12-2020

Linking Theory of Disruptive Technology with Nuclear Security: UAS as an Emerging and Disruptive Technology

Jason J. Karcz
University of Tennessee, Knoxville, jkarcz@vols.utk.edu

To the Graduate Council:

I am submitting herewith a thesis written by Jason J. Karcz entitled "Linking Theory of Disruptive Technology with Nuclear Security: UAS as an Emerging and Disruptive Technology." I have examined the final electronic copy of this thesis for form and content and recommend that it be accepted in partial fulfillment of the requirements for the degree of Master of Science, with a major in Nuclear Engineering.

Dr. Howard Hall, Major Professor

We have read this thesis and recommend its acceptance:

Dr. Lawrence Heilbronn, Dr. Brandon Prins

Accepted for the Council:
Dixie L. Thompson

Vice Provost and Dean of the Graduate School

(Original signatures are on file with official student records.)

Linking Theory of Disruptive Innovation with Nuclear Security: UAS as an Emerging and Disruptive Technology

A Thesis Presented for the
Master of Science
Degree
The University of Tennessee, Knoxville

Jason Joseph Karcz
December 2020

ACKNOWLEDGEMENTS

Given the type of year 2020 was, I want to thank those who were involved in helping and motivating me to keep writing this thesis throughout the year.

My committee chair, Dr. Howard Hall, was a huge help in planning the thesis process and developing a plan moving forward. The committee members, Dr. Lawrence Heilbronn and Dr. Brandon Prins, provided tremendous discussions that sparked ideas that supported this paper. I am greatly appreciative for all their patience and guidance throughout the year and would not have finished without them.

Lastly, I would like to thank my parents for their moral support during my time in the Master's program. When times were tough, they were always there for me to help me keep pushing through.

ABSTRACT

Technology used in nuclear security allows for many practical applications for securing material while simultaneously providing malicious opportunities for adversaries to potentially steal or misuse the material. Fixed sites and various modes of transport for nuclear and other radioactive material all can benefit from the use of new technology in mitigating against these threats. One emerging technology in nuclear security that is rapidly growing is the use of unmanned aerial systems (UAS). UASs provide a different dimension of security compared to methods that are traditionally used because of the added aerial characteristics of these devices. These devices offer new detection, delay, and response measures as operations are conducted using an aerial method rather than more traditional ground methods. Because of the increased popularity, availability, and capabilities of UAS technology, these tools are shifting trends in technology and how it is applied to nuclear security. The theory of disruptive innovation as it relates and applies to nuclear security is introduced as a guideline for assessing UAS technology. Additionally, regulation gaps relating to use of UAS technology in fixed site and transport security will be addressed. UAS technology is creating security incidents at nuclear sites and a new method of assessing this threat is needed to help determine the overall impact this technology is having in nuclear security and assist in distributing resources. A combination of a new dimension of use, increasing trends and security incidents, and lack of regulations shows signs that UAS is becoming a disruptive technology used in the nuclear security field.

TABLE OF CONTENTS

CHAPTER ONE:
INTRODUCTION AND GENERAL OVERVIEW

General Overview

Nuclear security of facilities and material in transport is a quickly evolving area which requires meticulous design and evaluation to ensure material is kept out of malicious hands. Security is sophisticated and involves many different methods and techniques to keep material secure. Traditionally security heavily involves guards, guns, and gates as the main methods for protecting nuclear material with sensors and cameras as supporting tools. While these methods have done well over the years, adversaries adapt and attempt to acquire material using new methods and technologies.

One emerging technology that has become a security concern at nuclear facilities is the unmanned aerial system (UAS, often referred to as a drone). Since the first commercial license issued by the Federal Aviation Administration (FAA) in 2006, UAS popularity has continuously grown. By 2016, UAS became a billion-dollar industry and has maintained steady growth since. (Alkobi, 2019). Because of the reputation this technology has built, they have become widely available and used in many parts of the United States.

Emerging technologies are defined as technologies that can have large impacts over a short period of time (Roth, 2020). In nuclear security, technologies used by adversaries to illicitly obtain nuclear material or disrupt a facility can cause severe impacts because of the uncertainty that comes with stolen material or damaged operations. This material could be used to make a dirty bomb and detonated in a metropolitan area or to damage a turbine at a facility and prevent electrical generation for a prolonged time. These are just a couple of impacts that UAS technology may have on nuclear facilities in the near future.

To aid in assessing various emerging technologies in nuclear security, the theory of disruptive innovation (disruptive theory) is introduced. This theory typically analyzes trends in business but has aspects which can be translated to trends for nuclear security technology. Given the traditional terrestrial methods used in nuclear security, UAS offers a new dimension for use in the air space over a nuclear facility. Because of the growing use, its versatility, and capabilities, UAS was the chosen emerging technology used throughout this paper. This new dimension, increasing availability and sighting trend, and lack of regulations in the United States suggest that UAS technology is a potentially disruptive technology within nuclear security.

UAS in Nuclear Security

UAS technology has branched out from military use to commercial use over the past decade. Over the years, drones have been designed to be smaller, lighter with increased payload, and fly further and faster with increased battery life (Roth, 2020). The FAA estimates there are over 1.5 million commercial drones in the United States, with this number increasing year by year (Meola, 2017). Skydio has developed a product for $1000 which contains 4k cameras, a battery life of approximately 23 minutes, and a range of 3.5 km (2.2 miles). This is considered one of the top models on the market. Other companies also have drones available for cheaper with similar capabilities. It should be noted that this paper does not endorse any company that produces UAS technology in any way. These are used only to demonstrate capabilities of modern-day drones.

UAS has begun to establish its identity in the world of nuclear security. Sightings of this technology at high profile sites have occurred around the world and cases involving UAS at these types of locations has increased over the years. Incidents are not just limited to the United States. France, Saudi Arabia, and other countries have noted UAS within their regions. While

public information surrounding these cases is fairly limited, the information that is available can still help identify trends and capabilities of this emerging technology.

UAS has a wide range of proactive uses. Quick response to an alarm can be beneficial to a nuclear facility to get eyes on whatever triggered a sensor within a geographical area. Added surveillance can aid in guards knowing material is secure or if there are suspicious actors in a surround area. Even the sight of a drone may deter a malicious actor from going through with any plans at a nuclear site. New uses of UAS technology are still developing, but they show signs of beneficial use for many applications at nuclear facilities.

Nuclear material is most vulnerable when it is mobile. This includes material that is being transferred on site from one building to another or material that is in transport. This vulnerability results from the material being exposed outside of a fixed storage site and the changing of ownership and/or location of the material. UAS provides an additional view for both protective forces and adversaries instead of traditional line of sight on the ground. This can allow the operator to maintain constant view of the material. For protective forces, this adds another level of security to continuously monitor the material and watch for threats, but for adversaries this gives an advantage in knowing where nuclear material is at all times.

Many times the intent behind a UAS security incident is malicious in nature even if the drone is used simply to take pictures. Other times larger drones can be used to deliver explosive payloads to a target in a short period of time. Regardless of this intent, this emerging threat has potential to become a major issue in nuclear security. If pictures are taken they could be sold to other parties who may intend on attacking a nuclear site. Additional surveillance may take not of operational features of a facility such as guard movements or shifts, camera locations or sensitive areas within the facility. Once information like this is identified, malicious actors could more

easily coordinate an attack at a facility to either illicitly obtain nuclear material or significantly disrupt a nuclear facility's operations. This is just one of many scenarios that an actor could accomplish using UAS technology. As more incidents occur, more knowledge can be obtained about the versatility of UAS at nuclear facilities and what new threats this technology can pose in nuclear security.

