A Phenomenological Study Examining the Vulnerability of U.S. Nuclear Power Plants to Attack by Unmanned Aerial Systems

Dissertation Manuscript

Submitted to Northcentral University

School of Business

in Partial Fulfillment of the

Requirements for the Degree of

DOCTOR OF BUSINESS ADMINISTRATION

by

TERENCE MICHAEL DORN

La Jolla, California

October 2020

Abstract

The research problem was an examination of the vulnerability of U.S. nuclear power plants to unmanned aerial system attacks. The purpose of this study was to examine the vulnerability of U.S. nuclear power plants against attack by UAS via the perceptions and experiences of twenty current and former managers, scientists, and contractors employed by the federal government and nuclear industry. The qualitative phenomenological research methodology was chosen because it was well-matched to collecting information regarding one's attitudes, the ability to examine complexities, gather an abundance of data, and identify patterns. The theoretical framework examined was that of national security. Themes identified were (1) the threat of UAS attack against U.S. nuclear power plants was real, and a present-day one; (2) there is an intentional effort for the secrecy of UAS incidents by the Nuclear Regulatory Commission; (3) it was imperative to understand what the goal of the attack would be, i.e., soft facility targets would be likely targeted and damaged by bad actors and damaged while hardened ones would not. Finding security vulnerabilities and immediately closing those security gaps must be done per the theory of national security. Per the Nuclear Regulatory Commission data, there have been 57 UAS incursions over 24 U.S. nuclear power plants in the past five years. Nuclear power plants as a vital component of the nation’s sixteen critical infrastructure sectors are vulnerable, and it is highly likely that all other sectors with fixed sites and well-advertised locations are equally vulnerable to attack by UAS and will remain so until Congress acts.

Acknowledgments

It is a pleasure to thank those who made this dissertation possible. I owe my deepest gratitude to my wife, Army Major (R) Nicole Dorn, and my two sons, Alan and Calvin. My wife and sons made me a far better man than I would have been without them. I owe my parents, U.S. Air Force Chief Master Sergeant (R) Al and Emel Dorn, everything for making me the man I am today. I could not have had better parents who did everything to put me on the right track to make me a successful and productive member of society. My only regret is that I did not endeavor to do this earlier so that my father could have witnessed it. Thanks to my brother Greg, sister Debra, Ken Wanzer and Chris Sanborn for their unending support. I am thankful for having served with and continued a lifelong friendship with U.S. Army Lieutenant Colonel (R) Dr. Mason Rice, his wife Emily, and son Walker: Captain (R) Mike and Brooke Armstrong; and Mr. George Grantham. Lastly, I wish to acknowledge the exceptional business program, instructors, and support personnel at Northcentral University. I am grateful for having had Dr. Ian Cole on my dissertation committee and Dr. Vicki Lindsay as chair. Dr. Lindsay possesses an exceptional mastery of APA 7, the English language, and has a great sense of humor. She and Ian provided flawless scholarly guidance to this old Soldier.

Table of Contents

List of Tables

List of Figures

Chapter 1: Introduction

The first recorded use of an unmanned aerial system (UAS) occurred in the U.S. during the Civil War when hot air balloons were used to monitor enemy forces by both the North and the South (Garamone, 2002; Holman, 2009). In 1849, Austria loaded incendiary bombs onboard hot air balloons in an attempt to end their siege of Venice, Italy (Garamone, 2002; Holman, 2009). The first powered UAS was unveiled in 1918 when the U.S. Army demonstrated "an aerial torpedo" called the Kettering Bug (Nguyen, 2019; Smithsonian National Air and Space Museum, n.d.). In 1982, the Israeli Air Force demonstrated the first modern age use of UAS when they successfully decimated the Syrian Air Force and its air defenses (Kreis, 1990). In 1991, the U.S. demonstrated their significant UAS capabilities in Desert Storm, including the first documented surrender of Iraqi military forces to a U.S. Navy UAS (Shelsby, 1991). In 2014, the Islamic State of Iraq and Syria made extensive use of readily available commercial UAS for offensive and defensive operations (Watson, 2017).

In 2018, the non-military use of a UAS shut down operations at Gatwick Airport near London (British Broadcasting Corporation, 2018a), resulted in the cancellation of 800 flights that affected over 100,000 travelers (Mueller & Tsang, 2018). The shutdown cost the government, airports, airlines, and passengers an estimated $65.5 million (Calder, 2019). Later that same year, two UAS were used in an apparent assassination attempt against President Maduro of Venezuela (British Broadcasting Corporation, 2018b). In September 2019, a Pennsylvania man used a UAS to drop small explosives on his ex-girlfriend's property (Spires, 2019; Forgie, 2019).

The emergence of UAS has had a profound impact worldwide. They have proven to be transformational and are simply a much more efficient and effective way to perform many businesses and government organizations' daily tasks. UAS have delivered positive benefits to many users, including surveillance of suspects for law enforcement, pesticide dispersion to farmlands, and tunnel surveillance utilizing ground-penetrating radar for mining companies. Additionally, society has also witnessed the despicable use of UAS by bad actors. These nefarious uses have included contraband drops into prisons, surveillance of law enforcement, airdrops of illegal drugs from UAS launched from Mexico; reconnaissance of government facilities, the dropping of hand grenade sized explosives by the Islamic State of Iraq and Syria on the U.S. and allied military personnel in Iraq and Syria (Chang, 2018; Tarantola, 2017; Albiges, 2019; Hennigan, 2018). The emergence of UAS in the modern area occurred in the early 1980s. Yet, governments had been slow to recognize the emerging threat that UAS posed to society and even slower address these threats to protect critical infrastructure and civilian targets.

The opportunity for economic and recreational advances expanded very rapidly, as well as the opportunities for bad actors to inflict considerable damage and injuries from an attack utilizing a UAS armed with weapons of mass destruction that have likewise proliferated (United Nations Office of Counter-Terrorism, 2018). Recent attacks have proven that the threat of an attack involving a UAS or other unmanned systems operating on land, sea, or undersea armed with mass destruction weapons is viable (United Nations Office of Counter-Terrorism, 2018). The advent of artificial intelligence, the rapidly expanding fifth-generation (5G) wireless technology for digital cellular communication networks, and low-cost software have combined to usher in miniature

drone swarms that could attack single or multiple targets from different approaches, altitudes, speeds, and times, all without the need for human input (Betz, 2017). It has been demonstrated that artificial intelligence allowed a swarm of UAS to simultaneously attack multiple targets (Schuety & Will, 2018). The challenge has intensified, and stopping one UAS is far less challenging than countering multiple UAS or a swarm of them simultaneously. Artificial intelligence has directed UAS to self-determine the best strategy for achieving its programmed mission, such as flying beneath air defense radars en route to a target or swarm on a single target from multiple directions (Schuety & Will, 2018). 5G networks have enhanced UAS remote capabilities and have given the bad-actor the capability to direct UAS attacks from another city, state, or even country (Patel, 2017). The enhanced communications networks have enabled bad actors to launch swarms of autonomous drones that have proven synchronization capabilities to get to their programmed targets at greater distances quickly and efficiently.

These technological advancements have combined with unmanned systems resulting in a rapidly evolving threat, yet the skies are not the only domain of concern. The technology has migrated rapidly into unmanned undersea and surface systems, thereby providing expanded potential delivery options of weapons of mass destruction. Unmanned surface systems and unmanned undersea systems have already transformed how data will be collected from the surface and undersea environments. They will be capable of being used by bad actors to threaten the nation's national security singularly or in conjunction with UAS platforms (Martin et al., 2019; Roblin, 2019).

Business analysts have mostly ignored the potential explosion in demand by the public and private entities for UAS. Their growing appetite for small and large, highly capable UAS is impacting the U.S. economy. UAS are inexpensive and are readily available throughout the U.S. and worldwide. Estimates are that the worldwide sales of UAS will grow from $4.9 billion to $14.3 billion over the next decade due primarily to a relaxation of U.S. airspace by the Federal Aviation Administration and growing demand by businesses for UAS (Pietsch, 2019). One of the more moderate economic forecasts predicts that commercial drones will have an annual impact of between $31 billion and $46 billion on the nation's Gross Domestic Product by the end of 2026 (Cohn, Green, Langstaff, & Roller, 2017). Demand has driven higher production rates and lowered prices for drones (Murison, 2016). Commercial uses are in its infancy with Amazon, Google, UPS, and others to use UAS to deliver packets, products, online orders to consumers rapidly. Using UAS to attack the Saudi Arabian oilfield served as a wake-up call to governments worldwide. Governments have been slow to recognize the potential threat that UAS could pose to critical infrastructure and the public. These are often referred to as soft targets due to their vulnerability and the ease with which a bad actor could launch an attack in various public settings and garner worldwide attention. Likewise, a successful attack against one or more nuclear power plants would attract the world press and affect the electric grid for a region of the U.S. and could result in rolling blackouts.

According to former Department of Homeland Security Secretary Kirstjen Nielsen:

> We know that terrorists are using drones overseas to advance plots and attacks, and we've already seen criminals use them along and within our borders for illicit purposes. We are working with Congress for the authorities needed to ensure we can better protect the American people against emerging drone threats. (Hennigan, 2018, para. 3)

This study was a first in the academic world as it will examine the vulnerability of nuclear power plants to attack via UAS. There was a lack of threat analysis, counter-strategies, and equipment despite the recent use of UAS to attack Saudi Arabia's critical infrastructure. Several instances listed reference how a few bad actors have used this technology to conduct attacks. These attacks served as the first study to conduct a scholarly examination of the threat to one aspect of the 16 sectors of critical infrastructure with the U.S. It will have implications worldwide.

Statement of the Problem

The problem that this study addressed was the perceived vulnerability of U.S. nuclear power plants to UAS attack. The U.S. government has indeed been slow to recognize and react to this threat. Experts in the government and private sector believe that UAS systems will become increasingly weaponized, and it is merely a matter of time before attacks grow (Sauer & Schörnig, 2012). France witnessed UAS attacks against its nuclear power plants. On July 3, 2018, two UAS flew into the restricted airspace around Lyon's nuclear power plant in central France (Tran, 2018; Ranson, 2017). One slammed into a building housing spent uranium fuel, while the other filmed the attack and returned to its operators (Tran, 2018). Fortunately, only the one UAS was severely damaged; there was no damage to the building and no containment loss nor impact on the spent fuel rods

containment. Yet, the attack represented what many thought a far-fetched possibility that had yet to materialize. The attack proved that the threat of a UAS attack upon a nuclear power plant is a present-day concern. The French authorities and plant personnel were powerless to stop the drones and could only stand by and watch as one crashed into the building's exterior. Greenpeace later claimed credit for the attack and stated it was merely a demonstration of the nuclear power plant's vulnerability to attack and lack of security (Tran, 2018). The 96 U.S. nuclear power plants reliably provide 19.7 percent of the nation's electrical grid (Department of Homeland Security, 2013). A successful attack against one or more nuclear power plants could result in a loss of electricity to entire regions of the U.S. The engagement strategy will involve the Department of Energy, the Nuclear Regulatory Commission, and the nuclear reactor owner-operators in the eastern half of the U.S.

Purpose of the Study

The purpose of this qualitative phenomenological study was to examine the vulnerability of U.S. nuclear power plants against attack by UAS and possible efforts to mitigate them. The study was a logical research endeavor to examine the problem statement discussed previously, the attack via conventional explosives or unconventional, i.e., chemical, biological, radiological, or nuclear payloads to not destroy nuclear power plants, but to shut them down. The timeframe was security at nuclear power plants today, and the study took three months. The study's location included multiple nuclear facilities located in the eastern U.S. Instruments included federal government resources, references, documents, and NVivo software to analyze the data. The bulk of the information was gathered via a review of existing open-source documents, but more

importantly, by one-on-one interviews with personnel who at one time possessed top-secret clearances employed by or associated with the Nuclear Regulatory Commission, the Department of Energy, the Department of Homeland Security, nuclear facilities, or other departments of the federal government and its army of support contractors. This study was an unclassified examination of the threat of attack posed by UAS against U.S. nuclear power plants. The biggest perceived limitation initially for this study was the number of people willing to sit down to discuss possible nuclear facility vulnerabilities. Initially, only eight to ten personnel, including representatives from management and scientists, agreed to be interviewed and participate fully in the study. By utilizing a qualitative phenomenological study, the data gathered through interviews provided insight into the target population's general perceptions. Thus, this phenomenological study offered the most considerable flexibility in investigating key personnel's perceptions of specific research questions, gathering evidence, and analyzing it for the best possible answers to the research questions (Gillham, 2000). One last reason I chose a qualitative phenomenological study was simply due to the federal government's lack of information reference this issue and the corresponding number of incidents captured thus far. The lack of information was intentional by the Nuclear Regulatory Commission since it directly impacted the trust and confidence that the American public had to produce safe, reliable energy. Ensuring and maintaining favorable public opinion must be one of the Nuclear Regulatory Commission's very highest goals.

Theoretical Framework

The theoretical framework for this qualitative phenomenological research study was national security. A nation's governmental responsibilities to provide for citizens'

national security have been echoed throughout the ages, as demonstrated in the writings of Thomas Hobbes in his seminal writing in 1651. A government is a protector, and it provides law and order and protects its citizens from internal and foreign foes (Hobbes, 1651). During the U.S.'s birth, George Washington firmly believed in a stable federal government that would protect the nation's security and the freedoms and liberties of its citizens (Marrin, 2001). President Trump outlined the federal government's responsibilities to the nation's citizens, "First, our fundamental responsibility is to protect the American people, the homeland, and the American way of life" (National Security Strategy of the United States, 2017, p. 4). The government remains the guarantor of security at the local, state, and federal echelons of government. While the threat environment is constantly changing with new emerging threats and players, a government's preeminent responsibility to protect its citizens has remained from times immemorial (The White House, 2017; Department of Homeland Security, 2019). New, more sophisticated threats are multi-dimensional and are of concern to most of the world's nations. Governments must increase their diligence against emerging threats and proactive in countering them to ensure their citizens' safety and security against any threat. (The White House, 2017; Department of Homeland Security, 2019)

The theoretical national security framework led to the formulation of the problem, purpose statements, and research questions. The framework of national security is paramount to the core of government responsibilities. The dismissal of the threat posed by UAS by the Nuclear Regulatory Commission in its unclassified release of *Enclosure Four* following its three-year-long security review demonstrated a bureaucratic mentality and inability to think pragmatically about the evolution of threat as based on an enhanced

hobbyist or commercial technologies (Nuclear Regulatory Commission, 2019, p. 1). The problem statement served as the foundation of this study, compounded by a clear purpose statement and supporting research questions intended to answer the central problem statement. An examination of the framework provided independent factors that impact the federal government's security assessments, a view of a threat to its citizens' safety and security and its existence, and subsequent actions. The federal government's responsibilities to recognize a threat as it strives to ensure national security are vital to this study. Recognizing a national security threat and countering it is inherent in the responsibilities of a nation. The Department of Defense has been "playing catch-up" to the threat posed by UAS to its troops and military equipment overseas. It has invested a great deal of money in companies to build a viable defensive system. The attack against the Saudi oilfields discussed earlier proved incredibly embarrassing to the U.S. a vital component of the Saudi's air defense network included the well-known and combat-proven PATRIOT system. It is unknown if it was manned or operational when the multiple cruise missile motherships and independent UAS launched off them and headed toward multiple separate targets within the massive facility. In the U.S. federal government, must reverence be given to the Department of Defense, and they often lead the research and technological advancements in national security-related systems and strategies. If it is behind, then the rest of the federal government efforts to counter this particular threat is paltry and in the earliest stages of development. This study examined specific entity responsibilities and highlighted a national security vulnerability that needs to be addressed immediately and not after the fact, as was the case of acknowledging the threat and greatly improved airport screening processes in the aftermath of 9/11.

Nature of the Study

The methodology was that of a qualitative research study, and the design was phenomenological as this allowed research into the perceptions of U.S. government employees, contractors, and scientists currently or formerly employed in the nuclear industry. The scripted interviews elucidated the population groups' perceptions to answer this study's problem statement. This study used a mix of interviews, documents, archival records, and participant observations. Data analysis used notes from the interviews, field notes from direct interaction, and observation based on video interviews. The analysis developed what researchers refer to as a holistic snapshot of the phenomenon. Data analysis explained why the phenomenon exists, evaluate its reason, and offered government strategies for resolving the vulnerability.

The phenomenological design was best suited to address the problem with the intentional limitations of accessing information that the federal government determined to be highly classified as directly related to national security. This design also allowed flexibility to examine the generalizations outlined in the problem statement, purpose statement, and research questions. Lastly, it examined the UAS overflights vis-à-vis the perceived threat that UAS posed to the U.S. nuclear industry and government members. The problem and purpose statements led to the development of the research questions. The phenomenological design determined what a select and small group of people perceived the UAS phenomenon's threat was at their workplace. The current and former nuclear employee's perceptions, perspectives, and understandings of the threat posed by UAS and all of these subjective factors were analyzed. They provided a formation of an understanding of the interviewee's perception and, if they had personal experiences of a

UAS overflight, how it affected their perceptions of the threat posed by UAS in general. The nuclear personnel all possess unique perspectives, are highly educated, intelligent, and are not generally disposed to emotionalism, and all have top-secret government clearances.

Research Questions

Two research questions provided insight and answers to the problem statement of this study. The perceived vulnerability is not a general one and may vary depending on the type and number of UAS and its payloads, which will probably be determined only after an attack.

Research Question 1. To what extent do UAS pose a threat to U.S. nuclear power plants?

Research Question 2. To what extent do actions need to be undertaken at U.S. nuclear power plants to counter the threat posed to them by UAS?

The first research question addressed the possible vulnerability of nuclear power plants to attack by UAS. While a single UAS flying directly into a building will likely have no impact on ongoing operations, the same system dispersing chemical, biological, nuclear, or radiological agents over that same facility may. Bad actors intend to disrupt, not necessarily to destroy their targets. As long as the nuclear power plants cease operations, the bad actors win. The type of payload dropped may shut down the facility for an extended period depending on the agent, the amount dropped, and how far it traveled into the facility. Another area of concern to the federal government may very well be how far the chemical, biological, radiological, or nuclear

agents expand out of the area and into public roadways, housing, or other general gathering locations.

The second research question was based on the validation of the first research question, and the subsequent actions that would be available to counter or mitigate the threat. These methods could involve technology to counter the attacking UAS via systems designed to disrupt the electronic activity occurring within the UAS or disrupt the signal from it to the operator. Other systems would involve kinetic materials fired at the UAS or laser beams designed to damage the electronics contained within.

Significance of the Study

In the modern age, the threat of homegrown or foreign terrorism, such as the Oklahoma government building attack by Timothy McVeigh, the Unabomber, Theodore John Kaczynski, and September 11, 2001, terrorist attacks have made safety a daily concern for citizens across the globe (FBI, 1995). I contend that this study is vital for understanding a threat to national security that currently exists, and that the federal government has yet to acknowledge the current vulnerabilities to the UAS threat and move toward mitigating and countering it. Unmanned aerial attacks have already occurred in Saudi Arabia against critical infrastructure. The Department of Homeland Security identified the following 16 sectors as critical infrastructure: chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; food and agriculture; government facilities; healthcare and public health; information technology; nuclear reactors, materials, and waste; transportation systems; and water and wastewater systems (U.S. DHS, 2020). The U.S. federal government views the threat of UAS attack similar fashion to an aircraft that

would serve as a bomber and drop conventional explosives. Due to the fortified buildings and enhanced security, the threat from UAS has been discounted as inconsequential by threat planners. The threat exists today to release chemical, biological, radiological, or nuclear materials over critical infrastructure, specifically the release over nuclear power plants would result in a shutdown of the facility, not its destruction. This study may well serve as a seminal study that contributes to the field with national security implications. There is a wide-ranging lack of scholarly research studies and literature.

The threat that a successful attack or simultaneous attacks on multiple nuclear power plants could directly affect the U.S. power grid. If focused regionally, the grid would suffer from the loss of steady electrical production. Nation-wide, 96 nuclear power plants contribute nearly 20 percent of the nation's daily electrical needs to the grid, surpassed in electrical production only by natural gas at 35 percent and coal at 27 percent (Energy Information Agency, 2019). Twenty states have no nuclear power plants, while Illinois is the leading state producer at 53 percent of its electrical requirements, and Iowa is the least reliant and productive at achieving a mere nine percent of its electrical requirements (Energy Information Agency, 2019). The nation's national security, the safety, and prosperity of its citizens are dependent upon the electricity produced by the 96 nuclear reactors that are located predominantly in the eastern half of the U.S. The 2011 Fukushima nuclear disaster was catastrophic for Japan and would be so for any nation with a similar nuclear incident of that nature and severity. At a minimum, any attack that shuts down the nuclear power plant or a series of them would result in rolling blackouts that would impact every aspect of daily life for those living within those regions and negatively impact the nation's Gross National Product.

Definition of Key Term

Three key terms must be understood to understand the problem statement, the purpose, and the research questions inherent in this study's conduct.

An unmanned system, unmanned vehicle, or drone:

- This refers to an unpiloted aerial, undersea, or surface craft operated via remote control or programmed for autonomous movement.
- Aerial, ground, or undersea drone, plus a controller and the software required to operate the system.

UAS, unmanned *aerial* vehicle, or drone:

- This refers to an unpiloted aerial craft operated via remote control or programmed for autonomous movement.
- The system or vehicle term refers to an aerial craft, plus a controller and the software required to operate the system.

USS

- Unmanned Surface System (land or sea)
- This refers to an unpiloted surface craft operated via remote control or programmed for autonomous movement.

UUS

- Unmanned Undersea System
- This refers to an unpiloted undersea craft operated via remote control or programmed for autonomous movement.

Weapons of mass destruction:

- Any explosive, incendiary, or poison gas device designed, intended, or can cause a mass casualty incident;
- Any weapon designed, intended, or can cause death or serious bodily injury to a significant number of persons through the release, dissemination, or impact of toxic or poisonous chemicals or their precursors;
- Any weapon involving a biological agent, toxin, or vector (defined in section 178 of U.S. Code title 18) designed, intended, or can cause death, illness, or serious bodily injury to a significant number of persons; or
- Any weapon that is designed intended or can release radiation or radioactivity causing death, illness, or serious bodily injury to a significant number of persons (Cornel Law School, n.d.

Summary

The emergence of UAS has had a profound impact worldwide, and new uses for them are growing. They have proven to be transformational and are simply a much more efficient and effective way to conduct daily life aspects for citizens and businesses. The problem to be addressed by this study is the vulnerability of U.S. nuclear power plants to UAS attacks. The purpose of this qualitative phenomenological study is to explore the state of security of the U.S. nuclear power plants against attack by UAS. The construct is the vulnerability of nuclear facilities to the UAS attack, either with explosives or dispersing weapons of mass destruction payloads, such as chemical, biological, radiological, or nuclear material. This qualitative phenomenological research focused on the theoretical framework of the concept of national security.

Chapter 2: Literature Review

The purpose of the qualitative phenomenological research study was to examine U.S. nuclear power plants' vulnerability to attack via UAS. This literature review will address several components, chief among them being the concept of national security. The national security strategy of the U.S. provides a framework for understanding the rationale behind the increasing use of UAS to conduct military and foreign policy. In the U.S., the concept of national security now encompasses proportionality, limited war, and preventive war via military UAS (Delahunty & Yoo, 2009). The historical basis for the emergence of UAS dates back to the U.S. Civil War in which both sides used manned hot air balloons for surveillance and unmanned when explosives were the payload (Garamone, 2002). The federal government has several departments, agencies, and commissions operating in the nuclear industry and defense arenas. Each has a unique area of responsibility and obligations. U.S. presidents and their administrations have justified the legality of UAS use upon the moral justification of proportional strikes and preventive war.

International law is based principally on one country's legitimate government's consent when asking for another government's armed assistance. Specific references to UAS or their use do not exist within international law. The best example of the proliferation of UAS was Turkey, which created an industrial complex and used them in armed conflict with the Kurds and as well as in Syria. The vulnerability of U.S. critical infrastructure to attack is high, primarily due to technological advancements that increase vulnerability. There is a lack of published and peer-reviewed articles reference the threat

posed by UAS to a nation's nuclear power plants and the methods to counter this growing threat.

The keywords used in searching databases were the following: UAS, unmanned aerial vehicles, unmanned aircraft systems, drones. The search used was Google, as well as the NCU Dissertation Database. The range of years researched was from 1776 to the present, and the type of literature was open source.

Theoretical Framework

National Security Theory. The definition of national security had remained unchanged for decades and is a government's responsibility to the security and defense of a nation, including its citizens, economy, and institutions (Romm, 1993). The threat(s) that nations face have evolved, and as such, so has national security, which now includes the threat posed by terrorists, international crime, maintaining the security and viability of a nation's economy, energy sources, environment, food industry, and cyber (Romm, 1993). The origins of national security threats have always included other nations. Still, they, too, have changed and now include non-state actors such as terrorist organizations, drug cartels, multinational companies, and natural disasters since they can have the same devastating impact on a nation as military conflict (Romm, 1993). The elements of national power, such as military, economic, political, and diplomatic, have been used throughout the ages against hostile nations (Paleri, 2008). Global insecurity may require involvement within specific regions and reinforcement of regional powers that could

have been battling climate change, economic disparities, and the proliferation of nuclear weapons (Paleri, 2008).

The concept of protecting one's borders dated back in history as far as the ancient Egyptians (Breen, 2016). The Chinese emperors built and utilized a wall to keep hordes of warring factions out of their kingdom (Cook, 2010). The rulers of the Byzantine, Roman, and Ottoman empires and monarchs in Europe and Russia, believed in the sanctity of their boundaries (Phillips, 2004; Parker, 2005). It was not until the late 1500s that the use of a definition articulated what kings and queens had done for a few thousand years.

