #6. Across all asset categories, respondents uniformly endorsed high urgency for implementing new or enhanced drone-mitigation measures, with no ratings of "1" recorded. For power plants (n = 24), 15 respondents (~63%) rated urgency at 5, 5 respondents (~21%) rated it 4, and 4 respondents (~17%) rated it 3, indicating strong consensus that protective enhancements at generation sites are critical. Transmission lines (n = 24) elicited slightly lower, but still substantial, concern: 16 respondents (~67%) rated urgency at 5, 2 respondents (~8%) at 4, 3 respondents (~13%) at 3, and 3 respondents (~13%) at 2, suggesting that while a few respondents saw a moderate urgency, the majority view aligns with immediate action.

Substations (n = 24) commanded the highest unanimity: 17 respondents (~71%) assigned a rating of 5 and 5 respondents (~21%) a 4, with only 2 respondents (~8%) at 3, underscoring their pivotal role in grid resilience. Control centers (n = 24) showed more distribution: 14 respondents (~58%) rated urgency at 5, 3 respondents (~13%) at 4, 5 respondents (~21%) at 3, and 2 respondents (~8%) at 2, reflecting some variation in perceived criticality of command-and-control nodes. Among other assets (n = 16), 12 respondents (75%) rated measures as highly urgent (5), 1 respondent (~6%) rated 4, 2 respondents (~13%) rated 3, and 1 respondent (~6%) rated 2. These patterns indicated a clear hierarchy of concern, with substations and power plants at the apex, while reaffirming that every component merits prompt security enhancements. The collected responses to the survey question are graphically displayed in Figure 9.

In addition to the quantitative ratings, this question included an open-ended section where participants could elaborate on their perspectives. The open-ended comments underscored a pervasive sense of urgency regarding grid vulnerability to drone incursions. One respondent,

SME #24, observed that “what the Ukrainian military have demonstrated can be accomplished with Walmart level drone technology is both amazing and terrifying”.

Several experts echoed this concern, SMEs #10 noted that “high vulnerability to potential drone attacks” and SME #12 stated that “all points of the grid are vulnerable in some aspect.” The accessibility and low cost of commercial off-the-shelf systems emerged as a central theme, SME #8 stated, “Drones are readily available for cheap and can be purchased in large numbers without restriction”, creating a threat that “could be easily weaponized”. As SME #7 cautioned, “commercial off the shelf (COTS) sUAS pose an ever-increasing credible threat to infrastructure at large. They are cheap, highly accessible, and easily modified by anyone with a basic understanding of electronics”. Compounding this danger is the stealthy nature of drone technology, which led SME #7 to warn of their “ability to go untracked and to avoid detection both in the air and from points of origin”.

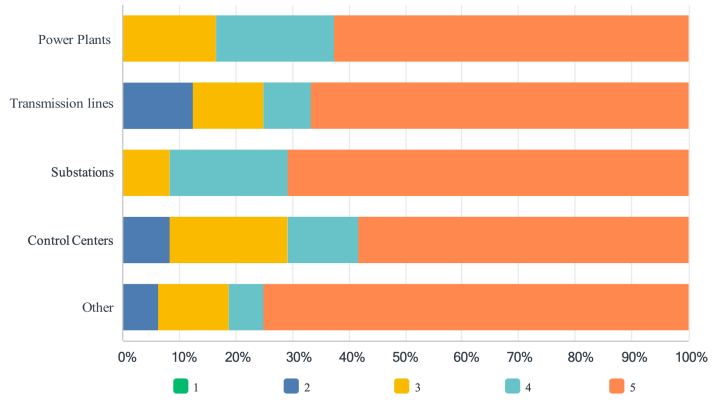
Drawing on observations from current Ukrainian-Russian war, SME #6 noted that “power infrastructure in general is highly susceptible to low cost, high volume drone/UAV attacks,” while SME #5 stressed that “given the small size of drones it wouldn’t be difficult to fly one into one of the above components, damaging it enough to knock out power”. Perhaps most starkly, SME #4 stated, “there is little to no infrastructure to safeguard the electrical grid from aerial attacks”, highlighting a critical gap in existing protective measures. Collectively, these reflections painted a picture of an electrical grid potentially at risk from inexpensive, easily modified drones that current defenses are ill-equipped to counter.

Figure 9

Survey Question #6 Results

(6) On a scale of 1 (Not Vulnerable) to 5 (Highly Vulnerable), how vulnerable do you perceive the following aspects of the Western Interconnection Electrical Grid to potential drone threats?

Answered: 24 Skipped: 0



	1	2	3	4	5	TOTAL	WEIGHTED AVERAGE
Power Plants	0.00% 0	0.00% 0	16.67% 4	20.83% 5	62.50% 15	24	4.46
Transmission lines	0.00% 0	12.50% 3	12.50% 3	8.33% 2	66.67% 16	24	4.29
Substations	0.00% 0	0.00% 0	8.33% 2	20.83% 5	70.83% 17	24	4.63
Control Centers	0.00% 0	8.33% 2	20.83% 5	12.50% 3	58.33% 14	24	4.21
Other	0.00% 0	6.25% 1	12.50% 2	6.25% 1	75.00% 12	16	4.50

Note. Werner, J. (2025). Survey Question #6 Results. Graphic generated via SurveyMonkey.com data presentation tool.

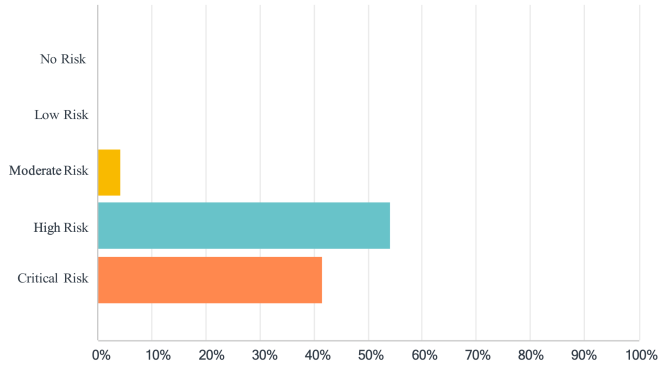
Survey Question #7. All 24 participants were asked to rate the overall risk that drone incursions pose to the Western Interconnection electrical grid using a five-point scale. None selected "No Risk" or "Low Risk." One respondent (~4%) assessed the threat as "Moderate Risk," while the majority characterized it as "High Risk" (thirteen participants, ~54%) or "Critical Risk" (ten participants, ~42%). The collected responses to the survey question are graphically displayed in Figure 10

Figure 10

Survey Question #7 Results

(7) How would you rate the severity of the risks posed by current aerial drone technologies to grid infrastructure?

Answered: 24 Skipped: 0



ANSWER CHOICES	RESPONSES	
No Risk	0.00%	0
Low Risk	0.00%	0
Moderate Risk	4.17%	1
High Risk	54.17%	13
Critical Risk	41.67%	10
Total Respondents: 24		

Note. Werner, J. (2025). Survey Question #7 Results. Graphic generated via SurveyMonkey.com data presentation tool.

Survey Question #8. Participants were asked in the online survey to evaluate the sufficiency of existing countermeasures against drone threats on a five-point agreement scale. No respondents selected “Strongly Disagree” or “Disagree,” and only one individual (~4%) remained “Neutral”. Eight participants (~33%) registered their endorsement by choosing “Agree,” while the majority, fifteen respondents (~63%), expressed strong confidence with “Strongly Agree.” These findings are illustrated in Figure 11.

When offered the chance to expand on their ratings, participants underscored the accelerating gap between drone capabilities and existing protections. One expert, SME #21, warned that “drones are getting cheaper, smarter, and more capable, which makes them easier for

bad actors to misuse," noting that "rules and defenses haven't quite caught up" to recent incursions near critical infrastructure. Two respondents, SME #20 and SME #11, emphasized the accelerating risk, noting "drone technology is rapidly evolving. Increased capability equates to increased risks," and that "drone technology and use is evolving faster than the industry and legislation can respond".

Drawing on battlefield examples, SME #8 observed that, "This technology has been used by groups and militaries around the world to damage and/or destroy infrastructure and infrastructure support facilities." Additionally, SME #7 reported that "state and non-state actors have already been seen utilizing a myriad of modified sUAS to attack personnel, infrastructure and vehicles in flag-on-flag conflict and insurgent operations". The immediacy of this potential threat was starkly conveyed by SME #6 who declared, "I don't think drones will become a critical threat. I think they already are one. As technology advances, they will only become more difficult to mitigate."

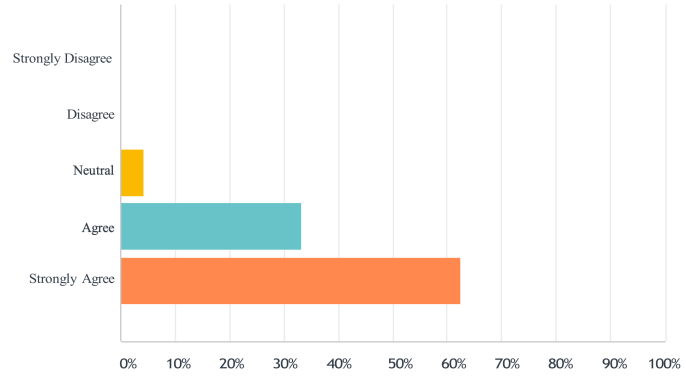
Technical countermeasures were not viewed as a cure-all, as SME #4 noted, "jammers are now being ineffective as drones become more autonomous and less dependent on an operator". By contrast, SME #2 offered a dissenting view, stating, "drones are still small and other than spying and small limited damage, don't think they are an issue to other than late power plants systems." Together, these responses indicated broad agreement that drone innovations are outpacing both regulatory frameworks and defense measures, heightening potential risks to the Western Interconnection grid.

Figure 11

Survey Question #8 Results

(8) To what extent do you agree with the following statement: “Emerging trends in drone technology will significantly increase risks to the Western Interconnection Electrical Grid in the next 5 years.”

Answered: 24 Skipped: 0



ANSWER CHOICES	RESPONSES	
Strongly Disagree	0.00%	0
Disagree	0.00%	0
Neutral	4.17%	1
Agree	33.33%	8
Strongly Agree	62.50%	15
Total Respondents: 24		

Note. Werner, J. (2025). Survey Question #8 Results. Graphic generated via SurveyMonkey.com data presentation tool.

Survey Question #9. Question 9 invited participants to assess the urgency of adopting new or enhanced security measures to counter drone-related threats, yielding 11 substantive responses and 13 respondents skipping this question (~49% and ~54% respectively) that aligned around four key themes. The first theme, International Conflict as Demonstration of Risk, used the Ukraine–Russia war to illustrate how commercially available drone systems could be weaponized with military-grade explosives. The second theme, Drone Threats in Terrorism and Non-State Actor Contexts, highlighted state-sponsored proliferation, such as Iran’s transfer of

"kamikaze" UAS to militant groups, as evidence of asymmetric warfare tactics targeting critical infrastructure.

The third theme, Domestic Incidents and Observations, cited concrete U.S. events, including a 2020 Pennsylvania substation attack and a coordinated surge of drone sightings near nuclear plants and transmission lines in December 2024, to underscore real-world vulnerabilities. Finally, General Awareness and Speculation of Risk reflected a precautionary stance among SMEs who, despite lacking direct incident knowledge, recognized the inevitability of drone assaults and the need for proactive defenses. These thematic insights underscored the need to strengthen grid security against potentially evolving aerial threats.

Figure 12

Survey Question #9 Responses

(9) How urgent do you believe it is to implement new or enhanced measures to improve grid security against drone-related risks?

Answered: 11 Skipped: 13

Theme 1: International Conflict as Demonstration of Risk

Theme 1, addressed international conflicts as illustrative examples of drone-related risks, reveals a clear consensus among SMEs on the practical demonstration of potential drone threats. SMEs explicitly referenced the ongoing conflict between Ukraine and Russia as a prominent scenario exemplifying the operational capabilities and strategic weaponization of commercial drones. Respondents specifically emphasized the use of widely accessible civilian drones, adapted, or enhanced with military explosives, demonstrating their potency and viability as offensive tools in contemporary warfare.

One respondent, SME #24, stated, "I think the Ukrainian war is the best example out there," acknowledging the conflict's clear demonstrations of the drone threats. Another

respondent, SME #2, elaborated further noting, “The Russian Ukrainian war has shown what off the shelf drones can do, but these are equipped with military explosives by armies with access to said explosives”, underscoring the critical role that readily accessible drone technology has played when integrated into conventional military arsenals. Additional participants echoed similar observations, SME #21 affirmed the relevance of the “Ukraine Russia war” as illustrative of this trend, with SME #24 explicitly stating, “I think the Ukrainian Russian war is the best example I have for the weaponization of commercial drones”. These consistent references collectively validate international conflict scenarios as empirical examples, emphasizing the practical need to thoroughly evaluate and proactively mitigate parallel drone risks within domestic critical infrastructure environments.

Theme 2: Drone Threats in Terrorism and Non-State Actor Contexts

The second theme highlighted drone threats posed by terrorist groups and other non-state actors, emphasizing SMEs’ concerns regarding their ability to use drones in targeted attacks against critical infrastructure. Respondents specifically cited Iran’s active role in disseminating drone technology to militant organizations. Citing Iran’s regional influence, SME #7 wrote, “Iran proliferates small one-way attack UAS to non-state players in the Middle East. These organizations utilize these ‘kamikaze’ drones to wreak havoc on target electrical grids on top of a plethora of other targets”. Such explicit references illustrate how drones, provided by state-sponsored actors to non-state groups, have become increasingly viable as weapons of asymmetric warfare, capable of disrupting critical infrastructure and thereby significantly elevating the threat perception.

Theme 3: Domestic Incidents and Observations

The third theme involved direct references to drone-related incidents occurring within the United States, underscoring tangible domestic risks to infrastructure security. SMEs offered examples of drone activity targeting critical domestic infrastructure. One respondent, SME #16, specifically noted, "A drone was used to attempt to disable a Pennsylvania substation in 2020", highlighting a specific event showing the actualization of drone threats domestically.

According to SME #3, "An unusual increase in drone activity was observed in December 2024 around US nuclear plants, military installations, electric transmission lines, airports, and rail stations, most of which experienced this activity within the same week". This account emphasizes the concern about the coordinated nature of such drone incidents, indicating potential strategic reconnaissance or deliberate probing of vulnerabilities. Collectively, these examples from SMEs substantiate the existence of probable drone threats within domestic contexts, amplifying the urgency of addressing possible vulnerabilities through improved surveillance, regulatory frameworks, and proactive security measures.

Theme 4: General Awareness and Speculation of Risk

The fourth theme reflected general awareness of potential drone risks despite the absence of personally known or documented incidents. SMEs deemed the threat plausible based on logic and situational awareness rather than specific events. Additionally, SME #5 warned, "I don't know of any, but I think it would be foolish to assume that it couldn't happen or that a terrorist organization hasn't eyed it as a target of opportunity." This perspective illustrates a precautionary posture, emphasizing that infrastructure security must anticipate emerging threats even without immediate historical precedent.

Survey Question #10. All 24 participants were asked to indicate their level of concern about drone-related risks to the Western Interconnection grid. None selected "Not Concerned"

or “Slightly Concerned,” and only one individual (~4%) chose “Moderately Concerned.” The majority, thirteen respondents (~54%), reported being “Very Concerned,” while ten participants (~42%) identified as “Extremely Concerned.” This distribution underscores a pronounced apprehension among SMEs, with over 95% of respondents expressing high to extreme concern, reflecting a collective recognition of the potentially significant threat drones pose to critical infrastructure security. The collected responses to the survey question are graphically displayed in Figure 13

In the open-ended portion of question 10, participants elaborated on the factors behind their high levels of concern. In SME #21’s view, “the combination of advancing capabilities, increasing incidents near critical infrastructure, and gaps in regulatory and defensive measures poses a credible and growing risk”, cautioning that “without substantial improvements in detection, coordination, and policy enforcement, the threat level is likely to escalate”. Another respondent stated being “highly concerned about drone threats due to their versatility”, underscoring the broad range of potential attack vectors. Regarding system architecture, SME #6 offered observations while noting limited knowledge of the Western Interconnection’s specific configurations:

> Interconnected or mesh networks have advantages and disadvantages. As long as there are sufficient redundancies, it should be more resilient to a high-volume drone attack. If single points of failure are exposed or unhardened, these points only serve as an increased vulnerability. I don’t have sufficient enough knowledge of the WIEG to make a deeply informed assessment of its specific vulnerability.

Looking ahead to broader conflict scenarios, one expert remarked, “we aren’t at war yet, but I think once we are these will be prime targets for attacks,” signaling anticipation of strategic

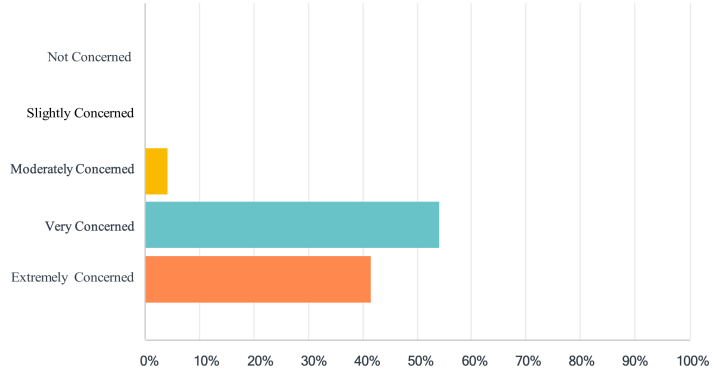
targeting under wartime conditions. Finally, the rising prevalence of drone use was highlighted by SME #01: “the use of drones by people seems to be increasing and it is a threat electrical infrastructure was not designed to mitigate.” Collectively, these comments reinforce that SMEs view drone-related risks as both immediate and escalating, driven by technological advances, evolving tactics, and entrenched deficiencies in current security frameworks.