Regulating UAS

Nuclear security consists of an important balance between policy and technology. Regulations allow for things to be better controlled and in nuclear security it allows for different technologies to be used and limited. They also allow for facilities and personnel to handle threats in a more systematic way to avoid conflicts with the public as often as possible.

The current status of regulations related to UAS in the United States is very limited. Currently the FAA controls all regulations related to UAS including at nuclear facilities; however, no regulations specifically for UAS at nuclear facilities exist or are not publicly available. While collaboration to develop regulations is unknown, policies should be developed to help control new threats around nuclear security to help prevent malicious actors from causing significant social or economic impacts of acquiring nuclear material.

The International Atomic Energy Agency (IAEA) has published a Nuclear Security Series (NSS) that helps guide Member States in developing strong nuclear security regimes. These guides and recommendations address various areas of nuclear security including guidelines for implementing security measures for nuclear and radioactive material in use, storage, and transport. Although the regulatory impact is not the main focus of this paper, it is important to highlight which areas of the NSS may have an impact on UAS in nuclear security because regulations play a key role in implementing nuclear security measures. Publications

within the NSS that may have an impact UAS include NSS 9-G (Rev. 1), NSS 11-G, NSS 26-G, and NSS 27-G.

Theory of Disruptive Innovation

Nuclear facilities often use different techniques to assess the site against various threats. It is important for these facilities to ensure their security designs are strong to prevent malicious actors from obtaining nuclear material or to ensure that important buildings or site areas are protected from threats. Vulnerability assessments are commonly used to help evaluate weaknesses within a nuclear facility's security design. Indices can be used to indicate how strong or weak a certain component of the system is to an adversary threat. Mock attacks can be done to simulate a real time attack at a facility to check vulnerable areas at a site and properly train guards to quickly respond to on site incidents. Additionally, tabletop exercises can be implemented to simulate a more scaled down simulation of an adversary threat attempting to obtain nuclear material.

While these methods can help visualize real time threats at a moment in time, they do not necessarily address the full impact a technology can have in nuclear security. Vulnerability assessments and tabletop exercises can be used to indicate system weaknesses as fixed-point methodologies, but it does not fully evaluate the impact of technologies that are used during an attack over a time period of interest. Because of this gap, the theory of disruptive innovation is introduced as a methodology that can analyze an innovation or technology in nuclear security over a period of time. This theory evaluates the impact an innovation has within a market (in this case nuclear security). To help with the evaluation of an innovation's impact, vulnerability assessments and other techniques can be used as qualitative data to reinforce whether a technology is disrupting nuclear security operations at a facility.

The theory of disruptive innovation was first developed by Christensen in 1995. The idea behind disruptive theory is to demonstrate how larger, incumbent businesses' products fall to entrant, smaller businesses. These smaller businesses initially target a more niche group of customers with new products which larger businesses often overlook. Once incumbent businesses learn about these small business innovations, they typically fail to catch back up with similar innovations, causing them to significantly weaken in that area of the market. The new innovation then disrupts the market by making a strong impact and establishing its prominent role in its target are (Christensen, Raynor, & McDonald, 2015).

During the disruption process, new innovations are often overlooked by the incumbent businesses. In nuclear security, emerging technologies at facilities may be unfamiliar or unexpected during a security incident which may allow them some initial success in the field. Adversaries may continue using these methods or innovations against facilities. Facilities in turn may continue to upgrade current systems instead of trying to develop ways to mitigate these new innovations because they expect the upgrades to be sufficient. Eventually these new innovations may reach more levels of success and carry significant consequences. Facilities may then try to develop new ways of countering these new innovations to minimize future attacks; however, if adversaries continue to develop methods using the new innovation and are more successful than not, this may indicate successful disruption in nuclear security.

Disruptive theory carries many characteristics which can be applied to nuclear security. This theory can be used to analyze a technology over a period of time instead of simply at a fixed point. Compared to a vulnerability assessment of a nuclear facility or transport operation, disruptive theory is more of a methodology to assess the way of thinking about an innovation and

how it got to a certain point. It has the potential to assist and be combined with a vulnerability assessment in distributing resources to either use or mitigate UAS technology in nuclear security.

This paper explains how this theory can be applied to nuclear security using various case studies and security incidents to develop a qualitative assessment of UAS in nuclear security over the past decade. While security design weaknesses can be evaluated using different methods, the disruptive theory of innovation aims to analyze the overall impact UAS has had over the past decade. Analogies are developed to structure the theory and are applied to various aspects of UAS and the disruption process to provide an evaluation of this technology.

CHAPTER TWO:
LITERATURE REVIEW:

The recreational and commercial use of UAS technology has increased over the past decade (Roth, 2020). As commercial drone capabilities increase, so do their applications as tools as well as their uses as a threat to security. New uses and threats are continuously being developed. Although the motives are still relatively unknown in the majority of cases, drone sightings have increased more in recent years at nuclear facilities around the world. These sightings must be assumed as malicious in all scenarios because of the nature of the facilities they were spotted at. Additionally, the lack of regulations around UAS use opens up opportunities for them to be used in many ways – both as protective tools and a threat. The following surveys current UAS applications and threats, disruption theory, and gaps in security regulations as applied to UAS technology.

UAS Uses in Nuclear Security

UAS as a Tool

Aaron et al. (2018) introduce general nuclear security uses of UAS technology over a variety of styles that are available in the current market including multi-rotor, tethered, and dirigible drones. While the list of applications is extensive, the authors describe three different scenarios for UAS use - fixed land shipment, mobile land shipment, and maritime transport - to demonstrate the versatility of the tool. Surveillance is consistently discussed in the paper as UAS can add miles of visible range and, with a high-resolution camera, real time footage of a vast area of land (Aaron, Anderson, & Fialkoff, 2018).

It can be clearly seen that UAS technology either enhances security measures with additional communication or provides a new dimension with new capabilities which ground security measures cannot provide. The simplest benefit that can be seen from the examples

presented in this paper is the visibility a drone can provide for both a shipment in transport or at a fixed site. Although the battery life of a UAS is only around 20 minutes, it can still give several miles of visibility especially if there are signs of a potential security incident. This can be especially useful during transport to check the route ahead and make sure it is secure. While the view would partially depend on the quality of camera used with a UAS, the visibility from a drone in the air would still be greater since a full 360^{o} view over several miles of an area can be captured. One drawback of this, however, is that visibility from a drone may be more restricted during inclement weather should an adversary choose to use a UAS that given day. While UAS can still be used on any given day regardless of visibility due to weather, the use of this device would be more limited during a heavy storm. Additionally, high winds could adversely affect functionality as the mobility of a lighter drone would be hindered.

Araújo and Gomera take a deeper dive into the uses of UAS in the nuclear security realm. The authors approach drone use from an inspection and detection perspective. They highlight the Fukushima incident in Japan and how UAS technology significantly aided response workers by quickly covering large areas of land minimizing the workers' exposure to radiation (Lochbaum, 2015). Other applications that are briefly mentioned in Araujo's and Gomera's paper are damage and maintenance inspections of nuclear facilities (Araújo & Gomera, 2016). Although it is not the scope of this paper, the use of drones during the Fukushima incident demonstrates safety aspects of using them in the nuclear field.

The theme of Araujo's and Gomera's paper is more how UAS can be used as an actual tool instead of bonus surveillance. Because time was so valuable during the Fukushima response and cleanup, drones were used to expedite the overall evaluation of the damage done by the core meltdown. The incident needed careful handling as high levels of radiation were present in

several locations near the facility. The use of UAS technology to inspect multiple locations (either from a combination of drones or quickly scanning the area with one) allowed for a quicker assessment of the area. Regardless of the approach, this method with drones would be more efficient than having individuals survey the land on foot.