The 1500s to 1700s. A nation's governmental responsibilities to provide for the national security of citizens had echoed throughout the ages. In 1532, Machiavelli wrote about this concept in his timeless *The Prince.* This work later became a significant influence upon the political views of the U.S. Founding Fathers as Machiavelli was a fervent believer in the republican form of government (McCormick, 2011).

In 1651, Thomas Hobbes wrote that a government was a protector; it provided law and order; it protected its citizens from internal and external threats. During the nation's birth, George Washington firmly believed in a stable federal government that would protect the nation's security and guarantee the freedoms and liberties of its citizens (Marrin, 2001). In 1648, the concept that a nation-state had sovereign control of domestic issues and national security arose out of the negotiations of the Peace of Westphalia (Holmes, 2015). The Peace of Westphalia comprised independent peace treaties signed between May and October and ended multiple European wars, which had claimed an estimated 8,000,000 lives (Clodfelter, 2017). The terms of the Westphalian sovereignty

translated into a state's sovereignty over its territory and became a principle in international law (Osiander, 2001).

Immanuel Kant believed that nation-states should place their national interests under the greater common good and accept international law (Kant, 1795). While the concept of national security was reasonably new, his idea of subjugating all nations to international rule did not receive widespread acclaim as he thought it would. In 1793, Carl von Clausewitz, a German theorist, wrote his timeless *On War,* in which he stated, “War is not an independent phenomenon, but the continuation of politics by other means" (as cited in Paret, 1976, p. 6). Suppose a nation was unsuccessful in its foreign policy. In that case, it must be perpetually prepared for war since it was the responsibility of the state to safeguard its citizens as well as its mere existence (Clausewitz, 1793). War was not merely a military endeavor but a total effort by the entire nation (Clausewitz, 1793). All citizens needed to focus on the war, no matter the cost, for the citizens' safety, and the nation's continuation was critical (Clausewitz, 1793). Machiavelli's writings of a republic influenced the founding fathers. Machiavelli heavily influenced Hamilton on the relationship of foreign policy to domestic policy. Still, Hamilton did not share in the degree of greed that Machiavelli believed that a republic needed to possess to survive (Machiavelli, 1532).

The 1800s to 1900s. Baron Antoine-Henri Jominian believed that military strategy must directly support a nation's security, national strategy, and associated national policies for national security is of supreme importance (Jomini, 1865). He gained acclaim for his writings on the strategic definition and uses of bases, strategic lines, and critical points. His operational success instructions put superior combat power at the

decisive point and time made him famous among the military strategists. Yet, Jomini was a fervent believer in the nation's responsibility to provide for its security and citizens, no matter the cost (Jomini, 1865).

An English historian named Andrew Preston discovered that between 1918 and 1931, the U.S. Presidents uttered the term national security only once in each of their terms (Fergie, 2019). That changed soon after President Franklin Delano Roosevelt used it in his first radio address in 1940. Roosevelt continued to use it in subsequent speeches to build consensus among the citizens and politicians due to the looming threat that the U.S. was facing from Nazi Germany and Japan. His fireside chats were especially useful in getting his message out to the public. Later in the decade, Princeton historian, Edward Mead Earle, promoted the concept of national security to all that would listen to his speeches and read his extensive writing (Fergie, 2019). His repeated use of national security took root within American society. As World War II loomed, national security took on a militarized connotation that allowed American citizens to view their place in the global geopolitical machine. Conflicts overseas appeared destined to spread to the shores of the U.S.; hence they were an immediate threat, and only national security and military preparedness would retard the enemy's advancement (Fergie, 2009). National security erased the boundaries between soldiers and civilians, domestic policy and foreign, peaceful coexistence, and a perpetual state of war as national security had become everyone's responsibility (Fergie, 2009). Military preparedness had previously involved only soldiers. It has become a collective effort that required civilians to do their parts to contribute, whether in the fields growing crops or in the industries building components of the nation's war machines (Fergie, 2009). Earle believed that the term

national defense was a passive response by a defender against an aggressive nation. National security required a constant state of readiness (Fergie, 2019).

In the U.S., the theory of national security became the cornerstone of U.S. foreign policy when President Harry S. Truman signed the National Security Act of 1947 (Department of State, 1947). At this time, the definition of national security would have included the protection of the nation and its citizens against an attack and other dangers. Walter Lippmann, an American writer and political commentator coined the term "Cold War" and viewed security as a nation's necessary ability to protect its core values (1922). For nearly a century, the term Cold War neatly encapsulated the concept of national security and the ever-present threat from the communists in the east.

The 2000s to the present. The use of UAS has become the preferred weapons system for U.S. national security. The rise of UAS, both in numbers and use, within the U.S., is directly manifested by their expanded use under national security guise while conducting limited war, preventive war, and proportional strikes. No other government instrument had been utilized more to exercise offensive military acts in support of U.S. national security than armed UAS.

In 2017, President Trump stated that the federal government had the responsibility to recognize emerging threats and devise measures to negate it while ensuring that its citizens' national security and safety is maintained (National Security Strategy of the United States, 2017). "First, our fundamental responsibility is to protect the American people, the homeland, and the American way of life" (National Security Strategy of the United States, 2017, p. 4). The guarantor of security within a nation is its local, state, and federal government. As the threat environment has always been an evolving one with

new threats and players, a government's preeminent responsibility to protect its citizens has remained from times immemorial (The White House, 2017; Department of Homeland Security, 2019).

History of UAS

As early as the American Civil War, both the Union and Confederate forces launched balloons to conduct the enemy forces' surveillance. Still, they were occasionally loaded with explosives as well (Garamone, 2002). The intent was for the balloons to fly over the front lines between the two forces and explode near a supply or ammunition depot. The surveillance of the enemy troop movement was incredibly useful. However, the new tactic of dropping explosives from the air proved ineffective as the wind frequently blew the balloons far away from their intended targets.

The Austrian navy used UAS in 1848 when they released unmanned hot air balloons, each carrying a 20 or 30-pound incendiary bombs in their baskets (Holomon, 2009). Unfortunately, the wind blew the balloons off course, and when the balloons burst and the bombs rained down, they fell outside of the city and did little actual damage (Piera, 1962).

In 1918, the U.S. Army demonstrated what they referred to as "an aerial torpedo," but was a UAS with an explosive device in the nose cone. The "Kettering Bug" had a rudimentary guidance system. The fuel load required calculations from the start point to the designated target. Once the fuel tanks were empty, the Bug would begin a steep dive that would cause the wings to separate, thereby creating an aerial torpedo (Nguyen, 2019; Smithsonian National Air and Space Museum, n.d.). Due to the time it took to get the Bug operational, it did not debut during World War I.

In World War II, the German developed the V-1, vengeance weapon, and the more extensive V-2 system. Both were armed with high explosives and would strike terror in the English citizens. While both had a rudimentary guidance system, the V-1 was Nazi Germany's first UAS. It's successor, the V-2, had a guidance system that would fly it to a specific target. Thus, it became the world's first guided ballistic missile (Neufeld, 1995). The Japanese tried to ignite the western U.S. into fires during World War II with high altitude balloons laden with incendiary explosives (Garamone, 2002). The Japanese believed that high altitude winds would carry them over the western U.S., where they might start massive fires in the highly forested region. Unfortunately, the Japanese ceased operations when they were unable to gauge the success of their efforts. The U.S. attempted the same tactic against the Japanese, but the results were equally disappointing since the technology did not exist to launch and control them remotely (Garamone, 2002).

Interest in unmanned aerials systems rebounded in the U.S. in the pre-Vietnam War era when modern technologies increased UAS capabilities. During the U.S. involvement in the Vietnam War, technology allowed the U.S. to make greater use of UAS for both routine and dangerous missions that would have been handled previously by manned aircraft. The U.S. used modified Firebee aircraft to conduct camera and signal reconnaissance during the day and night, general propaganda by dispensing leaflets, and air defense detection, identification, and targeting (Garamone, 2002). The success spurred the U.S. military to pursue more exceptional capabilities and UAS numbers, which became a growing arsenal of offensive-oriented systems.

In 1982, the Israeli Air Force intelligence warned of massive amounts of air defense units just across the border with Syria. The inherent vulnerability of Israel was that it was a small country with a small population. Thus, it could not afford significant losses of manpower nor equipment. As a result, the Israeli's developed UAS designed to spook the Syrian air defense units across the border. The Israeli Air Force would utilize these UAS to fly quickly over Syrian air space, resulting in the Syrians believing that they were under attack. They would turn on their air defense radars. The Syrian radars would radiate energy, which the Israeli's would then target. Behind this initial wave of UAS, the Israeli Air Force launched High-Speed Anti-Radiation Missiles (HARM) that ride the radar's emission of electro-magnetic radiation signals to the radar itself (Kutzscher, 1957). The Israeli Air Force fighters and bombers flew behind the first two waves and decimated the Syrian Air Force and thousands of high-value ground targets (Kreis, 1990). The success was due to technology, tactics, and training as the most critical factors in modern warfare, regardless of the weapon systems. There will always be a debate where these three factors stand to one another, but to possess all three in abundance would deter any rational enemy. The Israeli military proved in 1982 to be vastly superior to its Arab neighbors due primarily to its people, their discipline, its technology, namely its development and use of UAS, its tactics, and training programs (Kreis, 1990). Syria and its Russian supporters were oblivious to the evolution of this emerging technology into modern warfare. In Israel, strategically oriented professionals created a new weapon system to offset the enemy's superiority in numbers of aircraft, air defense systems, and soldiers. The mere fact drove the Israel government that their

very existence as a nation depended upon superiority in technology, tactics, and personnel.

In 1992, the U.S. intervened in the Balkan Conflict and exercised its UAS supremacy. The Department of Defense had been busy developing UAS since the end of the Vietnam War. The Navy had developed its Pioneer system, the Army the Hunter system, and the Air Force the Predator system to conduct reconnaissance, targeting, and even engaging targets with missiles (Vogel, 1999). All three services operated them in the Balkans but were surprised to discover that UAS required a much more extensive support network to operate than manned aircraft. These UAS offered safety for aircrews who were not flying while providing real-time surveillance of the battlefield via the UAS (Vogel, 1999). The U.S. continued to depend on its UAS during Operation Desert Storm in Iraq, Afghanistan, Somalia, and Yemen (Vogel, 1999). In 2014, the Islamic State of Iraq and Syria made extensive use of readily available, low-cost commercial unmanned aerials systems for both offensive operations (Watson, 2017). They were able to devise a mechanism to release a grenade size explosive underneath their commercially available UAS and then used them to attack soldiers and civilians who were out in the open.

The historical relevance is vital to understand the rise of armed UAS use by the U.S. in national security. The U.S. national security pillars of limited war, preventive war, and proportional strikes have replaced diplomacy's widespread use in the early 1960s and 1970s. While Secretary of State Pompeo is flying to hotspots around the world, the U.S. military is simultaneously moving military assets and personnel to demonstrate the U.S. resolve, all in the name of national security, via UAS strikes.

Aspects of the U.S. Federal Government

The U.S. federal government is responsible for protecting its citizens, lands, and interests, dating back to its inception. The federal government set up numerous departments, agencies, commissions, and services designed to accomplish this as experts in their respective responsibility areas. For the U.S. nuclear industry, government oversight and management were placed upon the Nuclear Regulatory Commission; for civilian aviation, the Federal Aviation Administration, and defense with implications for the use of troops and equipment within the homeland, the Department of Defense. The federal government section will examine the history and responsibilities of the Nuclear Regulatory Commission, the Federal Aviation Administration, and the Department of Defense, the morality of its use of UAS, and the use of the term preventive war.

Nuclear Regulatory Commission. In 1946, Congress drafted the Atomic Energy Act legislation, and President Truman signed the bill that created the Atomic Energy Commission with responsibility for nuclear regulation (Atomic Energy Commission, 1946). Eight years later, Congress updated the earlier law with The Atomic Energy Act of 1954, which allowed commercial nuclear power (Atomic Energy Commission, 1954). It affixed responsibility on the Atomic Energy Commission to encourage the use of nuclear power, to regulate the safe growth of the fledgling nuclear, commercial industry, all while maintaining the public's health and safety from radioactive hazards (Atomic Energy Commission, 1954). The Atomic Energy Commission received a great deal of backlash for having unsafe and lax regulations regarding radiation protection standards, the selection of reactor sites and safety, and environmental protection. In 1974, President Ford signed the Energy Reorganization Act and, in doing so, established the Nuclear

Regulatory Commission. The Nuclear Regulatory Commission's mission was twofold: first "to protect public health and safety while ensuring the safe use of radioactive materials; second the regulation of commercial nuclear power plants and other uses of nuclear materials, such as in nuclear medicine, through licensing, inspection and enforcement" (Nuclear Regulatory Commission, 2020, p. 1). The Nuclear Regulatory Commission regulatory enterprise encompassed three areas: commercial nuclear reactors that generate electricity as well as reactors required for research, testing, and training; nuclear materials required for medical, industrial, and academic facilities; the transportation, storage, and disposal of nuclear waste, material, and the decommissioning of nuclear facilities (Nuclear Regulatory Commission, 2020).

The U.S. experienced a boom in both the size and number of nuclear power plants in the late 1960s. The public became acutely aware of the dispute over reactor safety. Many critics attacked the Nuclear Regulatory Commission's surrender to the commercial nuclear industry over safety issues (i.e., nuclear core cooling systems, the integrity of the reactor system's various components, and quality; Nuclear Regulatory Commission, 2020). On March 28, 1979, the nuclear power plant at Three Mile Island in Pennsylvania suffered a catastrophic meltdown of Unit One, which resulted in a meltdown of half of the reactor's core and led to the creation of new tighter regulations and increased safety procedures and training for personnel (Nuclear Regulatory Commission, 2020).

As of October 2019, 96 nuclear reactors were operating at 58 nuclear power plants in 29 states (Zajac, 2012; U.S. Energy Information Administration, 2019). Of these plants, 61 plants had one reactor, 32 had two reactors, and three plants had three reactors

(see Table 1) whose cumulative efforts produced 19.7 percent of the nation's electrical requirements (U.S. Energy Information Administration, 2019).

In 1988, the Nuclear Regulatory Commission and the Muto Institute of Structural

Table 1

Nuclear Reactors and Electrical Production By State

State	Number of Operating Reactors	Total Nuclear Power Generated in Thousand Megawatt Hours	Percentage of State Requirement for Electricity Produced by Nuclear Power
Alabama	5	42,651	42%
Arizona	3	32,340	31%
Arkansas	2	12,691	21%
California	4	17,901	9%
Connecticut	2	16,499	48%
Florida	5	29,146	12%
Georgia	4	33,708	26%
Illinois	6	97,191	53%
Iowa	1	5,213	9%
Kansas	1	10,647	21%
Louisiana	2	15,409	16%
Maryland	2	15,106	44%
Massachusetts	1	5,047	16%
Michigan	3	32,381	29%
Minnesota	3	13,904	24%
Mississippi	1	7,364	12%
Missouri	1	8,304	10%
Nebraska	2	6,912	20%
New Hampshire	1	9,990	57%
New Jersey	4	34,032	45%
New York	6	42,167	33%
North Carolina	7	42,374	33%
Ohio	3	17,687	15%
Pennsylvania	9	83,199	39%
South Carolina	5	54,344	58%
Tennessee	3	31,817	40%
Texas	4	38,581	9%
Virginia	4	30,533	34%
Washington	1	8,128	7%

Note: The data was compiled from the U.S. Energy Information Administration, 2019.

Mechanics Incorporated of Tokyo, Japan, contracted Sandia National Laboratories to crash a plane into a steel-reinforced concrete wall that was a replica of the walls surrounding nuclear reactors at all nuclear power plants (Tulsa World, 1989). The test demonstrated that a manmade attack upon a nuclear reactor with an airliner would not breach the reactor's steel-reinforced concrete walls. This test occurred years before the terrorist attacks on September 11, 2001. A surplus U.S. Air Force F-4 Phantom fighter jet was procured, strapped to a rocket-powered rail system, and crashed into the 10-foot thick concrete wall at 500 miles per hour (Baker, 2017). The impact produced 2.4 inches of penetration by the jet's engines into the concrete block and moved it backward four feet (Tulsa World, 1989). The jet weighed 41,500 pounds when it hit the wall, which included more than 1,200 hundred gallons of water instead of jet fuel to simulate the weight of fuel and provide proper mass distribution (Baker, 2017). There were two critical issues with the demonstration that cast doubt on nuclear power plants' structural integrity when attacked by hijacked jetliners. First, when the two jetliners impacted the Twin Towers and brought them crashing down, it was not the jetliners' impact that damaged the massive steel beams that ran vertically up the entire length of the buildings. Instead, it was the resulting 2,000 degrees Fahrenheit fire that caused them to weaken and collapse. This Phantom test omitted jet fuel, so there was no resulting fire that may have weakened the steel-reinforced concrete block. Second, the attack angle was not what a jetliner would fly at if it were to dive toward a fixed nuclear power plant. The fact that a horizontal small fighter jet flying at 500 miles per hour moved the 10-foot thick, steel-reinforced concrete block back four feet ought to be an area of concern. A much larger and heavier jetliner flying at an angle closer to a near-vertical dive would not permit the

reactor's concrete walls to move back four or more feet due to the impact. This lack of impact absorption would result in be a cracking or breach of the walls.

The Nuclear Regulatory Commission regulatory responsibilities center on oversight of reactor safety, approval of applications and licensing for new reactors and renewal of existing ones, and high and low-level nuclear waste management. In the Nuclear Regulatory Commission's 2018 Strategic Plan, there were a total of seven security strategies listed, with number four being to "proactively identify, assess, and address threats, vulnerabilities, and security risks" (Nuclear Regulatory Commission, 2020, p. 1). In October 2019, the Nuclear Regulatory Commission completed a three-year-long security threat review of its nuclear power plants. While the results of the review were classified and withheld from the public, the Nuclear Regulatory Commission released a single page document from the security assessment, identified as *Enclosure 4*, which stated, "UAS posed no threat to the nuclear facilities" (Nuclear Regulatory Commission, 2019, p. 1). I inquired directly with the media spokesman for the Nuclear Regulatory Commission. The media director stated, “the staff concluded there were no significant vulnerabilities to nuclear power plants or category I fuel cycle facilities from adversarial use of commercially available UAVs. The staff did not intend to pursue any changes to licensees' defensive strategies." (S. Burnell, personal correspondence, February 20, 2020)

The abrupt dismissal by the Nuclear Regulatory Commission to the threat of attack via UAS resulted from a bureaucratic mentality and inability to think pragmatically about the evolution of a threat platform that originated as an enhanced hobbyist and commercial technology. The federal government's security assessments have been

viewed in light of the present-day threats rather than on emerging ones. A criticism of modern-day, senior military leaders was that they are well versed in battling the last war, but far less so for the next one. The same criticism is equally relevant to senior leaders within the federal government. They were likewise hindered by what they did not understand, thus incapable of formulating adequate strategies and resourcing the research and development necessary to quickly counter emerging threats.

Federal Aviation Administration. On May 20, 1926, President Coolidge signed the Air Commerce Act and created the Civil Aeronautics Administration, which provided federal oversight and regulation to the fledgling civil aviation (U.S. Department of Transportation, 1926). In 1958, the Federal Aviation Agency was created and responsible for serving as a single point of expertise and management for air traffic and safety (Federal Aviation Administration, 2020). President Johnson believed that there should be a single transportation department of the federal government that should coordinate, determine policies, programs, and regulate the entire U.S. transportation system (Federal Aviation Administration, 2020). In 1966, Congress authorized the creation of the U.S. Department of Transportation, and the Federal Aviation Agency became a subordinate agency with a name change from Agency to Administration (Federal Aviation Administration, 2020).

UAS had existed for decades, yet the Federal Aviation Administration did not formally acknowledge them until 2012. The Federal Aviation Administration Modernization and Reform Act of 2012 accomplished the following: first, the Federal Aviation Administration formally acknowledged UAS; second, it issued a waiver for the Department of Defense's most extensive UAS, the Global Hawk, to fly over U.S.

airspace; third, it issued interim operational guidelines for UAS use within the U.S.; fourth, it published its Integration of UAS in the National Airspace System Roadmap, the plan to incorporate UAS into the national airspace; fifth, it stated that the Air Traffic Control system and operators were not ready for what could be millions of independently owned and operated UAS (Federal Aviation Administration, 2020). However, the 2012 legislation did not address UAS use restrictions or its qualifying system parameters for all of its advancements. Thus, in 2018 the Federal Aviation Administration released new legislation that attempted to regulate a vast commercial market for UAS.

On October 5, 2018, the Federal Aviation Administration's Reauthorization Act of 2018, H.R.302, was passed by Congress and signed into law by President Trump (U.S. Congress, 2018). The 2018 Act established three categories of UAS pilots: the first was for UAS flown by certified remote pilots, including commercial operators who must be Part 107 qualified, i.e., actual pilots; the second was for UAS flown by recreational flyers and modeler community-based organizations and are registered as a "modeler;" the third was for UAS flown under an exemption under the Special Authority for Certain Unmanned Systems (U.S.C. 44807), or a Public Certificates of Authorization and these systems were registered as "non-modelers" and required a Part 107 pilots license (Federal Aviation Administration, 2020). The 2018 Act further directed that:

- Registration of all commercially purchased UAS became mandatory, but not for all hobbyist systems.
- Hobbyists were allowed to operate UAS greater than .55 pounds to no more than 55 pounds without a Part 107 pilot license.
- Hobbyist must fly their UAS no higher than 400 ft above ground level.

- Hobbyists must operate only within recreational fixed sites found on the FAA Drone Zone website.
- The FAA Drone Zone provided information on where to fly, register, and what constitutes a hobbyist UAS.
- All UAS were strictly prohibited from operating within five miles of an airport within three miles and one hour prior and one hour after a sporting event at a stadium. (Federal Aviation Administration, 2020)

The Federal Aviation Administration had begun developing a Low Altitude Authorization and Notification Capability automated system similar to transponders on jetliners to broadcast a UAS location, height, and speed to the Federal Aviation Administration. The Federal Aviation Administration had also begun to develop a mandatory knowledge and safety test for UAS operators, but neither of them had been completed at the time of this study. Lastly, the Federal Aviation Administration granted permission to the Department of Homeland Security to examine the threat posed by UAS, how they could be detected, and how the government should respond. This issue was essential to U.S. nuclear power plant owner-operators as they could not engage UAS threatening their facilities (S. Burnell, personal communication, February 20, 2020). In such an occurrence, the plant must immediately notify the Federal Aviation Administration, for it would be they who possess the authority and responsibility to manage U.S. airspace. Since they would be ill-equipped to secure U.S. airspace, they would notify the U.S. Air Force and the Federal Bureau of Investigation for assistance.

In the past decade, the UAS commercial market grew in sheer numbers, capabilities, and the emergence of autonomous systems. The Federal Aviation

Administration created the Drone Zone website to help register and share information about UAS use and the updated number of registered UAS. Bad actors would not be inclined to register the UAS they had built at home from components that are not controlled and readily available for purchase on the Internet. Since it was created, the Federal Aviation Administration has had the legal authority to regulate all aspects of civil aviation within the U.S. as well as over its surrounding international waters. The Federal Aviation Administration classified UAS as aircraft; therefore, all law enforcement and civilian attempts to engage UAS for any reason, i.e., loitering over one's property, flying overcrowded stadiums, and parades are federal crimes and are punishable by imprisonment for up to twenty years. The 1984 Aircraft Sabotage Act made it a felony to damage or destroy any aircraft, manned or unmanned (18 U.S. Code, section 32, U.S. Congress, 1984). If an irate homeowner were to jam the UAS or capture it with a net gun, the Federal Aviation Administration would consider those two acts of interfering with radio transmissions to violate the Communications Act of 1934 (Federal Communication Commission, 1934). Only the U.S. Secret Service and the Federal Bureau of Investigation received authority to engage UAS. All means for mediating the use of UAS within the U.S. have led directly to the Federal Aviation Administration.

Department of Defense. The U.S. Department of Defense's use of UAS dates back to World War I. Yet, it avoided developing counter systems to the real threat that it developed and grew accustomed to utilizing. Potential adversaries could develop and use UAS against U.S. troops and military equipment overseas. The U.S. began searching for a more capable offensive UAS, yet it had found itself unprepared to address the threat posed by unmanned aerials systems to its critical infrastructure, critical targets, and

citizens. These new technological machines that were designed initially for hobbyists had a utility to many industries. What was a single device that posed a limited threat had evolved into multiple systems or a swarm of UAS capable of attacking a single target or multiple ones, the public or critical infrastructure, virtually anywhere and at any time. The threat of an autonomous swarm whose size and numbers were limited only by the algorithm that controlled their independent actions, and cooperative nature increased autonomy, range, and capabilities (Coleborn & Bleek, 2018). Threatening technological developments had always been an area of concern to the world governments. The world had witnessed that technological evolution often occurred at an accelerated rate. The government's vigilance had to increase in light of emerging threats, and they had to be proactive in developing the means to counter them to ensure the safety and security of its citizens (The White House, 2017; Department of Homeland Security, 2019). The government had invested a great deal of money in companies to alter the software of existing, viable air defense systems that would include the threat posed by UAS. The attack against the Saudi oilfields proved embarrassing to the U.S. since crucial components of the Saudi's air defense network included the well-known and combat-proven PATRIOT air and missile defense system. It is unknown if it was manned or operational when the multiple cruise missile motherships and independent UAS launched off them and headed toward multiple separate targets within the massive facility. The Department of Defense often led the research and technological advancements in national security-related weapon systems and strategies. Yet, for the past five to 10 years, the Department of Defense invested resources and funding to the development of counter UAS and still had not produced a viable counter system. The rest of the federal

government had depended on the Department of Defense to lead the counter-effort, yet independent research and development had been initiated at multiple federal agencies, administrations, and departments a few years ago.