Figure 13

Survey Question #10 Results

(10) How concerned are you about drone threats to the Western Interconnection Electrical Grid?

Answered: 24 Skipped: 0



ANSWER CHOICES	RESPONSES	
Not Concerned	0.00%	0
Slightly Concerned	0.00%	0
Moderately Concerned	4.17%	1
Very Concerned	54.17%	13
Extremely Concerned	41.67%	10
Total Respondents: 24		

Note. Werner, J. (2025). Survey Question #10 Results. Graphic generated via SurveyMonkey.com data presentation tool.

Survey Question #11. Question 11 asked respondents to identify the factors that most elevated their concern about drone misuse in critical infrastructure. Participants identified unauthorized surveillance and intelligence gathering as a universal concern (100%, n = 24).

Physical attack potential on infrastructure and the technology's accessibility and affordability were each cited by 23 participants (~96%). Cybersecurity vulnerabilities, such as hacking and GPS spoofing, were noted by 13 respondents (~54%), while 15 (~63%) pointed to inadequate regulatory oversight or enforcement. The collected responses to the survey question are graphically displayed in Figure 14.

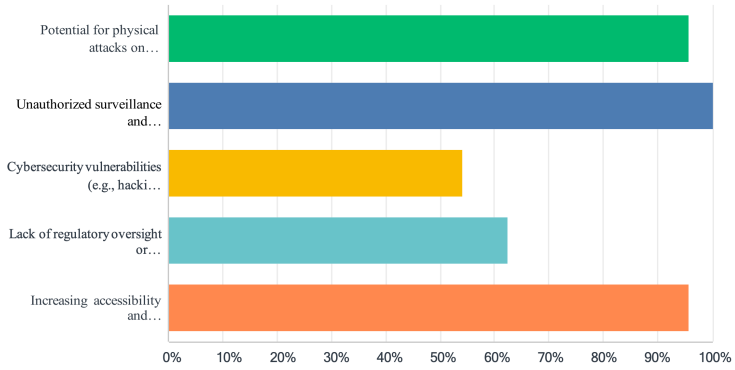
In the open-ended section of question 11, SMEs highlighted the urgent need for comprehensive countermeasures. One expert, SME #19, warned, "Drones pose a threat due to all of these factors, which is why the need for anti-drone measures and drone disaster preparedness and response is so critical." Another respondent, SME #14, cited "increasing technology, specifically" as a key driver of concern. A third, SME #11, highlighted systemic vulnerabilities, noting that "a lack of consistent security and prevention measures leave the grid susceptible to physical attacks and aging/unmanned infrastructure makes it difficult to update or implement new security measures across all points of grid operations." These comments reinforce the view that without cohesive, technology-informed defenses and standardized security protocols, the grid remains exposed to both evolving and longstanding threats.

Figure 14

Survey Question #11 Results

(11) Which of the following factors contribute most to your level of concern about the potential misuse of drone technologies in critical infrastructure areas? (Select all that apply)

Answered: 24 Skipped: 0



ANSWER CHOICES	RESPONSES	
Potential for physical attacks on infrastructure	95.83%	23
Unauthorized surveillance and intelligence gathering	100.00%	24
Cybersecurity vulnerabilities (e.g., hacking, GPS spoofing)	54.17%	13
Lack of regulatory oversight or enforcement	62.50%	15
Increasing accessibility and affordability of drone technology	95.83%	23
Total Respondents: 24		

Note. Werner, J. (2025). Survey Question #11 Results. Graphic generated via SurveyMonkey.com data presentation tool.

Survey Question #12. When asked in the online survey to assess their peers' level of concern about drone threats, no respondents reported "No Concern" or "Minimal Concern". Five participants (~21%) indicated "Moderate Concern", suggesting some awareness but limited urgency. The majority, sixteen SMEs (~67%), perceived "Significant Concern" within their agencies, reflecting broad recognition of the issue.

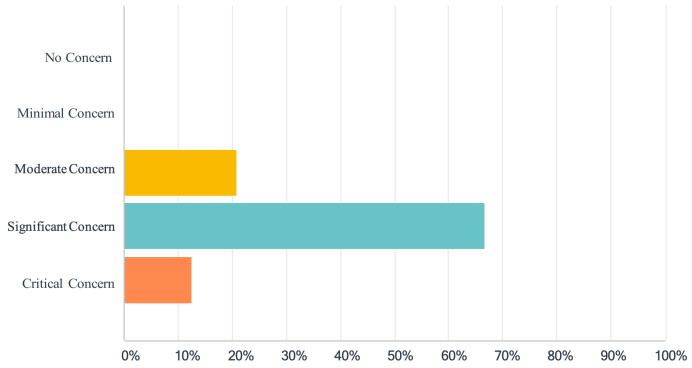
Three respondents (~13%) characterized peer sentiment as "Critical Concern," denoting an exceptionally high level of alarm. This distribution underscored that, while a few view the threat as emerging, most SMEs believe their colleagues regard drone risks as a pressing priority. See Figure 15 for a graphical display of this question's responses.

Figure 15

Survey Question #12 Results

(12) How do you perceive the overall level of concern among your colleagues or within your agency regarding drone threats?

Answered: 24 Skipped: 0



ANSWER CHOICES	RESPONSES	
No Concern	0.00%	0
Minimal Concern	0.00%	0
Moderate Concern	20.83%	5
Significant Concern	66.67%	16
Critical Concern	12.50%	3
Total Respondents: 24		

Note. Werner, J. (2025). Survey Question #12 Results. Graphic generated via SurveyMonkey.com data presentation tool.

Survey Question #13. Respondents to the online survey question 13 placed drone threats squarely among their top security concerns relative to other emerging risks. Eight experts (~33%) assigned them a "Moderate Priority", indicating they view drones as significant but not foremost. Ten participants (~42%) rated drone threats as a "High Priority", reflecting broad agreement on the need for robust countermeasures. A minority of six SMEs (25%) considered these risks the "Highest Priority", placing them above other challenges such as cyberattacks or natural disasters. No respondents relegated drone threats to lower tiers, underscoring consensus that they warrant at least moderate and for the majority, high attention within grid security planning.

In their open-ended remarks for question 13, participants acknowledged that drone threats currently compete with established risks like cyberattacks and natural disasters but are rapidly gaining priority due to accessibility, versatility, and emerging vulnerabilities. From SME #21's perspective, "drone threats are seen as a moderate priority compared to things like cyberattacks or natural disasters, but as drones become more advanced and easier to access, they're likely to become a bigger concern for grid security in the future." Drawing on recent conflicts, SME #19 emphasized the strategic lessons: "Throughout its war, Ukraine has demonstrated the versatility of drones and the need for robust countermeasures. The threat posed by drones cannot be understated." Two SMEs, #8 and #6, pointed to ease of acquisition and economic leverage, noting "It's easy for anyone to get a drone and cause problems with little to no training or experience," and "It's a low-cost solution to a high value problem." One respondent, SME #07, added:

> sUAS are the tip of the iceberg. They are a delivery system. The most significant threat and possibly the root cause of drone-based threats stems from GPS/SatCom/links security. As the cyber domain expands, so does infrastructure dependence. The same connection monitoring a grids output at a substation, is being used to explore vulnerabilities. i.e., spoofing drones may be more dangerous than a drone strapped with explosives.

Another participant further emphasized the convergence of accessibility and evolving functionality in shaping risk assessments, underscoring their perceived urgent need to address weaknesses at the intersection of physical and cyber domains. As SME #3 stated:

> Much of drones' risk comes from increased accessibility and capabilities. They allow for near-simultaneous monitoring of critical infrastructure across multiple sites, can be

hacked, and possess the capability to attack and disable critical infrastructure servicing large geographic areas. Most critical infrastructure already have robust cyberattack and natural disaster measures in place. Drones are still emerging, evolving, and presenting new risks, making them a high-priority threat.

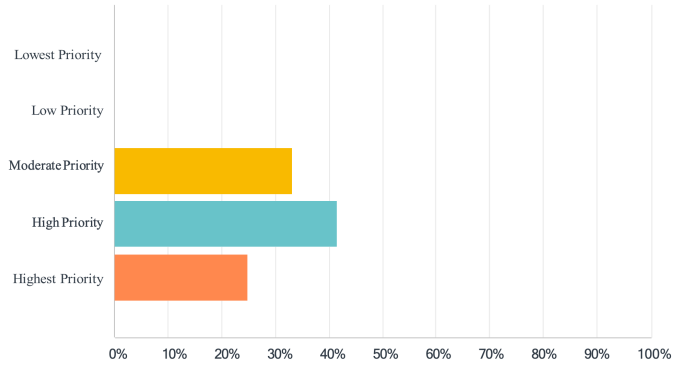
These comments illustrated that while drones offer a low-cost avenue to disrupt high-value targets, their integration with cyber-physical systems and evolving autonomy create complex vulnerabilities that likely demand urgent, multifaceted responses.

Figure 16

Survey Question #13 Results

(13) How would you prioritize drone threats in comparison to other emerging threats to grid security (e.g., cyberattacks, natural disasters)?

Answered: 24 Skipped: 0



ANSWER CHOICES	RESPONSES	
Lowest Priority	0.00%	0
Low Priority	0.00%	0
Moderate Priority	33.33%	8
High Priority	41.67%	10
Highest Priority	25.00%	6
Total Respondents: 24		

Note. Werner, J. (2025). Survey Question #13 Results. Graphic generated via SurveyMonkey.com data presentation tool.

Survey Question #14. Across the 24 SMEs, judgments of current counter-drone safeguards gravitate toward the lower end of the effectiveness spectrum. Two participants (~8%) described the measures as "Not Effective," while a clear majority, 14 respondents (~58%), regarded them as only "Slightly Effective". Another eight SMEs (~33%) saw them as "Moderately Effective", and none characterized them as either "Very Effective" or "Highly Effective". Collectively, these views conveyed a shared sense that existing protections offer, at best, limited value: respondents recognize some utility in present protocols yet stop well short of calling them robust. The absence of any high-confidence ratings emphasized a perceived vulnerability and signaled that current mitigations are lagging behind the rapidly evolving drone threat landscape.

The written feedback added depth to the survey results and showed clear themes. One participant, SME #21, wrote, "Protective measures against drone threats to the grid are still pretty limited, mainly because detection isn't consistent, response plans are underdeveloped, and the rules haven't kept up with how fast drone technology is evolving." That view matched several comments about the grid's physical state.

Respondents. SME #8 and SME #10, remarked, "The infrastructure was never designed with this specific threat in mind," and cited, "Aging and vulnerable infrastructure, slow efforts to implement new security measures, and inconsistent and/or insufficient security measures across operational locations and substructures." Together, these statements detailed why piecemeal fixes have not kept pace with rapid changes in drone technology. Other participants' responses focused on planning and analysis.

According to SME #7, "Major stake holders definitely understand the threat drones pose, but detailed studies are required to identify all vulnerabilities so that systemic fixes and

responses can be prepared in the event a material solution doesn't exist." Without this proposed groundwork, counter-drone spending could miss the most vulnerable attack points. Doubts about technology were blunt. One comment, from SME #13, asserted, "There is currently little to no protection from physical drone attacks," and another, from SME #4, warned, "Many of the products available to counter drones are expensive and ineffective. Swarms of drones attacking all at once are almost impossible to defeat." These views suggested why no one judged current measures very or highly effective.

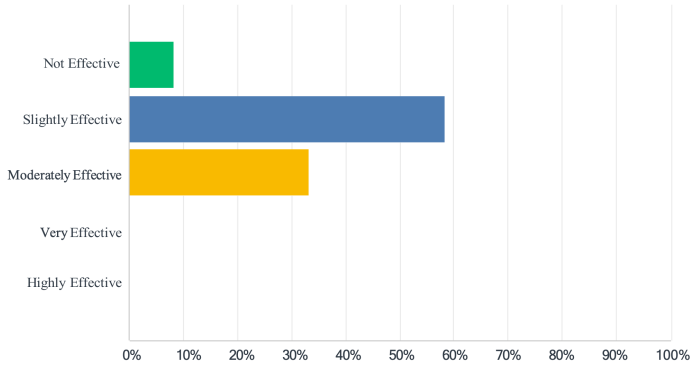
Information gaps also appeared in respondents written responses. In their survey responses, SMEs #5 and #6 acknowledged limited knowledge, stating "I don't actually know what counter measures are in place" and "My knowledge on this subject is insufficient to make an adequate assessment." Only one respondent, SME #2, offered a limited positive: "Established reporting systems and instructions have been established." Taken together, the quotes showed that existing safeguards were limited, uneven, and outpaced by the evolving drone threat. Respondents believed the grid needed coordinated planning, better intelligence, and more capable technology. The narrative evidence emphasized systemic, technical, and organizational shortfalls that suggested a coordinated, forward-leaning remediation strategy will be necessary.

Figure 17

Survey Question #14 Results

(14) How effective do you find the current protective measures in place to counter drone threats to the grid?

Answered: 24 Skipped: 0



ANSWER CHOICES	RESPONSES	
Not Effective	8.33%	2
Slightly Effective	58.33%	14
Moderately Effective	33.33%	8
Very Effective	0.00%	0
Highly Effective	0.00%	0
Total Respondents: 24		

Note. Werner, J. (2025). Survey Question #14 Results. Graphic generated via SurveyMonkey.com data presentation tool.

Survey Question #15. Of the 24 individuals solicited, 22 (~92%) provided evaluative responses while two (~8%) elected to skip this item. Among those who responded, exactly half (11 of 22; 50%) characterized interagency collaboration as "minimally coordinated", and the remaining half (11 of 22; 50%) rated it as "moderately coordinated". No respondents judged the coordination to be either "well-coordinated" or "highly coordinated", nor did any consider it to be entirely lacking. The findings showed that, while participants agree some joint effort exists, they seldom rated coordination above a moderate level. This gap suggested an opportunity exists for DOE, FERC, and WECC to strengthen formal linkages and information-sharing mechanisms.

Respondents uniformly emphasized that current interagency collaboration requires significant enhancement. One participant, SME #14, noted "Efforts to coordinate need to be a bigger priority," and another, SME #12, reinforced this by stating "More effort and coordination are needed." In survey responses, information gaps were evident: SME #5 remarked, "I don't

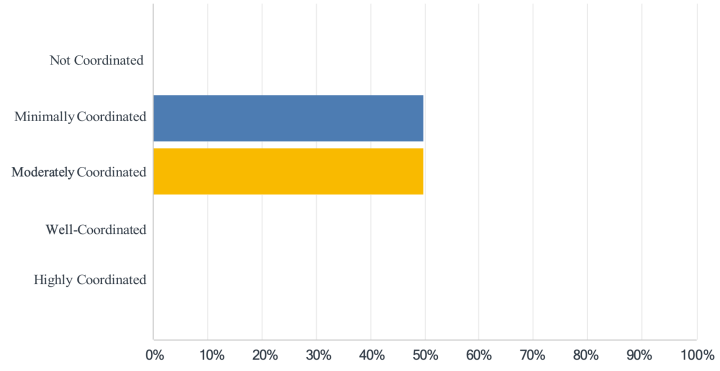
have enough information to form a good opinion," SME #6 observed, "My knowledge on this subject is insufficient to make an adequate assessment," and SME #7 stated, "I don't have enough data to make an assessment." Conversely, one participant, SME #4, acknowledged emerging progress, "I have seen efforts to streamline defensive efforts but much more cooperation needs to happen," yet simultaneously cautioned that "it's a known issue, but no firm response/plans on how to deal with it." Collectively, these comments reveal that while awareness of the drone threat exists, actionable coordination mechanisms and clarity around roles remain underdeveloped.

Figure 18

Survey Question #15 Results

(15) How well-coordinated are efforts between the DOE, FERC, and WECC in addressing the drone threat?

Answered: 22 Skipped: 2



ANSWER CHOICES	RESPONSES	
Not Coordinated	0.00%	0
Minimally Coordinated	50.00%	11
Moderately Coordinated	50.00%	11
Well-Coordinated	0.00%	0
Highly Coordinated	0.00%	0
Total Respondents: 24		

Note. Werner, J. (2025). Survey Question #15 Results. Graphic generated via SurveyMonkey.com data presentation tool.

Survey Question #16. Among the 24 SMEs who evaluated the urgency of strengthening grid security against drone threats, the distribution skewed decisively toward the highest urgency levels. No respondent considered the matter "Not Urgent" or even "Moderately Urgent", and only one participant (~4%) selected "Slightly Urgent", indicating that a negligible minority regard the issue as peripheral. By contrast, a clear majority, fourteen respondents (~58%) classified the need as "Very Urgent", while a further nine (~38%) deemed it "Extremely Urgent". Taken together, 23 of 24 participants (~96%) placed the problem in the upper tiers of urgency. This near-consensus stresses a shared conviction among grid-security experts that new or enhanced counter-drone measures warrant immediate attention and rapid implementation.

In their responses, SMEs conveyed a deep sense that the window for effective intervention is rapidly closing. They argued that the accelerating pace of drone innovation has already outstripped current safeguards, making enhanced countermeasures not merely advisable but imperative. One SME (#21) stressed the need for early and decisive action, observing that "it's becoming increasingly urgent to put stronger measures in place, because as drone technology advances and becomes more accessible, the risk to critical grid infrastructure grows faster than current protections can keep up."