Nuclear facilities are generally quite large and require frequent inspections to ensure proper operation. Because of the speed and mobility of drones, these devices could conduct more frequent inspections and examine areas of a reactor, for example, which are difficult to access. Alternatively, a drone could be used to inspect a reactor while operating or changing fuel. With an additional view on fuel while changing it, the material can be accounted for with more precision.

UAS as a Threat

Aaron et al. (2018) also provide a general overview of potential threats posed by UAS. These general threats include surveillance, collision (with or without a payload), improvised explosive device (IED), and radiation dispersion device (RDD). Surveillance, collision, and IED are applied to material in transport while RDD is discussed after material has been obtained by an adversary (Aaron, Anderson, & Fialkoff, 2018). Araújo and Gomera mention the above as applied to fixed site and add security shift schedules, and frequency jamming as further malicious uses of UAS in nuclear security (Araújo & Gomera, 2016). Martin et al. and Solodov et al. further reiterate the above threats posed by UAS technology (Martin, Tomkinson, & Scott, 2017) (Solodov, Williams, Al Hanaei, & Goddard, 2018).

Generic UAS threats have also been introduced. There are scenarios that did not directly involve a nuclear facility in which drones were used to cause some level of operation disruption. ISIS has been confirmed to be considering UAS for explosive devices. Although this has not been done on a nuclear facility, this type of threat must be considered as legitimate as the

consequences could have a catastrophic effect (Warrick, 2017). Solodov et al. also list several recent incidents involving UAS including a drone crashing at the White House and disruption of an airport in the United Arab Emirates due to drones simply flying around restricted airspace. These scenarios can be translated into possible security concerns for nuclear facilities as well since there is a chance the aforementioned scenarios can just as easily occur at a facility (Solodov, Williams, Al Hanaei, & Goddard, 2018).

While the threats demonstrated above have not occurred at a nuclear facility yet, they still must be heavily considered by personnel at any given site because of the severe consequences of a threat to a nuclear facility. This is also not a final list of possible threats an adversary could do to a nuclear site. Some additional threats could include confiscation of facility equipment (communication devices or light computer equipment for example) or extracting nuclear material after an attack has occurred. Disruption of daily operations or the loss of any material to a malicious actor could prove devastating. One thing to note from the above articles is that because the threat of UAS is relatively new and no direct attacks have occurred, there is no information on how a facility would respond if it was even prepared for an attack of a more severe nature.

Solodov et al. discuss several occurrences with UAS technology around nuclear sites as well as other major facilities around the world. These incidents occurred in recent years (2012-2016) and include sightings at airports, the White House, several French nuclear power plants, and the Savannah River Site. The authors also mention an incident in Israel where a UAV photographed a nuclear research center (Solodov, Williams, Al Hanaei, & Goddard, 2018).

The number of drone sightings around nuclear facilities has increased in recent years. The above mentions a single moment in 2012, but that number increased to at least 13 in France in

2014 and eight at the Savannah River Site in 2016 over the span of a few weeks. These are only a handful of examples that were documented, but the growing trend can be seen. In all of the above cases, there is no documentation of how the UAS were handled at the time, except in 2012 the UAV was shot down ten miles away from the site after the photos were taken. The article does not specifically discuss what response forces did while the drone was at the site, however.

A developing UAS threat that could impact nuclear facilities is the concept of swarming. Swarming involves unleashing multiple (sometimes hundreds or more) drones in a coordinated plan to meet a certain objective. These drones autonomously share information with one another and alter decisions based on information passed between the devices. This concept has been studied by several countries including China, Russia, and the United States. Kallenborn and Bleek (2018) discuss four payload types where UAS swarms could be of significant security concerns – chemical, biological, radiological, and nuclear uses. Either category could have severe impacts if a swarm of drones coordinated an attack on a target. One important note is that in a swarm, not every UAS would have to be on the attack. There can be roles of drones within a swarm including attack, sensor, communication, or even decoy drones (Kallenborn & Bleek, 2018).

One important feature of swarming that is mentioned is the roles different drones may play on a coordinated attack. While payload drones may be most often viewed as the key drone in a swarm, different sensors on drones could provide important information depending on the sensor that is attached. This could help an adversary identify a target more easily in inclement weather, nighttime, behind walls, or in other scenarios.

While chemical, biological, radiological, or nuclear weapon (as dirty bombs) scenarios using drones as a payload delivery are important considerations to analyze, simple explosive

devices attached to a UAS could cause major consequences during a coordinated attack. For a nuclear facility, this could involve multiple drones carrying light bombs to breach an outer wall or critical areas of the facility. These types of attacks could also attack areas not related to the nuclear material such as a turbine or guard gate to disrupt operations and have severe economic consequences if a plant shut down. The potential for drone attacks such as this is important to analyze and consider because the capabilities of modern-day drones allow for theoretical scenarios of swarming to easily become a reality.

Regulation of UAS in Nuclear Security

Federal Aviation Administration Regulations

Regulations for the use of drones in the United States, especially in nuclear security, are scarce. Currently the Federal Aviation Administration (FAA) controls all regulations of UAS in the United States' national airspace. In terms of national security, the FAA has prepared general regulations and guidelines in two key areas relevant for UAS operation at nuclear facilities – geo-fencing and prohibited or restricted airspace (FAA, 2016).

Geo-fencing limits access to certain airspace by combining GPS and radio frequency identification with a signal jammer in the area of interest. The FAA initially had proposed geo-fencing over certain areas to help control the use of UAS in restricted areas for security or safety reasons; however, this proposal was rejected and there are no geo-fencing requirements enforced by the FAA. They note that the cost of implementing software into recreational UAS cannot be justified at the present time. Also, it would be difficult to incorporate any software to existing devices as well as making an option to allow certain small aircraft to access restricted areas if necessary (such as a UAS used for surveillance at a nuclear facility). A constantly changing and updated database for surrounding terrain would present a complicated challenge as well.

Because geo-fencing is not a requirement under the FAA for restricted areas, nuclear facilities would have to choose to use this mitigation method on a case by case basis.

Under the FAA, prohibited or restricted areas are defined as areas of interest to national security and welfare. These include energy infrastructures (nuclear power plants) and other nuclear facilities (fuel fabrication or isotope production). As previously mentioned, one challenge of enforcing regulations of UAS in a restricted area would be identifying UAS which is used by an authorized operator for utility purposes.

While the FAA can regulate which specific areas are considered restricted or prohibited, this would not be enough to deter a malicious actor from using UAS at a nuclear facility. There are clear gaps in the FAA regulations of UAS operation which must be addressed in order to mitigate the threat of this technology in nuclear security. This would require the FAA to collaborate with the Nuclear Regulatory Commission (NRC) in drafting regulations for the use and handling of UAS technology at a nuclear facility.

Nuclear Security Series

The IAEA has released several documents in its Nuclear Security Series (NSS) as a way for Member States to strengthen their nuclear security regimes. The key recommendation and guidance articles provided in the NSS which could relate to the security of nuclear material are NSS 26-G and NSS 27-G for transport security of nuclear material and physical protection of nuclear material and nuclear facilities, respectively. Additionally, NSS 9-G and NSS 11-G provide guidance for security of radioactive material in transport and security of radioactive material in use and storage and of associated facilities, respectively. A combination of these four articles could help operators in using and regulating UAS in nuclear security operations appropriately.