The U.S. led the world in production and use of armed UAS: as of 2000, the U.S. possessed less than 50 systems, but by 2012, it possessed over 19,000, and its inventory and capabilities are unknown (Benjamin, 2013). The U.S. Department of Defense policy had been to prevent the type of autonomy in current and near-future weapon systems; therefore, a human had to be the chain of command and control (Department of Defense, 2017). Defense studies had unanimously recommended that the U.S. accept and accelerate the use of full autonomy for its obvious military potential to stay ahead of its strategic competitors (Department of Defense, 2016). All weapon systems had operated with a human in control, yet the advent of artificial intelligence could change that. Artificial intelligence had offered system autonomy to increase the survivability of the systems and enhance their operational capabilities. The UAS no longer needed to be specially designed and built military-grade systems due to commercially available systems.

The Morality of UAS Use by the U.S. Government.

There had been widespread criticism regarding the morality of using UAS to kill one's enemies, as well as the occasional collateral damage and deaths to those near the targeted individual(s) who may not have been combatants. The foundation of the moral argument justifying the use of UAS suggested that the use of a weapon with the potential to reduce collateral damage in war is morally preferable to using another, less precise and discriminating weapon (Maguire, 2015). UAS could be scalable, limited to surgical

strikes, and tailored for the target (Maguire, 2015). The ease with which the UAS use had also decreased the consequences of their use. What UAS have done is to allow the owners to engage in more wars for just causes. A just war then is a justifiable one; it is waged for moral purposes by a nation wishing to correct a wrong (Cox, 2017). The criteria are the "right to go to war" (*Jus ad Bellum*) and the "right conduct in war" (*Jus in Bello*): the first deals with the moral foundation for war, and the second the moral conduct of nations during the war (Resiman & Antoniou, 1994; Guthrie & Quinlan, 2007). The use of UAS eliminated the potential loss of aircrews, and if shot down, they could not be used for negotiation purposes as captured aircrews would have been (Ward, 2020).

As part of President Bush's War on Terrorism following the September 11, 2001, terrorist attacks, the U.S. accelerated its investments into UAS technologies (The White House, 2009). These systems also offered extensive Global Positioning System and precision location data verified by a robust satellite system; thus, they offer near-perfect targeting to its operators (The White House, 2009). Additionally, UAS operating costs were significantly less than a manned jet fighter. They offered a high degree of surprise and the ability to strike the enemy anywhere at any time. During the Bush administration, the use of UAS armed with missiles grew at an accelerated rate (Purkiss & Seale, 2017).

Proportionality

Proportionality had been the moral justification for the limited use of UAS as instruments of foreign policy and limited war. The benefit of eliminating terrorists weighed against innocent civilians killed in achieving it is morally reprehensible yet acceptable (Jinks, 2013). Based on unclassified data, UAS use in executing airstrikes

against terrorists increased ten-fold during President Obama's tenure over President Bush (Purkiss & Seale, 2017). The Obama administration referred to UAS as "exceptionally surgical and precise" (Purkiss & Serle, 2017, p. 1).

Limited Strike

The U.S. has long held that UAS use provided a limited and appropriate response. The moral argument against the use of UAS had been that of civilian casualties. The operators of UAS engaged in warfare had been entirely removed from the battlefields as were located many miles away. They operated their systems via video feed from the aerial platforms they are operating; thereby, the likelihood of mistakes increased. These warriors were hardly representative of the modern-day Warrior Ethos, code and culture for all military members. The U.S. military traced this code back to King Leonidas's stand and his three hundred strong Spartan force against Xerxes and his Persian army at Thermopylae in 480 B.C. (Bradford, 2004). The isolated air warriors are far removed from the battlefield; therefore, the odds of mistakes were higher. With increased engagements, UAS use led to increased anger and determination among the terrorists and did not deter them from further attacks.

Preventive War

The term preventive war had been used a great deal by the federal government to justify limited airstrikes in the ongoing war on terrorism. It is a precise, preemptive military offensive action that targets and eliminates threats (Delahunty & Yoo, 2009). From a historical perspective, such as the case of military actions between European powers, it would maintain the balance of power and the status quo (Delahunty & Yoo, 2009). Following the terrorist attacks on September 11, 2001, which claimed the lives of

3,000 U.S. citizens, President Bush focused on the nations that provided air and support to the terrorists and launched preemptive strikes against Afghanistan and Iraq (Delahunty & Yoo, 2009). The Bush administration justified the strikes as preventative war tactics (Delahunty & Yoo, 2009). In turn, the terrorist religious zealotry motivated their zealots through promises of eternal rewards in the after-life. It dictated the use of preventative war tactics to counter extremist organizations (Combs, 2006). Thus, the religious terrorists, many of whom came from oppressive societies and poverty, were the perfect candidates to recruit for executing tasks directed by God against their enemies (Wiktorowicz & Kaltenthaler, 2006). From the civilized world's perspective, President Bush's decision to pursue a preventive war against the Taliban and Al Qaeda in Afghanistan would qualify as a just war (Lee, 2009). A preventative war offered a proactive defense when an aggressor's actions are anticipated but unknown (Delahunty & Yoo, 2009).

International Law

The term Geneva Convention referred to the multiple conventions that occurred after World War II, which "defined the basic rights of wartime prisoners (civilians and military personnel), established protections for the wounded and sick, and established protections for the civilians in and around a war-zone" (The Geneva Convention, 1949, p. 223). It did not directly address instruments of war, such as UAS. For the U.S., UAS were initially used strictly for reconnaissance purposes. The Balkan Conflict

demonstrated the U.S. Air Force Predator system equipped with missiles, though none were fired until the U.S. entered the war in Afghanistan (Somerville, 2002).

International law allowed the legitimate government to ask for assistance from another nation, making the U.S.'s incursion and subsequent warfare into Afghanistan both legal and justified (Byrne, 2016; Doswald-Beck, 1986; Wippman, 1996). It did not specifically mention nor ban the use of UAS to execute warfare. Instead, it was focused on the consent by a legitimate government, even if the head of government had fled the capital or country. Consent had been cited by the U.S. to justify its ongoing operations supporting the lawful execution of its UAS program against terrorist organizations in Afghanistan, Iraq, Somalia, and Yemen (U.S. Department of Justice, 2017). Consent is a significant component differentiating the lawful use of UAS strikes under *Jus ad Bellum* and those that are not. The use of UAS by the U.S. in Iraq, Afghanistan, Somalia, and Yemen had been a response based entirely on legal requests, i.e., declared consent by the legal government for assistance (Schmitt, 2010). The U.S. later claimed that the preemptive use of UAS was an act of self-defense under J*us ad Bellum* in that UAS operations were in support of U.S. ground troops (Preston, 2015). In Pakistan, the situation is very different. The Pakistan government is in charge and exercises legitimate control over the country and had previously publicly withdrawn its consent for the U.S. to use it UAS within its borders. The legal advisor at the Department of State, Harold Koh, stated, in a 2010 speech to the American Society of International Law, that self-defense was the sole justification given for UAS strikes in the Obama Administration (U.S. Department of State, 2010).

UAS Proliferation

For over a decade, Turkey requested the U.S. made UAS for its military forces. The U.S. vehemently denied the requests due to Turkey's continued humanitarian onslaught against Kurdish separatists in the east and what the U.S. thought would inevitably continue (Prothero, 2020). Turkey looked to purchase UAS from Israel but was unimpressed with their performance, so it set about to build an industry. In 2009, the company Bayar was established, and responsibility was placed upon President Erdogan's son-in-law to build military-grade UAS (Prothero, 2020). Turkey had its first fully operation, medium-range military system within six years, which it immediately unleashed against the Kurds. In early 2020, the U.S. reversed course and pulled its troops out of the protective relationship it had built with the Kurds. The Russian government moved its military in and proclaimed that there would be peace in the region. The Russian failed almost immediately. In June, Syrian aircraft killed 33 Turkish soldiers near Idlib, Syria (Prothero, 2020). The Syrian forces threatened to demolish Idlib and force thousands of Syrian refugees into Turkey. Turkey responded in a surprise offensive and launched multiple waves of offensive sorties led by explosive-laden unmanned aerial swarms, which were reinforced by Turkish field artillery units, against the advancing Syrian military forces (Hacaoglu, 2020). They were so successful that the swarms located and destroyed Russian air defense units and Syrian fighter aircraft. It allowed Turkey to control air space through UAS alone (Hacaoglu, 2020). The creation of an industry where none existed previously was especially noteworthy for Turkey, but the dire consequences of a North Atlantic Treaty Organization (NATO) member nation engaging with open warfare with Russian would have had severe implications for NATO.

A great many businesses across multiple industries had examined the viability of UAS for commercial applications and had turned to it to transform daily workloads in a far more efficient and effective manner (Cohen et al., 2017). UAS and unmanned surface system deliveries had transformed the manner and speed of delivering goods to consumers. A 2013 economic study projected that UAS integration into the commercial delivery methods would generate an estimated 70,000 to 100,000 jobs in the U.S. (Association for Unmanned Vehicle Systems International, 2013). The integration of unmanned aerial delivery systems would positively impact the economy by nearly $14 billion (Association for Unmanned Vehicle Systems International, 2013). Part of the growth would be based on the manufacturing and associated services of UAS. While the investments have multiplied in the UAS market, regulatory requirements must be addressed by the Federal Aviation Administration and other government entities. Some of the more innovative UAS applications, such as unmanned aerial taxi's, may yet take many years to perfect. Industry stakeholders, their investors, and government entities have begun to strategize how this would impact the new capabilities into markets and how they would be regulated. There would need to be a widespread collaboration between government and private companies to allow heavier loads by UAS. Private companies' preliminary work have included commercial uses such as delivering products and many service industry opportunities to strengthen their use and society's dependence upon them.

There have been attempts to examine democracies that use UAS from those that do not. Many democracies had to deal with multiple threats and conflicts during their existence. Many governments viewed autonomous UAS as a panacea. The development

and use of lethal UAS made those same democracies far less democratic and prone to resort to force vis-à-vis their peaceful neighbors (Sauer & Schornig, 1992).

The protection of a nation's critical infrastructure must be assessed based on risk and the industry whose loss would be the most devastating to the nation. Yet, the U.S. had identified 16 critical infrastructure sectors, each with many independent facilities (Verner, Petit, & Kim, 2017). It is doubtful that the U.S. would be able to protect all sixteen sectors against attack all the time. A risk assessment must be performed to show the critical points and the most catastrophic for the nation. This information would assist in decision-making based on where government investment needs to occur and developing a priority list since resources were scarce, and everything cannot be a priority simultaneously. The risk assessment would also determine a government's rebuilding priorities should a natural or manmade disaster occur. An objective prioritization process would provide expert analysis and judgment to build resiliency. To help governments at the federal, state, and local levels have determined their priorities. The Argonne National Laboratory developed a computerized modeling framework capable of determining critical failure points throughout the infrastructure systems (Verner, Petit, & Kim, 2017). A well-developed process stressed factoring in time and resources, particularly after a disaster when infrastructure damage would restrict the amount of aid that can get into the disaster affected areas.

The Future of UAS

Newly developed software allowed UAS to maneuver out of the way and avoid objects thrown at them (Ackerman, 2019). The self-determination and action capability negated many defensive systems touted today as being safe to use within a city. One of

these uses a rifle-like device that fired a net toward a low flying UAS and captured it. Other versions included a much larger net mounted on an extensive UAS that could fly near a threat system and down it by shooting a net at it while both were flying through the air (Coxworth, 2018).

A British company named Vertical Aerospace recently demonstrated a heavy lift UAS that flew at fifty miles an hour with 550 pounds of cargo on board (Hood, 2018). Volocopter GmbH unveiled a 27 foot wide, seven-foot-tall, 18-rotor heavy-lift UAS capable of flying at 68 miles an hour while ferrying 440 pounds in cargo or passengers (Lai, 2019). Volocopter had been preparing its system as an air taxi in the ultra-competitive Dubai UAS taxi competition. Volocopter recently announced that it had teamed up with John Deere to create an agricultural heavy-lift UAS that would be more efficient for dropping chemicals from the air at a lower cost (Delbert, 2019).

Stealth technology had made the frontline U.S. fighter jets much more challenging to locate by enemy radars and have migrated into military UAS. The U.S. Air Force pursued a plan to pair the "Loyal Wingman" unmanned stealth fighter with frontline manned fighters, the F-22, and F-35, into all future conflicts (Trimble, 2020). The unmanned stealth aircraft would also serve as an "enemy aircraft" for the manned stealth fighter crews to conduct training against as it portrayed foreign fighters. Inevitably, stealth technology would eventually make its way into the commercial markets.

Technological advancement had UAS potentially acting as flying tankers that refueled U.S. Air Force planes. The most significant limitation of flying UAS would be that of battery life. The University of Berkley's High-Performance Robotics Laboratory

examined the commercial viability of flying batteries, small UAS that land atop larger UAS, and recharge them wirelessly as they fly (Liszewski, 2019). The Global Energy Transmission company had developed another novel approach to recharging UAS based on in-flight charging stations that would recharge UAS in a few minutes. The UAS would hover inside 32-foot diameter induction charging stations without ever having to land (Blain, 2018). As long as it had power, the recharge station would offer an unlimited number of commercial UAS the ability to recharge its batteries in under six minutes, which would allow them to continue with their deliveries (Blain, 2018).

The technology that led to success with UAS migrated into unmanned surface systems and unmanned undersea systems. UAS have proven to be very successful, both with hobbyists, in the commercial arena across the globe, as well as with many military forces. It was inevitable that global business entrepreneurs would look to the land and sea to take advantage of the same technologies that have made UAS much more capable and coveted. Scientific organizations have used unmanned surface systems that bear a striking resemblance to large surfboards with a mast to check on the growth of algae and the health of the undersea creatures on our planet (Jorge et al., 2019). Unfortunately, drug-trafficking organizations have operated in the undersea domain and have utilized unmanned undersea and unmanned surface systems for illicit trafficking purposes. Starship Technologies had demonstrated an unmanned surface system driven more than 30,000 miles in 100 cities while delivering 50,000 items (Starship Technologies, 2020). Unmanned surface systems and unmanned undersea systems would allow humans to safely and more efficiently serve as data collectors, transport cargo, and collect samples in a much more efficient manner. Following the 2011 Japanese earthquake and

tsunami disaster, surface and unmanned undersea systems helped clear debris and pollution from fishing beds, accessed the damaged Fukushima nuclear power plant's reactor buildings, and provided critical surveillance from within the facility (Lipscy, Kushida, & Incerti, 2013).

Bad actors would inevitably utilize unmanned surface systems and unmanned undersea systems to conduct attacks at seaports and to ferry weapons of mass destruction agents further inland via the twenty-five thousand miles of waterways within the U.S. (Boon, 2018). These surface and underwater systems would also be used as delivery devices to cripple the nation's communications and energy infrastructures by attacking oil rigs and undersea cables.

Moore's Law refers to the continual improvements in computing power, the almost magical computer chips found in all modern appliances, automobiles, and airplanes. The timeframe has been a doubling of computing power every 18 months (Denning & Lewis, 2017). One can only wonder what the next evolution of artificial intelligence might be if this doubling factor continues. For devices such as UAS, the future is both exciting and scary.

The Vulnerabilities of Modern Societies to UAS Attack

Famed Chinese strategist Sun Tzu, once stated, "To advance without the possibility of being checked, you must strike fast at the enemy's weakest points" (2011, p. 208). In 2014, French Lieutenant General (Retired) Ranson wrote, *The 2014 UAV Threat to French Nuclear Power Plants*, about the sole known attack against a nuclear power plant by UAS. As a result of the Middle East oil embargo in 1974, a determined French government turned elsewhere to satisfy its energy needs. France's nuclear power plants

provided 75 percent of its electrical requirements from 59 nuclear reactors, the most of any nation's energy needs (Ranson, 2014). Critics had concerns about nuclear power plants' security, and Greenpeace demonstrated the security vulnerabilities by conducting overflights of France's nuclear facilities with UAS. On one well-published occasion, it attacked a reactor building with a single UAS while another filmed it. The French government and nuclear industry did not wish to share what measures it had taken to secure the facilities, whereas many of its citizens demanded transparency. The French government believed that airports are the most likely and vulnerable critical infrastructure targets, followed by nuclear power plants. For the French authorities and many other governments, intelligence organizations' priority was to find the threat and neutralize it before it materialized over a nuclear power plant. Ranson's findings were that the French government was unable to defend its nuclear facilities and, at the time, had no counter technologies to detect, deter, deny, dissuade, or destroy UAS flying into their buildings (Ranson, 2014).

Ranson's conclusions coincided with the commission's findings that investigated the September 11, 2001, terrorist attacks against the U.S. The commission stated that the U.S. was unprepared for the attack of September 11, 2001. Part of the critical failures included a failure of imagination. The authorities tasked with protecting the nation had failed to put intelligence together, share and receive intelligence from our allies to provide a complete "picture" and think “outside the box.” The commission further stated that the government experts had failed to consider a civilian aircraft's viability as a highly explosive flying missile (The 9/11 Commission Report, 2004). The federal government had demonstrated a lack of imagination in its approach to acknowledging the threat posed

by manned aircraft and did not take action to counter the threat (The 9/11 Commission, 2004). This conclusion coincided with Ranson's conclusions when he detailed the French government's paralysis when confronted with UAS conducting overflights and even attacking one of its nuclear power plants.

In 2019, the first modern-day use of UAS to successfully attack a nation's critical infrastructure occurred in Saudi Arabia, the world's largest oil exporter. In 2017, it produced 12,000,000 barrels of petroleum products each day (U.S. Energy Information Administration, 2017). It possessed the second-largest oil reserves after Venezuela, which comprised 16 percent of the world's total (U.S. Energy Information Administration, 2017). The Saudi Aramco oil processing facilities, the world's largest, are located at Abqaiq and Khurais (U.S. Energy Information Administration, 2017).
The rebels in Yemen claimed that they had executed the attack in response to the Saudi Arabia support of the Yemen government (British Broadcasting Corporation, 2019). The rebels claimed that they had launched 10 UAS laden with explosives from Yemen. Still, U.S., Britain, and Saudi Arabian intelligence services claimed that the attack originated in Iran in two waves of over 25 UAS (Said, Malsin, & Donati, 2019). The attacks resulted in the closure of both facilities for repairs and reduced oil production by 50 percent (Said, Malsin, & Donati, 2019). The loss globally of five percent of oil production resulted in short-lived turmoil in the global financial markets (Said, Malsin, Donati, 2019). With billions spent on state-of-the-art air defense systems, none of those systems fired a single interceptor missile during the attack. Critics questioned the viability of modern air defenses against UAS or even swarms. The Saudi Arabian soldiers operating the air defense systems failed to engage a single target: their competency had been called into

question due to low readiness and training proficiency and being inattentive (Turak, 2019).

The successful attack caused governments to take notice. As for weapon platforms, swarms of UAS equipped with high explosives would get past modern-day air defenses and damage or destroy critical infrastructure. A massive unmanned aerial swarm would carry more explosives, more sensors to get the swarm to its target(s), and it would be far more likely to survive losses due to air defenses or system failure. The swarm would be scalable to a small size to attack a particular target or a larger size to attack a much larger target or even multiple targets. This flexibility would allow the aggressor nation to control the level of escalation it wished to demonstrate. The U.S. and other governments woke up to the possibility that terrorists could purchase a readily available commercial UAS and fly it into the engines of commercial or military planes. At the same time, they would remain safely hidden far away from the actual airport that they are attacking (Bunker, 2015).

In August 2018, two drones carrying explosives detonated above the forum where the President of Venezuela, Nicolás Maduro, was giving a speech (British Broadcasting Corporation, 2018b; Krieger & Faiola, 2018). This assassination attempt marked a significant change in the use of UAS as a means to topple governments by eliminating the head of state. Critics have suggested no assassination attempt; instead, it was a government operation designed to justify repression throughout the country (Krygier & Faiola, 2018).

Summary

For well over three centuries, theorists discussed the concept of national security. While many definitions differ, the fundamental core was transparent: a nation was responsible for recognizing a threat, present or emerging, and taking action to negate it as it continued to keep the security, safety, and prosperity of its citizens. Dating back to the Civil War era, balloons were used for manned surveillance of the enemy and unmanned bomb carriers. The Israeli Air Force demonstrated to the world the potential of UAS as devices of modern warfare. In doing so, they forever changed it.

The Nuclear Regulatory Commission security assessment to determine that UAS posed no threat to nuclear power plants was unusual since recent global events would suggest otherwise. The rapid advancement of UAS capabilities recently made a quantum jump, thanks primarily to the enhanced capabilities of artificial intelligence and the rollout within the U.S. of 5G networks. These two advancements now allow UAS to operate separate from human control, act and react on their own, and receive and transmit information faster. In this arena, international law was focused not on the specific instruments of warfare but rather on the legitimate government's lawful and legal consent for assistance by another nation.

A single UAS could successfully alter the fabric of our society. If it flew over a packed stadium or a nuclear power plant and dispersed chemical, biological, radiological, or nuclear material, it would fundamentally and forever change the U.S. just as the terrorist attacks on September 11, 2001, did.

Chapter 3: Research Method

The problem that this qualitative phenomenological study examined was the vulnerability of U.S. nuclear power plants to attack by the UAS capabilities, either with explosives or dispersing weapons of mass destruction payloads. The emergence of UAS was solely in the military domain for nearly four decades until entrepreneurs in China offered far smaller versions to the public (Kreis, 1990; Cohn, Green, Langstaff, & Roller, 2017). This vision resulted in a near monopoly by the Chinese, specifically Shenzhen Dà-Jiāng Innovations Sciences and Technologies Ltd., known worldwide as DJI (Schmidt & Vance, 2020). As of March 2020, DJI controlled 77 percent of the U.S. UAS market, and the next closest competitor was at four percent (Schmidt & Vance, 2020). The appetite of the public and private companies resulted in the birth of a new industry that was cheaper, more productive, and more efficient than the old methods, which were dependent upon human labor. Likewise, bad actors conceptualized ways to capitalize on this technology to reduce the threat from law enforcement to themselves. This continued progression of capabilities, size, payload, battery life resulted in the expanded use of UAS as an attack, transportation, and surveillance platform by bad actors. In this study, the qualitative research methodology and phenomenological design were selected because they were perfect for bringing the researcher closer to their study participants' perceptions. In this chapter, the following outline was adhered to: Research Methodology and Design; Population and Sample; Instrumentation; Study Procedures; Data Collection and Analysis; Assumptions; Limitations; Delimitations; Ethical Assurances; and a Summary.

Research Methodology and Design

This qualitative phenomenological purpose was to examine the vulnerability of U.S. nuclear power plants to attack by UAS. I chose a qualitative phenomenological research study methodology because the data collected would be based on the perception of key personnel in the nuclear industry. As such, I knew that it would be ideal for capturing the interviewee's perceptions, meanings, inferences, all subjective concepts vice an objective count, number, or measurement. The qualitative methodology was well-matched to collecting information regarding one's attitudes, the ability to examine complexities, gather an abundance of data, and identify patterns. A qualitative phenomenological research study examined participants' professional perspectives, opinions, and work experiences, allowing an informed examination of the phenomenon, which will not be constrained by time as are case studies. The phenomenological design would provide for the accumulation of data from multiple, highly experienced, educated personnel working in the nuclear industry or government. The specific phenomena at the center of this research study were based primarily on human perceptions and possibly real-world experiences. This research study had provided an understanding of human perspectives by observing an event and then describing the meaning of such events by the participants. This method was appropriate to address the security challenges that the Nuclear Regulatory Commission, Department of Homeland Security, and Department of Defense senior management officials and scientists. Lastly, there is an intentional effort by the federal government to hide information reference UAS overflights of all of its critical infrastructure facilities, not just nuclear power plants. Thus, there is a near-

complete lack of quantifiable information from which a researcher could conduct a quantifiable research study.

Population and Sample

The target population was a group of current or former nuclear industry and government employees. The population was highly educated and experienced federal employees and contractors. These individuals had been sworn to secrecy due to possessing some of the highest security clearances available. I chose this population because they are currently or were employees at U.S. nuclear power plants or support facilities as managers, scientists, or contractors. As this study is an unclassified document, I did not breach security clearance restrictions by delving into the classified arena and any other specific information in which they work or had worked. It is always ideal for an interview goal of 25 participants when conducting a qualitative phenomenological study (Creswell, 2018). I set an optimistic goal of 20 participants, despite the sensitivity of the vulnerability addressed and its apparent implications to national security. I relied heavily on snowballing and LinkedIn solicitation efforts to increase the number of participants. This strategy would provide an adequate number of participants, which would provide substantial data about the phenomenon and aid immensely to data triangulation and trustworthiness. These participants were purposive samples of current or former government employees or contractors supporting the U.S. nuclear industry or directly supporting nuclear power plants or facilities. This population maintained the highest security clearance available with special compartmentalized information access to nuclear material, including the specific facility capabilities, standard operating procedures within the industry and specific facilities, security

vulnerabilities, procedures, agreements, reports, and exercises. This elite segment of the general population was entirely appropriate as they were the best informed, educated, and experienced group of individuals to answer the primary and supporting research questions within this phenomenological study.

The purposive sample consisted of senior-level managers, scientists, and contractors who are or were employed at U.S. nuclear power plants or supporting facilities from U.S. federal departments and agencies. It also included individuals who were employed or still are at the state, local, territorial, and tribal echelons of government, the private sector, academia, and international organizations. The requirements for selecting participants was that one must be or have been in a senior management position, or a scientist or contractor supporting the Department of Energy with experience in the nuclear power plant field. The participants possessed computer science, physics, or nuclear specific degrees and had at least two years of experience. They were all willing to discuss their perceptions of the threat posed by UAS to U.S. nuclear power plants. My assurances of confidentiality and lack of interest in their demographic information convinced many participants to participate in this study. I kept the study, questions, answers, and discussion at an unclassified level, so at no time did any of the participants feel that I was attempting to compromise their security clearances. The pool of participants possessing multiple top-secret special compartmentalized access security clearances was small. Many of the participants expressed a reasonable fear of losing their job or security clearances to a research study that has not been sanctioned by the Department of Energy.