From SME #16's perspective, the window for action has already passed: "the time to address critical risks was 10–15 years ago, before drones became the threat to grid infrastructure that we recognize today. The industry, along with legislation, has been slow to address drone risks." In parallel, SME #15 warned: "The ability to manipulate a large number of drones

simultaneously across multiple geographic locations means critical infrastructure can be widely disabled with one coordinated attack." One massive attack would be catastrophic."

Several participants emphasized that preventative strategies must precede complete threat understanding. As one SME (#6) explained, "While I'm not sure of the specific current measures in place, based off of the speed at which technology is advancing, preventative measures should be put in place early and re-addressed often." Others, SMEs #4 and #5, distilled the imperative more succinctly: "The grid is very exposed, and it will probably take an attack to get law makers into action," and "If there isn't any mitigation in place there needs to be." One respondent, SME #3, stated:

> One of the greatest threats posed by drones is the simultaneous, or near-simultaneous, ability to disrupt multiple infrastructure and geographic locations, whether for the purposes of surveillance or physical attacks. The December 2024 drone sightings demonstrate the ease with which drones can infiltrate various high-risk sites and airspaces within a short period of time and raise significant questions about how effective current security measures would be against a wide-scale physical attack, which is why new or enhanced measures to improve grid security should be urgently examined.

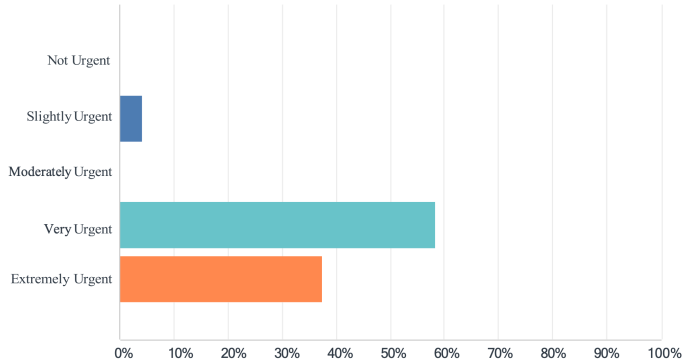
A minority, SME #2, view urged balance, cautioning that "again, there are other threats more pressing right now." Collectively, however, these insights reinforce a clear directive: without immediate and sustained enhancements, grid security will remain vulnerable to rapidly evolving drone capabilities. See Figure 19 for a graphical depiction of data collected.

Figure 19

Survey Question #16 Results

(16) How urgent do you believe it is to implement new or enhanced measures to improve grid security against drone-related risks?

Answered: 24 Skipped: 0



ANSWER CHOICES	RESPONSES	
Not Urgent	0.00%	0
Slightly Urgent	4.17%	1
Moderately Urgent	0.00%	0
Very Urgent	58.33%	14
Extremely Urgent	37.50%	9
Total Respondents: 24		

Note. Werner, J. (2025). Survey Question #16 Results. Graphic generated via SurveyMonkey.com data presentation tool.

Survey Question #17. SMEs were given the opportunity to identify shortcomings in existing drone-mitigation protocols; their observations described a stark picture of lingering vulnerabilities within the Western Interconnection's grid. Despite a modest (10 out of 24) participation rate, the depth and consistency of these insights compensated for the limited input. Collectively, the comments portrayed a layered risk landscape in which technical limitations, procedural inconsistencies, and knowledge deficits reinforced one another, widening the window of opportunity for hostile actors equipped with increasingly sophisticated drones.

Foremost among the cited weaknesses is the absence of robust, real-time detection and rapid-response mechanisms. Participants lamented outdated sensor suites, latency-prone alert

protocols, and legal barriers that constrain advanced counter-drone tools such as jamming, spoofing, or kinetic takedowns near critical sites. Equally troubling is the perceived patchwork deployment of security measures across facilities: primary control centers may be subject to rigorous surveillance, yet satellite substations can remain effectively unmonitored, encouraging an adversary to target the weakest link.

SMEs also criticized disaster-preparedness frameworks that still prioritize natural hazards, leaving operators without clear guidance for multi-regional, coordinated drone incursions. The problem is magnified by the pace of technological change: autonomous aircraft, swarm tactics, and home-built platforms often fall outside existing threat libraries, outstripping current deterrent strategies. Finally, several respondents concede a personal uncertainty about what counter-drone measures are actually enforced, a knowledge gap that hampers situational awareness and effective planning.

These intertwined deficiencies suggested that any credible mitigation strategy must advance along three fronts simultaneously. Such a strategy would need to modernize detection and neutralization technologies, synchronize security protocols across the grid's full geographic footprint, and systematically educate operators, regulators, and policymakers on evolving UAS capabilities. Without such an integrated approach, SMEs warned, the grid would remain vulnerable to a dynamic threat that is advancing far more rapidly than the defenses designed to contain it. The researcher identified five specific themes in the survey questions #17's responses, detailed below.

(17) What specific gaps or shortcomings do you see in existing protocols or technologies aimed at mitigating drone threats?

Answered: 10 Skipped: 14

Theme 1: Insufficient Detection and Real-time Response Mechanisms

A prominent theme among respondents highlighted significant gaps in real-time detection and immediate response capabilities. SMEs specifically noted limitations in existing surveillance measures, slow reaction protocols, and outdated regulatory constraints, complicating the use of effective counter-drone technologies. One participant, SME #21, explicitly described these concerns: "Some of the biggest gaps right now are the lack of real-time drone detection in many areas, unclear or slow response procedures when a drone is spotted, and outdated rules that make it hard to use things like jamming or takedown tech near critical sites." Another respondent, SME #2, underscored similar limitation, emphasizing the need for advanced technological solutions beyond human observation: "tech to identify drones other than people seeing or hearing them." Collectively, these insights underscored the potential need to modernize detection infrastructures and accelerate responsive interventions to mitigate drone threats effectively.

Theme 2: Inconsistent and Non-uniform Security Protocols

Participants frequently mentioned inconsistencies and non-uniformity in security protocols, resulting in varying degrees of vulnerability across different locations. One SME (#20) emphasized this disparity, noting explicitly that "the same security measures aren't deployed uniformly across all points of possible drone interference." Another, SME #07, highlighted a broader systemic vulnerability at a micro-level, despite robust protections at primary facilities: "As it stands, our grid is largely unmonitored, which leaves significant gaps in defense at a micro level. At a macro level, however, major control centers and power stations are subject to constant scrutiny." This disparity illustrated how inconsistent application of protective measures potentially leaves substantial portions of critical infrastructure exposed, suggesting the need for comprehensive, standardized defense protocols across the entire grid.

Theme 3: Lack of Specialized Preparedness and Response for Drone Threats

Respondents indicated shortcomings in existing preparedness frameworks, which primarily focus on natural disasters and conventional incidents rather than coordinated drone attacks. One SME (#13) directly identified this gap, explaining:

> Disaster preparedness protocols are primarily geared toward natural disasters in a given geographic region; however, power lines, substations, secondary and tertiary substructures are also highly vulnerable to coordinated drone attacks across multiple regions. There is an urgent need to enhance grid security, as well as to develop appropriate disaster response measures in the case of drone attacks.

Another respondent, SME #1, reinforced this by pointing out, "Many plants don't have a drone mitigation plan other than report drone activities", clearly reflecting a deficiency in proactive mitigation and response strategies. These perspectives emphasized the necessity of integrating drone-related scenarios into disaster planning and incident-response strategies.

Theme 4: Challenges Addressing Advanced Drone Technologies and Swarm Tactics

SMEs also described the difficulty of countering advanced drone technologies and tactics, particularly emphasizing the complexity of neutralizing drone swarms and autonomous drone capabilities. A participant, SME #4, specifically articulated this challenge:

> The swarm method is difficult to defeat without using kinetic effects which can harm the local populous. Some jammers take over the command signal, but more and more drones are becoming more sophisticated and do not require a command link. Additionally, the library of command links is only from the known drone companies. Home-built drones are not in the library.

Another respondent, SME #3, concisely captured related concerns: “Insufficient/inconsistent deterrent and protection strategies. Inability to anticipate and mitigate new drone capabilities.” These responses highlighted a critical technological and strategic gap in effectively countering evolving drone threats, calling attention to the necessity for continuous advancements in counter-drone technologies and tactics.

Theme 5: Knowledge Gaps and Uncertainty

Finally, some SMEs indicated limited awareness or insufficient knowledge regarding existing mitigation measures. This uncertainty or lack of specific knowledge itself potentially constituted a significant vulnerability in itself. Reflecting uncertainty, SME #5 and SME #6 reported, “I don’t know what mitigations are in place,” and “My knowledge on this subject is insufficient to make an adequate assessment.” These admissions underscored a critical awareness gap among stakeholders, reinforcing the potential importance of targeted education, training, and transparent communication regarding existing counter-drone protocols and capabilities.

‘Second Wave’ One-on-One Interviews

As stated earlier in this chapter, of the original snowball research goal of 30 participants, 24 (80%) SMEs responded to the studies anonymous online survey hosted by *SurveyMonkey.*com (i.e., ‘first wave’) request. Of those 24 participants, two volunteered to participate in the one-on-one interview (i.e., ‘second wave’) portion of this study. This ‘second wave’ was comprised of follow-up interviews with two of the 24 respondents who voluntarily provided their contact information at the end of the anonymous online survey so that the researcher could probe their original answers in greater depth.

During the ‘second wave’ follow-up, the researcher revisited the same nine open-ended items from the ‘first wave’ *SurveyMonkey.com* questionnaire, asking each of the two volunteer SMEs to elaborate on their earlier written responses. Conducted under a structured protocol, the interviews gave participants unrestricted time to clarify ratings, supply concrete examples, and introduce contextual details that could not be captured in the online format. Both sessions were completed via voice-only calls to accommodate the interviewee’s connection preferences. In both cases, probing prompts encouraged the SMEs to expand on underlying rationales and to discuss interdependencies among affordability, infrastructure exposure, and evolving counter-UAS measures.

To preserve study consistency, both second-wave participants were asked the original nine open-ended survey questions verbatim and in the same sequence as presented in the first-wave questionnaire. Both voice-only phone sessions were automatically transcribed, and the researcher reviewed the draft against the recording before sending the transcript to the interviewee for accuracy confirmation. Following verification, all personally identifiable information was removed, and the de-identified transcripts were imported into NVivo for thematic coding alongside the survey body. In line with the NU IRB’s requirements, participants had received, before scheduling their interview, an electronic packet containing the NU IRB approval notice, an information sheet detailing the study’s purpose and eligibility criteria, and a formal consent letter; these documents were also reviewed verbally at the start of each interview.

The thematic analysis drawn from the two follow-up interviews complemented the first-wave survey by addressing gaps left by the concise, structured items and by enabling data triangulation. By comparing interview themes with survey patterns, the researcher verified that the responses aligned with the study’s core problem statement and research questions, thereby

reinforcing analytic credibility (Yin, 2013). The interview data also provided better context grounded in the SMEs' professional experience, allowing for deeper interpretation of affordability, vulnerability, and counter-UAS challenges. This second-wave insight therefore sharpened the overall findings and strengthened the trustworthiness of the study's conclusions.

Demographics of Subgroup of 2 Individual Interviewees.

The 'second wave' interview data collection consisted of this researcher interviewing two of the 24 respondents to the online survey. The two volunteer interviewees represented a small but informative subset of the study's participants. They accounted for two of the 24 completed questionnaires, about 8% of the final survey sample, and two of the 30 SMEs initially sought through the initial 'first wave' snowball recruitment prices, or roughly 7% of the original target.

Table 2

Listing of the two Individual 'Second Wave' Interviewees

Interviewee #	SME Area	Age Range	Region
1	RPA Pilot	20s	Pacific
2	RPA Pilot	40s	Pacific
(Gender & ethnic data specifically not included to ensure anonymity)			

Note. Werner, J. (2025). Listing of the two Individual 'Second Wave' Interviewees. Table generated via Microsoft Excel (post-NVivo analysis).

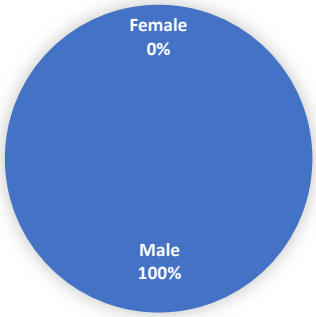
When weighing the value of narrating every follow-up response in full, the researcher concluded that a question-by-question transcript of the two interviews would add little beyond what the participants had already provided in the online survey. The second-wave discussions were intended to deepen, not duplicate, the first-wave findings by clarifying points of ambiguity and supplying concrete examples. Accordingly, instead of presenting the interview data alongside the survey results in parallel tables, the researcher extracted only those elements that enriched or diverged from the broader dataset, namely, illustrative quotations, striking examples,

and distinctive observations unique to the interviewees. This targeted approach preserved analytical focus while ensuring that meaningful nuances from the follow-up conversations informed the overall interpretation of the study.

Gender of Individual Interviewees. Of the two SMEs who volunteered for the one-on-one follow-up interviews, representing roughly 8% of the 24 survey respondents, both self-identified as male, yielding a gender ratio of 100 percent male and 0% female. No interviewee declined to report gender. This distribution, shown in Figure 21, underscored that the second-wave sample, though informative, reflected only a single gender and therefore did not capture potential gender-based differences in perspective. Neither interviewee declined to report their gender during the one-on-one interviews.

Figure 20

Breakdown of One-on-One Interview Participants' Genders

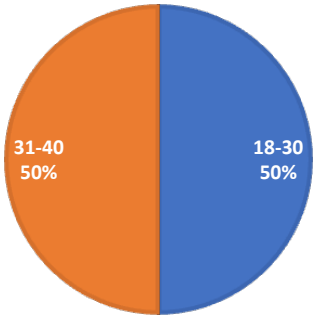


Note. Werner, J. (2025). Breakdown of One-on-One Interview Participants' Genders. Graphic generated via Microsoft PowerPoint.

Age of Participants. Each follow-up interviewee was asked to self-select an age band from the questionnaire's decade categories. Of the two volunteers, one (50%) reported an age between 18–30 years, and the other (50%) placed himself in the 31– 40-year bracket. Neither participant declined to disclose age. The resulting distribution is presented in Figure 22.

Figure 21

Age of Individual Interview Participants

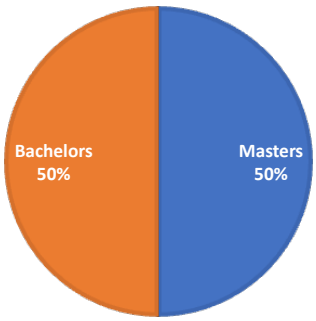


Note. Werner, J. (2025). Age of Individual Interview Participants. Graphic generated via Microsoft PowerPoint.

Education Level of Individual Interviewees. At the start of each follow-up interview, participants identified their highest academic degree. As displayed in Figure 23, one SME (50%) reported a bachelor's degree, whereas the second (50%) held a master's degree. Both participants provided this information without exception.

Figure 22

Education Level of Individual Interview Participants

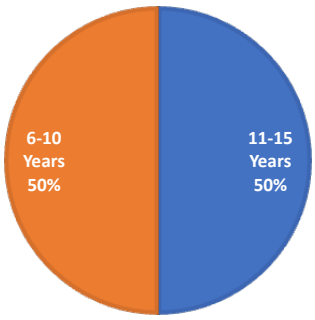


Note. Werner, J. (2025). Education Level of Individual Interview Participants. Graphic generated via Microsoft PowerPoint.

Relevant Professional Experiences of Individual Interviewees. Professional experience was captured by asking each interviewee to select a range representing total years in the field. As shown in Figure 24, one participant (50%) reported 11–15 years of relevant experience, while the other (50%) indicated 6–10 years. Both SMEs elected to supply this information in the one-on-one interviews.

Figure 23

Relevant Professional Experiences of Individual Interview Participants

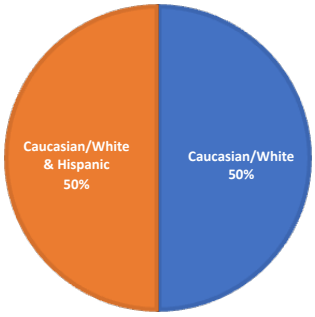


Note. Werner, J. (2025). Relevant Professional Experiences of Individual Interview Participants. Graphic generated via Microsoft PowerPoint.

Race/Ethnicity of Individual Interviewees. Racial and ethnic identity was self-reported using a select-all-that-apply question format. Figure 25 shows that one interviewee (50%) identified as both Caucasian/White and Hispanic, whereas the other (50%) selected only Caucasian/White. Neither respondent omitted an answer.

Figure 24

Race/Ethnicity of Individual Interview Participants



Note. Werner, J. (2025). Race/Ethnicity of Individual Interview Participants. Graphic generated via Microsoft PowerPoint.

Evaluation of Findings

This section presents a systematic assessment of the study's qualitative findings, linking the coded survey data to the three research questions that guided the inquiry. Using NVivo to organize, auto-code, and interrogate 24 completed questionnaires from SMEs at the DOE, FERC, and WECC, seven principal themes emerged. Each theme corresponds to one or more survey clusters and maps directly onto the study's focal constructs: perceived risk (RQ1), level of concern (RQ2), and perceived adequacy of safeguards (RQ3).