NSS 26-G, “Security of Nuclear Material in Transport”, is an implementing guide that was developed as a way to provide information for Member States to minimize the threat of unauthorized removal of nuclear material for an explosive device, unauthorized removal of nuclear material for later distribution, and sabotage of nuclear material during transport. This NSS guidance explains that a nuclear security regime should incorporate and maintain three key elements for transporting nuclear material. These elements are legislation and regulations relating to the transport of nuclear material, establishment of organizations to ensure this legislation is implemented during the transport process, and physical protection systems specifically used for transport. This guidance states that “physical protection responsibilities throughout the transport of nuclear material are clearly assigned to the shipper, the carrier, the receiver, or another relevant entity” (IAEA, 2015).

Transport security of radioactive material is addressed in NSS 9-G. NSS 9-G shares several similar characteristics with NSS 26-G except the material in focus is radioactive material instead of nuclear material. Transport security measures explained in NSS 9 are dependent upon the category of radioactivity of a given isotope (IAEA, 2020).

NSS 27-G has similar characteristics to NSS 26-G except this guidance focuses on physical protection of nuclear material in use and storage at nuclear facilities. This guidance shares similar elements to NSS 26-G with NSS 27-G with the exception that these are oriented around facilities with no consideration for transport. This guide emphasizes physical protection responsibilities in various areas including threat assessment, response to security events, and material accountability (IAEA, Physical Protection of Nuclear Material and Nuclear Facilities, 2018). Similar to NSS 27-G, NSS 11-G is an implementing guide used by the IAEA to promote security for the use and storage of radioactive material at facilities. Both NSS 27-G and NSS 11-

G have underlying goals of emphasizing the importance of regulations of both nuclear and radioactive material, respectively (IAEA, 2019).

Disruptive Theory of Innovation

Introduction to Disruptive Theory of Innovation

Disruptive theory of innovation (referred to as disruption theory) was first introduced by Christensen in 1995. Disruption theory is the idea that a smaller company can challenge a larger business by offering a product of its own that meets the needs of consumers. These needs are typically overlooked by the larger company when developing and improving products to its core customers. Figure 1 visualizes how larger companies typically overlook low end needs for a product quickly to suit the needs for the higher end of a market. This is typically how smaller companies are able to offer a product which appeals to a larger end of the market to disrupt the larger company (Christensen, Raynor, & McDonald, 2015).

In a later paper written by Christensen et al. (2018), a three-step description of the process for an innovation to become disruptive is explained. Initially, an incumbent company essentially saturates a market with products of certain capabilities. These appeal to a majority of their current customers but leaves a gap at the bottom of the market for possible products that might be attractive to a different group of customers. This gap is where new or smaller companies may focus on addressing the needs of a more niche target audience. Second, the product might be considered inferior to the top performing product introduced by an incumbent, but it may have a wider range of aspects that customers may prefer. Features such as convenience or price may be heavily viewed as the preferred option by customers and eventually

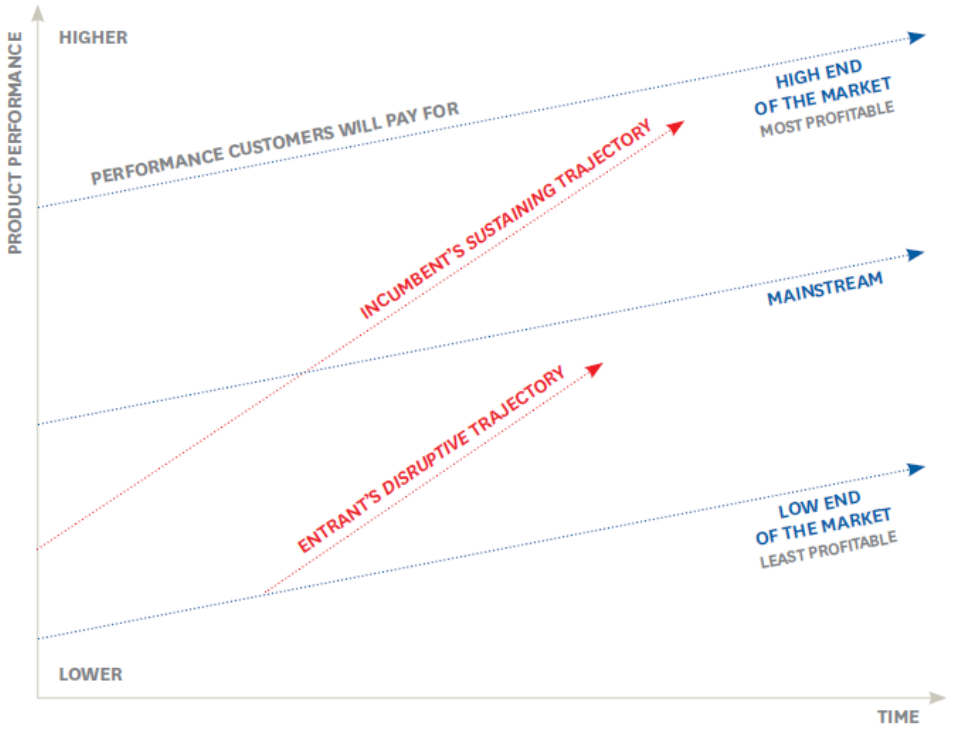

Figure 1. Theory of Disruptive Innovation Model (Christensen, Raynor, & McDonald, 2015)

expand to other user in the market. Finally, incumbents often do not find investing in this gap worthwhile, so it opens opportunities for new, smaller companies to focus on this area with little to no competition. Eventually the incumbent falls behind with new products centered around the gap, and thus a disruptive innovation is born (Christensen, McDonald, Altman, & Palmer, 2018).

One important note is that the theory of disruptive innovation is viewed more as a process rather than a fixed-point analysis. A timeline is used from when a product is first introduced into a market until either the present day or when a product successfully overtook an incumbent in a market. For example, digital photography was of great interest to many camera companies such as Sony, Canon, and Kodak. Sony and Canon had already distinguished themselves in the camera market and were attempting to develop digital cameras. In 1999, Kodak invested large amounts of money in an attempt to maintain is status in the market; however, this money was used to research a more sustaining innovation rather than disruptive. A sustaining innovation is one that improves upon a current product to increase its performance and capabilities to its wide user base. Kodak switched its investments from a sustaining innovation to one that was disruptive, the Easy Share camera. Its simple design and new digital capabilities disrupted the digital camera market and allowed Kodak to overtake the lead in market shares within two years of releasing the new camera to the public (Christensen, 2006).

It is also interesting to note the "gap" that is mentioned in Christensen's later article. This area of a market is where certain aspects of a market are overlooked or ignored, opening opportunities for people to develop products that meet customers' wants in this area. This gap may be wider or narrower depending on the market, but it allows for new innovations to be developed and introduced to the public. Disruptive innovations are also developed in this area, so pinpointing these technologies and their development or implementation status is important.

The incumbent can then quickly adapt to the customers' needs in this area, in the hopes of developing its own product to suppress a competitor or entrant in the market.

A dangerous aspect of the theory of disruptive innovation comes from the second point mentioned by Christensen et al. (2018). The fact that a product may be considered inferior to an incumbent is a key aspect of the theory which allows an entrant's product to disrupt a market. Incumbents do not see initially see a disruptive innovation as a threat to their market base early on which gives the new product time to develop and grow in the market. This eventually takes customers away from an incumbent, slowly weakening its grasp in its market.