Instrumentation

The primary instrument that I utilized in this study were scripted questions. Furthermore, I used the same voice intensity, volume, and manner when I asked each participant the same questions during each of the 20 interviews. The interviews focused explicitly on soliciting participants' opinions directly related to the study's two research questions. The scripted interview questions had full Institutional Review Board committee approval. The questions provided a unique insight inside the perceptions of those that work or have worked in U.S. nuclear power plants and related facilities or support of them. The scripted interview questions are located in Appendix A. The interview process was a strictly scripted one and conducive for video interviews via Skype for Business, Microsoft Teams, or Zoom. I decided to guarantee each participant that I, as the interviewer, would provide confidentiality to the identity and position, either currently or in the past, of each of the participants. This guarantee would allow for a large amount of data to be collected quickly and would be inexpensive to conduct. Observation would provide first-hand information to participants via Skype, Zoom, or Microsoft Teams. It allowed for a degree of honesty on the part of the participants via behavioral observation. Using audio recording, I would be able to record the interviews and review the transcriptions for accuracy. I decided to use Otter premiere to transcribe the audio recordings into Word documents. This approach would prove to be efficient and effective, as well as a timesaver. There were no monetary incentives for any of the participants.

Study Procedures

After receiving approval from the Northcentral University Institutional Review Board, I reviewed all of the archived material and government documents that I had accumulated. Second, I initiated the participant recruitment process, which included utilizing LinkedIn. I am an employee of the Department of Homeland Security and already had leads on fellow employees who possessed the experience and expertise in this study's focus area. Third, I emailed the NCU Voluntary Consent Form to the participants, see Appendix B, before our scheduled interviews. Fourth, I scheduled one participant per day. While I envisioned the scripted conversation to take an hour, I set aside the remainder of the day if the interviews ran longer than anticipated, review the transcript, my notes, and consolidate the data into categories for analysis. By doing this, I was immersed in being completely focused on what had transpired with one participant for the entire day. All of the interviews were coordinated at a date and time convenient to the participant, and the audio was recorded. All participants agreed to have the audio of our interview recorded for transcription purposes. I strictly adhered to the scripted questions, but I also allowed the participants to talk for as long as they wished to do so and deviate. This strategy resulted in additional information that I found useful and interesting. This tactic uncovered additional facts, issues, or information that proved to be useful. Fifth, snowballing produced significant leads for additional participants. I reached out to these leads, and most were willing to participate in the study.

Per the Institutional Review Board's mandatory requirements for the safeguarding of participant information, I have secured all physical and electronic data to protect the identities of all twenty participants (Northcentral University, 2015). I have minimized the

risk of compromising confidentiality with all research materials by storing all study-related on an encrypted drive and storing it in a secure, sensitive facility. It will remain secured for 36 months following the completion of this study, after which I will destroy all of it.

Data Collection and Analysis

There were many methods of collecting qualitative data, but I used a combination of a review of archived documents, open-source documents, interviews, notes and field notes, direct observations, and a transcription of the recorded interviews. Access to archival records was severely limited, yet research was conducted through a limited ability to access archival records and documents. All of the unclassified material that I used was available online through access to the various federal government agencies, such as the Nuclear Regulatory Commission and the Department of Energy libraries.

The data collection occurred in a highly organized manner and was categorized, which helped analyze the participant's perceptions. I also factored in my observations of their behavior during the interviews. Coding was an essential tool in qualitative research because this particular research method was dependent upon gathering as much data as possible about a phenomenon to analyze it. I accomplished this by using the data provided by each participant to develop a list of answers which served as specific codes. I linked similar topics together and sorted the information into categories. I had to recode the data in a few instances (Creswell, 2018). The data analysis used transcriptions from the interviews, my notes from the interviews, and field notes from research conducted before the interviews based on archived and current material. I had intended to conduct a video interview with all of the participants, so observation of the participants, combined

with my review of archived documents and open-source document reviews, developed a holistic snapshot of the phenomenon. This plan occurred with eighteen of the twenty participants, while the other two were phone interviews. The data analysis explained why the phenomenon exists, evaluated its reason, and offered government strategies for negating the vulnerability. Thematic coding identified participant answers linked by a common theme, which allowed them to sort them into categories. Coding was based on observing the UAS phenomenon and supporting questions focused on the study's two main research questions. Coding occurred after the interviews had been concluded. The interview notes that I took greatly influenced the key to coding for this study. I frequently referred back to my two research questions to guarantee that the study was conducted in a thorough, honest, and transparent manner with the findings based solely on the data accumulated.

All of the data collected were reviewed, coded, and synthesized for common themes. NVivo 12 Pro proved to be well suited for performing qualitative data analysis as I prepared to publish the results of the study (NVivo, n.d.). NVivo provided a degree of intuitive analysis and visualizations and aided in the organization and qualitative data management from several sources (NVivo, n.d.).

The data were analyzed in a five-step process: familiarization, identifying a thematic framework, indexing, charting, mapping, and interpretation. Familiarization involved a detailed examination of the data while searching for ideas and themes. That information was categorized, which then allowed for rapid indexing and charting of the information to examine the data's dimension and characteristics. The mapping and interpretation synthesized and mapped the most critical aspects of the collected data.

Assumptions

The first assumption was that all participants would answer the questions asked of them during the interview truthfully and would be honest throughout our exchange. I did not know any of the participants personally, so I could not vouch for their integrity. I had no reason to suspect any of the 20 participants would be dishonest. I also did not believe that the government employees would attempt to alter this study's findings and conclusions by providing erroneous data. The second assumption of this study was that the participants would have preconceived notions, possibly based on media reports, personal experience, or work meetings. It was also entirely equally possible that the participants would have had preconceived notions, no prior experience, or any work-related discussions, thus were oblivious to the phenomenon at the heart of this study. They may have attended work meetings in which overflights by UAS were discussed, read work bulletins of incidents, or simply discussed the topic with fellow employees. A third assumption was that the sample group's inclusion criteria that I searched for would have almost assured me that some of the participants would have had experiences with the UAS phenomenon. The participants possessed years, in some cases, decades of experience. Thus, it was highly probable that some would have had experience with the phenomenon. A fourth assumption was that nuclear power plant security forces do not use UAS to patrol their facilities. This approach would allow rapid response and counter-surveillance to threats to the security of nuclear power plants. The responsiveness, efficiency, and low cost associated with operating UAS makes them ideal for sending out to conduct surveillance of an entire installation or segments of it. A fifth assumption was that there existed standard operating procedures at each nuclear power plant regarding

how their actions should they experience a UAS incident at their particular facilities. This assumption would provide study validation in that the threat posed by UAS was real and that procedures had been created for reacting to this specific threat. Presumably, steps would include notifying federal agencies and local law enforcement.

This study's credibility had been built upon the reader's confidence in how the data was collected, analyzed, and findings determined. To accomplish this, I intended to prolong the engagement of the participants during the interviews. The scripted interview questions were designed to generate useful discussion, honesty, and an avenue for discussing other phenomenon issues or items between the interviewee and myself. I conducted member-checking by offering to send each participant a transcript of the interviews once the transcription effort was complete and asked each to check for accuracy in capturing their experiences and opinions.

The transferability of the findings of the study would almost certainly have applicability to other contexts with the 16 sectors of the U.S. critical infrastructure paradigm and internationally. This applicability would be accomplished by a detailed description of the phenomenon to provide valid conclusions that could be equally applicable to other settings and critical infrastructure (Lincoln & Guba, 1985).

The study's dependability and the data, findings, and conclusions were developed to be repeatable. To accomplish this, I decided to refer this study to a fellow researcher for an external audit. I asked him to examine the process, the accuracy of the processes and the findings to ensure that they were objective and logical, which would confirm that the findings of the study were solely based on the information garnered from the participants and research material and not on researcher's bias (Lincoln & Guba, 1985).

Limitations

Limitations were common and affect all research studies, including this one. A qualitative method, such as phenomenology, does not generally lead to repetition. My intent was focused on eliminating or minimizing any limitations that would affect the repeatability of this study. The scripted interview was in an area of national security that was highly sensitive, and participants could have attempted to positively frame, or limit to a degree, their responses. An additional limitation would have been a small sample size. A larger sample was generally preferred. There were a limited number of exceptionally trained, experienced, educated personnel in possession of the top-secret security clearances necessary to work at such facilities. Most would be decline participation based on personal fears and beliefs. An additional limitation was the shortage of empirical data to support my research, which was intentional on the part of the federal government and the nuclear industry due to its apparent implications to national security and the stability of the nation's generation of a stable electrical grid. The generalization of conclusions drawn from the findings could have been a limitation. Once the participants were interviewed and the data analyzed, it became possible to extend the generality of the findings to operations with all 96 of the nuclear power plants currently in operation within the U.S. Additionally, they would even apply to other sectors of critical infrastructure with the U.S. and even globally (Congressional Research Service, 2020; Department of Homeland Security, 2013). The ability for generalization might even extend to the U.S. nuclear weapons complex. The National Nuclear Security Administration referred to this entity as the nation's Nuclear Security Enterprise, and it consisted of laboratories, production and assembly plants, a geologic waste repository,

and a testing facility (Congressional Research Service, 2020). This study's extent was focused solely upon U.S. nuclear power plants located on the East Coast of the U.S.

Delimitations

Delimitations kept the research goals from becoming too large to complete with a single research study. As a result of having defined the population of interest to this study, I quickly determined the criteria to exclude participants, i.e., non-federal government or contractors not employed in the nuclear industry or support organizations. This delimitation was chosen for practical purposes. I searched for a very specific strata of the general population that had been or was employed by the federal government in a capacity supporting nuclear power plants that would possess the first-hand experience with the phenomenon necessary to answer the two research questions. The following were the delimitations of this study.

The first delimitation were an assessment of the security of U.S. nuclear power plants. This study's focus was on the vulnerability of nuclear power plants to an attack by a UAS and not on the facilities' overall security to repel other forms of attacks, such as a ground attack, conventional aircraft, and seaborne systems. These alternate means of executing an attack were all outside the scope of this study.

The second delimitation were validation of U.S. nuclear power plants' security procedures or invalidating aspects of it about countering the threat posed by UAS. How the security personnel assigned to protect each nuclear facility react to an attack would be classified. If released in this study, it would detail precisely how the security forces would react to an attack. Bad actors could plan an attack by capitalizing on this information.

This particular field of study was of great personal and professional interest to me. I followed in my father's footsteps and decided to join the Army. I served for nearly three decades, and my area of expertise was air defense. I served in the Pentagon on 9/11 and was wounded when the plane impacted the building. In my personal and professional opinion, the subsequent investigations demonstrated a lack of serious attention to security shortfalls at the U.S. airports, which enabled the terrorists planned actions. I contend that the same laissez-faire approach has been repeated in the U.S. government's inaction with the present-day threat posed by UAS. In a background review of available literature, it was surprising how little relevant research had been performed in this arena of national security. Part of the answer may be due to the Nuclear Regulatory Commission's restrictive nature and uncooperative nature to share information. I desire to increase awareness, action, and further research in this arena that is directly related to the national security of the U.S. and its global nuclear energy producers.

Ethical Assurances

I confirm that this study proposal received approval from Northcentral University's Institutional Review Board before any data was collected. At no time did the study shift from an academic study into a government-based one. The risk of identifying the study participants was assessed as minimal. Still, because of the topic's sensitivity and the participants' security clearances and employment contingent on maintaining a top-secret security clearance, I guaranteed the confidentiality of their personal information before each interview occurred. Due to the study's implications for national security, the information shared by the participants, and all material, rights, and privacy, all data was secured at all times in a locked container in a secure facility and on an encrypted storage

device. This study's material will be maintained for thirty-six months following my successful dissertation defense before my committee, after which I will destroy the material.

Summary

This research effort examined the vulnerability of U.S. nuclear power plants to attack by UAS. Technological advancements in artificial intelligence combined with communication evolution had added to the threat that UAS posed to U.S. nuclear power plants and even to all 16 sectors of the nation's critical infrastructure. This qualitative phenomenological study allowed the researcher to develop an in-depth understanding of the phenomena from using a scripted interview to gain the perceptions of nuclear facility management and scientists vis-à-vis the evolving threat that UAS poses to nuclear power plants. This study's methodology was designed to be efficient and effective in determining the perceptions of a select sample of highly experienced, educated, and senior government officials, scientists, and contractors.

Chapter 4: Findings

The problem addressed in this study was a perceived vulnerability of U.S. nuclear power plants to attack by UAS. This qualitative phenomenological study's purpose was to examine the vulnerability of U.S. nuclear power plants against attack by UAS. This research study focused on two research questions: Research Question 1. To what extent do UAS pose a threat to U.S. nuclear power plants? Research Question 2. To what extent do actions need to be undertaken at U.S. nuclear power plants to counter the threat posed to them by UAS? The research framework was built around answering those two research questions. This chapter will address the study's approach, the trustworthiness of the data, credibility, transferability, dependability, results, findings, research questions supported by interview question data, evaluation of the findings, and the summary.

Approach. Each of the 20 participants was asked 15 in-depth, open-ended interview questions about their perceptions about the threat posed by UAS to U.S. nuclear power plants. Video conferencing via Zoom and Microsoft Teams allowed for visual observations of the participants. Due to the study's sensitivity and to alleviate participants' reluctance, I intentionally chose not to collect demographic data. This strategy proved reassuring and, combined with my guarantee of confidentiality and identification of each participant by an alphabetical letter, promoted open dialogue and honesty. The questions provided an opportunity for the participants to expand their responses to capture their perceptions, real and perceived, of the threat posed by UAS. The information was themed and coded using NVivo 12 Pro data analysis software (QSR International, 2020). Each interview was analyzed using codes and categories; then, upon

completing the analysis of all twenty interviews, all were analyzed across each other's codes and categories. This process produced themes from the data. An external audit was conducted to review the process of data collection and analysis. The interviews were conducted in August 2020 and were audio-recorded and later transcribed by using Otter software. After each interview, I immediately went through my notes and the Otter transcription to ensure 100 percent accuracy. I offered to conduct member checking with all twenty participants, but all declined my offer to review their transcript. A total of 14 participants mentioned in the post-interview dialogue that they had been nervous at the start due to concerns about the questions, but after they went through the interview, they felt very relaxed and did not feel that they had been asked about sensitive information nor made uncomfortable with the line of questioning. Before this study, there were no known research studies in this arena, principally due to the secrecy of the information of UAS incursions into and over U.S. nuclear power plants and other sectors of the U.S. critical infrastructure.

Trustworthiness of the Data

This study used a mix of interviews, documents, archival records, open-source documents, and participant observations to instill trustworthiness. Procedures to implement credibility, transferability, dependability, and confirmability were initiated before the data collection process ensured this study's trustworthiness. All participants were provided the informed consent form before 18 video conferencing interviews and two phone interviews. During each interview, I intentionally reviewed their consent and administrative requirements before commencing the interviews. Each interview was conducted in the same manner. Participants were asked the same questions, thereby

ensuring consistency. Participant trust was established before the interview when I stressed the lack of requesting demographic information on participants and explaining the value of their answers to the nation over the long-term. Participants consistently provided professional opinions and perceptions; some of the participants' personal experiences were directly tied to the study's two research questions. Data analysis was conducted precisely and consistently based on notes from teleconferencing and audio interviews, transcripts, field notes from direct interaction, and observations based on video interviews. NVivo Qualitative Analysis Software 12 Pro processed the raw data and produced thematic coding, themes, and analysis reports for credibility and trustworthiness (NVivo, 2020).

Credibility. To instill credibility that the research findings were comprehensive and well-developed, and to ensure that the findings were robust, I used various triangulation methods. First, I used methodological triangulation by utilizing two data collection methods: interviews and observations. Second, I used data triangulation by utilizing 20 participants and asking each the same questions in the same manner. Lastly, I used member-checking by sharing the known data, interpretations, and conclusions accumulated thus far with each participant after the interview had ended. I also offered each participant the opportunity to review the transcript of their interview afterward. This offer was an attempt to ensure that each participant clarified any potential misstatements, reflect their answers and intentions accurately and provide any additional information that they may have thought of after the interview had been completed.

Transferability. To instill transferability, I utilized a triangulation of sources. I used interviews of three different segments of the government and nuclear industry to garner

different perspectives and interviewed each on different days and times. Presumably, all were in private settings, but participants could have had their door open or had others nearby. This study's results and conclusions might be equally relevant, generalizable, and in similar contexts, transferable to nearly all of the 16 sectors of the U.S. critical infrastructure since they too are stationary and their locations are well-publicized and available via open sources on the Internet.

Dependability. To instill dependability, I chose a multi-faceted approach. My goal was to ensure that I established credibility, transferability, and dependability since confirmability would be a consequence of those actions. First, I utilized a research log and recorded ideas, preconceptions, and observations on the data collected after each interview. I also noted possible implications for further research, generalization to other critical infrastructure sectors, and applicability to global partners. Second, I requested an external audit by Dr. Mason Rice, an outside researcher, to check for objectivity in the data collection process and to assess researcher bias. Dr. Rice found that the data collection, analysis of the data gathered, and findings had been conducted objectively, and he did not find researcher bias.

Results

The results were organized to identify their relevance to the two research questions at the heart of this study. The study results were derived from the analysis of responses to 15 open-ended questions asked during the one-on-one interviews with 20 participants, field notes, and government documents. The current and former government employees were more aware of the processes to close their perception of U.S. nuclear power plants' vulnerability to attack. The scientists and contractors were more aware of

the threat that UAS posed, the impact of being attacked by a UAS swarm, and the likelihood of soft target damage from these attacks within the compound of the nuclear facilities.

The following was a breakdown of the participants: Participants D, L, and T were current government employees; Participants A, B, and M were currently employed as scientists; Participants C, F, and H were currently employed as contractors supporting the federal government; Participants O, P, Q, and R were retired government employees; Participants G, I, J, K, and S were retired scientists; and finally Participants E and N were retired contractors (see Table 2).

The 20 interviews were conducted between August 1 and 26, 2020. Each participant was asked the same 15 questions (see Appendix A) in the same manner. This approach supported the qualitative analysis of a phenomenological study, gaining information from 20 participants whose experiences and career choice provided the expertise and perceptions developed over many years to support this study's two research questions.

Table 2

Employment Dynamics of the Twenty Study Participants

Current Employees	**Former Employees**
Government – 3	Government - 4
Scientists – 3	Scientists – 5
Contractors – 3	Contractors - 2

Notes: Of the 20 participants, nine were current employees of the government or commercial nuclear industry; eleven were former or retired employees.

The qualitative methodological approach provided a means of gathering the perceptions of 20 experts in the nuclear field who had perceptions of U.S. nuclear power plants' vulnerability to attack by UAS. Once analyzed, the data provided three themes and four surprises, all of which directly related to both of this study's research questions. Each respondent was assigned a unique alphabetical identifier to ensure their confidentiality. Due to the sensitivity of the participants' information, no identifying information is included in the results.

Theme 1. The threat of one UAS attack or multiple UAS attacks against U.S. nuclear power plants was real.

Theme 1 arose from the answers given for the interviews and dialogue between researcher and interviewee arising out of questions and participants' answers. The answers to Interview Questions 1-10 supported this theme. This first theme directly answered Research Question 1 (To what extent do UAS pose a threat to U.S. nuclear power plants?) and was overwhelmingly supported by the participants' answers to multiple interview questions. A total of 17 participants succinctly answered that "the threat is real." Of the three do did not agree, one participant summarized their position by stating that "I don't believe that they are a threat today, but the technology is advancing so rapidly that they soon will be a threat."

All 20 participants agreed, and Participant C summarized the sentiments when he stated:

> UAS were conducting overflights of U.S. nuclear power plants regularly despite the Nuclear Regulatory Commission's best efforts to hide these incursions, but if

> the media were to get a hold of information that UAS had successfully attacked a nuclear power plant, it would result in the end of the nuclear industry as we know it!

Another participant articulated it for himself and others when he stated, "everyone in the nuclear power plant industry knows of UAS overflights because they are occurring more and more often. This is nothing new."

Participant B summarized the sentiments echoed by the other sixteen participants when he stated:

> The electrical structures carrying electricity away from the nuclear power plant, the spent fuel ponds, and the large pipes extracting water from the nearby water sources for use within the nuclear power plant is what I would expect an enemy to target and attack.

Another participant stated, "it would not take a lot of explosive material to bring down the electrical structure upon which the lines reside that take electricity away from the plants to our customers." Yet, another participant summarized other participant comments when he stated:

> I would focus on an attack on the large water pipes that bring water into the plant. While the reactor room is sealed, including its cooling water, the water extracted from the nearby river is used in many other areas of the plant. If this supply were cut off, it would shut down our operations.

Theme 2. **There has been an intentional effort for the secrecy of UAS incidents by the Nuclear Regulatory Commission.**

Theme 2 arose from the answers given for the interviews and dialogue between researcher and interviewee arising out of questions and participants' answers. The answers to Interview Questions 11-14 supported this theme. This second theme answered Research Question 2 (To what extent do actions need to be undertaken at U.S. nuclear power plants to counter the threat posed to them by UAS?) and was overwhelmingly supported by the participants' answers to multiple interview questions. When asked about the plant security personnel staying at their posts if UAS attacked them, one participant said that security "would remain at their post, possibly shelter in place." He also stated, "the nuclear power plant would continue to operate if it was attacked by UAS armed with conventional explosives." Another participant stated, "We are trained to operate during hurricanes and plant issues with the reactors. Dropping hand grenade sized explosives will not change how we perform our jobs." The perception of a highly dedicated and professional security force manning their posts in the event of an attack ended when the question moved from conventional explosives to payloads of chemical, biological, radiological, and nuclear material. If attacked by UAS dispersing chemical agents, 15 participants felt the plant security personnel would not remain at their post; 14 security personnel would not remain if biological agents were dispersed; 13 participants felt security personnel would not remain if radiological agents were dispersed; finally, 18 participants did not believe that security personnel would remain if nuclear agents were released. One participant articulated the sentiments of his fellow participants when he stated, "as soon as chemical, biological, radiological, and nuclear agents are dropped on us, it is game over!" All twenty participants agreed that the dispersion of a chemical, biological, radiological, or nuclear agent would be an

escalation by the terrorists. The only force trained for it would be the nation's military forces.

When asked about engaging UAS, one participant summarized the sentiments of this group best when he said, "we are not equipped, trained, resourced, or legally allowed to engage UAS overflights. They will only continue in number and frequency until either Congress wakes up or a plant is attacked." The perception of all 20 participants was that a UAS swarm attack's viability was a more significant present-day threat. Participant A summarized the sentiments of the group best when he stated, "no-one is going to attack with 1or 2 drones when you can send a swarm to annihilate us. That is what I would do if I were going to attack our plant."

Theme 3. **There was much that the federal government could do to counter the threat of UAS attacks.**

Theme 3 arose from the answers given for the interviews and dialogue between researcher and interviewee arising out of questions and participants' answers. The answers to Interview Question 15 supported this theme. This third theme answered Research Question 2 (To what extent do actions need to be undertaken at U.S. nuclear power plants to counter the threat posed to them by UAS?) and was supported by the participants' answers to multiple interview questions.

When the participants were asked about the strategies that the federal government could undertake to reduce the threat of an attack by UAS, four participants believed that congressional involvement and oversight was necessary to address the present-day vulnerabilities of nuclear power plants attack by UAS. One of those participants summed it up when he stated, "Congress is in bed with the nuclear industry. Their re-election

campaigns always need funding. That is the only answer to the non-action to this threat." Another four participants perceived that legislative changes were necessary, and their sentiments were summarized when one stated:

> Congress is probably receiving kickbacks from the nuclear industry and are intentionally not looking into the threat posed by UAS nor UAS incursions because the Nuclear Regulatory Commission is telling them that there is no problem. If Congress got involved and if the Nuclear Regulatory Commission's leadership were held responsible, things would change immediately.

An additional four participants perceived that the Federal Aviation Agency must redefine their definition of a UAS as they are currently defined as aircraft and legally assume identical protections that small aircraft and passenger jets receive. One participant summarized it best for these four when he stated, "as long as UAS are considered the legal equivalent of aircraft, no-one can do anything to stop them at the facility, at our homes, anywhere unless we want to go to prison for bringing down an aircraft in flight."

Research Question 1. To what extent do UAS pose a threat to U.S. nuclear power plants?

The answers to Interview Questions 1-10 during the one-on-one interviews support Research Question 1. They will follow in chronological order.

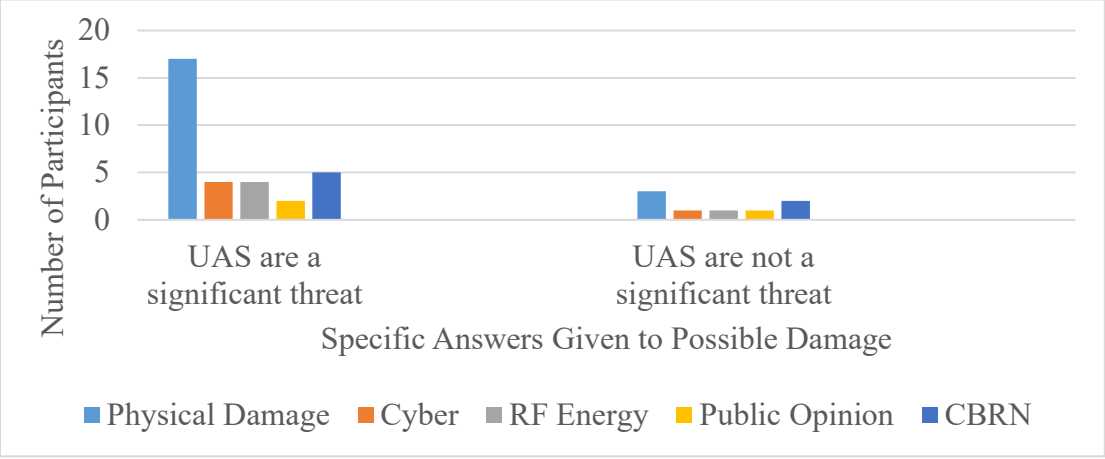
Interview question 1: What is your perception of the threat posed to U.S. nuclear power plants by a UAS? Please explain.