The researcher organized this evaluation into three distinct phases. First, perceptions of risk were examined by correlating asset-level vulnerability ratings with evidence from recent conflict cases. Second, the level of concern was measured, highlighting inter-agency differences in threat prioritization and subject-matter knowledge. Third, the adequacy of current counter-UAS measures was evaluated using effectiveness ratings, urgency assessments, and comments on inter-agency coordination. Tables 3 through 5 summarize the top themes for each research question, and the narrative that follows integrates numeric distributions with verbatim responses to explain the findings.

Throughout this section, the researcher adhered to two analytic priorities. The first was to maintain a clear audit trail from raw survey responses to thematic conclusions, and the second

was to interpret SME perceptions within the broader technological and organizational context of the Western Interconnection. By combining percentage breakdowns with illustrative quotations, the section demonstrates how affordability, exposure, evolving technology, and coordination shortfalls collectively shape expert judgments about drone-related risks and defenses.

Research Question 1:

What is the perceived risk level among Subject Matter Experts (SMEs) from the DOE, FERC, and WECC, regarding the potential of current and near-future aerial drone technologies to cause damage or destruction to key aspects of the Western Interconnection Electrical Grid infrastructure?

Table 3

Top Three Themes for Research Question #1

Key Themes	***# of Distinct Comments that touch on theme****	***RQ #***
Cheap, plentiful, modifiable drones	**6**	RQ 1
Grid infrastructure widely exposed / under-protected	**26**	RQ 1
Real-world conflicts validate the threat	**18**	RQ 1

Note. Werner, J. (2025). Top Three Themes for Research Question #1. Table generated via Microsoft Excel (post-NVivo analysis).

Theme #1: Cheap, Plentiful, and Modifiable Drones (RQ #1 / Survey Questions 6-9)

SMEs drew a direct line between the falling cost of small UAS and the high vulnerability scores they had assigned across grid assets. Of the 24respondents, 23 (~96%) rated substations "Very" or "Highly Vulnerable", while 21 (~88%) did the same for transmission lines; even power plants and control centers attracted 18 (~75%) and 16 (~67%) top-tier scores, respectively. Participants consistently anchored these judgments in what one described as the ability to

purchase “Drones are readily available for cheap and can be purchased in large numbers without restriction,” calling them a “low-cost solution to a high-value problem”.

This perceived affordability acted as a force-multiplier in risk calculations: 23 respondents (~96%) selected “High” or “Critical Risk” in Q7. In Q8, 22 (~92%) “Agreed” or “Strongly Agreed” that drone threats would intensify within five years, citing rapid advances in autonomy and payload capacity. Open-ended examples supplied in Q9, many referencing the Ukraine conflict and earlier substation incidents, reinforced the conclusion that both financial and technical barriers to drone-based attacks had deteriorated, enabling even opportunistic actors to target the Western Interconnection’s most exposed components.

Theme #2: Grid Infrastructure Widely Exposed / Under-Protected (RQ #1 / Survey Questions 6-9)

The survey data showed a near-unanimous belief that the Western Interconnection’s physical assets lacked adequate shielding from aerial threats. Substations drew the starkest judgment: 23 of 24 SMEs (~96%) scored them “4” or “5” on the vulnerability scale, describing them as “prime targets” with “little to no infrastructure to safeguard the electrical grid from aerial attacks”. Transmission lines followed, with 21 respondents (~88%) assigning the same top-tier ratings and citing their long, rural spans as “highly vulnerable to coordinated drone attacks”.

Facilities traditionally viewed as hardened were not spared: 18 SMEs (~75%) marked power plants as “very” or “highly” vulnerable, and 16 (~67%) did so for control centers, noting that antenna fields and adjacent yards remained “exposed and aging”. These asset-level scores fed directly into the overall severity assessment: 23 participants (~96%) selected “High” or “Critical Risk” in Q7. Again, in Q8, 22 (~92%) “Agreed” or “Strongly Agreed” that the threat

would escalate within five years, arguing that existing perimeter security was never designed to counter small, low-cost UAS. Collectively, the qualitative commentary portrayed a grid whose sprawling, lightly defended infrastructure offered an inviting attack surface for increasingly capable and affordable drones.

Theme #3: Real-World Conflict Validate the Threat (RQ #1 / Survey Questions 6-9)

Open-ended responses in Q9 confirmed that SMEs grounded their risk assessments in real-world battlefield evidence, specifically the Ukrainian Russian war, rather than speculation. Of the 24 participants, 18 (~75%) referenced the Ukraine–Russia war, and nine (~38%) mentioned Iranian one-way UAS strikes or the 2020 Pennsylvania substation attempt, arguing that low-cost drones had already disabled or disrupted energy assets abroad. One respondent concluded that "Throughout its war, Ukraine has demonstrated the versatility of drones and the need for robust countermeasures. The threat posed by drones cannot be understated."

These real-world examples were not offered as peripheral anecdotes: 17 of the 18 SMEs who referenced them (~94%) also selected "High" or "Critical Risk" in Q7, and 16 (~89%) "Agreed" or "Strongly Agreed" in Q8 that drone-related risks would intensify within five years. By translating overseas incidents into a North American context, respondents moved the threat from abstract possibility to demonstrated capability. These responses reinforced the consensus that the Western Interconnection's infrastructure faces a probable and escalating danger from weaponized small UAS.

Research Question 2:

What is the quantifiable level of concern among SMEs from the DOE, FERC, and WECC regarding current and near-future aerial drone technologies as a potential threat to the Western Interconnection Electrical Grid infrastructure?

Table 4

Top Theme for Research Question #2

Key Themes	***# of Distinct Comments that touch on theme****	***RQ #***
Divergent prioritisation & knowledge gaps	**11**	RQ 2

Note. Werner, J. (2025). Top Theme for Research Question #2. Table generated via Microsoft Excel (post-NVivo analysis).

Theme #4: Divergent Prioritization and Knowledge Gaps (RQ #2 / Survey Questions 10-13)

The survey results captured a wide spread of concern and prioritization, underscoring heterogeneity in expertise and organizational focus. For Q10, 17 of the 24 SMEs (~71%) classified themselves as "Very" or "Extremely Concerned", five (~21%) settled on "Moderately Concerned", and two (~8%) chose the lower end of the scale, noting limited situational awareness. One participant wrote, "my knowledge on this subject is insufficient to make an adequate assessment".

That dispersion repeated in Q12: 10 respondents (~42%) believed their colleagues held "Critical" concern, seven (~29%) judged it "Significant", five (~21%) saw only "Moderate" worry, and two (~8%) perceived minimal attention to the issue. Prioritization rankings in Q13 likewise split the group: 11 SMEs (~46%) rated drone threats as "High" or "Highest Priority", seven (~29%) placed them at a "Moderate" level, and six (~25%) relegated drones to "Low" or "Lowest Priority", asserting that "there are other issues that are more pressing". These response spreads, coupled with qualitative admissions of knowledge deficits, explained why the study recorded a spectrum rather than a consensus on concern levels. Expertise varied, organizational agendas differed, and information gaps persisted, producing a fragmented picture of how urgently SMEs believed drone risks should be addressed.

Research Question 3:

What is the perceived adequacy of the measures taken by the DOE, FERC, and WECC in safeguarding the Western Interconnection Electrical Grid infrastructure from current and near-future aerial drone technology attacks?

Table 5

Top Three Themes for Research Question #3

Key Themes	***# of Distinct Comments that touch on theme****	***RQ #***
Technology outpacing law, policy & counter-UAS tools	**7**	RQ 3
Detection & response remain immature	**7**	RQ 3
Inter-agency coordination gaps	**3**	RQ 3

Note. Werner, J. (2025). Top Three Themes for Theme for Research Question #3. Table generated via Microsoft Excel (post-NVivo analysis).

Theme #5: Technology Outpacing Law, Policy, and Counter-UAS Tools (RQ #3 / Survey Questions 14-17)

Respondents consistently judged existing safeguards inadequate because drone capabilities had outpaced both regulation and defensive technology. In their assessments of effectiveness (Q14) they rarely described current measures as more than modestly satisfactory, pointing to an aging suite of countermeasures and SME #4 noting in Q8 that "Jammers are now being ineffective as drones become more autonomous and less dependent on an operator." Open-ended comments portrayed a widening gap between rapidly evolving threats, swarming autonomy, Global Navigation Satellite System (GNSS) spoofing, weaponized payloads, and the comparatively slow cadence of policy updates.

Discussion of inter-agency coordination (Q15) amplified this theme: several SMEs noted fragmented lines of authority and uneven information sharing, and SME #11 observed that

"drone technology and use is evolving faster than the industry and legislation can respond". When asked about urgency (Q16), most framed immediate action as imperative, warning that incremental upgrades would not close a gap that was growing. The catalogue of shortcomings recorded in Q17, limited detection grids, unclear engagement rules, insufficient legal authority to disable rogue drones, underscored a shared conviction that policy inertia had eroded confidence in the counter-UAS regime. Participants portrayed a defense architecture caught in permanent catch-up, compelling them to question the adequacy of present measures for protecting the Western Interconnection against increasingly sophisticated drone threats.

Theme #6: Detection and Response Remain Immature (RQ #3 / Survey Questions 14-17)

When SMEs reflected on the adequacy of present counter-UAS measures (Q14), they typically judged them only "Slightly" or "Moderately Effective", citing persistent detection blind-spots, slow response protocols, and products that are expensive and ineffective. One participant, SME #4, stated "Swarms of drones attacking all at once are almost impossible to defeat." Another participant, SME #21, stressed a "lack of real-time drone detection in many areas, unclear or slow response procedures", adding that field personnel were still "unsure who has the authority to take down a hostile drone."

These practical shortcomings fueled the sense of urgency captured in Q16, where respondents framed immediate upgrades as indispensable rather than optional, and they populated the detailed gap lists in Q17 with calls for wider sensor coverage, faster decision cycles, and legally vetted engagement rules. The collective narrative portrayed a defense posture in which some technology did exist, but remained fragmented: sensors were not networked, alerting paths were ambiguous, and rehearsed playbooks were scarce. In short, operational readiness and rules of engagement have not kept pace with potential drone threats, leaving SMEs

doubtful that the current system could protect the Western Interconnection if confronted with a coordinated drone attack.

Theme #7: Inter-Agency Coordination Gaps (RQ #3 / Survey Questions 14-17)

When SMEs assessed collaboration among DOE, FERC, and WECC (Q15), almost every rating fell in the lower half of the scale: 11 of 24 respondents (~46%) judged the partnership "Minimally Coordinated" and another 11 (~46%) deemed it merely "Moderately Coordinated". Only two SMEs (~8%) perceived the relationship as "Well Coordinated", and none selected the highest tier. One participant summed up the prevailing sentiment: "I have seen efforts to streamline defensive efforts, but much more cooperation needs to happen", underscoring the view that joint initiatives remained informal and uneven.

These organizational shortfalls aligned with subdued confidence in existing counter-UAS measures (Q14). Fourteen SMEs (~58%) rated current protections "Slightly Effective", eight (~ 33%) labelled them "Moderately Effective", and two (~8%) declared them "Not Effective". No respondent considered the measures "Very" or "Highly Effective". Confronted with this combination of modest effectiveness and fragmented oversight, respondents pressed for rapid improvement. In Q16, 14 SMEs (~58%) classified the need for new safeguards as "Very Urgent" and nine (~38%) as "Extremely Urgent", while only one respondent (~4%) saw the matter as merely "Slightly Urgent".

Open-ended gap lists in Q17 detailed the practical consequences of poor alignment: patchy sensor deployment, inconsistent engagement rules, and unclear lines of authority that left detection blind-spots unaddressed and response protocols sluggish. SMEs argued that no technical fix would succeed until the three entities established a shared doctrine, interoperable procedures, and real-time information exchange. In essence, they portrayed coordination as the

linchpin of any future counter-UAS strategy, without it, even promising technologies would remain under-utilized, and the Western Interconnection would stay exposed.

Summary

The central problem this research addressed was whether the Western Interconnection is adequately prepared to withstand current and near-term threats posed by low-cost, commercially available drones. Guided by Freeman's (1984, 2015) Stakeholder Theory, the findings emphasized that coordinated action among DOE, FERC, and WECC is essential to closing gaps in risk awareness, counter-UAS technologies, and organizational coordination. By linking affordability, infrastructure exposure, and real-world conflict precedent, the research highlighted the professional knowledge and technical capacity grid-security stakeholders must strengthen to safeguard critical assets. The results carry direct implications for policymakers, operators, and technology vendors seeking to craft integrated, forward-leaning defenses.

The research data collection proceeded in two waves. First, 24 SMEs (80% of the targeted sample) completed an anonymous SurveyMonkey.com questionnaire covering perceived asset vulnerability, concern levels, and safeguard adequacy. Second, two respondents participated in structured follow-up interviews, providing deeper insight into the initial responses. Together, these inputs captured a diverse cross-section of perspectives spanning geography, hierarchy, and expertise.

Chapter 5 moves beyond reporting findings to interpret their broader significance through the lens of stakeholder theory and risk-assessment frameworks. It explores the practical implications for regulators, operators, and technology stakeholders, offering policy recommendations grounded in both operational feasibility and regulatory constraints. The

chapter also addresses key research limitations and outlines future directions to strengthen the Western Interconnection's resilience against current and emerging drone threats.

Chapter 5: Implications, Recommendations, and Conclusion

The problem to be addressed by this study is the threat that current and emerging aerial drone technologies pose to the Western Interconnection electrical power grid, as perceived by subject matter experts (SME) from the U.S. Department of Energy (DOE), the Federal Energy Regulatory Commission (FERC), and the Western Electricity Coordinating Council (WECC). The purpose of this descriptive qualitative study was to analyze and identify the severity of risk posed by current and emerging commercial aerial drone technology to America's Western Interconnection Electrical Grid Infrastructure. Guided by Freeman's (1984, 2015) Stakeholder Theory, this research sought to understand how SMEs perceived the severity of these risks, the adequacy of existing counter-UAS measures, and the effectiveness of interagency coordination across the grid's operational footprint. The findings indicated that SMEs viewed potential drone threats as both urgent and inadequately addressed, highlighting systemic shortfalls in detection capabilities, legal authorities, and collaborative response frameworks.

This research study contributed to the broader conversation on critical infrastructure security by focusing on aerial drone threats, an emerging domain that has received limited scholarly and regulatory attention despite growing real-world incidents. While existing literature has often emphasized cyber threats or physical sabotage, this research offered stakeholder-informed insights into aerial vulnerabilities specific to the unique geographic and organizational complexity of the Western Interconnection. By collecting and analyzing expert perspectives from across multiple agencies, the research generated original findings that reflect both operational realities and regulatory challenges.

To support these goals, the researcher employed a qualitative design utilizing a structured, NU IRB-approved survey, distributed to SMEs through a snowball sampling

approach. The target sample size was 30 professionals with direct ties to the Western Interconnection, of whom 24 participated. Two SMEs also engaged in one-on-one interviews to clarify and elaborate on key themes. The purpose of this chapter was to interpret the significance of these findings, offer targeted recommendations for practice, identify limitations of the research, and propose future directions to help strengthen the Western Interconnection's resilience against evolving drone threats.

Implications

With an overarching research objective of clarifying the current landscape of UAS risks to the Western Interconnection electrical grid, this inquiry intentionally engaged a geographically and organizationally diverse group of grid-security SMEs. Twenty-four experts, 80% of the original purposive target of 30, completed an anonymous survey, and two of these participants volunteered for an in-depth follow-up interviews conducted via Zoom or telephone. Collectively, these qualitative efforts captured a range of perspectives from professionals representing multiple control areas, ownership models, and technical specializations across the 1.8-million-square-mile grid.

The findings suggested three interconnected insights for the grid-security community. First, there was overwhelming agreement on the severity of the drone threat, with 23 out of the 24 respondents, rating the risk as "High" or "Critical," and an equal proportion judging counter-UAS improvements to be "Very" or "Extremely" urgent. This pattern points to a growing gap between threat velocity and the pace of policy adaptation. Respondents emphasized the need for accelerated FAA, DOE, and DHS rulemaking to legitimize real-time detection, electronic interdiction, and, where warranted, kinetic defeat capabilities. In the absence of such authority,

utilities remain limited to passive observation, a vulnerability some described as “little to no infrastructure to safeguard the electrical grid from aerial attacks.”

Second, participants identified clear operational and technological priorities. Substations and long-distance transmission corridors received the highest vulnerability ratings, primarily due to physical exposure and insufficient sensor coverage. Respondents recommended prioritizing funding for layered detection systems and hardening of these assets. Many also warned that conventional GPS-jamming solutions are increasingly ineffective against autonomous or swarm-capable drones. These views suggest the need for adaptive defense architectures capable of real-time identification, attribution, and neutralization across diverse drone platforms.

Third, the findings emphasized that even the most advanced technologies are unlikely to succeed without effective organizational coordination. Out of the 24 total participating SMEs, 22 SMEs rated interagency collaboration as only “minimally” or “moderately” coordinated, and none viewed existing partnerships as well integrated. Through the lens of Freeman’s Stakeholder Theory, this fragmentation undermines shared situational awareness and inhibits the diffusion of effective practices. Respondents called for formal doctrine, interoperable data-sharing protocols, and standardized joint-response frameworks across the Western Interconnection

Beyond these practical and policy considerations, the study also contributed to academic discourse by applying Stakeholder Theory to an emerging technological risk domain. By anchoring SME perspectives in this theoretical framework, the research highlighted how competing institutional incentives shape infrastructure vulnerability. Future studies may extend these insights by incorporating quantitative approaches, such as cost–benefit modeling or incident simulation, to further evaluate the effectiveness of proposed counter-UAS strategies.