The authors give a clear description of what disruption theory is and how a technology or product can be considered disruptive. They define a path in which a technology takes and how it develops into a true disruptive technology. Typically, this path involves developing a product with characteristics that appeal to a different group of customers that upgrades to current products do not necessarily attract. Potentially disruptive technologies often do not have the same quality as newly updated products; however, the lack of competition or motivation by incumbents to develop their own version allows for the new innovations to slowly begin to enter and eventually overtake a market. Although the theory is related to business, the way the authors lay out the path for an innovation to become disruptive can allow for an analogous comparison to a different field, in this case nuclear security. This analogy is discussed in more detail in the following chapters of this paper.

King and Baatartogtokh assessed and reviewed the idea behind Christensen's disruption theory. They begin with the underlying question of "how widely applicable is the theory of disruptive innovation?". Their biggest critique and analysis come from the predictive power of disruption theory by the original definition given by Christensen. The underlying question is –

can this theory successfully predict the impact an innovation may have in its market? They state four key elements of disruption theory in their analysis: incumbents improving over a trajectory (as seen previously in Figure 1), sustaining innovation pace based on customer needs, incumbent capability to respond to a disruptive innovation, and incumbents succumbing to the disruptive innovation (King & Baatartogtokh, 2015).

The four key characteristics for disruptive entertainment mentioned by King and Baatartogtokh can provide a check list for determining if a technology is disruptive. First, incumbents notice a disruptive innovation appear on the market. Revenue may not significantly decline at the start, so an incumbent would simply ignore the product and continue with its own research and development of sustaining innovations in its field. This sustaining innovation then appeals to its current customer base, with a small portion of customers not quite being satisfied with the new updates. This dissatisfaction may come from the new product being too expensive, too complicated to use, or currently unavailable in their area. The third component then discusses the incumbent's capabilities of catching up to an innovation once it has disrupted its market. This would occur after the incumbent notices a significant decline in revenue as a result of the disruptive innovation now competing in the market. An incumbent then begins to research and develop a product of its own to try to compete with the disruptive innovation. Its ability to successfully adapt and counter the new innovation is critical for the incumbent to sustain in the newly dynamic market. Finally, after a certain time has elapsed, the incumbent succumbs to the disruptive innovation. In the previous example mentioned using digital photography, this would be the point when Kodak became the leading shareholder over Sony and Canon in the digital photography market. While the incumbent may not necessarily dissolve due to a disruptive innovation, the new product is further advanced than ones under development by the incumbent.

Because of this, the entrant and its disruptive innovation now lead in the market over the previous leaders.

One important issue to note within the article is that most sources came from interviews with experts, so some subjectivity may be displayed within the information presented. On the other hand, they note that Christensen's original theory does not have much statistical support, giving a general subjective perspective back in 1995 when the theory was first developed (King & Baatartogtokh, 2015).

Schmidt and Druehl further analyze what it means for an innovation to be considered disruptive by developing a framework that looks into different areas of the previously mentioned "gap" in a market. They list three scenarios for how a disruptive innovation enters the market: the fringe-market, the detached-market, and immediate implementation. A fringe-market is the market that develops if the differences between the new and old market are very incremental. The detached-market develops if the product that is offered is different than that in an old market to the point where price is not a factor in a consumer's decision in choosing the new product. These two markets are created over an arbitrary period of time while the innovation develops and grows. Alternatively, an immediate scenario occurs when the innovation quickly sells and attracts the consumers in the "gap" region (Schmidt & Druehl, 2008).

To determine the initial threat of a disruptive innovation, Schmidt and Druehl (2008) presented their three step framework – identification of different areas of the market and product attributes, resources companies are willing to spend for the disruptive product, and determine which areas of the market that customers would be willing to pay for again in the future. The example given involves the disk drive. For the first step, different attributes of the product include capacity and size. These were the most flexible areas of the disk drive to manage, and

thus were highlighted. In studies done by the author, it was determined that both features had a higher willingness to invest in because of the attractiveness to customers. Finally, varying capacities and sizes are analyzed as options for consumers to use and how different combinations of these attributes disrupted the market. Three product scenarios are then explained for the fringe-market, detached-market, and immediate scenarios. The fringe-market disruptive innovation path takes the form of a smaller size and capacity. Since size is considered a favorable factor for the development of disk drives, this product may attract customers for that alone even if the capacity was not quite what current products offered. A second scenario involving a detached-market is shown using the smallest possible size and accompanying capacity. This difference in size compared to the fringe-market scenario opens up more opportunities for smaller target customers early on while the technology develops to maintain its size but increase capacity and lower the cost per capacity. The third scenario presented involves the immediate disruptive technology. The disk drive is kept at the same size and capacity as the old market, but is sold with no sales support which allows for a lower cost (Schmidt & Druehl, 2008).

Identifying a potential disruptive innovation can be difficult without a structured system. The framework presented above attempts to create that structure to aid in determining when a product is becoming disruptive. Any new product that has different capabilities than ones in a current market might be considered as potential disruptive innovations; however, Schmidt and Druehl suggest ways to identify these before they make significant impacts in the market. The final immediate scenario may not be of much use for nuclear security; however, the detached market highlights a brand-new area of focus for a product in its own new market. In terms of nuclear security, a fringe market may have aspects that can be applied to new technologies that

are used proactively or maliciously. UAS is not necessarily a new technology for a facility's security design, but it stems off of an older market (traditional nuclear security) to find areas that could benefit or improve the market in a more effective manner.

Regulating Disruptive Innovation

Cortez discusses how disruptive innovation causes disruption in regulatory space and how to create regulatory framework for these types of innovations. The author introduces the term "regulatory disruption" which, by the author's definition, is when a product falls within an agency's regulation, but does not line up with the agency's existing regulatory framework. This would be due to certain characteristics and functions of the disruptive innovation (Cortez, 2014).

Two approaches are introduced by the author. One involves using informal threats using the Food and Drug Administration (FDA) as the example agency while the other involves a more aggressive approach using the Federal Communications Commission (FCC) as the example agency. The two took different approaches to regulating new innovations with different results coming from each.

The FDA began attempting to regulate various health software by using less stringent agency threats; however, these threats were deemed stringent weak as the agency showed little control over the dynamic nature of software development. Early on, they used a constant slogan which said they would "apply the least degree of regulatory control necessary to provide reasonable assurance of safety and effectiveness". They continued this approach for several years which resulted in several software releases with flaws which occasionally even led to some deaths (Cortez, 2014).

Alternatively, the FCC took a more aggressive approach with its regulations of a disruptive innovation. The internet took the world by storm and quickly became a challenge for

the FCC to regulate its service. In the early 2000s, the FCC publicly announced a threat to internet service providers should they violate rules around net neutrality. A company did just this and as a result the FCC created a "legally binding rule" to enforce regulating internet freedoms. As a result, this rule began strictly enforcing internet services in the U.S (Cortez, 2014).

A "regulatory toolkit" for disruptive innovations has also been developed by Cortez. This contains four key components for regulatory decision-making: timing, form, durability, and enforcement. Timing consists of when an agency should focus on regulating an innovation. Form is the type of regulation an agency introduces. These can consist of a rule, adjudication, guidance, or some other way of regulating an innovation. This pairs with durability which is defined as how long a certain form is implemented for an innovation before it is altered. Finally, enforcement is defined as how strict a regulation is imposed on an innovation and what kind of sanctions are imposed with a regulation violation (Cortez, 2014).