Participants A, B, C, D, E, F, G, H, I, J, K, L, M, N, O, S, and T (17) answered that their perception of the threat posed by UAS was that the threat was real and could inflict physical damage; Participants P, Q, and R (3) did not share that perception at

present. Of the three, Participant P stated, "the technology is advancing so rapidly that they will be a threat soon." Participants Q and R echoed the perception and sentiments stated by Participant P. Participants A, B, C, D, E, F, G, H, I, J, K, L, M, N, O, S, and T (17) believed that physical damage to the nuclear facility was a real possibility; Participants P, Q, and R (3) perception was again best summarized by Participant P when he stated, “physical damage to the nuclear facility was not a probability due to the limited payload capacity of modern-day UAS." Participants A, B, M, and T (4) perceived that UAS could also serve as platforms from which a bad actor could initiate a radiofrequency (RF) or cyber-attack against the nuclear facilities that it was targeting (see Figure 1). Radio waves and microwaves could quickly be emitted by an antenna on an aircraft or UAS and were one form of electromagnetic energy, referred to as RF energy. A burst of RF energy aimed at nuclear power plant sensors, communications, alarms, and other electronic devices could disable them. A cyber-attack could infect the software operating

Figure 1

Perception Of The Threat Posed by UAS



Note: The data was gathered through one-on-one interviews with 20 respondents.

systems of the plant. Operating systems could still be infected by sloppy employees who chose not to abide by the security standards and rules established by the commercial company that owns and operates the nuclear power plant.

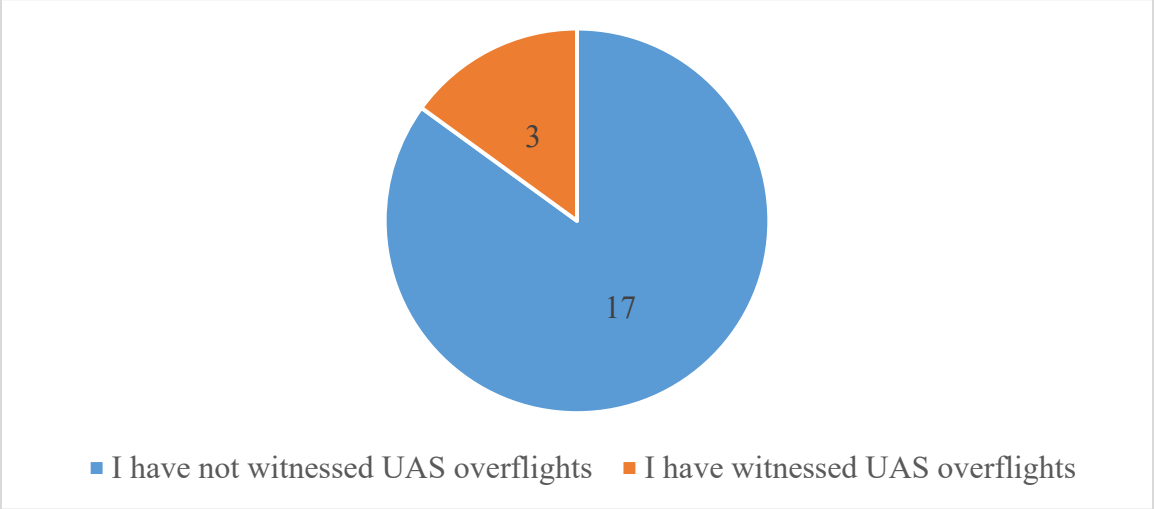
Participants J and S (2) mentioned that public perception was of significant importance to the nuclear industry and the federal government. Even if the damage from a UAS attack was negligible, these two participants perceived that the larger issue would be the media getting hold of the story and the subsequent effect on the American public's perception. The perceptions of the two were best stated by Participant J when he stated, "if the media were to get a hold of information that UAS had successfully attacked a nuclear power plant, it would result in game-over for the industry!" This last point was entirely dependent on media coverage or filmed attacks posted on the worldwide web. The first point would generate far more interest and outcry than the latter, which the federal government would argue was manufactured. Participants P, Q, and R (3) did not perceive a threat of damage by a UAS attack. Participant A perceived an RF attack possible, while Participant B perceived that cyber was a threat.

Interview Question 2. Do you have experience with UAS conducting overflights or other maneuvers over nuclear power plants? Please explain.

A total of 17 participants answered that they did not have personal experience with a UAS conducting overflights of their U.S. nuclear power plants. Participant G, M, and T (3) had personally witnessed overflights of U.S. nuclear power plants and other sectors of the U.S. critical infrastructure facilities (see Figure 2). Participant G summarized the perception and sentiments of the three best when he stated, "everyone in

Figure 2

Experience with UAS Overflights



Note: The data was gathered through interviews with 20 respondents.

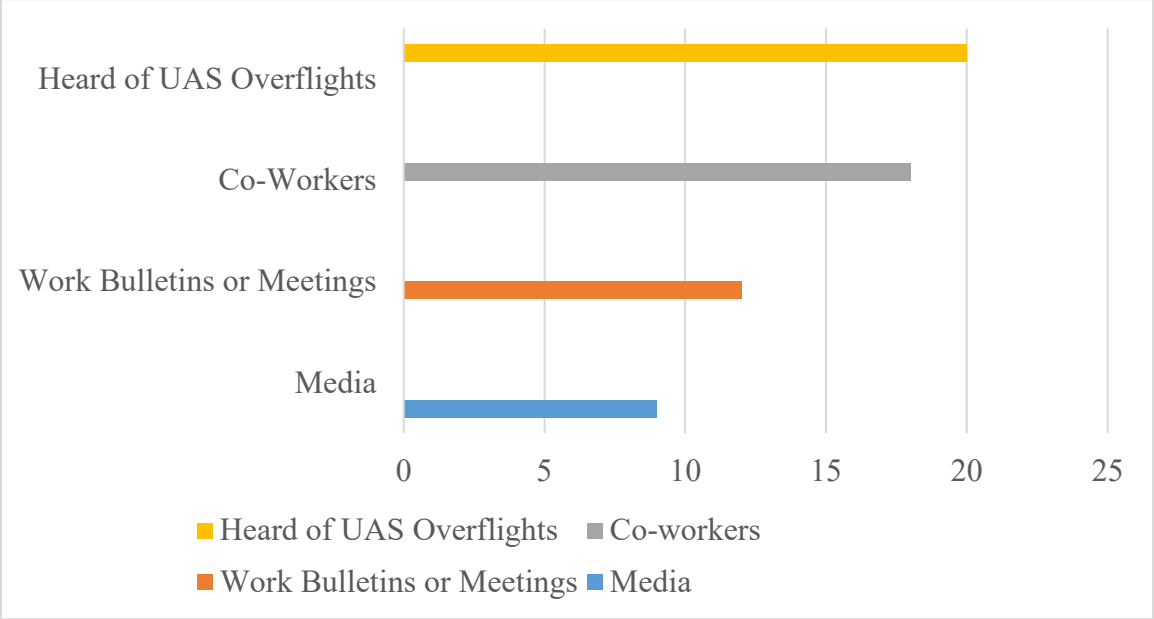
the industry knows that we have UAS overflights all the time. No-one talks about it publicly because we have been ordered to keep our mouths shut."

Interview Question 3: Have you heard of UAS overflying nuclear power plants? Please explain.

All 20 participants had heard of incidents of nuclear power plant overflights by UAS. All but participants C, L, and O (3) had heard of unmanned aerial incidents from co-workers; Participants D, F, G, H, K, L, N, O, Q, R, S, and T (12) had gained knowledge from work bulletins or meetings and co-workers; lastly, Participants A, B, C, D, E, F, G, J, K, O, and T (11) had heard of incidents via the media (see Figure 3). Participant C best articulated it for himself and J and P when he stated, "everyone in the nuclear power plant industry knows of UAS overflights because they are occurring more and more often. This is nothing new."

Figure 3

Knowledge Of UAS Overflights



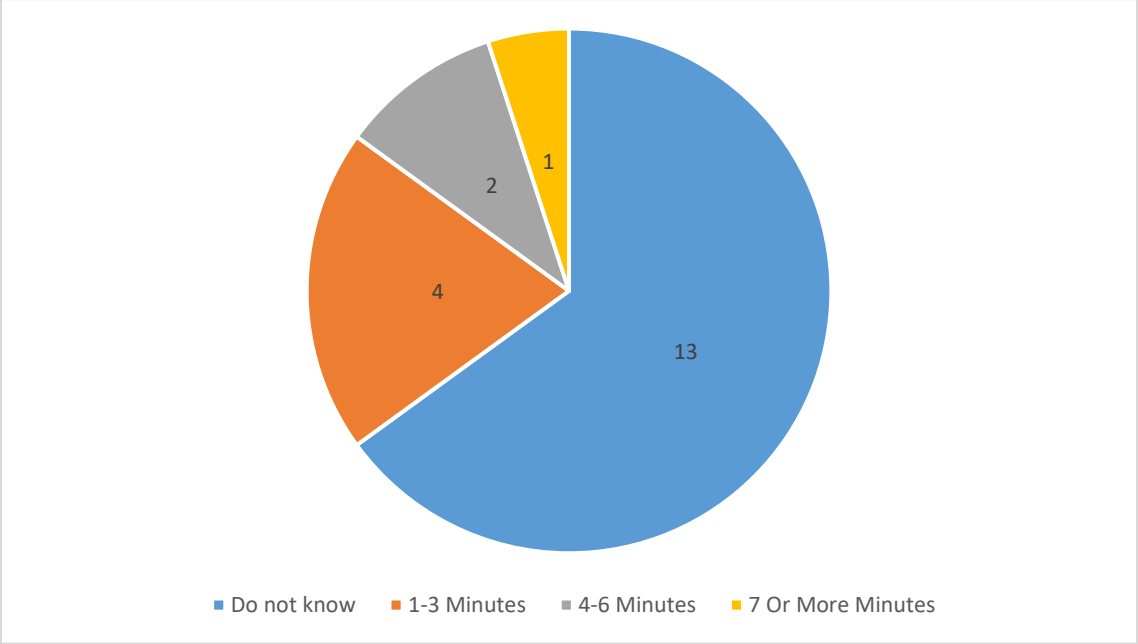
Note: The data was gathered through interviews with 20 respondents.

Interview Question 4: If so, how long did the UAS fly over the facility? Please explain.

Participants A, B, C, D, F, G, I, K, N, O, P, Q, and R (13) did not know how long the overflights by UAS lasted. Participants E, H, J, and L (4) had heard that the UAS flew over the nuclear power plants for approximately one to three minutes; Participants S and T (2) heard that the overflights lasted an estimated approximately four to six minutes, and Participant M (1) heard that the flight lasted for more than seven minutes. All of the answers given for the duration of the overflights were entirely based solely on the information shared with them by co-workers, work meetings, or bulletins, or via the media (see Figure 4). Participant E made a comment that accurately summarized the

Figure 4

Knowledge Of The Duration Of UAS Overflights



Note: The data was gathered through interviews with 20 respondents.

statements made by all 20 participants who had heard of but did not know the duration of the overflights when he stated:

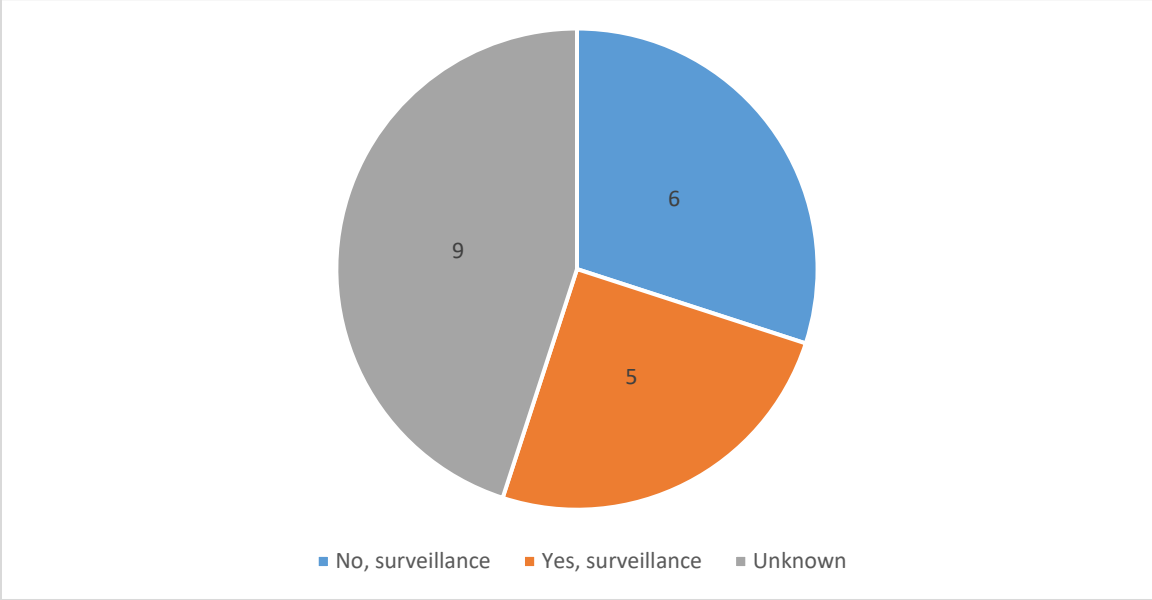
> The duration of the drone overflights isn't as important as the mere fact that they are overflying our nuclear facilities at will, and we are not doing anything about it. The Nuclear Regulatory Commission knows this too and is being quiet about it.

Interview Question 5: Did the UAS perform any threatening behavior? Please explain.

Participants D, E, H, J, L, M, P, S, and T (9) stated that they could not characterize the overflights of UAS as threatening or not. Participants A, B, C, F, G, and I (6) perceived that the UAS conducting overflights were conducting surveillance, but this

Figure 5

UAS Performing Threatening Behavior



Note: The data was gathered through interviews with 20 respondents.

did not constitute threatening behavior in their opinions. Participants J, K, N, O, and R (5) perceived that the UAS overflights were also conducting surveillance, but this *did* constitute threatening behavior (see Figure 5). Of the five, Participant N summarized this best when he stated, “based upon my time in the military, surveillance is an intelligence-gathering process that serves as a prelude to an attack at a later date and time."

Interview Question 6: Have you heard of such incidents from co-workers or discussed the perception of the threat posed by UAS to nuclear power plants? Please explain.

All 20 participants had heard of UAS incidents at their work locations. All 20 had discussed the threat that UAS posed to their facilities with co-workers (see Figure 6). Participant R summarized the comments from all twenty participants when he stated:

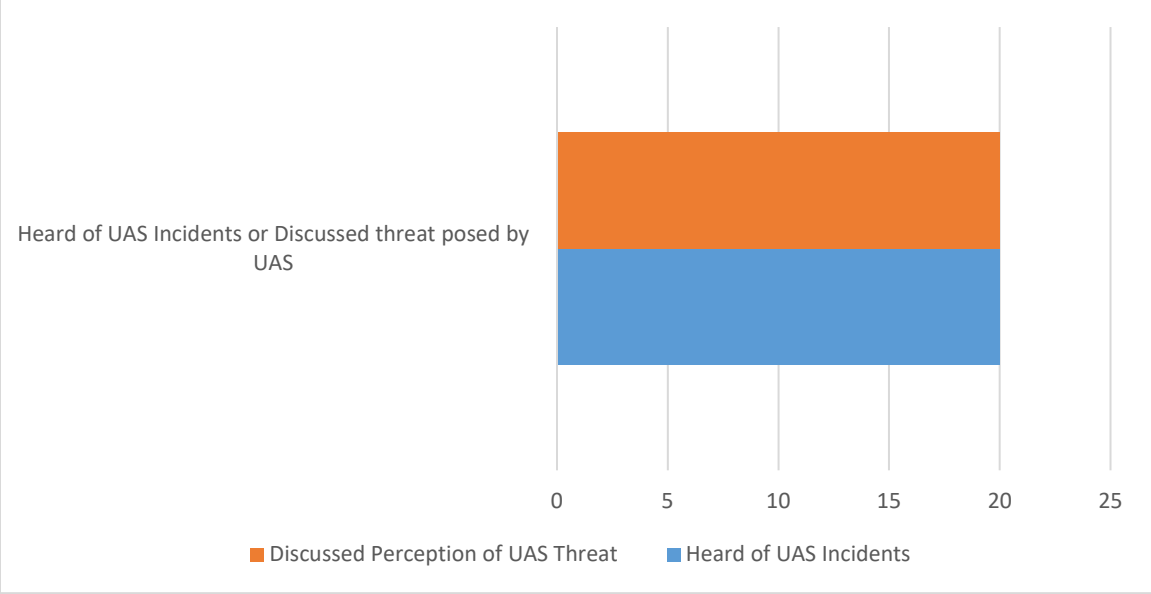
Employees discuss this phenomenon all the time, but we do it privately because if our supervisors heard us, we would be in trouble. Despite the company's best efforts, people will always behave similarly. When feeling threatened, employees will discuss the problem, perceived or real, with their co-workers.

Interview Question 7: Do you believe that UAS could successfully execute an attack on nuclear power plants? Please explain.

All 20 of the participants' perceptions' were that UAS could successfully execute an attack against a nuclear power plant. Participants G, M, and T (3) perceived that the focus of their attack would be against a hardened facility within the nuclear power plant, such as the nuclear reactor building itself. The perceptions of the remaining 17 were that

Figure 6

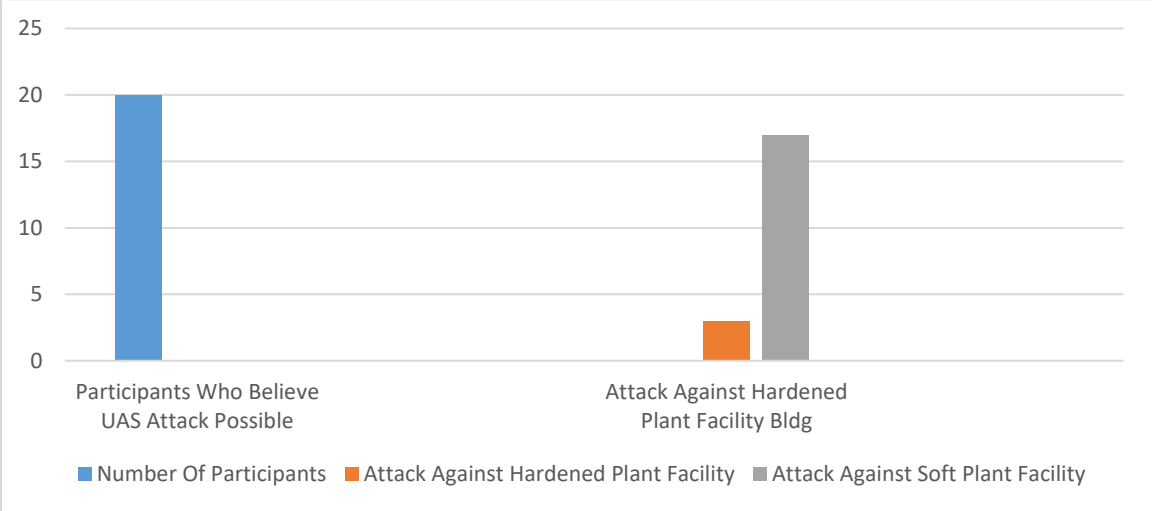
Awareness Of UAS Incidents



Note: The data was gathered through interviews with 20 respondents.

Figure 7

Plant Attack By A UAS



Note: The data was gathered through interviews with 20 respondents, and two questions were answered in this figure.

the target of such an attack would be focused on soft targets (see Figure 7). Participant S summarized the sentiments echoed by the other 16 participants when he stated:

> The electrical structures carrying electricity away from the nuclear power plant, the spent fuel ponds, and the large pipes extracting water from the nearby water sources for use within the nuclear power plant is what an enemy would target and attack. It would not take a lot of explosive material to bring down the electrical structure upon which the lines reside that take electricity away from the plants to our customers.

Participant Q best summarized other participant comments when he stated:

> I would focus on an attack on the large water pipes that bring water into the plant. While the reactor room is sealed, including its cooling water, the water extracted

> from the nearby river is used in many other areas of the plant. If this supply were cut off, it would shut down our operations.

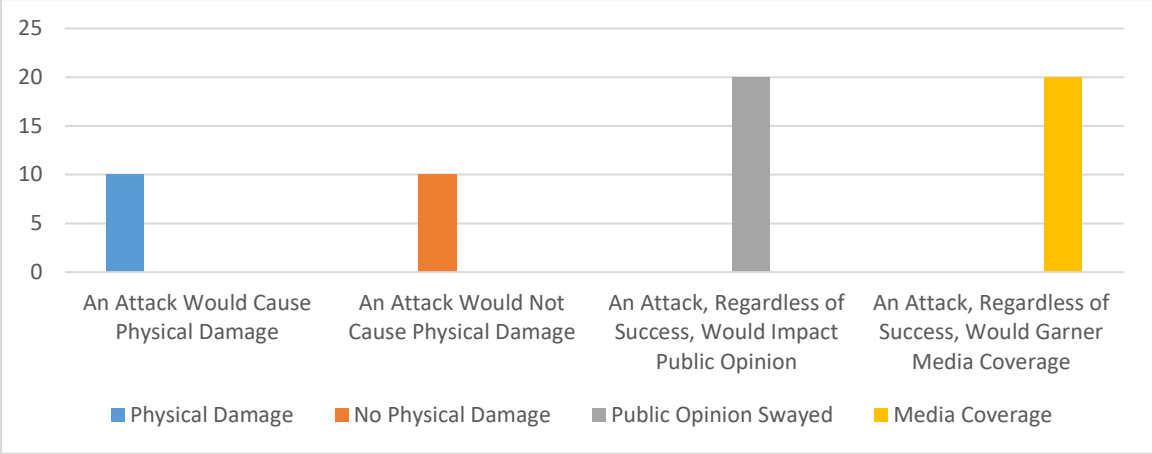
Interview Question 8: Do you believe that such an attack would shut down operations at the facility? Please explain.

Participants A, B, C, D, E, J, K, M, N, and O (10) perceptions were that a UAS attack would cause physical damage at a nuclear power plant and result in a shut-down of operations. The other half of the participants' perception was that no physical damage would be incurred, and the plant would continue to operate. All 20 participants perceived that public opinion would be impacted, but with a caveat that it would only occur if the UAS attack resulted in significant damage or if the incident were brought to the public (see Figure 8). All 20 of the participants' perceptions were best summarized by Participant A when he stated:

> If there was a drone attack, there would surely be media coverage. If the incident was brought to the attention of the public or if the public were made aware of the attack due to the widespread damage, it would most likely have had to have been the result of a highly successful attack resulting in widespread devastation or a complete loss of electrical production from that facility. There is no way that the Nuclear Regulatory Commission could cover that up. If an attack were to occur and word got out to the American public, it would be likely that the nuclear power industry's future would hang in the balance.

Figure 8

UAS Attack Results In A Plant Shutdown



Note: The data was gathered through interviews with 20 respondents.

Interview Question 9. Do you believe that the threat of attack by a UAS armed with conventional explosives is a viable one? Please explain.

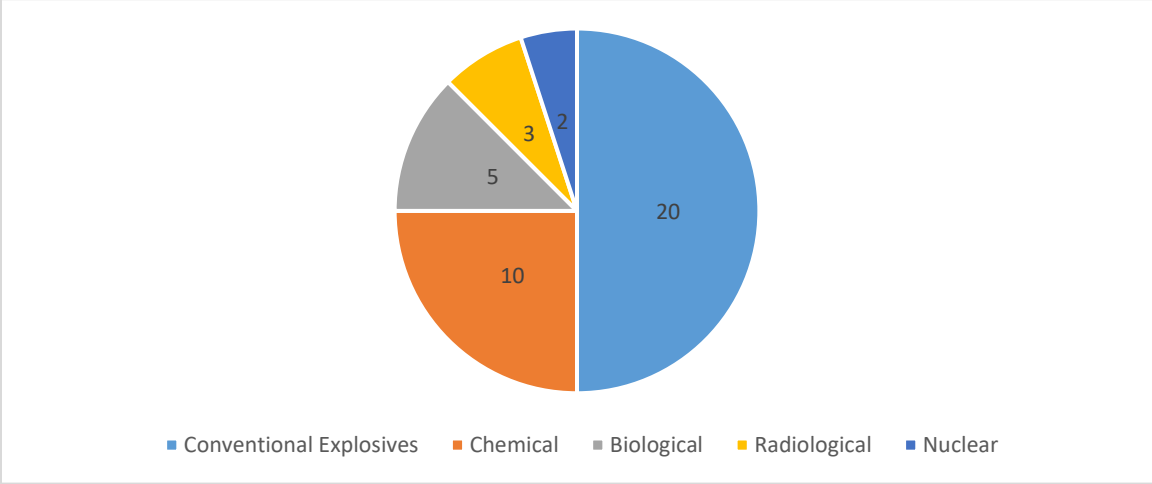
Interview Question 10. What are your views about the viability of a UAS attack that is dispersing chemical, biological, nuclear, or radiological agents over a nuclear power plant?

The data from questions 9 and 10 were combined in Figure 9. All 20 participants' perception was that a UAS attack using conventional explosives against a nuclear power plant was viable (see Figure 9, right half of the pie chart). Participant A captured the sentiments of the 20 participants best when he stated, “drones buzz nuclear power plants all the time. There is nothing that we can do to stop an attack should we get attacked.”