Research Question #1

What is the perceived risk level among Subject Matter Experts (SMEs) from the DOE, FERC, and WECC, regarding the potential of current and near-future aerial drone technologies to cause damage or destruction to key aspects of the Western Interconnection Electrical Grid infrastructure?

Twenty-four SMEs from the DOE, FERC, and WECC, representing cyber, physical security, operations, and regulatory oversight, shared their insights through an NU IRB-approved qualitative survey. Two participants also took part in follow-up interviews, which confirmed the consistency of survey-based themes but revealed no new perspectives. Together, their responses reflect widespread concern over the vulnerability of grid infrastructure to current and emerging unmanned aircraft systems (UAS).

Substations emerged as the top vulnerability: 17 of the 24 respondents rated them "Highly Vulnerable," another 5 SMEs selected "Very Vulnerable," and only 2 SMEs chose middle-range responses. Transmission lines elicited nearly equal concern, while three-quarters of respondents rated power plants as highly at risk. Two-thirds did the same for control centers, reflecting a shared perception that most grid components lie within operational reach of low-cost, commercially available drones.

When asked to assess the overall drone threat to the grid, none of the SMEs selected "No Risk" or "Low Risk." One rated it "Moderate," while 13 of the 24 respondents selected "High Risk" and 10 out of the 24 respondents marked it as a "Critical Risk." These responses reflected three primary concerns: the affordability and accessibility of off-the-shelf drones, the vast and lightly defended geography of the Western Interconnection, and real-world demonstrations from foreign conflicts showing how low-cost UAS can disrupt energy infrastructure.

Participants described the drone market as overflowing with inexpensive, easily modifiable aircraft that can be purchased in bulk without restriction, SME #6 called it "a low cost solution to a high-value problem." This affordability, combined with the grid's expansive and unevenly defended footprint, was viewed as a critical enabler of vulnerability. Eighteen SMEs referenced events in Ukraine, Iranian one-way drone attacks, or the 2020 attempted strike on a Pennsylvania substation as evidence that small commercial drones already possess the ability to disable vital energy assets. One interviewee, SME #19, summarized this trend by stating, "Ukraine has demonstrated the versatility of drones and the need for robust countermeasures."

The convergence of inexpensive drone technology, broad geographic exposure, and real-world precedents led SMEs to categorize the Western Interconnection as being at high to critical risk. Without rapid advancement in counter-UAS systems capable of addressing swarm coordination, autonomous navigation, and enhanced payload delivery, 10 of the 24 participants SMEs warned that current vulnerabilities could become significantly more difficult and costly to remediate in the near future. These findings directly support the central problem and purpose of the study by illustrating that professionals responsible for safeguarding the Western Interconnection already perceive the threat environment as severe and escalating.

This aligns with literature in Chapter 2, which highlights the accelerating gap between drone capabilities and defensive readiness, and it reinforces the relevance of Freeman's (1984, 2015) Stakeholder Theory (Pietrek, 2022; Yadav et al., 2022). From this theoretical perspective, the persistent vulnerability is not merely a technological gap, but a reflection of fragmented stakeholder coordination and diffuse authority, which undermines proactive and integrated security responses. While the consistency of responses across agencies suggests a credible

expert consensus, these findings should be interpreted in light of certain limitations. The use of self-reported data introduces the possibility of perception bias, and the sample was drawn from a purposive snowball method limited to professionals connected with DOE, FERC, and WECC. Broader inclusion of utility field personnel, law enforcement, or FAA representatives might have yielded more diverse or contrasting views.

The societal implications are significant: while a nationwide blackout from drone swarms remains unlikely, participants viewed localized, high-impact disruptions, such as attacks on substations or transmission corridors, as increasingly probable. Given the essential nature of electricity to public safety, healthcare, and emergency response, even a brief disruption can trigger cascading consequences. These insights underscore the urgency of coordinated, cross-agency counter-UAS investment and policy reform to ensure grid resilience in the face of rapidly advancing aerial threats.

Research Question #2

What is the quantifiable level of concern among SMEs from the DOE, FERC, and WECC regarding current and near-future aerial drone technologies as a potential threat to the Western Interconnection Electrical Grid infrastructure?

Among the 24 SMEs surveyed, concern about drone threats to the Western Interconnection was both widespread and nearly unanimous. When asked directly how concerned they were (Survey Question 10), no participant selected “Not Concerned” or “Slightly Concerned,” and only one out of the 24 participants rated the issue as “Moderately Concerned.” The remainder split between “Very Concerned”, 13 SMEs, and “Extremely Concerned”, 10 SMEs, placing total high-to-extreme concern above 95% (23 out of 24 SMEs) among participants.

Follow-up items clarified the basis for this elevated concern. All respondents flagged unauthorized surveillance as a significant concern. Nearly all, 23 of 24 SMEs, highlighted the ease of weaponizing off-the-shelf drones and their widespread availability, while 15 participants pointed to insufficient regulatory oversight as a major gap. In addition, 13 SMEs emphasized cyber vulnerabilities such as GPS spoofing and data-link hacking. Open-ended responses reinforced these themes, citing advancing drone capabilities, a rise in incidents near critical infrastructure, and persistent defensive shortcomings as converging factors that present a credible and growing risk. As SME 19 warned, "robust countermeasures can't wait."

Concern about drone threats extended beyond individual perspectives and appeared embedded in broader organizational culture. This concern appeared embedded in broader organizational culture. When asked in Survey Question 12 how their colleagues perceive drone risks; none selected "No Concern" or "Minimal Concern." Five SMEs described the prevailing sentiment as "Moderate," 16 SMEs rated it as "Significant," and three SMEs rated it as "Critical," indicating a widely shared sense of institutional urgency. In Survey Question 13, when asked to rank drone threats relative to other hazards, 16 SMEs rated them as a "High" or "Highest" priority, placing them above natural disasters and cyberattacks for many.

Taken together, these responses support the study's central problem and purpose by confirming that the aerial threat environment is perceived as both urgent and under-addressed. These perceptions align with literature cited in Chapter 2, which has begun to highlight drone proliferation as a disruptive force in critical infrastructure protection. They also reinforce Freeman's (1984, 2015) Stakeholder Theory, suggesting that the escalating concern arises not only from technical vulnerabilities, but also from misaligned institutional priorities and fragmented governance across the Western Interconnection.

While the consistency of responses suggests a credible expert consensus, the findings must be viewed in light of several limitations. First, the purposive snowball sample may have elevated risk-sensitive perspectives, particularly among participants specializing in physical and cyber security. Second, the study's regional scope may not reflect drone threat assessments in other grid regions or infrastructure sectors.

As for societal implications, SMEs did not predict a large-scale blackout as an imminent outcome. However, most warned that localized, high-impact incidents, such as surveillance incursions or physical attacks on substations, are increasingly likely. Without near-term reforms in detection, coordination, and policy enforcement, participants anticipate that concern will continue to rise, along with the complexity and cost of securing the grid.

Research Question #3

What is the perceived adequacy of the measures taken by the DOE, FERC, and WECC in safeguarding the Western Interconnection Electrical Grid infrastructure from current and near-future aerial drone technology attacks?

Across all twenty-four SMEs, current counter-UAS measures were widely viewed as insufficient to protect the grid from aerial threats. When asked to assess the effectiveness of existing safeguards (Survey Question 14), two participants rated them "Not Effective," 14 SMEs chose "Slightly Effective," and eight SMEs marked "Moderately Effective." None considered existing protections to be "Very" or "Highly Effective," reinforcing the impression that drone defenses remain underdeveloped.

Explanatory responses emphasized inconsistent detection coverage, untested response protocols, and statutory limitations. As one SME noted, "rules haven't kept up with how fast drone technology is evolving." Another described the situation as "little to no protection from

physical drone attacks," warning that under current conditions, drone swarms would be "almost impossible to defeat."

Perceptions of interagency coordination echoed this limited confidence. Among the 22 respondents who answered Survey Question 15, exactly half (11 SMEs) rated coordination between DOE, FERC, and WECC as "Minimally Coordinated," and the remaining half as "Moderately Coordinated," with no responses in the upper tiers. Participants pointed to fragmented authority, uneven information-sharing, and poorly rehearsed joint procedures. One comment summarized the issue as "much more cooperation needs to happen."

These governance gaps translated into high urgency ratings for improved safeguards. Fourteen SMEs classified the need for new measures as "Very Urgent," and nine of the 24 participants rated it as "Extremely Urgent." Only one SME rated it lower, forming near-unanimous support for immediate reform.

These results speak directly to the purpose and problem statement of the study: whether current protections are adequate against evolving aerial threats. As detailed in Chapter 2, literature on layered defense and drone-specific vulnerabilities has identified many of the same gaps that SMEs observed, including outdated detection systems, legal ambiguity, and organizational silos. These findings also support Freeman's (1984, 2015) Stakeholder Theory, illustrating how fragmented stakeholder alignment and lack of unified leadership result in operational inertia.

While findings were consistent, interpretation should consider sample characteristics. Participants were selected through purposive, security-oriented sampling, which may have led to stronger critiques of existing systems. Further, the study did not include utility line crews, FAA

airspace managers, or private-sector drone vendors who might have provided contrasting perspectives.

From a societal standpoint, SMEs did not foresee immediate, catastrophic grid failure. However, they consistently warned that in the absence of reform, localized drone incursions could damage substations or transmission corridors, causing high-consequence outages. Delayed investments in integrated detection, real-time threat classification, and statutory clarity may increase the likelihood of such incidents. Without coordinated action, what is improbable today may become increasingly likely in the near future.

Recommendations for Practice

Protecting the Western Interconnection from drone incursions, as reflected in stakeholder perspectives captured through this study, will require a deliberately layered and integrated system of countermeasures, an approach supported by existing literature on defense-in-depth and multi-domain security architecture (Nakashima et al., 2020; FAA, 2022). Participants repeatedly cited geography- and coverage-driven gaps: 21 of 24 SMEs flagged long, rural transmission spans as especially vulnerable, and open-ended responses described patchy, non-uniform sensor deployment that creates detection blind-spots and leaves segments effectively unmonitored. Their insights point to the operational need for a sensor mesh that includes passive RF, acoustic arrays, electro-optical systems, and AI-enabled sensor fusion software to generate a continuous, low-latency situational picture, an application of the fusion-based surveillance principles detailed in Chapter 2 (Rigaud et al., 2024). However, the research qualitative data also suggest that detection alone may be insufficient.

Respondents overwhelmingly recommended a standing interagency coordination cell housed within WECC's reliability center and jointly staffed by DOE, FERC, FAA liaisons,

utility control-room personnel, and state energy officials. This aligns with literature on unified command and distributed response frameworks (Freeman et al., 2007), supporting the idea that institutional collaboration and clarified authority pathways improve operational responsiveness. To that end, SMEs emphasized the need for revised statutes and interagency memoranda of understanding that expand authority for non-kinetic defeat tools and delineate operational roles, findings that reflect recurring legal and jurisdictional gaps described in previous policy analyses.

Equally prominent was the concern that current defeat technologies and response playbooks are outdated. Among the 10 SMEs who detailed gaps, several criticized aging and/or ineffective counter-UAS tools and urged modernization. These findings echo trends discussed in Chapter 2 on the limitations of legacy kinetic options and the promise of flexible, software-driven approaches (DHS, 2013; Dawson et al., 2021). To ensure effective integration, respondents proposed piloting such tools at select tier-one substations and control centers to surface false-positive rates, maintenance needs, and operator adaptation, an incremental approach recommended in literature on technology fielding and validation.

Training was another actionable priority: 4 out of the 24 participating SMEs explicitly called for stronger preparedness and response planning, underscoring the need to build shared situational awareness and clarify authority hand-offs. This mirrors calls in the literature for experiential learning and dynamic contingency planning in critical infrastructure sectors. Lastly, participants urged the creation of a joint red-blue threat-intelligence program that integrates global incident trends with internal vulnerability testing, an adaptive feedback loop that supports continuous improvement. Framed within the theoretical lens of organizational learning and resilience engineering (Sutcliffe & Weick, 2007), this recommendation emphasizes the need for responsive defenses that evolve in step with drone autonomy, payload miniaturization, and

swarm coordination. These recommendations interpret the research's perception-based findings in ways that align with relevant theories and operational frameworks, while remaining mindful of the research's limited geographic and organizational scope.

Recommendations for Future Research

Building on the themes uncovered in this study, future scholarship could extend beyond perception-based analysis by incorporating mixed-method or experimental designs that directly address the study's limitations, namely self-reported data, purposive sampling, and single-region focus. Controlled field trials, for instance, could examine how commercially available quadcopters interact with representative grid components, such as substation transformers, high-voltage conductors, or control-room antenna arrays, thereby exploring SME concerns through observable and measurable outcomes. Parallel experiments could assess emerging counter-UAS technologies under terrain and weather conditions typical of the Western Interconnection, focusing on detection latency, false-alarm rates, and system reliability, while integrating cost-benefit analysis not addressed in the present study.

To overcome the narrow time frame reflected in this research, longitudinal case studies could track how DOE, FERC, and WECC implement layered defenses across multiple operating cycles, documenting organizational learning and policy adaptation over time. Comparative policy analyses across other critical infrastructure sectors and international grid operators facing similar drone threats may further broaden the scope of understanding by identifying alternative legal authorities and coordination strategies. Taken together, these efforts represent a logical next step: a phased research program combining field testing and long-term organizational study to build on today's stakeholder-informed insights and support a more comprehensive, evidence-supported framework for drone defense across the Western Interconnection.

Conclusion

This research surveyed twenty-four SMEs from the DOE, FERC, and WECC, and interviewed two of them, to explore how experts perceived the adequacy of existing defenses in protecting the Western Interconnection, a 1.8-million-square-mile grid serving over 80 million customers across fourteen U.S. states, two Canadian provinces, and northern Baja California, from current and emerging UAS threats. A total of 23 out of 24 participants characterized the drone threat as "High" or "Critical" and judged new counter-UAS measures "Very" or "Extremely" urgent; only two participants considered current safeguards even moderately effective, leaving substations and long-distance transmission corridors especially exposed to inexpensive, rapidly evolving drones. These findings connect prior incident reports and scenario analyses with stakeholder perspectives, revealing a widely shared perception that UAS capabilities are outpacing both regulatory frameworks and physical defenses.

Consistent with Freeman's (1984) Stakeholder Theory, a diverse array of 24 SMEs attributed this protection gap less to technical limitations than to fragmented governance, and emphasized the need for interoperable detection systems, shared doctrine, and clear statutory authority to address hostile drones. The findings suggest that safeguarding the Western Interconnection will require an integrated, interagency defense-in-depth strategy. Without coordinated action, continued advances in autonomy, swarm coordination, and payload capacity may further erode grid resilience. Addressing this challenge is vital to both regional reliability and national security, and future research should pair these stakeholder insights with cost-benefit analyses of specific counter-UAS investments.

References

Advanced Air Mobility. (2019, January 6). Aviation Planning. https://aviationplanning.design.blog/advanced-air-mobility/

Ahmed, F., Mohanta, J. C., Keshari, A., & Yadav, P. S. (2022). Recent Advances in Unmanned Aerial Vehicles: A Review. *Arabian Journal for Science and Engineering*, *47*, 7963–7984. https://doi.org/10.1007/s13369-022-06738-0

Akbarzadeh, S., & Naeni, A. (2025). Iranian Drones at the Service of Authoritarian Geopolitics. *Geopolitics*, 1–25. https://doi.org/10.1080/14650045.2025.2468769

Al-Nahhal, M., Ibrahim Al-Nahhal, Dobre, O. A., Kumar, S., Chang, D., & Li, C. (2022). Learned Signal-to-Noise Ratio Estimation in Optical Fiber Communication Links. *IEEE Photonics Journal*, *14*(6), 1–7. https://doi.org/10.1109/jphot.2022.3222264

Alsoliman, A., Rigoni, G., Callegaro, D., Levorato, M., Pinotti, C. M., & Conti, M. (2023). Intrusion Detection Framework for Invasive FPV Drones Using Video Streaming Characteristics. *ACM Transactions on Cyber-Physical Systems*. https://doi.org/10.1145/3579999

Arun, R., Mostefa Bourchak, Alshahrani, H., & Juhany, K. A. (2023). Synthesis and characterization of lightweight unmanned aerial vehicle composite building material for defense application. *Biomass Conversion and Biorefinery*. https://doi.org/10.1007/s13399-023-04736-2

Attacks on Saudi Oil Facilities: Effects and Responses. (2019). In *CRS INSIGHT* . Congressional Research Service. https://crsreports.congress.gov/product/pdf/IN/IN11173

Aven, T. (2011). *Quantitative Risk Assessment* (pp. 2–6). Cambridge University Press. https://ebookcentral.proquest.com/lib/nu/detail.action?docID=674640&query=Quantitative%20Risk%20Assessment#

Bans-Akutey, A., & Tiimub, B. M. (2021). Triangulation in Research. *Academia Letters*, *2*(3392). https://doi.org/10.20935/al3392

Barka, E., Kerrache, C. A., Benkraouda, H., Shuaib, K., Ahmad, F., & Kurugollu, F. (2019). Towards a trusted unmanned aerial system using blockchain for the protection of critical infrastructure. *Transactions on Emerging Telecommunications Technologies*, *33*(8). https://doi.org/10.1002/ett.3706

Barnes, J. (2015). Qualitative research from start to finish (2nd edn.). *Neuropsychological Rehabilitation*, *27*(8), 1156–1158. https://doi.org/10.1080/09602011.2015.1126911

Barua, Z., Barua, S., Aktar, S., Kabir, N., & Li, M. (2020). Effects of misinformation on COVID-19 individual responses and recommendations for resilience of disastrous consequences of misinformation. *Progress in Disaster Science*, *8*, 100–119. https://doi.org/10.1016/j.pdisas.2020.100119

Bertalanffy, L. V. (1968). *General System Theory: Foundations, Development, Applications*. Braziller.