Within nuclear security, regulations are important as they establish a standard for procedures and protocols at nuclear facility. Although development is a tedious process, the sensitivity and severity of the security of nuclear material can help prioritize new policies surrounding the field. Regulations can help to minimize adverse impacts emerging technologies have in nuclear security. Innovations such as UAS are a sort of middle ground in that they are not exclusive to nuclear facilities and are recreationally used around the world. Because of this, the FAA and NRC may be required to collaborate more carefully with different agencies such as the Department of Commerce or Small Business Administration in developing nuclear security regulations or policies. This would be done so as not to compromise independent businesses' production of UAS. Collaborations with these agencies or businesses can also open

opportunities for companies to account for restricted airspace (such as more detailed geofencing) enforced by the FAA when developing future UAS products.

Depending on the quantity and severity of cases involving UAS at high profile sites, regulations may be more prioritized to help lessen the threat of UAS. The following section discusses known case studies involving drones, the outcome of each incident, and a proposed structure for the theory that can be applied to different areas of focus outside of business (including nuclear security).

CHAPTER THREE:
MATERIALS AND METHODS

Additional information was gathered and combined with the current literature to help explain how a business model can be translated to the nuclear security field as a way of evaluating emerging technologies. Security incidents where UAS was involved were presented to show the growing trend of UAS use around nuclear facilities and other high-profile areas. Although some cases are not at nuclear facilities, they are important to consider because they have aspects that can present similar security risks at nuclear facilities.

The fundamentals of the disruptive theory of innovation that were discussed in Chapter Two were then analyzed to give a general structure for how the theory can be applied to nuclear security at facilities. Disruptive theory has characteristics that are analogous to aspects of nuclear security. Although disruptive theory is a business model, it has the potential to be used as an additional assessment of emerging technologies within a chosen time frame of reference to help determine the past, current, and future impacts it may have within nuclear security.

Once the structure and process were developed, the case studies were used to fit aspects of disruptive theory to UAS technology. The incidents presented were analyzed to determine how much they aligned with the disruptive theory of innovation. This discussion is presented in Chapter Four to explain the use of the theory in nuclear security and how it has potential to be a useful tool in analyzing innovations within nuclear security.

Case Studies

Incidents involving UAS have occurred around the world over the past decade. Various case studies were found which demonstrate UAS technology trends within nuclear security. While the whole story behind a case study may not be fully known to a reader, it can still provide

useful information for portraying the threat or application of UAS. Cases used in this study were at nuclear facilities; however, there are cases available which demonstrate other uses for UAS as a threat or tool that did not occur at nuclear facilities. It should be noted that the cases used were only what was openly available – there may be other cases of UAS sightings that were not made public.

The cases highlighted in the following chapter come from Israel, France, Saudi Arabia, and the United States. While the situations in each country were different, they show different ways in which UAS can be used. Although some did not take place at a nuclear facility, currently there is no reason to believe that a security incident of the same or similar scenario could not occur at a facility. Each case is evaluated and analyzed to find patterns or trends that can be applied to disruptive theory. The translation developed in the following section is then used to justify the use of the theory in nuclear security. For reference, the incidents that are highlighted occurred from 2012 to 2019.

Developing a Translation of Disruptive Theory

The fundamentals of disruptive theory have been described in Chapter Two. These pillars give a structure that opens opportunity to translate this theory into other fields, including nuclear security. By using features that can be applicable to nuclear security, disruptive theory can provide an additional method of evaluating technologies either used as beneficial tools at facilities or as malicious tools by adversaries. It can give a new perspective on how technologies have or may impact in nuclear security.

It is important that disruptive theory be broken into a structured format in order to create a more versatile application of the theory. This can allow the theory to be expanded outside of the business world and used to analyze technologies in other fields like nuclear security. The

translation presented in this paper aims to use emerging technologies, namely UAS, in nuclear security as an example to demonstrate disruptive theory in a different application.

The development for applying the theory's translation to nuclear security was as follows:

1. Identify the main steps and reference time frame of the disruptive process.
2. Establish nuclear security equivalent terminology with the business terminology within disruptive theory.
3. Connect the definitions with the structure of disruptive theory.
4. Based on the nuclear security format of the theory, determine the level of disruption by the technology of interest based on examples of its use within a reference time frame.

The initial step involved choosing a time frame for reference and developing a more rigid structure of the disruptive theory of innovation. Simply analyzing the impact of UAS during one incident would not be sufficient evidence of disruption (or lack of) because the theory requires patterns and trends to determine the impact an innovation has in a given market. Patterns are best determined over a ranged period of time to better understand where a product started and how it got to the place in the market that it is currently at.

Next, terminology for nuclear security was developed to be analogous to business terms. The key terms for the scope of this paper were: consumer, potential disruptive innovation, incumbent, market, sustained innovation, incumbent trajectory, and incumbent capability. These definitions were found to be the most relevant in analyzing disruptive theory for use in nuclear security. Each term applied to a critical aspect of nuclear security from either a facility or an adversary perspective. This was done to present application of the theory from both sides of the field to better analyze the practicality of disruptive theory in nuclear security as whole.

Better organizing and structuring of the disruptive theory has potential to enhance its applicability outside of the business world. King and Baatarogtokh's explanation of disruptive theory is a good starting point for developing four clear pillars of the disruptive theory process. These four steps in the process were recognizing a new disruptive innovation on the market, continuation of the incumbent's products with sustaining innovations, the incumbent's failure to catch up to the new innovation on the market, and finally the incumbent succumbing to the disruptive innovation. The framework introduced by Schmidt and Druehl was then combined into this structure to fill in some missing gaps of the four-step structure of King and Baatarogtokh. By doing so, the structure of the disruptive theory of innovation was laid out in the following steps:

1. Identifying the innovation to analyze.
2. Determining the frame of reference to for the innovation.
3. Recognizing of the potential disruptive innovation by the incumbent on the market.
4. Identifying market areas that appeal to consumers and what attributes the product offers.
5. Continuing to develop sustaining innovations.
6. Budgeting resources to spend on developing a product to match the disruptive innovation.
7. Failing to catch up to the disruptive innovation.
8. Succumbing to the disruptive innovation.

Once terms were defined for nuclear security, they were mapped to the disruptive theory process mentioned above. This step filled in the blanks of the process and laid out a way for the

theory to be applicable to nuclear security using UAS as the example innovation. Once fitted to the structure, an analysis of the innovation was developed.

The final step involved determining the level of disruption of the innovation. Disruptive theory does not have a way of evaluating the impact of a disruptive innovation unless an incumbent completely succumbs to the product by going bankrupt. The level of disruption in each case involving UAS was the outcome of the security incident. The impacts addressed from each case were then discussed to explain the application of disruption theory to UAS and the overall practicality of the theory in nuclear security.

CHAPTER FOUR:
RESULTS AND DISCUSSION

Translation of the Disruptive Theory of Innovation

Nuclear security is a dynamic environment. It is critical to evaluate every aspect to protect the material from malicious actors. The following translation of the disruptive theory of innovation is presented to describe its practical use outside the business realm. Nuclear security terms were defined in a way to match up with the business terms used in disruptive theory. Facility and adversary perspectives were considered when defining the terms. This allowed for different ways of using the theory in evaluating UAS technology. Each step in the process developed in Chapter Three is analyzed to present the disruptive theory of innovation's potential for the nuclear security world. The nuclear security equivalent definitions from facility and adversary viewpoints can be found in Table 1 and Table 2, respectively.

General Definitions

The market for the disruptive theory of innovations was defined as nuclear security. For both facilities and adversaries, security can be considered as the market because it involves everyone who may use UAS technology. Since the market is where an innovation would be advertised, UAS can be used as a beneficial or malicious tool, it becomes the market for the scope of this paper. This definition is important because it is what businesses aim their products at to maximize the products' impact within the market.