When the question was changed from conventional explosives to chemical, biological, radiological, and nuclear agents, the answers provided were varied (see Figure

Figure 9

UAS Attack Agents



Note: The data was gathered through interviews with 20 respondents; the right side addresses question 9, the left side question 10.

9, left half of the pie chart). The perception of participants A, B, D, F, G, H, M, P, R, and S (10) was that an attack by UAS dispersing chemical agents would be successful. Participants E, I, N, O, and T (5) combined perception because an attack by UAS dispersing biological agents would be successful. The perception of participants C, J, and S (3) was that an attack by UAS dispersing radiological agents would be successful. Finally, the perception of participants K and L (2) was that an attack by UAS dispersing nuclear agents would be successful (see figure 9). Participant C summarized the sentiments of 10 participants when he stated that, "we are trained for a radiation leak from the plant, but not for an attack by aircraft or UAS dispersing chemical, biological, radiological, and nuclear material over the plant." Out of the same 10 participants, participant A summarized it best when he commented:

> In my view, I think if we determined quickly that chemical, biological, radiological, or nuclear was being dropped on us, there would be widespread terror. I'd head home to get out of the danger area and to take care of my family. I would figure that the country was under attack similar to 9/11.

Again, out of the same ten participants, participant B stated:

> We are a bunch of civilians, not the military. We do our job because we are paid well to do them, not because we are willing to die for our country like the military. Suppose we were threatened with chemical, biological, radiological, and nuclear agents. In that case, I think that there is a good chance that the majority of the workforce not employed inside the reactor's control room would head home or for the hills.

Finally, out of the same ten participants, participant M commented, "I do this for the pay and benefits. I am not here to die for my company."

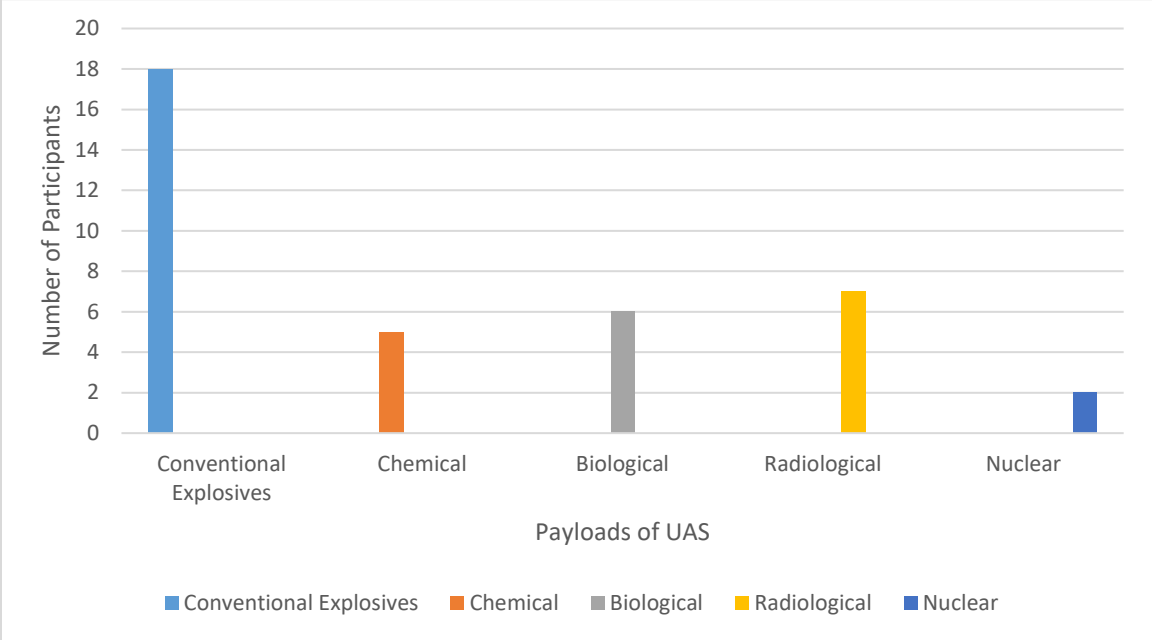
Research Question 2. To what extent do actions need to be undertaken at U.S. nuclear power plants to counter the threat posed to them by UAS? The answers to Interview Questions 11-15 support Research Question 2. They will follow in chronological order.

Interview Question 11. What would the personnel operating a nuclear power plant do if they were informed that the facility was under attack by a UAS? Please explain.

Interview Question 12. What would employees do if it was determined that a UAS was dispersing chemical, biological, nuclear, or radiological agents over the facility? Please explain.

Figure 10

Facility Employees Continue To Operate The Plant If Attacked



Note: The data was gathered through interviews with 20 respondents. All 20 responded to the question about conventional explosives, but the numbers who felt that the security forces would remain dropped when asked about chemical, biological, radiological, and nuclear agents.

The data from questions 11 and 12 were combined in figure 10. The perception of participants A, B, C, D, E, F, G, H, I, J, L, M, N, O, P, Q, R, and S (18) were that plant employees would remain at their post, possibly shelter in place and ensure that the nuclear power plant continued to operate if it was attacked by UAS armed with conventional explosives. Participant H summarized this group's sentiment best when he stated, “we are trained to operate during hurricanes and plant issues with the

reactors. Dropping hand grenade sized explosives will not change how we perform our jobs.” Participants K and T (2) 's perceptions were that employees would not remain at their posts if the nuclear power plant were attacked by UAS armed with conventional explosives.

The perception of a highly dedicated and professional security force manning their posts in the event of an attack ended when the question moved from conventional explosives to payloads of chemical, biological, radiological, and nuclear material (see Figure 10). The perceptions of participants A, B, I, S, and T (5) were that facility employees would remain at their posts if it were to be determined relatively quickly that the UAS attack was dispersing a chemical payload, while Participants C, D, E, F, G, H, I, J, K, L, M, N, O, P, Q, R, and S (15) did not. The perceptions of participants A, B, I, R, S, and T (6) was that plant employees would remain at their posts if the facility were attacked with biological payloads, while Participants C, D, E, F, G, H, I, J, K, L, M, N, O, P, Q, R, and S (14) did not. Participants A, B, I, I, K, R, S, and T (7) perceived that plant employees would remain at their posts if attacked with radiological payload, while Participants C, D, E, F, G, H, J, L, M, N, O, P, and Q (13) did not. Finally, the perceptions of participants R and T (2) were that plant personnel would remain at their posts if they discovered that the attack involved nuclear material, while the other 18 participants did not. These results were best articulated by Participant L when he said, “as soon as chemical, biological, radiological, and nuclear agents are dropped on us, we are at war!”

The stark difference in the perceived confidence of the participants in the plants' security force can be attributed to the relatively “new use” of unconventional

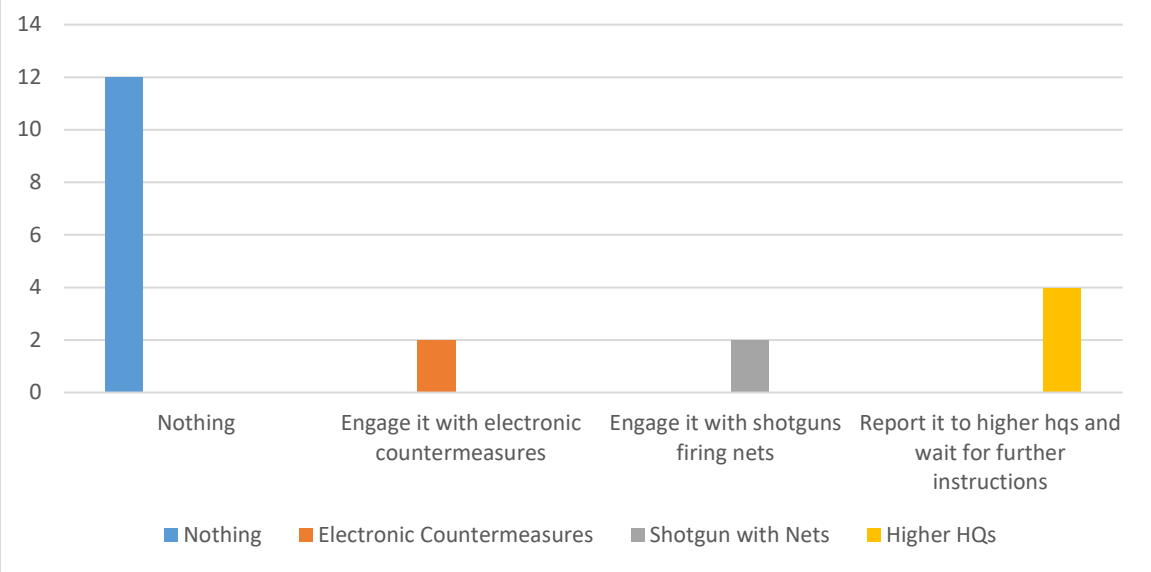
agents upon targets within the U.S. None of the participants could not speculate on the likelihood of whether bad actors could access within the U.S. or sneak into the country chemical, biological, radiological, or nuclear agents for use in UAS attacks. Yet, all agreed that it would be an escalation in terrorism and that the plant security force was not trained for dealing with chemical, biological, radiological, and nuclear attacks.

Interview Question 13. What could a U.S. nuclear power plant do to stop an attack by a UAS? Please explain.

The perception of participants A, B, C, D, G, H, I, K, N, P, R, and S (12) was that there was nothing that the security personnel at a nuclear power plant could do if UAS attacked it. Participant A summed up the sentiments of this group best when he said, "we are not equipped, trained, resourced, or legally allowed to engage UAS

Figure 11

Actions If Attacked By A UAS



Note: The data was gathered through interviews with 20 respondents.

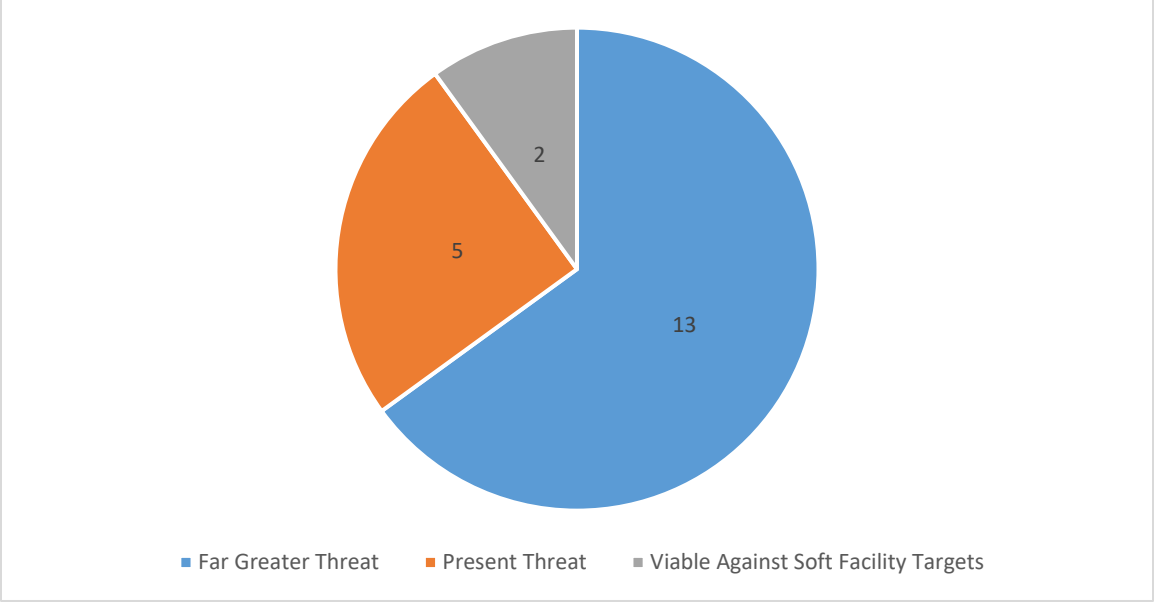
overflights. They will only continue in number and frequency until either Congress wakes up, or a plant is attacked." Participants E and F (2) perceived that the plant personnel possessed and were authorized to engage UAS with electronic countermeasures (i.e., jamming the offender). Participants J and T (2) perceived that the plant security personnel possessed the ability to engage UAS with shotguns firing nets. Finally, Participants L and M (2) perceived that the plant security personnel would only report it to higher headquarters and await further guidance (see Figure 11).

Interview Question 14. What do you think of the viability of an attack by a swarm of UAS? Please explain.

The perception of all 20 participants was that a UAS swarm attack's viability was a more significant present-day threat. Participant A summarized the sentiments of

Figure 12

Attack Potential By A UAS Swarm



Note: The data was gathered through interviews with 20 respondents.

the group best when he stated, “no-one is going to attack with one or two drones when was a more significant present-day threat. Participant A summarized the sentiments of the group best when he stated, “no-one is going to attack with one or two drones when you can send a swarm to annihilate us. That is what I would do if I was going to attack our plant.” Participants A, B, G, S, and T (5) perceived that it would be a far greater threat than a single or multiple UAS attack. Participants F and J (2) perceived that an attacking swarm of UAS would be successful only if the plant facility's soft targets were the targets (see Figure 12).

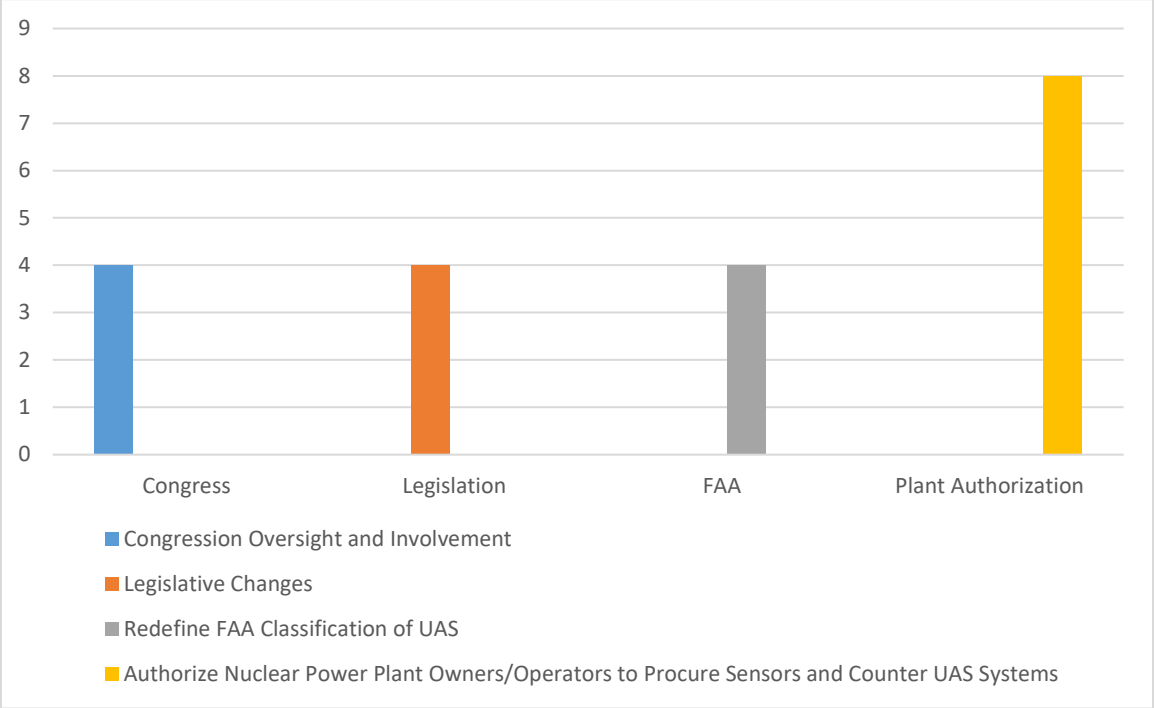
Interview Question 15. Are there strategies that the federal government could undertake to reduce the threat of an attack by UAS? Please explain.

Participants L, R, S, and T (4) perceived that congressional involvement and oversight was necessary to address the present-day vulnerabilities of nuclear power plants attack by UAS. Participant R summed up these four sentiments when he said that “Congress is in bed with the nuclear industry. Their re-election campaigns always need funding. That is the only answer to the non-action to this threat.” Participants C, F, G, and O (4) perceived that legislative changes were necessary. These same four shared the sentiments that were best articulated by Participant F when he stated:

> Congress is probably receiving kickbacks from the nuclear industry and are intentionally not looking into the threat posed by UAS nor UAS incursions because the Nuclear Regulatory Commission is telling them that there is no problem. If Congress got involved and if the Nuclear Regulatory Commission's leadership were held responsible, things would change immediately.

Figure 13

Federal Strategies To Reduce The Threat Of UAS Attack



Note: The data was gathered through interviews with 20 respondents.

Participants K, L, R, and T (4) perceived that the Federal Aviation Agency must redefine its definition of a UAS. They are defined as aircraft and legally assumed identical protections that small aircraft and passenger jets received. Participant T summarized it best for these 4 when he stated, "as long as UAS are considered the legal equivalent of aircraft, no-one can do anything to stop them at the facility, at our homes, anywhere unless we want to go to prison for bringing down an aircraft in flight." Lastly, Participants A, B, D, G, L, M, P, and Q (8) perceived that the owners and operators of the nuclear power plants needed the authorization to procure sensors to detect approaching UAS and counter systems to engage and stop them if necessary (see Figure 13).

Evaluation of the Findings

The three themes that came out of the analysis of the data collected via interviews, archive files, documents, and observations directly supported answers to the study's two research questions:

Research Question 1: To what extent do UAS pose a threat to U.S. nuclear power plants?

Research Question 2: To what extent do actions need to be undertaken at U.S. nuclear power plants to counter the threat posed to them by UAS?

Theme 1: The threat of UAS attack against U.S. nuclear power plants was real and was overwhelmingly supported by the participants, both in their answers to the interview questions and in open dialogue. France has maintained a favorable public opinion on its dependence and use of nuclear power plants to produce 75 percent of its electrical requirements despite Greenpeace's efforts to film UAS "attacks" and repeated overflights of their nuclear facilities (Tran, 2018; Ranson, 2017). All 20 participants perceived that the media would be involved if the attack was successful and word got out despite government efforts to hide it.

Theme 2: There has been an intentional effort for the secrecy of UAS incidents by the Nuclear Regulatory Commission, which was entrenched in the statements of the participants, but when they were asked to elaborate on their beliefs of secrecy, they did not have any examples of proof, just their professional and personal opinions. The perceptions of the 20 participants encompassed those of multiple managers, scientists, and contractors. It was employees' perceptions, many of whom have decades of experience in their present or past nuclear industry-related jobs. All 20 participants

perceived that public opinion was critically important to the nuclear industry, yet, this could change quickly should there be a loss in confidence in the federal government and in the owners and operators of nuclear power plants to secure their facilities against UAS attack. A total of 15 participants confided that they knew that the Nuclear Regulatory Commission was aware of UAS overflights and incursions into the restricted space above U.S. nuclear power plants. These 15 felt that the Nuclear Regulatory Commission was intentionally withholding the data of these incidents.

The participants' data indicated that the government was purposely ignoring the threat and that nothing was being done to deal with U.S. nuclear power plant vulnerabilities to UAS. Many had personal opinions about the cause of the reluctance, but half of the participants perceived an intentional desire by the Nuclear Regulatory Commission to withhold acknowledgment of the threat posed by UAS. At the time of this document's writing, the owner and operators of U.S. nuclear power plants were precluded by the Nuclear Regulatory Commission from purchasing sensors and counter UAS technology. To close this vulnerability, Participant A captured the sentiment of many of the participants when he said, “it will take a multi-faceted approach to solve this. Better now before we are attacked than after we have been attacked, and radiation exposure is widespread.”

Theme 3: There was much that the federal government could do to counter the threat of UAS attacks. While the 20 participants had different thoughts on how the government could counter the threat, all believed that the government could counter the threat of UAS attacks before they were imminent. The majority of the participants perceived that Congress should get involved, and nothing would change until it did.

Others believed that legislative changes were necessary to enact change. Finally, some believed that the Federal Aviation Agency needed to alter the legal definition of UAS if a change was to occur. The Federal Aviation Administration classified UAS as aircraft. Therefore, all law enforcement and civilian attempts to engage UAS for any reason (i.e., even if the UAS was loitering over one's property, flying over crowded stadiums, and over parades) would be against federal laws and various legal codes, resulting in possible punishment by imprisonment for up to twenty years (Federal Aviation Administration, 2020). The 1984 Aircraft Sabotage Act made it a felony to damage or destroy any aircraft, manned or unmanned (18 U.S. Code § 32, U.S. Congress, 1984).

The participants who believed that Congress and legislative changes were needed were best expressed by Participant R, who best represented the government bureaucrats. He stated:

> Government employees know precisely how to close the vulnerability of nuclear power plants to attack by UAS. We would force Congress to get involved through press releases, opinion pieces while highlighting the threat posed to nuclear power plants by UAS.

After analyzing the participants' answers and my notes, I was surprised by four findings that I was not expecting. First, six participants who had been employed at U.S. nuclear power plants, some for decades, believed that the nuclear facilities where they had worked, possessed counter UAS technologies and were authorized to use the technology against those UAS that displayed hostile behavior. Per the national security framework of this study, if the federal government could not guarantee the protection of nuclear power plants, then it should allow the owner and operators of said facilities to

provide for their security, to include procuring the necessary sensors and engagement equipment necessary to thwart UAS operators (White House, 2017).

The second unexpected finding was that two participants, both of whom were employed by the federal government during the interview process, commented that since the U.S. nuclear power plants have restricted operating zones above them, denoting no-fly zones to all flying vehicles that stretch from ground level to 10,000 feet in elevation, anything that flew into that restricted airspace should be automatically considered hostile and engaged with counter systems. This shoot first, investigate later mentality would work well in a war zone, but it would not work in or near a populated civilian area within the U.S.

The third unexpected finding was that one-third of the participants best stated by Participant C, when he said:

> It was imperative to understand the goal of the attacks. It could be to damage the reactors at the plant, but that would not be very likely. More likely the attack would be to shut down the facility through a focused attack on the soft targets outside of the nuclear reactor, such as the water pools in which spent fuel rods reside or the electrical infrastructure for transmitting the electricity from the plant to distribution centers.

If the theoretical framework was applied, then the federal government, through the Nuclear Regulatory Commission, should have directed that soft targets should have been reinforced or moved if possible to more secure areas, such as military bases or other federal lands with strict security. Any highly successful attack would probably have received media coverage, dependent upon the federal government's success to withhold

such an incident. Thus, the battle to retain public support would have begun. Greenpeace used this strategy, unsuccessfully, in their televised UAS attack upon the French nuclear power plant near Lyons in 2018 (Tran, 2018; Ranson, 2017).

A fourth unexpected finding was that one-third of the participants believed that if media coverage and public support were the aim of bad actors, it would be far easier and much more successful if the targets of a UAS attack were public events, such as a sporting game in a stadium or an attack of the Capitol Building or other well-known federal government buildings inside of Washington, D.C. Three-quarters of the participants perceived that a highly successful UAS attack would likely be executed via swarms of UAS and not by a single or small number of UAS. The same respondents feared a swarm attack as being far more deadly, both in destructive power and in the ability to instill fear among the public, than a single or small number of UAS.

The following articles were released after I had finished the interviews. A small number of researchers had submitted multiple Freedom of Information Act requests to the Nuclear Regulatory Commission because they felt that UAS incursions were regularly occurring and were being hidden from the public. A year later, the Nuclear Regulatory Commission released a treasure trove of information. The article's relevance to this study was immense as it encompasses both of this study's research questions, directly supports the problem statement of this study and provides validation for this study:

> A researcher submitted a Freedom of Information Act request to the Nuclear Regulatory Commission. This had to do with a suspected incident at the Palo Verde Generating Station, Arizona. In a trove of documents and internal correspondences related to the event, officials from the Nuclear

> Regulatory Commission described the incident as a "drone-a-palooza" and described concerns about the potential for a future "adversarial attack" involving small unmanned aircraft and the need for defenses against them. A plant officer noticed five or six drones flying over the site late on September 29, 2019. On September 30, 2019, four drones were [once again] observed flying in, through, and around the owner-controlled area.
>
> Just a month after it occurred, the Nuclear Regulatory Commission decided to formally decline to require owners of U.S. nuclear power and waste storage facilities to defend against drones. “Staff has determined that nuclear power plants and Category I fuel cycle facilities do not have any risk-significant vulnerabilities that could be exploited using unmanned aerial vehicles and result in radiological sabotage. (Rogoway & Trevithick, 2020, pp. 5)

Business and news articles based on recently released UAS activities over government facilities proved invaluable to this study. The Palo Verde incident in September 2019 highlighted what many of the participants shared. UAS incidents were occurring over U.S. nuclear power plants, and the Nuclear Regulatory Commission seemed unwilling to share this information or do anything about them. While not a participant in this study, physicist Edwin Lyman (Rogoway & Trevithick, 2020, pp. 5), summarized the incident and its implications:

> The Nuclear Regulatory Commission’s irresponsible decision ignores the broad spectrum of threats that drones pose to nuclear facilities and is out of step with policies adopted by the Department of Energy and other government agencies.