Bertsia, V., & Poulou, M. (2023). Resilience: Theoretical Framework and Implications for School. *International Education Studies*, *16*(2), 1. https://doi.org/10.5539/ies.v16n2p1

Birt, L., Scott, S., Cavers, D., Campbell, C., and Walter, F. (2016). Member checking: A tool to enhance trustworthiness or merely a nod to validation? *Qualitative Health Research*, 26(13), pp. 1802–1811.

Blom, J. D. (2010). *Combat Studies Institute Press US Army Combined Arms Center Unmanned Aerial Systems: A Historical Perspective*. Combat Studies Institute Press. https://usacac.army.mil/sites/default/files/documents/cace/CSI/CSIPubs/OP37.pdf

Boss, P., Doherty, W. J., Larossa, R., Schumm, W. R., & Steinmetz, S. K. (2008). *Sourcebook of family theories and methods a contextual approach* (pp. 325–355). New York, Ny Springer.

Bridoux, F. and Stolehorst, J. (2022). Stakeholder governance: Solving the collective action problems in joint value creation. *The Academy of Management Review, 47*(2), pp. 214–236.

Calandrillo, S., Oh, J., & Webb, A. (2020). Deadly Drones? Why FAA Regulations Miss the Mark on Drone Safety. *Stanford Technology Law Review*, *23*, 182.

Caparini, M., & Gogolewska, A. (2021). Governance Challenges of Transformative Technologies. *Connections: The Quarterly Journal*, *20*(1), 91–100. https://doi.org/10.11610/connections.20.1.06

Carrasco-Casado, A., & Mata-Calvo, R. (2020). *Free-space optical links for space communication networks*. ArXiv.org. https://arxiv.org/abs/2012.13166

Castillo-Montoya, M. (2016). Preparing for interview research: The interview protocol refinement framework. *The Qualitative Report, 21*(5), pp. 811-831.

Chowdhury, N., & Gkioulos, V. (2021). Cyber security training for critical infrastructure protection: A literature review. *Computer Science Review*, *40*, 100361. https://doi.org/10.1016/j.cosrev.2021.100361

Comiskey, J. (2018). How do college homeland security curricula prepare students for the field? *Journal of Homeland Security Education*, 4,20-40.

Cohen-Almagor, R. (2022). Michael Walzer's Just War Theory and the 1982 Israel War in Lebanon. *Israel Studies*, *27*(3), 166–189. https://doi.org/10.2979/israelstudies.27.3.08

Corbin, J. and Strauss, A. (2008). *The Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory* (Third Edition). Los Angeles, CA: Sage Publications, Inc.

Creswell, J. W. (2013). *Research design: Qualitative, quantitative, and mixed methods approaches* (4th ed.). Sage Publications Ltd.

Current Unmanned Aircraft State Law Landscape. (2023, March 27). Www.ncsl.org. https://www.ncsl.org/transportation/current-unmanned-aircraft-state-law-landscape#:~:text=Today%2C%20over%201.1%20million%20recreational

Daniel, B. (2018). Empirical Verification of the 'TACT' Framework for Teaching Rigor in Qualitative Research Methodology. *The Qualitative Research Journal*, 18(3), pp. 262-275.

Dawson, M., Bacius, R., Gouveia, L. B., & Vassilakos, A. (2021). Understanding the Challenge of Cybersecurity in Critical Infrastructure Sectors. *Land Forces Academy Review*, *26*(1), 69–75. https://doi.org/10.2478/raft-2021-0011

Denzin, N. K., Lincoln, Y. S., Giardina, M. D., & Cannella, G. S. (2023). *The SAGE Handbook of Qualitative Research* (6th ed., pp. 121–141). SAGE Publications, Incorporated. https://ebookcentral.proquest.com/lib/nu/detail.action?docID=31337795

Department of Defense. (2015). *Unmanned Aircraft Systems (UAS)*. Defense.gov. https://dod.defense.gov/UAS/

Department of Homeland Security. (2013). *NIPP 2013 Partnering for Critical Infrastructure Security and Resilience*. U.S. Department of Homeland Security.

https://www.cisa.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf

Department of Homeland Security. (2021, July 16). *As Drone Popularity and Potential Risk Soars Science and Technology Preparedness.* Department of Homeland Security; U.S. Department of Homeland Security Science and Technology. https://www.dhs.gov/science-and-technology/news/2021/07/16/feature-article-drone-popularity-and-potential-risk-soars-st-prepares

El-Adle, A. M., Ghoniem, A., & Haouari, M. (2023). The cost of carrier consistency: Last-mile delivery by vehicle and drone for subscription-based orders. *Journal of the Operational Research Society*, *75*(5), 821–840. https://doi.org/10.1080/01605682.2023.2210604

ElMarady, A. A., & Rahouma, K. (2021). Studying Cybersecurity in Civil Aviation, Including Developing and Applying Aviation Cybersecurity Risk Assessment. *IEEE Access*, *9*, 143997–144016. https://doi.org/10.1109/access.2021.3121230

Energy Security. (2024, February 8). Energy.gov; Office of Cybersecurity, Energy Security, and Emergency Response. https://www.energy.gov/ceser/energy-security

FAA. (2020a). *Aeronautical Information Manual - AIM - Controlled Airspace.* Faa.gov. https://www.faa.gov/air_traffic/publications/atpubs/aim_html/chap3_section_2.html

FAA (2020b, April 09). *What Does the FAA Consider as Commercial Drone Use?*. Pilot Institute. https://pilotinstitute.com/commercial-drone-use/

FAA. (2021, November 15). *A brief history of the FAA | Federal Aviation Administration*. Faa.gov. https://www.faa.gov/about/history/brief_history

FAA. (2022a). *Airworthiness Certification Overview.* Faa.gov. https://www.faa.gov/aircraft/air_cert/airworthiness_certification/aw_overview

FAA. (2022b). *Timeline of Drone Integration.* Faa.gov. https://www.faa.gov/uas/resources/timeline

FAA. (2023, December 31). *Drones by the Numbers.* Faa.gov. https://www.faa.gov/node/54496

FAA. (2024). *Unmanned Aircraft Systems (UAS) | Federal Aviation Administration*. Faa.gov. https://www.faa.gov/uas

Faulkner, S. S., & Faulkner, C. A. (2019). *Research methods for social workers: a practice-based approach* (3rd ed.). Oxford University Press.

Federal Energy Regulatory Commission. (2022, August 16). *What FERC Does*. Www.ferc.gov. https://www.ferc.gov/what-ferc-does

Foerstl, K., Kirchoff, J. and Bals, L. (2016). Reshoring and insourcing: Drivers and future research directions. The International Journal of Physical Distribution and Logistics Management, 46(5), pp. 492-515.

Franke, F., Burger, U., & Hühne, C. (2023). A novel reduced order model for drone impacts with aircraft structures. *CEAS Aeronautical Journal*. https://doi.org/10.1007/s13272-023-00646-1

Freeman, R. (2015). *Strategic Management: A Stakeholder Approach*. Cambridge, UK: The Cambridge University Press.

Freeman, R. (1984). *Strategic Management: A Stakeholder Approach*. Boston, MA: Pitman Publishing.

Freeman, R. E., Parmar, B. L., Harrison, J. S., Wicks, A. C., Purnell, L., & de Colle, S. (2010). Stakeholder Theory: The State of the Art. *Academy of Management Annals*, *4*(1), 403–445. https://doi.org/10.5465/19416520.2010.495581

Freeman, R., Martin, K., and Parmar, B. (2007). Stakeholder capitalism. *The Journal of Business Ethics, 74*(1), pp. 303–314.

García-Gascón, C., Castelló-Pedrero, P., & García-Manrique, J. A. (2022). Minimal Surfaces as an Innovative Solution for the Design of an Additive Manufactured Solar-Powered Unmanned Aerial Vehicle (UAV). *Drones*, *6*(10), 285. https://doi.org/10.3390/drones6100285

Giambona, E., Graham, J. R., Harvey, C. R., & Bodnar, G. M. (2018). The Theory and Practice of Corporate Risk Management: Evidence from the Field. *Financial Management*, *47*(4), 783–832. https://doi.org/10.1111/fima.12232

Goel, S. (2020). National Cyber Security Strategy and the Emergence of Strong Digital Borders. *Connections: The Quarterly Journal*, *19*(1), 73–86. https://doi.org/10.11610/connections.19.1.07

Hammersley, M. and Atkinson, P. (1993). *Ethnography: Principles in Practice*. New York City, New York: Routledge Publishing.

Haugstvedt, H. (2023). A Flying Reign of Terror? The Who, Where, When, What, and How of Non-state Actors and Armed Drones. *Journal of Human Security*, *19*, 1–7. https://doi.org/10.12924/johs2023.19010001

Hecken, T., Sunpeth Cumnuantip, & Klimmek, T. (2021). Structural Design of Heavy-Lift Unmanned Cargo Drones in Low Altitudes. *Springer EBooks*, 159–183. https://doi.org/10.1007/978-3-030-83144-8_7

Hennink, M. and Kaiser, B. (2022). Sample sizes for saturation in qualitative research: A systematic review of empirical tests. *Social Sciences & Medicine, 292*(1), pp. 114-152.

Helm, J. M., Swiergosz, A. M., Haeberle, H. S., Karnuta, J. M., Schaffer, J. L., Krebs, V. E., Spitzer, A. I., & Ramkumar, P. N. (2020). Machine Learning and Artificial Intelligence: Definitions, Applications, and Future Directions. *Current Reviews in Musculoskeletal Medicine*, *13*(1), 69–76. https://doi.org/10.1007/s12178-020-09600-8

Holling, C. S. (1973). Resilience and Stability of Ecological Systems. *Annual Review of Ecology and Systematics*, *4*(1), 1–23.

Homeland Security. (2023). *Critical Infrastructure.* U.S. Department of Homeland Security. https://www.dhs.gov/archive/science-and-technology/critical-infrastructure

Hussein, M., Nouacer, R., Corradi, F., Ouhammou, Y., Villar, E., Tieri, C., & Castiñeira, R. (2021). Key technologies for safe and autonomous drones. *Microprocessors and Microsystems*, *87*, 104348. https://doi.org/10.1016/j.micpro.2021.104348

ICAO. (2019). *Convention on International Civil Aviation - Doc 7300*. Icao.int. https://www.icao.int/publications/pages/doc7300.aspx

Ivanović, Z., & Baić, V. (2020). Drones as a Permanent and Present Danger. *Kriminalističke Teme*, *20*(5), 43–56. https://doi.org/10.51235/kt.2020.20.5.43

Jacob, S. A., & S. Paige Furgerson. (2012). Writing Interview Protocols and Conducting Interviews: Tips for Students New to the Field of Qualitative Research. *The Qualitative Report*, *17*(42), 1–10. https://doi.org/10.46743/2160-3715/2012.1718

Jason, L., & Glenwick, D. (2016). *Handbook of Methodological Approaches to Community-Based Research : Qualitative, Quantitative, and Mixed Methods* (pp. 33–41). Oxford University Press.

Jensen, E., & Laurie, C. (2025). *An Introduction to Qualitative Data Analysis - SAGE Research Methods*. Methods.sagepub.com. https://methods.sagepub.com/video/an-introduction-to-qualitative-data-analysis

Jensen, E. and Laurie, C. (2017). *An Introduction to Qualitative Data Analysis*. Washington, DC: Sage Publications, Inc.

Kalinin, M., Krundyshev, V., & Zegzhda, P. (2021). Cybersecurity Risk Assessment in Smart City Infrastructures. *Machines*, *9*(4), 78. https://doi.org/10.3390/machines9040078

Kallenborn, Z., Ackerman, G., & Bleek, P. C. (2022). A Plague of Locusts? A Preliminary Assessment of the Threat of Multi-Drone Terrorism. *Terrorism and Political Violence*, *35*(7), 1556–1585. https://doi.org/10.1080/09546553.2022.2061960

Kindervater, K. H. (2016). The emergence of lethal surveillance: Watching and killing in the history of drone technology. *Security Dialogue*, *47*(3), 223–238. https://doi.org/10.1177/0967010615616011

Krichen, M., Adoni, W. Y. H., Mihoub, A., Alzahrani, M. Y., & Nahhal, T. (2022, May 1). *Security Challenges for Drone Communications: Possible Threats, Attacks and Countermeasures*. IEEE Xplore. https://doi.org/10.1109/SMARTTECH54121.2022.00048

Labib, N. S., Brust, M. R., Danoy, G., & Bouvry, P. (2021). The Rise of Drones in Internet of Things: A Survey on the Evolution, Prospects and Challenges of Unmanned Aerial Vehicles. *IEEE Access*, *9*, 115466–115487. https://doi.org/10.1109/access.2021.3104963

Lachow, I. (2017). The upside and downside of swarming drones. *Bulletin of the Atomic Scientists*, *73*(2), 96–101. https://doi.org/10.1080/00963402.2017.1290879

Lappas, D., Fessakis, G., & Karampelas, P. (2022, June 1). *Recognizing the Threats of Drone Surveillance. A Case Study*. IEEE Xplore. https://doi.org/10.1109/IVMSP54334.2022.9816320

Ledesma, J. (2014). Conceptual Frameworks and Research Models on Resilience in Leadership. *SAGE Open*, *4*(3). https://doi.org/10.1177/2158244014545464

Lee, D., & Shim, D. H. (2018). A Mini-drone Development, Genetic Vector Field-Based Multi-agent Path Planning, and Flight Tests. *International Journal of Aeronautical and Space Sciences*, *19*(3), 785–797. https://doi.org/10.1007/s42405-018-0052-0

Lehto, M., & Hutchinson, B. (2020). Mini-drones swarms and their potential in conflict situations. *Journal of Information Warfare*, *20*(1), 33–49. https://doi.org/10.34190/iccws.20.084

Lincoln, YS. & Guba, EG. (1985). Naturalistic Inquiry. Newbury Park, CA: Sage Publications.

Lowe, A., Norris, A. C., A. Jane Farris, & Babbage, D. (2018, January 22). *Quantifying Thematic Saturation in Qualitative Data Analysis*. ResearchGate; SAGE Publications. https://www.researchgate.net/publication/322659061_Quantifying_Thematic_Saturation_in_Qualitative_Data_Analysis

Mahmood, Y. A., Ahmadi, A., Verma, A. K., Srividya, A., & Kumar, U. (2013). Fuzzy fault tree analysis: a review of concept and application. *International Journal of System Assurance Engineering and Management*, *4*(1), 19–32. https://doi.org/10.1007/s13198-013-0145-x

McBride, J., & Siripurapu, A. (2021, May 14). *How Does the U.S. Power Grid Work?* Council on Foreign Relations. https://www.cfr.org/backgrounder/how-does-us-power-grid-work

Methods & Tactics | National Counterterrorism Center. (2024). Www.dni.gov. https://www.dni.gov/nctc/methods.html#sarin

Mezzofiore, S. M. (2018, December 20). *Police hunt drone pilots in unprecedented Gatwick Airport disruption*. CNN. https://www.cnn.com/2018/12/20/uk/gatwick-airport-drones-gbr-intl/index.html

Mica, J. L. (2012, February 14). *Text - H.R.658 - 112th Congress (2011-2012): FAA Modernization and Reform Act of 2012*. Www.congress.gov. https://www.congress.gov/bill/112th-congress/house-bill/658/text

Miličević, Z. M., & Bojković, Z. B. (2021). From the Early Days of Unmanned Aerial Vehicles (UAVS) to Their Integration into Wireless Networks. Vojnotehnički Glasnik / Military Technical Courier, *69*(4), 941–962. https://doi.org/10.5937/vojtehg69-33571

Mills, K. (2019). *Big Data for Qualitative Research*. New York, NY: Routledge Publishing.

Mittal, V., & Goetz, J. (2025). A quantitative analysis of the effects of drone and counter-drone systems on the Russia-Ukraine battlefield. *Defense & Security Analysis*, 1–14. https://doi.org/10.1080/14751798.2025.2479973

Mohsan, S. A. H., Zahra, Q. ul A., Khan, M. A., Alsharif, M. H., Elhaty, I. A., & Jahid, A. (2022). Role of Drone Technology Helping in Alleviating the COVID-19 Pandemic. *Micromachines*, *13*(10), 1593. https://doi.org/10.3390/mi13101593

Mohsan, S. A. H., Othman, N. Q. H., Li, Y., Alsharif, M. H., & Khan, M. A. (2023). Unmanned Aerial Vehicles (UAVs): Practical aspects, applications, Open challenges, Security issues, and Future Trends. *Intelligent Service Robotics*, *16*(1), 109–137. https://doi.org/10.1007/s11370-022-00452-4

Moschetta, J.-M., & Namuduri, K. (2017). *Introduction to UAV Systems* (J. H. Kim, J. P. G. Sterbenz, K. Namuduri, & S. Chaumette, Eds.). Cambridge University Press; Cambridge University Press. https://www.cambridge.org/core/books/abs/uav-networks-and-

communications/introduction-to-uav-systems/E330889D142C0619D63FBF6DF33488BD

Munawar, H. S., Hammad, A. W. A., & Waller, S. T. (2022). Disaster Region Coverage Using Drones: Maximum Area Coverage and Minimum Resource Utilisation. *Drones*, *6*(4), 96. https://doi.org/10.3390/drones6040096

National Museum of the United States Air Force. (2015, April 7). *Kettering Aerial Torpedo "Bug."* National Museum of the US Air Force™. https://www.nationalmuseum.af.mil/Visit/Museum-Exhibits/Fact-Sheets/Display/Article/198095/kettering-aerial-torpedo-bug/

Newcome, L. R. (2004). *Unmanned Aviation: A Brief History of Unmanned Aerial Vehicles*. American Institute Of Aeronautics And Astronautics.