UAS was defined as the potential disruptive innovation to be analyzed and applied to the theory. In terms of nuclear security, UAS is a relatively new technology being used by facility personnel and adversary threats. While publicly known incidents involving UAS may be limited, the technology has begun making an impact in the field and drawn heavy attention by nuclear facilities. Adversaries are also learning new and innovative ways of using this

Table 1. Disruptive theory analogies from a nuclear facility perspective

Business Term	Nuclear Security Equivalent
Market	Nuclear security
Potential disruptive innovation	UAS technology
Incumbent	Adversary forces
Consumer	Nuclear facility
Incumbent trajectory	Continuation of traditional adversary tactics
Sustained innovation	Improvements to adversary equipment (firearms, vehicles, etc)
Incumbent capability	Adversary methods against UAS
Incumbent succumbing	Adversary threat mitigated using UAS

Table 2. Disruptive theory analogies from an adversary perspective

Business Term	Nuclear Security Equivalent
Market	Nuclear security
Potential disruptive innovations	UAS technology
Incumbent	Nuclear facility
Consumer	Adversary
Incumbent trajectory	Security methods
Sustained innovation	Improvements to traditional security methods
Incumbent capability	Nuclear facility UAS mitigation regulations/protocols
Incumbent succumbing	Facility security measures fail/nuclear material or other sensitive information obtained

technology in ways which may catch a facility off guard. Some of these tactics may include more than just surveillance such as a kinetic attack or material smuggling. Cases involving various uses of UAS are discussed later in this chapter.

Nuclear Facility Perspective

The initial analysis for translating disruptive theory was done from a protective nuclear facility perspective. UASs can inspect hazardous areas of a facility including around a reactor or dangerous mechanical components like a turbine. This could help mitigate any tampering of critical parts of a facility. Facilities are constantly protecting vital areas that contain nuclear material or areas that are vital to the operation of the facility. UAS technology offers benefits that can bolster a nuclear facility's security design including added visual capabilities and quick response to an alarm that may be triggered.

In the context of the literature presented in Chapter Two, the consumer is defined as the individual or group who uses a product within that product's target market. Because the market and product have been defined as nuclear security and UAS technology, respectively, the consumer in the market for UAS would be the nuclear facility or personnel from the facility for protective or proactive tools. Nuclear facilities' research and use of UAS technology for security purposes is an indication that a new innovation has entered a market and is being used by its target consumers.

Next the incumbent was defined as the group in nuclear security that bases its success on current available products (or methods). In this case, adversaries can be considered the incumbent against a nuclear facility because they are the group defending themselves against the potential impact of a disruptive innovation presented to the market. In the previous example involving Kodak's digital camera, Sony and Canon were considered as the incumbents because they were the leading companies in the camera market. The incumbent and consumer are two of

the major pieces involved in applying disruptive theory because they are the backbone of whether or not an innovative technology is successfully implemented in nuclear security.

Sustained innovations are innovations whose capabilities and performance are improved to maintain their use to a wide base of users. Instead of developing something that could disrupt the market, an incumbent will instead improve upon its products to keep its current consumer audience. In nuclear security, sustained innovations can be considered as traditional technologies or tactics that are commonly used and upgraded by the incumbent. In this case, since the incumbent is viewed as the adversary, sustained innovations developed by this group would be upgrades to vehicles, weaponry, or any tools which a malicious group might traditionally use to illicitly obtain nuclear material or disrupt operations at a facility. Because UAS has not been traditionally used in the past by adversary groups (or information about its use is unavailable to the public), they would not be considered as a sustained innovation in nuclear security from this perspective. Until there is enough data to confirm that UAS is now almost expected during any security incident, it was not considered in this definition.

The final two definitions for disruptive theory as it pertains to nuclear security are incumbent trajectory and incumbent capabilities. Incumbent trajectory is the prediction of the incumbent's success of its sustained innovations based on the new innovation introduced to the market. From a nuclear facility perspective, this would be the success of adversary tactics on a facility when UAS is involved from the facility's side. The incumbent capabilities would then be defined as the adversaries new methods of countering a facility's use of UAS to protect the material or critical areas of the facility If UAS use by a nuclear facility then successfully counters adversary threats to a defined level of satisfaction (ideally 100%), then the incumbent

would succumb to this disruptive technology until it developed its own disruptive innovation to disrupt nuclear facility operations at a high success rate.

Adversary Perspective

On the other end of the spectrum is the perspective of the adversary and malicious actors' use of UAS on a nuclear facility. UAS offers new threats on nuclear facilities which must be considered to successfully protect nuclear material or vital parts of nuclear facilities. Some of these threats include surveillance, direct kinetic attacks, or quick removal of material from a facility. If used properly, UAS could catch a facility off guard and allow for malicious groups to succeed in illicitly obtaining nuclear material for malicious use.

The market and potential disruptive innovation were nuclear security and UAS technology, respectively, and remained the same for the adversary perspective. In this case, the consumer was defined as the malicious actor using UAS to illicitly obtain nuclear material or disrupt nuclear facility operations. Some examples of adversary use of UAS against facilities includes hidden surveillance, explosive deliveries, or removal of material from the area. Swarming could even enhance the effects of these threats. These will be discussed in greater detail at the end of this chapter.

The incumbent defending against the potential disruptive innovation from the adversary perspective is the nuclear facility. It was not confirmed that facilities use UAS for practical purposes as this information may not be available on the open web. Therefore, it was assumed that facilities did not use UAS technology for the incumbent definition. If an incumbent succumbs to a disruptive innovation, then it may heavily regress or even go bankrupt. From this, facilities acting as incumbents is appropriate because if security measures fail during a security incident, the outcome would be significant.

Sustained innovations of the incumbent from an adversary's perspective were considered as typical security measures a nuclear facility may employ in its security design. Facilities are on constant alert and use a variety of tools and methods to implement their security systems. Cameras, alarms, sensors, guards, guns, and gates are commonly used by facilities to deter actors from unauthorized access and attempts at stealing nuclear material. For a sustained innovation, some of these technologies currently used may be upgrade to state-of-the-art systems to help further reinforce a facility. This would essentially ignore potential use of UAS by a nuclear facility, which falls in line with the definition of sustained innovation presented by Christensen in 2006.

Incumbent trajectory from the adversary perspective was defined as the success of facilities to deter an attack with UAS involved from the adversary side. If UAS becomes a prominent threat and cannot be successfully handled by facilities, then this may indicate that facilities will succumb to UAS and attacks from malicious actors will become more common. Conversely, incumbent capabilities would be resources a facility would spend to deter UAS threats. Alternatively, capabilities could be the time facilities have to respond to a fast growing UAS threat should one facility report a major security incident.

For the adversary perspective, the incumbent succumbing would be nuclear facilities. This could be a number of things including material being obtained or a major disruption to nuclear facility operation. For example, a damaged turbine at a nuclear power plant could have severe economic consequences, could shut down a facility for an indefinite time, and be very expensive to fix. An example of a security incident similar to this is presented in the next section.

Security Incidents Involving UAS – A Growing Trend

UAS technology is a growing trend worldwide. With the increase in availability and capability, this emerging technology has begun popping up around areas of national security. In 2012 a rudimentary drone was spotted at a nuclear facility in Israel. In 2014 and 2016, a combined twenty-one separate sightings around nuclear facilities were seen around nuclear power plants in France and the Savannah River Site in the United States. In every scenario, the motive was unknown, but the intent must be considered malicious due to the nature of the facilities where these incidents occurred.