> Congress should demand that the Nuclear Regulatory Commission require nuclear facility owners to update their security plans to protect against these emerging threats. Many companies are developing technologies to protect critical infrastructure from drone attacks through early detection, tracking, and jamming. If the Nuclear Regulatory Commission were to add drones to the design basis threat, nuclear plant owners would likely have to purchase such systems. Laws would also have to be changed to allow private facilities to disrupt hostile drone flights. But plant owners are loath to spend more on safety and security when many of their facilities struggle to compete with cheap natural gas, wind, and solar. The Nuclear Regulatory Commission seems more interested in keeping the cost of nuclear plant security low than protecting Americans from terrorist sabotage, causing a reactor meltdown. (Rogoway & Trevithick, 2020, p. 6)

As damning as the Nuclear Regulatory Commission release of information was due to multiple requests under the Freedom of Information Act, which led to the Rogoway and Trevithick article, the UAS related information hidden by the Nuclear Regulatory Commission got even worse. The interviews had been completed when on September 8, 2020, the Nuclear Regulatory Commission released a massive amount of information regarding UAS incursions over U.S. nuclear power plants. The resulting treasure trove of previously restricted data, now open source, revealed that 24 separate nuclear facilities within the U.S. had been overflown 57 times by UAS between December 2014 and October 2019 (Hambling, 2020). Out of the 57 incidents, 8 were resolved, but 49 were not, but they were closed, which indicates that the Nuclear Regulatory Commission “has no idea who the perpetrators are or what they intended, and

has given up on finding them" (Hambling, 2020, p. 5). The document release also acknowledged that the Nuclear Regulatory Commission is well aware of UAS incursions but does not view them as a threat. The Nuclear Regulatory Commission has simply accepted UAS flyovers and had not taken further action, presumably because none have exhibited a threat to nuclear power plants (Hambling, 2020). That mentality is contrary to the 2017 National Security Strategy for safeguarding the nation (The White House, 2017). As long as a UAS or swarms of UAS are allowed to fly over nuclear facilities with impunity, there is a threat and cause to be very concerned. Overflights for surveillance can provide invaluable intelligence of where to drop explosives or disperse chemical, biological, radiological, or nuclear agents, and at the bad actors choosing, initiate the attack. Based on the released data, the Nuclear Regulatory Commission has accepted UAS overflights of nuclear power plants as a routine occurrence. Presumably, this position would change when they dropped explosives, or dispersed chemical, biological, radiological, and nuclear agents over the facilities, or initiated another form of attack such as radio frequency (RF) or cyber.

The findings of this study demonstrated three themes. The first theme encompassed the threat of a UAS attack or multiple UAS attacks against U.S. nuclear power plants were real and a present-day one, thus nuclear power. Plants were vulnerable to attack by UAS. The second theme was the participants' perceptions of an intentional effort for the secrecy of UAS incidents by the Nuclear Regulatory Commission. The 2020 article by Rogoway and Trevithick, and the 2020 article by Hambling, which were based on the Nuclear Regulatory Commission's release of information, validated this theme. The third theme was that nothing would change to address this vulnerability until

Congress takes an active interest in it and the Federal Aviation Administration changes its legal definition and protection of UAS as aircraft. Finding security vulnerabilities and closing those security gaps is an absolute must per the theory of national security. As mentioned previously in Chapter 2, Sun Tzu once said, "to advance without the possibility of being checked, you must strike fast at the enemy's weakest points" (2011, p. 208). Unfortunately, this study's findings indicated that the U.S. was vulnerable to a UAS attack at each of the 96 nuclear power plants. Hambling pointed out that, according to the Nuclear Regulatory Commission's data, there were 57 UAS incursions over 24 U.S. nuclear power plants in the past five years. Because of these incursions, a bad actor could have invaluable data gathered from the UAS surveillance flights over these 24 nuclear facilities and would know precisely how to approach the targets the actor wished to attack. Since the other critical infrastructure sectors were also stationary, it would be a safe assumption that they were equally vulnerable to attack by UAS. I initiated a follow-up inquiry with the Nuclear Regulatory Commission Public Affairs Office on September 8, the same day of the second release of UAS incursion incident information. I was curious that the release of data had changed the Nuclear Regulatory Commission's leadership opinion. Their public affairs officer responded that the Nuclear Regulatory Commission's position remained unchanged in that they did not view UAS as a threat (S. Burnell, personal communication, September 8, 2020).

The most relevant document uncovered in the Nuclear Regulatory Commission's archives was *Enclosure 4,* released by the Nuclear Regulatory Commission after their three-year-long security study, which concluded that UAS do not pose a threat to nuclear power plants (Nuclear Regulatory Commission, 2019, p. 1). The Nuclear Regulatory

Commission's security report dismissed the threat posed by UAS, yet when viewed in light of the recently released information, it portrayed an intentional effort of withholding information and obfuscation by the Nuclear Regulatory Commission (Rogoway & Trevithick, 2020).

Summary

An analysis of the data collected substantiated both Research Question 1: To what extent did UAS pose a threat to U.S. nuclear power plants? and Research Question 2: To what extent actions would need to be undertaken at U.S. nuclear power plants to counter the threat posed to them by UAS? The most important data to come out of this study were the three themes that were apparent after the data was analyzed, which were the following: the threat of one UAS attack or multiple UAS attacks against U.S. nuclear power plants was real; there has been an intentional effort for the secrecy of UAS incidents by the Nuclear Regulatory Commission, and finally there was much that the federal government could initiate to counter the threat of UAS attacks. The perceptions of all 20 of the participants were that U.S. nuclear power plants were vulnerable to attack by UAS, that UAS could successfully execute an attack, and that this vulnerability would not change until Congress got involved and passed new legislation, and the Federal Aviation Administration changed the legal definition of UAS. Great care was taken to guarantee the data's trustworthiness, credibility, transferability, and dependability. An external audit of the processes stated that the study had been conducted logically and did not demonstrate that researcher bias had affected the process or results. There was a lack of research in this arena, possibly due to a suppression of UAS incursions of U.S. nuclear power plants and the difficulty of acquiring information. The recent release of

information by the Nuclear Regulatory Commission answered this study's two research questions and validated this study.

Chapter 5: Implications, Recommendations, and Conclusions

The problem that this study addressed was the perceived vulnerability of U.S. nuclear power plants to UAS attack. This study examined the perception of U.S. nuclear power plants' vulnerability to attack by UAS by conducting interviews with 20 current or retired members of the federal government and nuclear industry, reviewing government documents, and analyzing the subsequent data. It was an incredibly exciting and rewarding experience that provided unique insight courtesy of 20 brave participants who traded my guarantee of their confidentiality for their honest answers and shared experiences based on many years, in some cases, decades of experience in the U.S. nuclear sector.

This qualitative phenomenological research study methodology was chosen because the data collected would be based on the perception of key personnel in the nuclear industry. Thus, it would be ideal for capturing the interviewee's perceptions of the phenomenon being studied. The qualitative methodology was well-matched to collecting information regarding one's attitudes, the ability to examine complexities, gather an abundance of data, and identify patterns. This qualitative phenomenological research study examined participants' professional opinions and work experiences, allowing for an informed examination of the phenomenon, which was not constrained by time as are case studies.

A common limitation of qualitative methods, such as this phenomenology study, would not generally lead to repetition. A second limitation could have been that the participants' data collected via the scripted interview could have been affected by intentional dishonesty. Initially, I had been concerned about a small sample size, but this

concern did not come to fruition. A focused solicitation was made for former nuclear industry employees and government, scientists, and contractors who worked in this arena, which resulted in 20 participants. A third limitation was the shortage of empirical data to support my research, which, I discovered, could have been intentional on the part of the federal government and the nuclear industry due to its apparent implications to national security and the nation's stability electrical grid. Due to the recent release of information due to multiple Freedom of Information Act requests from independent researchers, it would be interesting to see if the Nuclear Regulatory Commission continued to hide UAS incursions from the public or if its leadership would share information. The fourth and final limitation of this could have been the generalization of conclusions drawn from the findings. The data analysis indicated that the recommendations and conclusions might be equally applicable to nuclear plants belonging to U.S. partner nations worldwide and other sectors of critical infrastructure. Thus, the concern about the generalization of the findings being a limitation did not come to fruition.

The data analysis supported three themes of significant importance, both to this study and the Nuclear Regulatory Commission. The themes were: the threat of one UAS attack or multiple UAS attacks against U.S. nuclear power plants was real; there had been an intentional effort for the secrecy of UAS incidents by the Nuclear Regulatory Commission; and finally, there was much that the federal government could do to counter the threat of UAS attacks. The data results indicated that the participants perceived UAS as a threat, attacks upon U.S. nuclear power plants were inevitable, and an intentional strategy by the Nuclear Regulatory Commission to ignore this threat. This chapter will

conclude this study with its implications, recommendations for practice and future research, and finally, the study's conclusions.

Implications

Research Question 1. To what extent do UAS pose a threat to U.S. nuclear power plants?

Theme 1. The threat of one UAS attack or multiple UAS attacks against U.S. nuclear power plants was real.

Theme 1 emerged from the answers given for the first ten interview questions. This first theme directly answered Research Question 1 and was overwhelmingly supported by the participants' answers to multiple interview questions. An overwhelming consensus of participants perceived that the threat posed by UAS to nuclear power plants was real. The participants also felt that UAS are conducting overflights of U.S. nuclear power plants regularly. This theme was supported by Ranson's 2014 article about the attack against a French nuclear power plant by UAS and by an article written by Said, Malsin, & Donati in 2019 describing the cruise missile and UAS attack against the Saudi Arabian oilfield and refinery. Two cruise missiles flew as aircraft at the altitude that passenger aircraft fly in and made gradual turns as it headed into the oilfield and refinery area, where over a dozen UAS dropped off of it, and all then focused on separate targets (Malsin & Donati, 2019).

Research Question 2. To what extent do actions need to be undertaken at U.S. nuclear power plants to counter the threat posed to them by UAS?

Theme 2. There has been an intentional effort for the secrecy of UAS incidents by the Nuclear Regulatory Commission.

Theme 2 arose from the answers given for the interviews and dialogue between researcher and interviewee arising out of questions and participants' answers. This second theme answered Research Question 2 and was overwhelmingly supported by the participants' answers to multiple interview questions. The participant's perception was that of a highly dedicated and professional security force that would man their posts in the event of an attack using conventional explosives. The participant's perception was that the security forces would not man their posts if the UAS attack dispersed chemical, biological, radiological, and nuclear material. All participants agreed that the dispersion of a chemical, biological, radiological, or nuclear agent would be an escalation in terrorism and that the nuclear power plant security forces were not trained for it. This theme was supported by Rogoway and Trevithick's (2020) articles and Hambling (2020) when they analyzed the multiple UAS incursions information that was recently released due to multiple Freedom of Information Act requests of the Nuclear Regulatory Commission.

Theme 3. **There was much that the federal government could do to counter the threat of UAS attacks.**

This third theme answered Research Question 2 (To what extent do actions need to be undertaken at U.S. nuclear power plants to counter the threat posed to them by UAS?) and was supported by the participants' answers to multiple interview questions. Participants believed that only congressional involvement and oversight would rectify nuclear power plants' present-day vulnerabilities to attack by UAS. Other participants believed that it would take new federal legislation to counter the threat posed by UAS, while others believed that the Federal Aviation Administration would need to alter the

current legal definition of UAS to enact change and confront the present-day vulnerabilities of U.S. nuclear power plants to attack by UAS. Lastly, a segment of participants believed that each nuclear facility must have the authority to procure sensors and counter-UAS equipment to deal with UAS incursions before they turn into attacks. This last perception was supported by Ranson's 2014 article written after the "UAS attack" of a nuclear power plant in Lyons by Greenpeace. Ranson believed that the French government did not acknowledge the threat to nuclear power plants and had done nothing to mitigate the threat through developing counter UAS technologies and sensors.

Recommendations for Future Practice

The recommendations for practice would be for the Nuclear Regulatory Commission to do the following: acknowledge the vulnerability of nuclear power plants to UAS attack; request an outside government agency conduct a vulnerability assessment and security review of this nation's nuclear power plants; conduct an internal workforce assessment of the vulnerability of nuclear power plants to UAS attack; be transparent with UAS incursions with the public; report the UAS incursions and their possible consequences to Congress, and train and equip nuclear power plant security personnel to operate the sensors and counter UAS systems necessary to defend their facilities. A recommendation for practice for Congress would be to become involved in oversight of the Nuclear Regulatory Commission and pass legislation to tighten the current vulnerabilities of nuclear power plants to UAS attack. Lastly, a recommendation for practice for the Federal Aviation Administration would be to change the legal definition

of UAS as being equivalent to passenger aircraft. Thus, forgoing the protections against defensive actions by law enforcement and others that UAS now enjoy.

Recommendations for Future Research

This study was the first known research study to examine U.S. nuclear power plants' vulnerabilities to attack by UAS. As such, there should be additional research in this arena. This study must be followed by additional research because it is likely that this study and its findings, conclusions, and recommendations may be equally relevant to our global partners' nuclear power plant vulnerabilities. In addition, the other 15 sectors of U.S. critical infrastructure are stationary, and their location is widely available on the Internet. Thus, it is highly likely that the generalization of this study's findings and conclusions would be equally relevant to the other sectors. In addition to U.S. nuclear power plant vulnerabilities, research needs to be conducted into the vulnerabilities of the other 15 sectors of the U.S. critical infrastructure to attack by UAS. An unforeseen threat posed by UAS uncovered during this study should be researched, that being, UAS platforms using cyber and RF attacks against the software and hardware systems that operate within the U.S. nuclear power plant industry. This attack aspect should be researched based on the professional opinions of participants of this study as U.S. nuclear power plants and all sectors of U.S. critical infrastructure. The U.S. may be equally vulnerable to attack via these means. Lastly, I would encourage research into the emerging threat platforms that are unmanned surface systems (USS), ground and sea, and unmanned undersea systems (UUS) and vulnerabilities that they could exploit in an attack upon U.S. critical infrastructure. The technological advancements that have made UAS a colossal military and private hobbyist success and are in the infancy stage of its

introduction into commercial uses and have already migrated into USS and UUS systems. Those three domains of operation, the aerial, surface on land and atop the water, and the undersea, are the next arena for tremendous growth, use, and will change how we do business in those domains, and of course, will provide a new threat platform from which a bad actor could attack critical infrastructure. These would be the logical next steps for future researchers.

Future researchers can look at this vulnerability, and perhaps they will have access to more documents, possibly additional data on UAS incidents that the Nuclear Regulatory Commission was forced to release. This qualitative phenomenological study was supported by the observations and perceptions of highly educated and experienced personnel associated with the nuclear industry and government over many years and even decades of service. With the release of additional information, i.e., UAS incidents, the opportunity for a quantifiable or mixed research design study will become more likely.

Conclusions

A recently released article titled *The Night A Mysterious Drone Swarm Descended On Palo Verde Nuclear Power Plant* described overflights and surveillance by a mysterious swarm of UAS over the most productive U.S. nuclear power plant in Palo Verde, Arizona, in September 2019 (Rogoway & Trevithick, 2020). This incident was kept from the public by the Nuclear Regulatory Commission (Rogoway & Trevithick, 2020; Hambling, 2020). A follow-up article based on multiple Freedom of Information Act requests indicated that the UAS incursion problem was more common than the Rogoway and Trevithick article indicted. Hambling pointed out in *Dozens more mystery drone incursions over U.S. nuclear power plants revealed* after he combed

through a treasure trove of recently released information by the Nuclear Regulatory Commission, that there have been 57 UAS incursions over 24 U.S. nuclear power plants in the past five years. These real-world incidents, kept from the public by the Nuclear Regulatory Commission, answered both of this study's research questions and singularly provided validation for this study. The actions by the Nuclear Regulatory Commission to shield the incident from the public were anathema to its inherent and unwavering responsibilities to maintain the safe operations of nuclear power plants, securing such facilities against possible attack, thereby contributing to the national security of this nation. The threat from UAS increased as new technology and capabilities were brought to the industry. Many aspects of proven technologies and capabilities had already migrated from UAS to the unmanned surface, ground and sea, and unmanned undersea systems.

The problem addressed by this qualitative phenomenological research study was to examine the vulnerability of U.S. nuclear powerplants to attack by UAS. It used the interviews, government archived, and open-source documents to conduct a first-ever research study into an area previously ignored, due perhaps to the intentional withholding of information by the U.S. Nuclear Regulatory Commission. This study's importance is that it dared to conduct an unclassified study of the vulnerability of one of the U.S. sixteen sectors of critical infrastructure. If nuclear power plants are vulnerable, it is highly likely that the other 15 sectors with fixed sites are equally vulnerable to attack by UAS.

The "take-home message" of the entire study is that U.S. nuclear power plants are vulnerable to attack by UAS, and nothing will correct this unless Congress takes an

active interest and provides oversight of the troubling industry and the government entities responsible for ensuring that nuclear facilities are safe from attack. This vulnerability was based upon UAS attacks or incursions executed in multiple worldwide locations. The threat posed by UAS to U.S. nuclear power plants has been ignored but must be acknowledged by the Nuclear Regulatory Commission, especially in light of the recent release by the Commission of a treasure trove of documents. The federal government is responsible to its citizens to provide for the nation's national security against foreign and domestic enemies. The 20 current and former employees of the government with expertise in the nuclear arena believed that the threat was real and that U.S. nuclear power plants were vulnerable to attack by UAS, especially a swarm of UAS. Action must be taken to counter the threat and close the vulnerability as it directly impacts the national security of the U.S.

References

Ackerman, E. (2019). Event camera helps drone dodge thrown objects. *IEEE Spectrum.* https://spectrum.ieee.org/automaton/robotics/drones/event-camerahelps-drone-dodge-thrown-objects

Albites, M. (2019). Drones dropping off packages pose new threat to prisons. Governing the future of states and localities. https://www.governing.com/news/headlines/Drones-Dropping-Off-Packages-Pose-New-Threat-to-Prisons.html

Amazon. (n.d.). *Amazon prime air.* Amazon. https://www.amazon.com/Amazon-Prime-Air/b?ie=UTF8&node=8037720011

Arksey, H., & Knight, P. (1999). *Interviewing for social scientists*. Sage Publishing, London.

Association for Unmanned Vehicle Systems International. (2013). The economic impact of unmanned aircraft systems integration in the United States. https://higherlogicdownload.s3.amazonaws.com/AUVSI/958c920a-7f9b-4ad2-9807-f9a4e95d1ef1/UploadedImages/New_Economic%20Report%202013%20Full.pdf

Babbie, E. (1995). *The practice of social research*. Wadsworth Publishing, Belmont, CA.

Baker, M. (2017). Officials crashed a jet into nuclear reactor facility to test its walls. https://interestingengineering.com/crashed-jet-nuclear-reactor-test

Bergmann, K. (2019). Attacks on Saudi infrastructure illustrate limitations of protection. *Defense Review Asia*, *13*(3), 12–13. https://search-ebscohost-com.proxy1. ncu.edu/login.aspx?direct= true&db=tsh&AN=139334635&site=eds-live

Betz, E. (2017). *Artificial intelligence gives drones abilities we've only dreamed about*. Discover.https://www.discovermagazine.com/technology/artificial-intelligence-gives-drones-abilities-weve-only-dreamed-about

Blain, L. (2018). In-flight charging gives drones unlimited autonomous range. https://newatlas.com/in-air-drone-charging-unlimited-range/56363/

Bless, C., & Higson-Smith, C. (2000). *Fundamentals of social research methods, an African perspective* (3rd ed.). Juta Publishing, Cape Town, South Africa

Bloor, M. (1997). Techniques of validation in qualitative research: a critical commentary. In G. Millar & R. Dingwall (Eds.). *Context and method in qualitative research* (pp. 37-50). Sage Publishing, London.

Blum, S. (2018). *We still have no idea how to deal with drones*. Popular Mechanics. https://www.popularmechanics.com/flight/drones/a25653640/gatwick-drones-disable-deterrence/

Boon, N. (2018). 25,000 miles of safe swimming and great fishing. https://williampennfoundation.org/blog/25000-miles-safe-swimming-and-great-fishing

Breen, C. (2016). Espionage in ancient Egypt. *The SAGE Encyclopedia of Surveillance, Security, and Privacy*. http://dx.doi.org/10.4135/9781483359922.n163

British Broadcasting Corporation. (2018a). *Gatwick airport: drone ground flights*. https://www.bbc.com/news/uk-england-sussex-46623754

British Broadcasting Corporation. (2018b). *Venezuela President Maduro survives "drone assassination attempt."* https://www.bbc.com/news/world-latin-america-45073385

British Broadcasting Corporation. (2019). Saudi Arabia oil facilities ablaze after drone strikes. https://www.bbc.com/news/world-middle-east-49699429

Bradford, E. (2004). *Thermopylae: the battle for the West* (1st Da Capo Press pbk. ed.). New York: Da Capo Press.

Bunker, R. (2015). *Terrorist and insurgent unmanned aerial vehicles: use, potentials, and military implications.* Carlisle, Pa.: Army War College, Strategic Studies Institute

Burnell, S. (February 10, 2020). Personal communication.

Burns, S. (2017). *Drone meets delivery truck*. UPS. https://www.ups.com/us/es/services/knowledge-center/article.page?kid=cd18bdc2

Calder, S. (2019). *Gatwick drone disruption cost over $65.5M*. Independent. https://www.independent.co.uk/travel/news-and-advice/gatwick-drone-airport-cost-easyjet-runway-security-passenger-cancellation-a8739841.html

Chang, L. (2018). *Emerging tech: FBI hostage rescue team bamboozled after criminals unleash drone swarm.* Digital trends. https://www.digitaltrends.com/cool-tech/drones-fbi-raid/

Clausewitz, C. (1793). *On War*. Reprinted by Princeton University Press, Princeton, New Jersey.

Clodfelter, Michael (2017). *Warfare and armed conflicts: a statistical encyclopedia of casualty and other figures, 1492–2015.* McFarland & Company, Inc., Jefferson, North Carolina.

Cohn, P., Green, A., Langstaff, M., & Roller, M. (2017). *Commercial drones are here: the future of UAS.* McKinsey & Company: Capital Projects and Infrastructure.https://www.mckinsey.com/industries/capital-projects-and-infrastructure/our-insights/commercial-drones-are-here-the-future-of-unmanned-aerial-systems

Cook, Scott (2010). San De and warring states views on heavenly retribution. *Journal of Chinese Philosophy*. 37: 101–123. http://doi.org/10.1111/j.1540-6253.2010.01622.x

Coombs, W.T. (2006). The protective powers of crisis response strategies: managing reputational assets during a crisis. *Journal of Promotion Management*, Vol. 12, pp. 241-260. https://www.researchgate.net/publication/280153851_Coombs_WT_2006_The_protective_powers_of_crisis_response_strategies_Managing_reputational_assets_during_a_crisis_Journal_of_Promotion_Management_12_241-260

Congressional Research Service. (2020). The U.S. nuclear weapons complex: overview of Department of Energy sites. https://fas.org/sgp/crs/nuke/R45306.pdf

Cornell Law School. (n.d.). *18 U.S. Code § 178.Definitions*. Legal Information Institute. https://www.law.cornell.edu/uscode/text/18/178

Cox, R. (2017). "Expanding the history of the just war: the ethics of war in ancient Egypt." *International Studies Quarterly*. Vol. 61, no. 2, pp. 371 - 384. http://doi.org/10.1093/isq/sqx009

Coxworth, B. (2018). DroneCatcher drone netting drone gets an upgrade. *New Atlas.* https://new atlas. com/dronecatcher/55056/

Crabtree, B. & Miller, W. (1992). *Doing qualitative research: multiple strategies*. Sage Publications, Washington, DC.

Creswell, J. W. V. (2018). Qualitative inquiry & research design: choosing among five approaches. Retrieved from https://search-ebscohostcom.proxy1.ncu.edu/login .aspx?direct=true&db=edsbvb&AN=edsbvb.BV044632262&site=eds-live

Danner, M. (2004). Torture and truth: America, Abu Ghraib and the war on terror. New York Review of Books Publishing, New York.

Defense Science Board. (2016). *Defense science board: summer study on autonomy.* Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, Department of Defense. Washington, DC. https://www.esd.whs .mil/Portals/54/Documents/DD/issuances/dodd/300009p.pdf

Delahunty, R. J., & Yoo, J. (2009). The Bush Doctrine: can preventative war be justified? *Harvard Journal of Law and Public Policy*, Vol. 32, Issue 3, pp. 843-865. http://www.harvard-jlpp.com/wp-content/uploads/sites/21/2017/12/JLPP_32__3.pdf

Delbert, C. (2019). Here's John Deere's crop dusting drone. *Popular Mechanics.* https://www.popular mechanics.com/technology/infrastructure/a29728347/john-deere-volocopter/

Denning, P. & Lewis, T. (2017). Exponential laws of computing growth. *Communications of the ACM*, Vol. 60, pp. 54-65. https://cacm.acm.org/magazines/2017/1/211094-exponential-laws-of-computinggrowth/

Department of Defense. (2017). *Directive 3000.09: autonomy in weapon systems*. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/300009p.pdf

Energy Information Agency. (2019). *January 2019: Monthly Energy Review.* https://www.eia.gov/ totalenergy/data/monthly/archive/00351901.pdf

Federal Aviation Administration. (2020). *UAS by the numbers*. https://www.faa.gov/uas /resources/by_the_numbers/

Federal Bureau of Investigation. (1995). *Oklahoma City bombing.* https://www.fbi.gov/history/famous-cases/oklahoma-city-bombing

Federal Bureau of Investigation. (1996). *Unabomber.* https://www.fbi.gov/history/famous-cases/unabomber

Federal Communication Commission. (1934). *Communications Act of 1934.* https://transition.fcc.gov/Reports/1934new.pdf

Fergie, D. (2019). *The strange career of national security.* https://www.theatlantic.com/ideas/archive/2019/09/the-strange-career-of-national-security/598048/

Forgie, A. (2019). *Man indicted for using drone to drop explosives on ex-girlfriend's home*. KUTV.https://kutv.com/news/nation-world/man-indicted-for-using-drone-to-drop-explosives -on-ex-girlfriends-home

Garamone, J. (2002). *From U.S. Civil War to Afghanistan: a short history of unmanned aerial vehicles.* https://archive.defense.gov/news/newsarticle.aspx?id=44164

Gardner, T. (2016). *Eighth drone spotted in SRS skies.* http://aikenstandard.com/article/20160706/AIK0101/160709671

Gillham, B. (2000). *Case study research methods*. Wellington House, London.