Noble, H. and Heale, R. (2019). Triangulation in Research, with Examples. *Evidence-Based Nursing*, 22(1), pp. 67-68.

Nouacer, R., Hussein, M., Espinoza, H., Ouhammou, Y., Ladeira, M., & Castiñeira, R. (2020). Towards a framework of key technologies for drones. *Microprocessors and Microsystems*, *77*, 103142. https://doi.org/10.1016/j.micpro.2020.103142

Office of Cybersecurity, Energy Security, and Emergency Response (CESER) | LinkedIn. (2023). Www.linkedin.com. https://www.linkedin.com/company/office-of-cybersecurity-energy-security-and-emergency-response

Office of Energy Infrastructure Security (OEIS). (2024, January 31). Www.ferc.gov. https://www.ferc.gov/office-energy-infrastructure-security-oeis

OLRC Home. (2018, October 5). Uscode.house.gov; Office of the Law RevisionCounsel United States Code.

https://uscode.house.gov/browse/prelim@title49/subtitle7/partA/subpart3&edition=prelim

Onag, G. (2020, October 2). *ABI Research: Drone market worth US$92 billion by 2030*. FutureIoT. https://futureiot.tech/abi-research-drone-market-worth-us92-billion-by-2030/

Onohwakpor, J., Atamu, M., & Oniovoghai. (2020). The Use of Drone Technology as an Effective Tool in Providing Information Services in Nigeria. In *ProQuest* (pp. 1–10). Library Philosophy and Practice. https://go.openathens.net/redirector/nu.edu?url=https://www.proquest.com/scholarly-journals/use-drone-technology-as-effective-tool-providing/docview/2646986529/se-2

Parker, C., Scott, S., & Geddes, A. (2019). *Snowball Sampling*. Methods.sagepub.com. http://methods.sagepub.com/foundations/snowball-sampling

Planning Considerations: Complex Coordinated Terrorist Attacks. (2018). In *fema.gov*. https://www.fema.gov/sites/default/files/2020-07/planning-considerations-complex-coordinated-terrorist-attacks.pdf

Pietrek, G. (2022). Threats to critical infrastructure. The case of unmanned aerial vehicles. *Journal of Modern Science*, *49*(2), 120–133. https://doi.org/10.13166/jms/155797

Public Law 112-95. (2012). FAA Modernization and Reform Act of 2012. United States Government Publishing Office. https://www.govinfo.gov/content/pkg/PLAW-112publ95/html/PLAW-112publ95.htm

Raab, J. and Kenis, P. (2009). Heading toward a society of networks: Empirical developments and theoretical challenges. *The Journal of Management Inquiry, 18*(1), pp. 198–210.

Rea, A., Marshall, K., & Farrell, D. (2021). Capability of web-based survey software: an empirical review. *American Journal of Business*, *37*(1), 1–13. https://doi.org/10.1108/ajb-07-2019-0058

Reichhardt, T. (2009, October 6). *Alfred Nobel's rocket camera*. Smithsonian Magazine; Smithsonian Magazine. https://www.smithsonianmag.com/air-space-magazine/alfred-nobels-rocket-camera-117825125/

Richards, M. and Schwartz, L. (2002). health services research? Ethics of qualitative research: Are there special issues for *The Journal of Family Practice, 19*(2), pp. 135-139.

Rigaud, M., Buekers, J., Bessems, J., Basagaña, X., Mathy, S., Nieuwenhuijsen, M., & Slama, R. (2024). The methodology of quantitative risk assessment studies. *Environmental Health : A Global Access Science Source*, *23*(1), 13. https://doi.org/10.1186/s12940-023-01039-x

Ripley, W. (2015, April 22). *Drone with radioactive material found on Japanese Prime Minister's roof*. CNN. https://www.cnn.com/2015/04/22/asia/japan-prime-minister-rooftop-drone/index.html

Rogers, J., & Kunertova, D. (2022). *The Vulnerabilities of the Drone Age: Established Threats and Emerging Issues out to 2035*. University of Southern Denmark. https://portal.findresearcher.sdu.dk/en/publications/the-vulnerabilities-of-the-drone-age-established-threats-and-emer

Rogoway, T., & Trevithich, J. (2020, July 29). *The Night A Mysterious Drone Swarm Descended On Palo Verde Nuclear Power Plant The mysterious case ofmass drone incursions over America's most powerful nuclear power plant that only resulted in more questions and no changes.* Nrc.gov; Nuclear Regulatory Commission. https://www.nrc.gov/docs/ML2033/ML20332A109.pdf

Salkind, N. (2012). *Exploring Research (8th Edition*). New York, NY: Pearson Publishing.

Sands, G. (2022, September 30). *FBI warns drones pose potential risk to critical infrastructure after some spotted over Louisiana chemical facilities | CNN Politics*. CNN. https://www.cnn.com/2022/09/30/politics/drones-risk-critical-infrastructure-spotted-louisiana-chemical-facilities/index.html

Schulzke, M. (2018). Drone Proliferation and the Challenge of Regulating Dual-Use Technologies. *International Studies Review*, 497–517. https://doi.org/10.1093/isr/viy047

Scott, C., & Medaugh, M. (2017). Axial Coding. *The International Encyclopedia of Communication Research Methods*, 1–2. https://doi.org/10.1002/9781118901731.iecrm0012

Secretary of Defense. (2018, August 18). *Guidance for the Domestic Use of Unmanned Aircraft Systems in U.S. National Airspace*. Media.Defense.Gov; 1000 Defense Pentagon Washington, DC 20301-1000. https://media.defense.gov/2018/Nov/05/2002059511/-1/-1/1/Guideance-For-the-Domestic-Use-of-Unmanned-Aircraft-Systems-in-US-National-Airspace.PDF

Shaikhanov, Z., Badran, S., Jornet, J. M., Mittleman, D. M., & Knightly, E. W. (2023). Remotely Positioned MetaSurface-Drone Attack. *Proceedings of the 24th International Workshop on Mobile Computing Systems and Applications*, 110–116. https://doi.org/10.1145/3572864.3580343

Sims, A. (2018). The Rising Drone Threat from Terrorists. *Georgetown Journal of International Affairs*, *19*(1), 97–107. https://doi.org/10.1353/gia.2018.0012

Skydio Inc. (2024). Www.skydio.com. https://www.skydio.com

Sukamto, B., Raihan, R., & Untoro, U. (2023, December 31). *Legal Transformation in the Digital Era: Regulatory Adaptation and Innovation*. Www.atlantis-Press.com; Atlantis Press. https://doi.org/10.2991/978-2-38476-180-7_32

Support for Matrice 600 Pro. (2024). DJI. https://www.dji.com/support/product/matrice600-pro

Tech Talk: Identify Drone Autonomy - Drone Industry Insights. (2019, March 7). https://droneii.com/drone-autonomy

Technology Risk Assessment. (2024, January 30). It.cornell.edu. Retrieved February 2, 2024, from https://it.cornell.edu/it-risk-consultation/technology-risk-assessment#:~:text=Technology%20Risk%20Assessments%20(TRAs)%20help

Unger, S., Heinrich, M., Scheuermann, D., Katzenbeisser, S., Schubert, M., Hagemann, L., & Iffländer, L. (2023). Securing the Future Railway System: Technology Forecast, Security Measures, and Research Demands. *Vehicles*, *5*(4), 1254–1274. https://doi.org/10.3390/vehicles5040069

U.S. Air Force. (2014, October 27). *RQ-4 Global Hawk*. U.S. Air Force. https://www.af.mil/About-Us/Fact-Sheets/Display/Article/104516/rq-4-global-hawk/

U.S. Air Force. (2015, September 23). *MQ-9 Reaper*. U.S. Air Force; U.S. Air Force. https://www.af.mil/About-Us/Fact-Sheets/Display/Article/104470/mq-9-reaper/

U.S. Department of Defense. (2022). *Our Forces*. https://www.defense.gov/About/Our-Forces/

U.S. Department of Energy. (2023). *About Us*. Energy.gov. https://www.energy.gov/about-us

U.S. Department of State. (2019). *Foreign Terrorist Organizations*. United States Department of State; Bureau of Counterterrorism. https://www.state.gov/foreign-terrorist-organizations/

U.S. EPA. (2019, June 13). *About the U.S. Electricity System and its Impact on the Environment | US EPA*. US EPA. https://www.epa.gov/energy/about-us-electricity-system-and-its-impact-environment

Western Electricity Coordinating Council. (2024). *Overview, News & Similar companies.* ZoomInfo. https://www.zoominfo.com/c/western-electricity-coordinating-council/41927559

Western Interconnection. (2023, October). Www.wecc.org. https://www.wecc.org/epubs/StateOfTheInterconnection/Pages/Western-Interconnection.aspx

Yadav, G., Kanika Singh Rajpoot, & Bazil, A. (2022). Synthetic Aperture Radar(SAR) Image of Small Unmanned Aerial Vehicle (sUAV). *2022 International Conference on Augmented Intelligence and Sustainable Systems (ICAISS)*. https://doi.org/10.1109/icaiss55157.2022.10011085

Yin, R. (2013). *Qualitative Research from Start to Finish*. New York, NY: The Guilford Press.

Xiao, C., Wang, B., Zhao, D., & Wang, C. (2023). Comprehensive investigation on Lithium batteries for electric and hybrid-electric unmanned aerial vehicle applications. *Thermal Science and Engineering Progress*, *38*, 101677. https://doi.org/10.1016/j.tsep.2023.101677

Zikmund, W., Babin, B. J., Griffin, M., & Griffin, M. (2013). Business research methods. South-Western.

Zimmerman, K. (2023). Managing the Terrorism Threat with Drones, 13. *Journal of National Security Law and Policy*, *13*(2), 319–336. https://www.mybib.com/#/projects/wPYdZp/citations/new/article_journal

Zwickle, A., Farber, H. B., & Hamm, J. A. (2018). Comparing public concern and support for drone regulation to the current legal framework. *Behavioral Sciences & the Law*, *37*(1), 109–124. https://doi.org/10.1002/bsl.2357

Appendix A

Search Terms, Combinations, and Categories

Basic Search Terms and Combinations

1. Drones
2. Unmanned Aerial Vehicles (UAV)
3. Electrical grid infrastructure
4. Commercial drones
5. Drone technology risks
6. Aerial drones and electrical grids
7. UAV applications in electrical grids
8. Commercial drone regulations
9. Drone surveillance risks
10. UAV impact on infrastructure security
11. Drone technology advancements
12. Commercial drones and electrical grid vulnerability
13. UAV and infrastructure security and risk assessment
14. Drone technology and regulatory challenges
15. Unmanned Aerial Vehicles and critical infrastructure protection
16. Drone surveillance and electrical grid stability

Stakeholder Perspectives

1. SME perceptions on UAV risks
2. Regulatory responses to UAV threats
3. Stakeholder theory in drone regulation
4. Impact of drones on utility companies
5. Public safety concerns with UAVs

Technological and Regulatory Aspects

1. Technological risks of UAVs
2. Cybersecurity threats posed by drones
3. UAV regulation by FAA
4. Anti-drone technology and infrastructure
5. UAV policy frameworks

Drone Technologies

1. Unmanned Aerial Vehicles (UAVs)
2. Autonomous drones

3. Recreational drones
4. Commercial drones
5. Drone surveillance
6. Drone payload capacity
7. Drone range and endurance
8. Drone autonomy levels

Drone-Specific Risks

1. Drone risk scenarios
2. Drone threats
3. Drone misuse
4. Drone security breaches
5. Drone impact on critical infrastructure
6. Drone-induced vulnerabilities

Types of Drones

1. Fixed-wing UAVs
2. Rotary-wing UAVs
3. Hybrid UAVs
4. Micro UAVs
5. Nano UAVs

Drone Capabilities

1. Drone surveillance
2. Drone payload capacity
3. Drone range and endurance
4. Drone autonomy levels
5. Drone obstacle avoidance
6. Drone navigation systems
7. Drone real-time data processing
8. Drone AI and machine learning
9. Drone remote sensing

Drone Applications

1. Drones in infrastructure inspection
2. Drones in surveillance
3. Drones in agriculture
4. Drones in environmental monitoring
5. Drones in disaster response
6. Drones in public safety

Communication and Control

1. Drone communication links
2. RF links for drones
3. Satellite communication for drones
4. Cellular networks and drones
5. Optical communication for drones
6. Drone remote control systems

Drone Types, Capabilities, and Applications

1. Drone payload capacity
2. Drone range and endurance
3. Drone obstacle avoidance
4. Real-time data processing
5. AI-driven drone applications
6. Drone GPS and navigation
7. Drone imaging and camera technology
8. Drone battery technology
9. Drone propulsion systems
10. Fixed-wing UAVs and payload capacity
11. Rotary-wing UAVs and autonomy levels
12. Hybrid UAVs and range and endurance
13. Micro UAVs and obstacle avoidance
14. Nano UAVs and navigation systems
15. Fixed-wing UAVs and infrastructure inspection
16. Rotary-wing UAVs and environmental monitoring
17. Hybrid UAVs and disaster response
18. Micro UAVs and indoor surveillance
19. Nano UAVs and public safety
20. Drone surveillance and critical infrastructure
21. Drone payload capacity and agriculture
22. Drone range and endurance and disaster response
23. Drone autonomy levels and public safety
24. Drone obstacle avoidance and environmental monitoring

Communication and Control

1. RF links and drones
2. Satellite communication and UAVs
3. Cellular networks and drone control
4. Optical communication and drones
5. Remote control systems and UAVs

Infrastructure Targets

1. Western Interconnection Electrical Grid
2. Electrical grid infrastructure
3. Power plants

4. Substations
5. Transmission lines
6. Distribution networks
7. Energy infrastructure

Vulnerabilities

1. Infrastructure vulnerabilities
2. Physical vulnerabilities of electrical grids
3. Cybersecurity vulnerabilities in power grids
4. Drone-induced vulnerabilities
5. Infrastructure security gaps

Security and Protection

1. Critical infrastructure protection
2. Physical security of electrical grids
3. Cybersecurity measures for power grids
4. Anti-drone technologies
5. Emergency response protocols
6. Infrastructure resilience
7. Impact of drones on electrical grids
8. Drone threats to critical infrastructure
9. Risk assessment for electrical grid security
10. Drone interference with power systems
11. Drone attack scenarios on infrastructure

Infrastructure and Vulnerabilities

1. Western Interconnection Electrical Grid and infrastructure vulnerabilities
2. Power plants and drone-induced vulnerabilities
3. Substations and cybersecurity vulnerabilities
4. Transmission lines and physical vulnerabilities
5. Distribution networks and infrastructure security gaps
6. Western Interconnection Electrical Grid and critical infrastructure protection
7. Electrical grid infrastructure and anti-drone technologies

8. Power plants and cybersecurity measures
9. Substations and physical security
10. Transmission lines and emergency response protocols
11. Impact of drones on electrical grids and physical security
12. Drone threats to critical infrastructure and cybersecurity measures
13. Risk assessment for electrical grid security and anti-drone technologies
14. Drone interference with power systems and infrastructure resilience
15. Drone attack scenarios on infrastructure and emergency response protocols

Security Measures and Impacts

1. Critical infrastructure protection and impact of drones on electrical grids
2. Physical security of electrical grids and drone interference
3. Cybersecurity measures for power grids and drone threats
4. Anti-drone technologies and impact on electrical grid security
5. Emergency response protocols and drone attack scenarios

Regulatory Bodies and Policies

1. FAA regulations on drones
2. DOE policies on UAVs
3. FERC regulations
4. WECC policies
5. National security policies on UAVs
6. Drone laws and regulations
7. International drone regulations
8. Government policies on critical infrastructure protection

Privacy and Safety Concerns

1. Privacy concerns with drone technology
2. Public safety and UAV operation
3. Data protection and drones
4. Surveillance laws and drones

5. Safety regulations for drone operations

Security Measures and Protocols

1. Anti-drone technologies
2. Drone detection systems
3. Counter-drone measures
4. Emergency response protocols
5. Infrastructure security policies

Impact and Compliance

1. Impact of regulations on drone usage
2. Compliance with drone regulations
3. Legal challenges of drone technology
4. Regulatory adaptation to technological advancements
5. Government oversight of drone operations

Privacy, Safety, and Drone Operations

1. Privacy concerns and UAV operation
2. Public safety and drone regulations
3. Data protection and drone technology
4. Surveillance laws and drone usage
5. Safety regulations and UAV operations
6. Anti-drone technologies and regulatory policies
7. Drone detection systems and public safety
8. Counter-drone measures and infrastructure protection
9. Emergency response protocols and drone incidents
10. Infrastructure security policies and UAV threats

Impact of Regulations and Legal Compliance

1. Impact of regulations on drone technology and critical infrastructure
2. Compliance with drone regulations and energy sector
3. Legal challenges and UAV operations
4. Regulatory adaptation and technological advancements