Guthrie, C. & Quinlan, M. (2007). *Just war: the just war tradition: ethics in modern warfare*. Bloomsbury Publishing, New York.

Hacaoglu, S. (2020). *Turkey's killer drone swarm poses Syrian air challenge to Putin.* http://www.msn.com/en-us/news/world/turkeys-killer-drone-swarm-poses-syria-air-challenge-to-putin/ar-BB10BdPA?li=BBnb7Kz&ocid=iehp

Hambling, D. (2020). *Dozens more mystery drone incursions over U.S. nuclear power plants revealed.* https://www.forbes.com/sites/davidhambling/2020/09/07/dozens-more-drone-incursions-over-us-nuclear-power-plants-revealed/#84041d06296b

Hennigan, W. (2018). *Experts say drones pose a national security threat – and we aren't ready*. Time. https://time.com/5295586/drones-threat/

Hill, P. (2018). *Drone spraying and spreading becoming reality*: future farming. https://www. futurefarming.com/Tools-data/Articles/2018/9/Drone-spraying-and-spreading-becoming-reality-335322E/

Hobbes, T. (1651). *Leviathan, or the matter, form and power of a commonwealth ecclesiastical and civil.* University Press, London.

Holloway, I. (1997). *Basic concepts for qualitative research*. Blackwell Science, Oxford, England.

Holman, B. (2009). *The first air bomb: Venice, 15 July 1849*. Air minded. https://airminded.org /2009/08/22/the-first-air-bomb-venice-15-july-1849/

Holmes, K. (2015). *What is national security? A 2015 Index* of U.S. military strength. https://www.heritage.org/sites/default/files/2019-10/2015_IndexOfUSMilitaryStrength _What%20Is%20National%20Security.pdf

Hood, B. (2018). *Watch an electric VTOL aircraft fly successfully with the weight of 3 people.* https://robbreport.com/motors/aviation/vertical-aerospace-evtol-aircraft-video-2875086/amp/#referrer=https%3A%2F%2Fwww.google.com&_tf=From%20%251%24s

International Atomic Energy Agency. (2019). *Country nuclear power profiles: France*. https://cnpp.iaea.org/countryprofiles/France/France.htm

Islam, S., Ahmed, M. & Islam, S. (2018). A conceptual system architecture for countering the civilian unmanned aerial vehicles threat to nuclear facilities. *International Journal of Critical Infrastructure Protection.* Vol. 23, pp. 139-149. http://doi.org/10.1016/j.ijcip.2018.10.003

Jinks, D. (2013). *The rules of war*. Oxford University Press, Oxford, England.

Jomini, A. (1865). *Treatise on grand military operations: or, a critical and military history of the wars of Frederick the great, as contrasted with the modern system.* D. van Nostrand Publishing, New York.

Jorge, V., Granada, R., Maidana, R., Jurak, D., Heck, G., Negreiros, A., Santos, D., Goncalves, L. & Amroy, A. (2019). A survey on unmanned surface vehicles for disaster robotics: main challenges and directions. *Sensors.* Vol. 19, pp. 702. https://doi.org/10.3390/s19030702

Kallenborn, Z. & Bleek, P. (2018). *Swarming destruction: drone swarms and chemical, biological, radiological, and nuclear weapons.* The nonproliferation review, vol. 25, issue 5-6, pp. 523-543. https://doi.org/10.1080/10736700.2018.1546902

Kant, I. (1995). *The metaphysics of morals*. Cambridge University Press, Cambridge, England.

Kreis, J. (1990). Unmanned aircraft in Israeli air operations. *Air Power History.* Vol. 37, No. 4, pp. 46-50. http://www.jstor.org/stable/26271146

Krygier, R. & Faiola, A. (2018*). Maduro speech interrupted by explosions in what Venezuelan government calls a 'failed attack.* The Washington Post. https://www.washingtonpost.com/ world/maduro-speech-interrupted-by-explosions-in-what-venezuelan-government-calls-a-failed-attack/2018/08/04/a5c361c6-983c-11e8-80e1-00e80e1fdf43_story.html

Kvale, S. (1996). *Interviews: An introduction to qualitative research interviewing*. Sage Publishing, Washington, DC.

Lai, R. (2019). *Volocopter's massive utility drone can carry up to 440 pounds*. Engadget. https://www.engadget.com/2019-10-30-volocopters-massive-utility-drone-can-carry-up-to-440-pounds.html

Lee, S. (2008). *Weapons of mass destruction: are they morally special? War: Essays in Political Philosophy.* Cambridge University Press, Cambridge, MA. https://doi.org/10.1017/CBO9780511840982

Lincoln, Y. & Guba, E. (1985). *Naturalistic inquiry*. Sage Publishing, Newbury Park, CA.

Lippmann, W. (1922). *Public opinion*. New York: Harcourt, Brace and Company.

Lipscy, P., Kushida, K., & Incerti, T. (2013). The Fukushima disaster and Japan's nuclear plant vulnerability in comparative perspective. *Environmental Science & Technology*. Vol. 47, issue 12, pp. 6082–6088. http://doi.org/10.1021/es4004813

Liszewski, A. (2019). *Flying replacement batteries could massively boost a drone's flight time*. Gizmodo. https://gizmodo.com/flying-replacement-batteries-could-massively-boost-a-dr-1838627300/amp#referrer=https%3A%2F%2Fwww.google.com&amp_tf=From%20%251%24s

Lofland, J., & Lofland, L. (1999). Data logging in observation: fieldnotes. In Bryman & Burgess (Eds.), *Qualitative research* (Vol. 3). Sage

Machiavelli, N. (1532). *The prince*. Antonio Blado d'Asola Publishing. Rome, Italy.

Maguire, L. (2015). *The ethics of drone warfare*. Philosophy Talk. https://www.philosophytalk.org/blog/ ethics-drone-warfare

Marrin, A. (2001). *George Washington and the founding of a nation.* Dutton Juvenile Publishing, New York.

Martin, B., Tarraf, D., Whitmore, T., DeWeese, J., Kenney, C., Schmid, J., & DeLuca, P. (2019). *Advancing autonomous systems: an analysis of current and future technology for unmanned maritime vehicles*. Rand Corporation. Rand Corporation Publishing, Santa Monica, CA. https://www.rand.org/pubs/research_reports/RR2751 .html

McCormick, J. (2011). *Machiavellian democracy.* Cambridge University Press, New York.

Miles, M. & Huberman, A. (1984). *Qualitative data analysis, a sourcebook of new methods.* Sage Publishing, Washington, DC.

Mueller, B. & Tsang, A. (2018). *Gatwick airport shut down by deliberate drone incursions.* The New York Times. https://www.nytimes.com/2018/12/20/world/europe/gatwick-airport-drones.html

Murison, M. (2016). *Consumer drone sales to increase tenfold by 2021*. Dronelife. https://dronelife.com/2016/07/11/consumer-drone-sales-increase/

Nash-Hoff, M. (2013). *What is the importance of unmanned vehicles to our economy.* Industry Week. https://www.industryweek.com/technology-and-iiot/emerging-technologies/article/ 21960764/what-is-the-importance-of-unmanned-vehicles-to-our-economy

The National Commission on Terrorist Attacks Upon the United States. (2004). *The 9/11 commission report.* Government Information Library. https://govinfo.library.unt.edu /911/report/911Report.pdf

Neufeld, M. (1994). The rocket and the reich: Peenemünde and the coming of the ballistic missile era. The Free Press Publishing, New York.

Nguyen, T. (2019). *The history of drone warfare.* ThoughtCo. https://www. thoughtco.com/history-of-drones-4108018

NVivo. (n.d.). *Discover the power of NVivo*. NVivo. https://www.qsrinternational.com/ nvivo-qualitative-data-analysis-software/home

Nuclear Regulatory Commission. (2019). *Executive summary for "technical analysis of unmanned aerial vehicles for nuclear power plants and category I fuel cycle facilities: Encl. 4 to classified security report."* https://www.nrc.gov/docs /ML1930 /ML19302E409.pdf

Nuclear Regulatory Commission. (2020). *About NRC*. https://www.nrc.gov/about-nrc.html

Orend, B. (2013). *The morality of war*. Broadview Press, New York.

Osiander, A. (2001). Sovereignty, international relations, and the Westphalian myth. *International Organization*. 55 (2): 251–287. http://doi.org/10.1162/00208180151140577

Paleri, P. (2008). *National security: imperatives and challenges*. Tata McGraw-Hill Publishing, New Delhi, India.

Paret, P. (1976). *Clausewitz and the state: the man, his theories, and his times*. Princeton University Press, Princeton, New Jersey.

Parker, Geoffrey (2005). *Compact history of the world*. London: Times Books.

Patel, N. (2017, October 27). *The sky is the limit in 5G game of drones*. eInfochips. https://www.einfochips .com/blog/sky-limit-5g-game-drones/

Pence, E. (2019). *Iran's drones and missile attack on Saudi Arabia is a huge problem*. The National Interest. https://nationalinterest.org/blog/buzz/irans-drone-and-missile-attack-saudi-arabia-huge-problem-90011

Phillips, J. (2004). *The Fourth Crusade and the sack of Constantinople*. https://www.historytoday.com/archive/crusades/fourth-crusade-and-sack-constantinople

Pieri, P. (1962). *Storia militare del Risorgimento*. Einaudi, Turin, Italy.

Preston, S. (2015). *The legal framework for the United States' use of military force since 9/11 speech at the annual meeting of the American society of international law. http://*www.defense.gov/Speeches/Speech.aspx?SpeechID=1931.

Prothero, M. (2020). *Turkey used a new weapon in Syria that was so effective it looks like Russia won't dare confront Turkey directly*. https://www.yahoo.com/news/turkey-used-weapon-syria-effective-174456745.html

Purkiss, J. & Serle, J. (2017). *Obama's covert drone war in numbers: ten time more strikes than Bush*. https://www.thebureauinvestigates.com/stories/2017-01-17/obamas-covert-drone-war-in-numbers-ten-times-more-strikes-than-bush

Rahe, P. (2006), *Machiavelli's liberal republican legacy*, Cambridge University Press

Ranson, A. (2017). The 2014 UAV threat to French nuclear power plants. *National Security & the Future*, *18*(1/2), 125–142.

Reid, D. (2019). *Saudi Aramco reveals attack damage at oil production plants*. CNBC. https://www.cnbc.com/2019/09/20/oil-drone-attack-damage-revealed-at-saudi-aramco-facility.html

Reisman, W. & Antoniou, C. (1994*). The laws of war*. New York: Vintage

Roblin, S. (2019). *Don't just call them "drones:" a guide to military unmanned systems on air, land, and sea.* Forbes. https://www.forbes.com/sites/sebastienroblin/2019/09/30/dont-just-call-them-drones-a-laypersons-guide-to-military-unmanned-systems-on-air-land-and-sea/#1d90302e2b00

Rogoway, T. & Trevithick, J. (2020). *The night a mysterious drone swarm descended on Palo Verde Nuclear Power Plant.* https://www.thedrive.com/the-war-zone/34800/the-night-a-drone-swarm-descended-on-palo-verde-nuclear-power-plant

Romm, J. (1993). *Defining national security: the nonmilitary aspects*. Pew Project on America's Task in a Changed World (Pew Project Series). Council on Foreign Relations Press, New York.

Saar, E. & Novak, V. (2005). *Inside the wire*. New York: Penguin

Said, S., Malsin, J. & Donati, J. (2019). *U.S. blames Iran for attack on Saudi oil facilities.* The Wall Street Journal. https://www.wsj.com/articles/drone-strikes-spark-fires-at-saudi-oil-facilities-11568443375

Sang, L. (2019). *Drone strikes target world's largest oil processing facility, Saudi oilfield; attack claimed by Iranian backed rebels*. Fox News. https://www.foxnews. com/ world/drone-attack-saudi-oil-facility-iran-rebels

Sauer, F. & Schörnig, N. (2012). Killer drones: The 'silver bullet' of democratic warfare? *Journal of Military Ethics*, Vol. 43, issue 4, pp. 363–380. http://doi.org/10.1177/0967010612450207

Schmidt, B. & Vance, A. (2020). *DJI won the drone wars, and now it's paying the price.* https://www.bloomberg.com/news/features/2020-03-26/dji-s-drone-supremacy-comes-at-a-price

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

Schmitt, M. (2010). Drone attacks under the *Jus as Bellum* and *Jus in Bello*: clearing the fog of law. *Yearbook of International Humanitarian Law,* Vol. 13, pp. 311-326

Schuety, C., & Will, L. (2018). *An air force "way of swarm": using wargaming and artificial intelligence to train drones*. War On The Rocks.

https://warontherocks.com/2018/09/an-air-force-way-of-swarm-using-wargaming-and-artificial-intelligence-to-train-drones/

Segall, M. (2017). Yemen has become Iran's testing ground for new weapons. *Jerusalem Center for Public Affairs*, Vol. 17, Number 5. https://jcpa.org/article/yemen-has-become-irans-testing-ground-for-new-weapons/

Shelsby, T. (1991). *Iraqi soldiers surrender to AAI's drones.* The Baltimore Sun. https://www.baltimoresun.com/news/bs-xpm-1991-03-02-1991061100-story.html

Smithsonian National Air and Space Museum. (n.d.). *Kettering bug (aerial torpedo) microfilm drawings and index, 1917-1920*. https://airandspace.si.edu/collection-objects/kettering-bug-aerial-torpedo-microfilm-drawings-and-index-1917-1920

Solodov, A., Williams, A., Al Hanaei, S., & Goddard, B. (2018). Analyzing the threat of unmanned aerial vehicles (UAV) to nuclear facilities. *Security Journal*, Vol. 31, Issue 1, pp. 305-324. http://doi.org/10.1057/s41284-017-0102-5

Spires, J. (2019). *Man charged after allegedly dropping explosives from a drone on ex-girlfriend's property*. Drone DJ. https://dronedj.com/2019/09/21/man-charged-drop-explosives-drone-ex-girlfriend/

Starship Technologies. (2020). *A revolution in local delivery.* https://www.starship.xyz/company/

Street, A. (1998). *Informing inside nursing: ethical dilemmas in critical research*. Suny Publishing, New York.

Small UAS. (2020). *XAG establishes five-million-yuan fund for drone disinfection operation to fight Coronavirus outbreak.* sUAS News: the business of drones.

https://www.suasnews.com/2020/02/xag-establishes-five-million-yuan-fund-for-drone-disinfection-operation-to-fight-coronavirus-outbreak/

Tarantola, A. (2017). *The rise of drone crime and how cops can stop it: The only way to stop a bad guy with a drone is a good guy with an RF rifle*. Engadget. https://www.engadget.com/2017/10/11/drone-crime-how-cops-stop-it/

The 9/11 Commission Report. (2004). *Final report of the national commission on terrorist attacks upon the United States*. https://www.govinfo.gov/content/pkg/GPO-911REPORT/pdf/GPO-911REPORT.pdf

The National. (2015). *Recreational drones bring Dubai airport traffic to a halt.* http://thenational.ae/uae/transport/recreational-drones-bring-dubai-airport-traffic-to-a-halt

The White House. (2009). *Policies of the Bush Administration: 2001-2009.* https://georgewbush-whitehouse.archives.gov/infocus/bushrecord/documents/Policies_of_the_Bush_Administration.pdf

The White House. (2017). *The national security strategy of the United States of America*. https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf

Tran, P. (2018). *Defense news: watch this UAV crash into a French nuclear power station*. Defense News. https://www.defensenews.com/unmanned/2018/07/03/watch-this-uav-crash-into-a-french-nuclear-power-station/

Trimble, S. (2020). *Stealthy UAS unveiled for USAF target, loyal wingman needs*. https://aviationweek.com/defense-space/stealthy-uas-unveiled-usaf-target-loyal-wingman-needs

Tulsa World. (1989). *480 mph F-4 Phantom jet crash test data reported*. https://www.tulsaworld.com/news/480-mph-f-4-phantom-jet-crash-test-data-reported/article_25f19d32-0dd2-5f61-8750-c28637bf5dd6.html

Turak, N. (2019). *How Saudi Arabia failed to protect itself from drone and missile attacks despite billions spent on defense systems.* https://www.cnbc.com/2019/09/19/how-saudi-arabia-failed-to-protect-itself-from-drones-missile-attacks.html

United Nations Office of Counter Terrorism. (2018). *The protection of critical infrastructures against terrorist attacks: compendium of good practices*. https://www.un.org/sc/ctc/wp-content/uploads/2019/01/Compendium_of_Good_Practices_Compressed.pdf

U.S. Department of Homeland Security (2008). *History: Who became part of the Department?* http://www.dhs.gov/xabout/history/editorial_0133.shtm

U.S. Department of Homeland Security. (2011). *Critical infrastructure sector partnerships*. http://www.dhs.gov/files/partnerships/editorial_0206.shtm

U.S. Department of Homeland Security. (2013). *National Infrastructure Protection Plan (NIPP) 2013: partnering for critical infrastructure security and resilience*. https://www.dhs.gov/sites/ default/files/publications/National-Infrastructure-Protection-Plan-2013-508.pdf

U.S. Department of Homeland Security. (2019). *Strategic framework for countering terrorism and targeted violence.* https://www.dhs.gov/sites/default/files/publications/19_0920_plcy_strategic-framework-countering-terrorism-targeted-violence.pdf

U.S. Department of State. (1947). *National Security Act of 1947*. https://history.state. gov/milestones/1945-1952/national-security-act

U.S. Department of State. (2010). *The Obama administration and international law: Harold Hongju Koh speech to the annual meeting of the American society of international law*. https://2009-2017.state.gov/s/l/releases/remarks/139119.htm

U.S. Department of Transportation. (1926). *Air Commerce Act.* https://www. transportation. gov/content/air-commerce-act

U.S. Energy Information Administration. (2017). *Country analysis brief: Saudi Arabia.* https://www.eia.gov/international/content/analysis/countries_long/Saudi_Arabia/saudi_arabia.pdf

U.S. Congress. (2018). H.R.302, The FAA Reauthorization Act of 2018. https://www.congress.gov/bill/115th-congress/house-bill/302/text?q=%7B%22search%22%3A%5B%22FAA+Reauthorization%22%5D%7D

Verner, D., Petit, F., & Kim, K. (2017). Incorporating prioritization in critical infrastructure security and resilience programs. *Homeland Security Affairs* 13, Article 7. https://www.hsaj. org/articles/14091

Vogel, S. (1999). Unmanned navy planes to spread wings for NATO. https://www. washingtonpost.com/wp-rv/inatl/longterm/balkans/stories/ planes041299.htm

Walzer, M. (2000). *Just and unjust wars,* 3rd ed. New York: Basic Books.

Ward, A. (2020). *The ridiculous failed coup attempt in Venezuela, explained.* https:// www. vox.com/2020/5/11/21249203/venezuela-coup-jordan-goudreau-maduro-guaido-explain

Watson, B. (2017). *Defense one: the drones of ISIS*. Defense One. https://www.defenseone.com /technology/2017/01/drones-ISIS/134542/

Wiktorowicz, Q. & Kalthenthaler, K. (2006). The rationality of radical Islam. *Political Science Quarterly*, Vol. 121, Number 2, pp. 295-319. https://www.uakron.edu/dotAsset/1a1a3052-2dbe-4911-8cc3-c8f234229e9b.pdf

Yap, J. (2014). *Suz Tzu: warcraft*. Joey Yap Research International Sdn Bhd Publishing, Kuala Lumpur, Malaysia

Appendices

Appendix A – Scripted Interview Questions

Introduction: good afternoon _____. My name is Terry Dorn, and I am writing a dissertation on the threat that UAS may pose to nuclear power plants. Thank you very much for taking the time out of your schedule to talk with me today and agree to participate in this study. This interview will be audio recorded to transcribe your answers to maintain 100% accuracy and for subsequent data analysis and findings and recommendations. The 15 questions that I will ask you are unclassified, as is this study. At no time will I ask you, nor do I want you to divulge classified information.

The federal government and many in the industry have coined the term UAS. For this interview, I will simply refer to unmanned aerial vehicles, unmanned aircraft systems, and drones as UAS.

The following are my study's two research questions: Research Question 1. To what extent do UAS pose a threat to U.S. nuclear power plants? Research Question 2. To what extent do actions need to be undertaken at U.S. nuclear power plants to counter the threat posed to them by UAS?

Per the Institutional Review Board's mandatory requirements for the safeguarding of participant information, all physical and electronic data will be secured at all times to protect the identity information of all participants. I will minimize the risk of a compromise of confidentiality with all research materials by storing all study-related material on an encrypted drive, and it and any physical material will be stored in a secured, sensitive facility for thirty-six months following the completion of this study. After this period, it will be destroyed. I guarantee that I will maintain your confidentiality at all times.

There are no financial incentives for participating in this study. My intent is not to gain fame and fortune; instead, I wish to highlight what I believe is a known vulnerability in which the federal government has been slow to recognize and to act upon. Do you have any questions about anything that I have covered to this point? I will now begin the interview.

1. What is your perception of the threat posed to U.S. nuclear power plants by a UAS? Please explain.
2. Do you have experience with UAS conducting overflights or other maneuvers over nuclear power plants? Please explain.
3. Have you heard of UAS overflying nuclear power plants? Please explain.
4. If so, how long did the UAS fly over the facility? Please explain.
5. Did they perform any threatening behavior? Please explain.
6. Have you heard of such incidents from co-workers, or discussed the perception of the threat posed by UAS to nuclear power plants? Please explain.
7. Do you believe that UAS could successfully execute an attack on nuclear power plants? Please explain.
8. Do you believe that such an attack would shut down operations at the facility? Please explain.
9. Do you believe that the threat of attack by a UAS armed with conventional explosives is a viable one? Please explain.
10. What are your views about the viability of a UAS attack that is dispersing chemical, biological, nuclear, or radiological agents over a nuclear power plant? Please explain.

11. What would the personnel operating a nuclear power plant do if they were informed that the facility was under attack by a UAS? Please explain.
12. What would employees do if it was determined that a UAS was dispersing chemical, biological, nuclear, or radiological agents over the facility? Please explain.
13. What could a U.S. nuclear power plant do to stop an attack by a UAS? Please explain.
14. What do you think of the possibility of an attack by a swarm of UAS? Please explain.
15. Are there strategies that the federal government could undertake to reduce the threat of an attack by UAS? Please explain.

Is there anything else that you wish to add? Do you know of another individual that would agree to participate in this study by answering these same questions? If you would like me to email you the transcription of today's interview in a Word document to review, I can do so. Thank you again for your time and participation today.

Appendix B – NCU Voluntary Consent Letter

Introduction

My name is Terence Michael Dorn. I am a doctoral student at Northcentral University and am conducting a research study on U.S. nuclear power plants' vulnerability to attack by UAS. The name of this research study is "A Phenomenological Study Examining the Vulnerabilities of U.S. Nuclear Power Plans to Attack by UAS." I am seeking your consent to participate in this study. Your participation is entirely voluntary, and I am here to address your questions or concerns at any point during the study.

Eligibility

You are eligible to participate in this research if you:

1. Are a current or former government manager, scientist, or a private contractor supporting the Department of Energy, the Nuclear Regulatory Commission, or another federal department or agency whose responsibilities support nuclear power plants or related nuclear facilities.
2. Related nuclear facilities can include those associated with U.S. federal departments, agencies, and organizations such as privately owned and operating nuclear research laboratories and other private companies that directly support the U.S. nuclear industry.
3. Possess a Ph.D. in computer science, physics, nuclear science, or a related degree and have at least two years of experience.

I hope to include 20 people in this research.

Activities

In this study, participants will:

1. Participation in a 1:1 interview with me that will consist of a 90-minute session.
2. The interview will be conducted over Microsoft Teams, Zoom or another video chat software system that you and I have access to.
3. You may skip any question that you do not wish to answer. The questions will be unclassified, and at no time will we discuss classified material.

Risks

There are no foreseeable risks or discomforts associated with this study. To decrease the potential for risks, I will guarantee your confidentiality at all times. For your participation, your identity will be an alphabetical letter. Only I will have access to the interviews and transcripts, and they will be secured in a locked container when not in use. You may skip any question and stop your participation at any time.

Benefits

If you participate, there are no direct benefits to you.

This research may increase the body of knowledge in the subject area of this study.

Privacy and Data Protection

I will secure your information with these steps: I will secure all physical and electronic data to protect all participants' identity information. I will minimize the risk of a compromise of confidentiality with all research by storing all study-related on an encrypted drive, and it will be stored in a secured container for three years following the completion of this study. After three years, I will destroy all study-related data.

Follow on researchers will not be able to link the data from your participation back to you. Your identity will remain confidential, and I will designate your identity with an alphabetical identifier. Only I will know your name.

This data could be used for future research studies or distributed to other investigators for future research studies without additional informed consent from you or your legally authorized representative.

I will securely store your data for three years. Then, I will delete the electronic data and destroy paper data.

How the Results Will Be Used

The data and subsequent findings and conclusions will be published in a dissertation. They may be presented in a public forum. The participants' general makeup could be divulged, but at no time will I divulge individual names, data, and places of employment. At no time will participants be identified in the dissertation or any public presentations or discussions.

Contact Information

If you have questions, you can contact me at t.dorn5118@o365.ncu.edu or 703.678.9941.

My dissertation chair's name is [Dr. Vicki Lindsay]. She works at Northcentral University and is supervising me in the research. You can contact her at vlindsay@ncu.edu or 480.666.5640.

If you have questions about your rights in the research or if a problem or injury has occurred during your participation, please contact the NCU Institutional Review Board at irb@ncu.edu or 1-888-327-2877 ext. 8014.

Audio recording

I would like to use Zoom as a voice recorder to record your responses.

Voluntary Participation

If you decide not to participate or stop participation after you start, there will be no penalty to you: you will not lose any benefit you are otherwise entitled to.