5. Government oversight and drone operations

Drone Technology Innovations

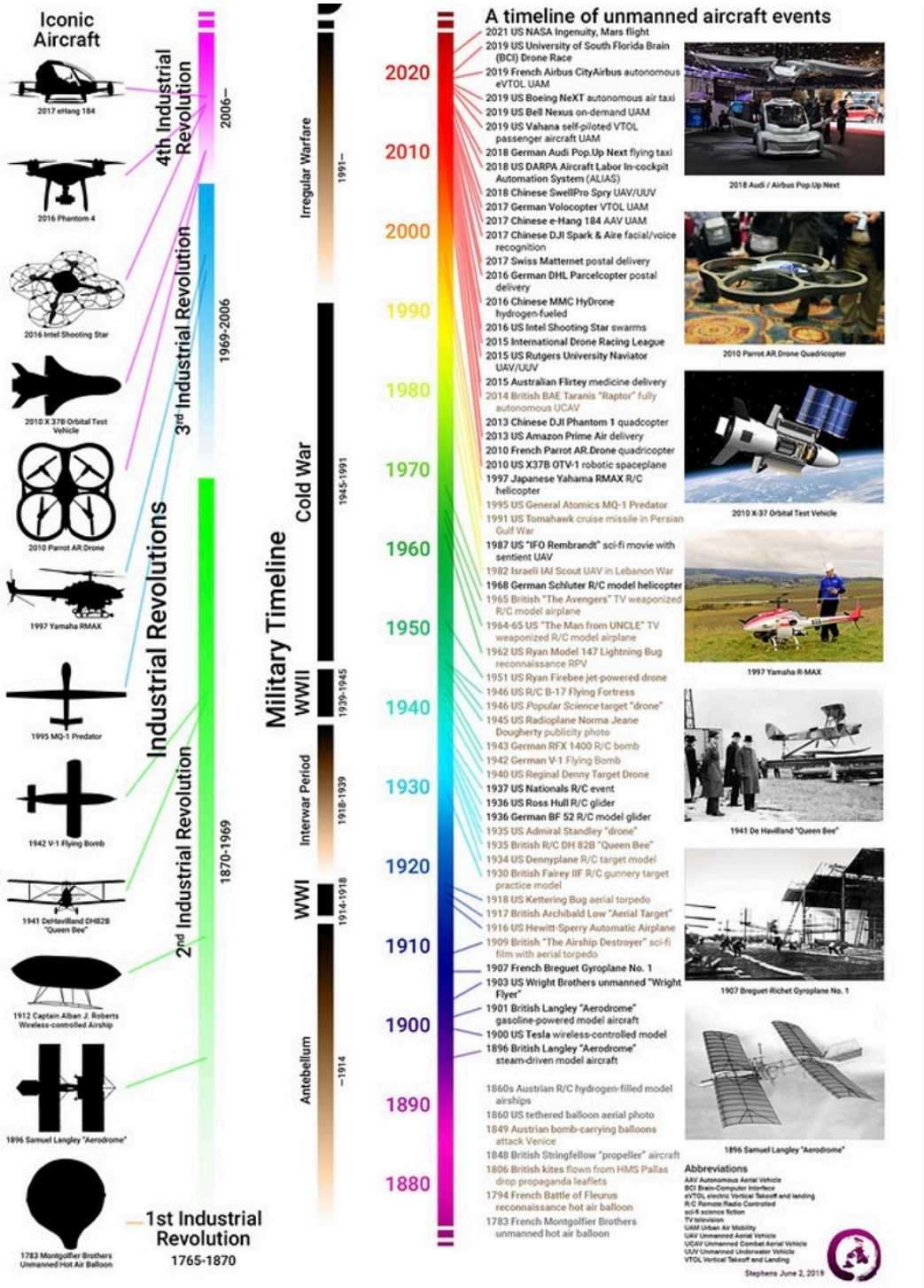
1. Innovations in drone technology
2. Advanced UAV systems
3. Next-generation drones
4. Cutting-edge drone technologies
5. Drone engineering advancements
6. Drone AI and machine learning
7. Drone navigation systems
8. Autonomous drone technology
9. Drone communication systems
10. Drone sensor technology

Applications of Advanced Technologies

1. Drones in infrastructure inspection
2. Drones in agriculture
3. Drones in environmental monitoring
4. Drones in disaster response
5. Drones in public safety
6. Drones in logistics and delivery
7. Drones in surveillance
8. Drones in construction

Appendix B

History of Drone Technology Development



Appendix B. First published by Aviation Planning, *Advanced Air Mobility,* on January 6th, 2019.

Appendix C

Study Letter Outlining Research Instrumentation and Eligibility Criteria

Recruitment Email

My name is Justin Werner. I am a doctoral candidate at National University. I'm conducting a qualitative research study to examine the risks posed by current and emerging drone technologies to the Western Interconnection electrical grid. This study also evaluates the adequacy of existing protective measures based on the insights of Subject Matter Experts (SMEs) from the U.S. Department of Energy (DOE), the Federal Energy Regulatory Commission (FERC), and the Western Electricity Coordinating Council (WECC).

I am recruiting professionals who are currently working with or advising on issues related to the Western Interconnection electrical grid, particularly in areas such as Electrical Engineering, Grid Security, Aerospace and Drone Technology, Cybersecurity, Counterterrorism, or related regulatory and policy fields.

If you decide to participate in this study, you will be asked to complete the following activities:

1. Participate in an anonymous online survey via SurveyMonkey.com.
2. Optional: Volunteer for a follow-up one-on-one virtual interview. At the end of the survey, participants will have the opportunity to sign up for a virtual phone or Zoom interview by providing a name (real or pseudonym) and contact information (email and/or phone number).

During the survey and optional interview, you will be asked questions related to:

- Demographics (e.g., years of professional/academic experience in relevant fields).
- Perceptions of the risks drone technologies pose to the Western Interconnection electrical grid.
- Views on the adequacy of current protective measures and suggestions for improvement.

Thank you for considering participation in this voluntary research study. Your insights are invaluable to this research.

Appendix D

Online Anonymous Survey Consent

Hello,

My name is Justin Werner. I am a doctoral candidate at National University. I'm conducting a qualitative research study examining the risks posed by current and emerging drone technologies to the Western Interconnection electrical grid. This study also evaluates the adequacy of existing protective measures based on the insights of Subject Matter Experts (SMEs) from the U.S. Department of Energy (DOE), the Federal Energy Regulatory Commission (FERC), and the Western Electricity Coordinating Council (WECC).

Eligibility Criteria:

To participate, you must be:

- A professional currently working with or advising on issues related to the Western Interconnection electrical grid, particularly in areas such as Electrical Engineering, Grid Security, Aerospace and Drone Technology, Cybersecurity, Counterterrorism, or related regulatory and policy fields.

The survey will ask for:

1. Basic demographic information (e.g., years of professional experience in relevant fields).
2. Perspectives on the risks of drone technology to the Western Interconnection electrical grid.

3. Opinions on the effectiveness of current measures and recommendations for mitigating identified risks.

The survey will take approximately 15-20 minutes to complete.

Participation is voluntary, and all responses will remain anonymous. No identifying information will be collected or linked to your responses.

Additionally, if you have any questions regarding your rights as a human subject and participant in this study, or to report research-related problems, you may email the National University IRB.

*By clicking "**Next**" and completing the survey, you indicate your informed consent to participate in this research. If you do not wish to participate, please close this browser window.*

Appendix E

Consent Letter for Adult One-on-One Interview Zoom Participants

My name is Justin Werner. I'm a doctoral candidate at National University, conducting research for my dissertation titled "*Emerging Drone Risks and Protective Measures: A Study on the Western Interconnection Electrical Grid.*" This study aims to assess the risks posed by current and emerging drone technologies to the Western Interconnection electrical grid and evaluate the adequacy of existing protective measures based on the insights of subject matter experts (SMEs) from the U.S. Department of Energy (DOE), the Federal Energy Regulatory Commission (FERC), and the Western Electricity Coordinating Council (WECC).

This form will give you information about the research to help you decide whether you would like to participate and/or your data to be used. Please read this form and ask any questions you have.

What will happen during the research?

If you agree to participate, you will:

1. Part I: Complete an anonymous online survey hosted on SurveyMonkey.com. The survey will ask open-ended questions designed to gather your expert perspectives on drone-related risks and protective measures for critical infrastructure.
2. Part II: Upon completing the survey, you will have the opportunity to volunteer for a one-on-one confidential interview by providing your preferred contact information (real name or pseudonym, email, and/or phone number). If selected, I will contact you to schedule the interview.

The one-on-one interviews will last approximately 30 minutes and will be conducted virtually (via phone, Zoom, or similar platforms). These interviews will build upon your survey responses and allow for more in-depth discussion of key topics.

Why is this research being done?

The purpose of this study is to identify perceived risks associated with drone technologies and assess the adequacy of protective measures for the Western Interconnection electrical grid. Insights from this research may inform strategies to enhance infrastructure resilience and security.

Who can participate?

You are invited to participate because of your expertise and experience relevant to drone technologies or critical infrastructure protection. I aim to include approximately 30 participants in this study.

To help ensure a diverse and comprehensive range of insights, you are encouraged to share this survey with other SMEs who may be qualified and interested in contributing to this research. Participants should have expertise in areas such as electrical grid security, drone technologies, regulatory frameworks, or critical infrastructure protection. Please recommend or forward the survey link to those in your professional network who meet these criteria.

What are the potential risks of participating?

- There are no anticipated risks or discomforts associated with participation.
- Participation is voluntary, and you may skip any question or withdraw from the study at any time without penalty.

What are the potential benefits of participating?

- Contributing to a better understanding of risks posed by drone technologies.
- Helping to identify protective measures to safeguard critical infrastructure, potentially influencing future policies and strategies.

How will your information be protected?

- Your participation will remain confidential, and your identity will not be disclosed in any publications or presentations.
- Pseudonyms will be used to ensure anonymity.
- All electronic data will be encrypted and password-protected, while physical materials (if any) will be securely stored.
- After three years, all collected data will be securely destroyed, excluding what is published in the dissertation.

Voluntary Participation

Your participation is entirely voluntary. You may withdraw at any time without penalty or decline to answer specific questions. If you wish to withdraw after providing data, you may contact me to request the removal of your information.

Who should I call with questions or problems?

For questions about the research, contact the researcher via the university email on file. For questions about your rights as a research participant, to discuss problems, complaints, or concerns about research, or to obtain information or to offer input, please contact the NU Institutional Review Board.

Can I withdraw from the research?

If you decide for your data to be included in this research, you can change your mind and decide to remove your data from the research at any time in the future. Please let me know that you no longer wish for your data to be included, and I will delete all data collected from you.

Opting out of this research

If you would like to "opt out" your data from this research, please contact the researcher via the university email on file.

Appendix F

Survey/Interview Questions Specific to Each Research Question

Participants Demographics

Survey Questions:

1. What is your Gender?
    - Male
    - Female
    - Prefer not to say
    - Other (specify)
2. What is your approximate age?
    - 18 – 30 Years of Age
    - 31 – 40 Years of Age
    - 41 – 50 Years of Age
    - 51 – 60 Years of Age
    - 61 – 70 Years of Age
    - 71+ Years of Age
    - Prefer not to say
3. What is the highest level of education you have completed?
    - Graduated from high school
    - Associate degree
    - Bachelor's degree
    - Master's degree
    - Doctorate degree (or other terminal post-graduate degree)

- Prefer not to say

4. How many total years of relevant professional experience do you currently posses?
    - 0 – 5 Years of Experience
    - 6 – 10 Years of Experience
    - 11 – 15 Years of Experience
    - 16 – 20 Years of Experience
    - 21 – 25 Years of Experience
    - 26 – 30 Years of Experience
    - 31+ Years of Experience
5. What is your racial or ethnic identity? (Select all that apply)
    - African American / Black
    - American Indian / Alaskan Native
    - Asian
    - Caucasian / White
    - Hispanic
    - Middle eastern
    - Native Hawaiian / Pacific Islander
    - Prefer not to say
    - Other (please specify)

Research Question 1 (RQ1):

What is the perceived risk level among SMEs from the DOE, FERC, and WECC, regarding the potential of current and near-future aerial drone technologies to cause

damage or destruction to key aspects of the Western Interconnection Electrical Grid infrastructure?

Survey Questions:

6. On a scale of 1 (Not Vulnerable) to 5 (Highly Vulnerable), how vulnerable do you perceive the following aspects of the Western Interconnection Electrical Grid to potential drone threats? *(Please explain your rating. What factors influenced your assessment?)*
    - Power plants
    - Transmission lines
    - Substations
    - Control centers
    - Other (please specify)
7. How would you rate the severity of the risks posed by current aerial drone technologies to grid infrastructure? *(Please explain your rating. What factors influenced your assessment?)*
    - 1 – No Risk (Drones pose no threat to grid infrastructure)
    - 2 – Low Risk (Drones present minimal potential for disruption)
    - 3 – Moderate Risk (Drones could pose occasional threats, but existing protections are largely sufficient)
    - 4 – High Risk (Drones pose a frequent or growing threat that requires additional security measures)
    - 5 – Critical Risk (Drones present an immediate and severe threat to grid security)
8. To what extent do you agree with the following statement: "Emerging trends in drone technology will significantly increase risks to the Western Interconnection Electrical Grid

in the next 5 years." *(Please explain your rating. What factors influenced your assessment?)*

- 1 – Strongly Disagree (No foreseeable increase in drone-related risks)
- 2 – Disagree (Minor increases in risk, but manageable with current measures)
- 3 – Neutral (Some risk increase expected, but impact remains uncertain)
- 4 – Agree (Significant risk increase anticipated, requiring enhanced countermeasures)
- 5 – Strongly Agree (Drones will become a major and urgent threat to grid security)

9. Can you describe specific scenarios where drones have already demonstrated risk to infrastructure within or beyond the grid system? *(Open-ended)*

Research Question 2 (RQ2):

What is the quantifiable level of concern among SMEs from the DOE, FERC, and WECC regarding current and near-future aerial drone technologies as a potential threat to the Western Interconnection Electrical Grid infrastructure?

Survey Questions:

10. How concerned are you about drone threats to the Western Interconnection Electrical Grid? *(Please explain your rating. What factors influenced your assessment?)*

- 1 – Not Concerned (Drones pose no significant threat)
- 2 – Slightly Concerned (Minimal threat, unlikely to cause major disruptions)
- 3 – Moderately Concerned (Some risk, but current protections are somewhat sufficient)
- 4 – Very Concerned (Significant risk, requiring increased security measures)

- 5 – Extremely Concerned (Critical threat, posing an urgent need for mitigation)

11. Which of the following factors contribute most to your level of concern about the potential misuse of drone technologies in critical infrastructure areas? *(Select all that apply)*
    - Potential for physical attacks on infrastructure
    - Unauthorized surveillance and intelligence gathering
    - Cybersecurity vulnerabilities (e.g., hacking, GPS spoofing)
    - Lack of regulatory oversight or enforcement
    - Increasing accessibility and affordability of drone technology
    - Other (please specify)
12. How do you perceive the overall level of concern among your colleagues or within your agency regarding drone threats? *(Please explain your rating. What factors influenced your assessment?)*
    - 1 – No Concern (Drones are not considered a risk)
    - 2 – Minimal Concern (Few acknowledge it as a potential issue)
    - 3 – Moderate Concern (Some discussions, but not a priority)
    - 4 – Significant Concern (Regular discussions and security measures in place)
    - 5 – Critical Concern (High-priority threat with active mitigation efforts)
13. How would you prioritize drone threats in comparison to other emerging threats to grid security (e.g., cyberattacks, natural disasters)? *(Please explain your rating. What factors influenced your assessment?)*
    - 1 – Lowest Priority (Drone threats are negligible compared to other risks)
    - 2 – Low Priority (Drones are a minor concern but not a primary threat)

- 3 – Moderate Priority (Drones pose a comparable risk to other threats)
- 4 – High Priority (Drones are a significant concern, close to top threats)
- 5 – Highest Priority (Drone threats surpass or equal the most critical risks)

Research Question 3 (RQ3):

What is the perceived adequacy of the measures taken by the DOE, FERC, and WECC in safeguarding the Western Interconnection Electrical Grid infrastructure from current and near-future aerial drone technology attacks?

Survey Questions:

14. How effective do you find the current protective measures in place to counter drone threats to the grid?
    - 1 – Not Effective (Current measures offer little to no protection)
    - 2 – Slightly Effective (Some deterrence, but major vulnerabilities remain)
    - 3 – Moderately Effective (Adequate protections exist, but improvements are needed)
    - 4 – Very Effective (Strong protections in place, but some refinements required)
    - 5 – Highly Effective (Current measures are comprehensive and sufficient)
15. How well-coordinated are efforts between the DOE, FERC, and WECC in addressing the drone threat? *(Please explain your rating. What factors influenced your assessment?)*
    - 1 – Not Coordinated (No alignment or collaboration between agencies)
    - 2 – Minimally Coordinated (Some interaction, but lacks structured efforts)
    - 3 – Moderately Coordinated (Collaboration exists but needs improvement)
    - 4 – Well-Coordinated (Agencies work together effectively with some gaps)
    - 5 – Highly Coordinated (Seamless and proactive coordination across agencies)

16. How urgent do you believe it is to implement new or enhanced measures to improve grid security against drone-related risks? *(Please explain your rating. What factors influenced your assessment?)*
    - 1 – Not Urgent (No immediate need for changes)
    - 2 – Slightly Urgent (Enhancements would be beneficial but not a priority)
    - 3 – Moderately Urgent (Some risks require attention, but current measures are fairly sufficient)
    - 4 – Very Urgent (Significant risks demand improved measures soon)
    - 5 – Extremely Urgent (Immediate action is needed to address critical risks)
17. What specific gaps or shortcomings do you see in existing protocols or technologies aimed at mitigating drone threats? *(Open-ended)*