Israel

One of the simplest cases of UAS technology seen near a nuclear facility was back in 2012 in Israel. Hezbollah militia members created a drone using makeshift parts. The drone was caught taking pictures of the Dimona nuclear research center before flying off back to its origin. In this case, the device was shot down approximately 10 miles from the research center. The intent of the Hezbollah was unknown in this case and it is not known if the surveillance feed was viewed at a remote facility (Times-Dispatch Staff, 2012).

This incident in Israel demonstrated the ease at which UAS could be accessed. In this case, it was made from various parts from an outside source. After the device was recovered, authorities determined that this drone had similar capabilities as drones available at a store.

In terms of disruptive theory (as a fixed scenario), this case can be broken down using the translation described in the Materials and Methods section. The incumbent (nuclear facility) was not prepared for the small business innovation (adversary UAS). Incumbent protocol and handling was the use of ammunition to bring down the drone. Incumbent succumbing would occur in this incident if it was confirmed that surveillance feed was sent to an adversary remote

facility. This was not confirmed during this incident; however, given the sensitivity of information about a nuclear facility, it cannot be assumed the information was not transmitted.

France

France also experienced UAS sightings over several of its nuclear facilities. As previously mentioned, sightings occurred in 2014 over 13 nuclear power plants in the country (Phillips & Gaffey). Similar to Israel, the intentions of the drone operations were not entirely clear; however, the incidents were still worrisome to France's national security.

In 2018, another UAS incident occurrent in France when Greenpeace, an international environmental organization, flew a drone (and an additional drone filming the other drone) into a nuclear power plant and crashed it into a wall. The purpose of this incident was to demonstrate the vulnerabilities and lack of airspace protection of a nuclear facility by using UAS technology. The device essentially went untouched while in flight and crashed into a wall which housed spent nuclear fuel (Gliadkovskaya, 2018).

Disruptive theory can be applied to these incidents in France as a short process. In either French case presented, the incumbent is the nuclear power station while the small business innovation is the UAS technology used by the consumers (anonymous parties and Greenpeace). In 2014, the drone operators started out with a more "harmless" use of the technology. Although anonymous with unclear intent, it should be assumed that the drones were used for surveillance and transmitting information about these power plants to a remote location. This fixed point scenario may not suggest disruptive characteristics; however, when paired with the later instance in 2018, it can show the evolution of the technology and how it can be used against nuclear security.

The Greenpeace incident demonstrated a significant feature of UAS technology as well as flaws in the security design of the power plant. First, although not explicitly stated in any public

reports, it should be noted one of the drones from a 2014 incident could have been operated by Greenpeace. With that in mind, 2014 and 2018 could show the progress of how an organization begins to plan malicious intent against a nuclear facility. Even if Greenpeace was absent from 2014, this time frame still demonstrates the evolution of uses of UAS against nuclear facilities, with 2018's incident exhibiting a bigger impact than previous situations. Additionally, this is one of the first documented situations where UAS infiltrated a facility's security system and reached a highly sensitive area of the complex. Although no material was stolen from the facility, this situation is still analogous to an incumbent succumbing to a disruptive technology due to security measures failing to mitigate the UAS threat.

United States – Savannah River Site

The Savannah River Site (SRS) experienced several drone sightings over the course of about two weeks in July 2016. This is one of the earliest publicly known incidents of UAS technology used at a nuclear facility in the United States. During these sightings, the drones were spotted within unrestricted SRS air space near sensitive areas including a mixed oxide facility. Once again the intent of these drones was unknown, but each was perceived as a threat because the SRS is a facility with concern for national security (Gardiner, 2016).

This case involving UAS had many similarities to France's cases in 2014; however, the SRS is not a nuclear power plant and instead processes nuclear fuel for alternative uses. The intent was unknown in this case as well, but this initial presence of UAS at a United States nuclear facility is significant as it can trigger future incidents involving the technology.

Applying the fundamentals of disruptive theory at a fixed point in the SRS incident yielded similar a similar outcome as France in 2014. The small business innovation did not necessarily overtake the incumbent, but the incumbent did not do anything to keep up with the innovation's presence - the SRS did not capture or shoot down any UAS while in the site's air

space. In both situations, a lack of protocol or regulations against mitigating a UAS threat caused the outcomes which occurred since the drones returned to their origins.

Saudi Arabia

An incident involving a UAS attack on an oil refinery in Saudi Arabia was recorded in 2019. Unlike the incidents previously mentioned, this attack did not occur at a nuclear facility; however, it is an incident that should be analyzed to present a real life attack using drones that had a major impact after the incident. During this incident, drone strikes were launched against the Saudi Aramco oil processing facility in Abqaiq. The resulting damage cut Riyadh's oil production in half (Kagan, 2019). Another attack was also launched 150 miles away in the Khurais oil fields. The combination of these attacks caused roughly 6,000,000 barrels of oil/day to be lost in Saudi Arabia and caused barrel prices to rise approximately $9/barrel (Krane, 2020).

This incident did not involve a nuclear facility and the drones used were closer to military grade; however, an attack on a larger scale can be useful to analyze the threat of UAS in general and the impact it has potential to cause. An oil refinery has several similarities to a nuclear facility including generation of an energy source and large operating equipment. Both of these aspects are vital to the operation of either facility and any form of assault on either could cause major damage as demonstrated in the Saudi Aramco attack. If a nuclear facility were attacked in a similar fashion, the reactor may be targeted as this is the main source of energy at the facility. Turbines, pipelines, or other important buildings may be targeted as well to significantly disrupt operations at the nuclear facility.

One thing to note is that while recreational drones are more widely available to adversaries than military grade drones, they still have potential to cause widespread damage to a nuclear facility although the payloads would be more limited. Swarming could still create a major threat because instead of a single 100 lb bomb strapped to a larger UAS, ten smaller

drones carrying 10 lb payloads could instead be used in a coordinated attack. Additionally, more drones might be more difficult to contain around a nuclear facility especially if guard or counter measures are limited. These could target less reinforced buildings, such as administrative or operator buildings, and halt operations at a nuclear facility. Because drones can be autonomous and operated from long distances, tracing these back to the sources might be difficult and take time, allowing for the operator(s) to coordinate the hit anonymously.

Regulatory Gaps Involving UAS

Federal Aviation Administration and Nuclear Regulatory Commission

Currently there are no regulations in the United States involving UAS use or how to mitigate this threat at nuclear facilities. Everything related to UAS is dictated by the FAA. This causes issues in the nuclear security field as the only regulations available define facilities as restricted airspace for UAS. Without regulations, UAS technology has the opportunity to play a large role in nuclear security as a tool and a threat.

It is not openly known as to whether the NRC is in communication with the FAA in developing regulations for mitigating UAS threats at nuclear facilities. The occurrences in the United States from 2016 may not have been enough to warrant discussion for regulations; however, other incidents with drones that were not made public may have occurred and gave the organizations reason to begin discussing regulations.

One big regulatory gap is deciding which agency has full authority in the air space of a nuclear facility. The FAA can control the air space over a nuclear facility, but further action towards UAS in that air space is not regulated. This could cause some confusion on how to handle suspicious drones in the area as the FAA handles airspace, but the drone would be in the general area of a nuclear facility. The issue of when a suspicious UAS can and should be

handled becomes the main issue that must be clearly addressed for a given situation by either a federal guidance or regulation.

UAS in Nuclear Security Series

The IAEA's NSS documents provide guidance for the protection of nuclear and radioactive material at facilities and in transport. UAS technology is not mentioned in any of the four NSS documents previously listed. One possible reason for this is the relative newness of UAS in nuclear security to the point that the IAEA has not decided to pursue recommendations on how to handle UAS threats.

A major challenge in developing a guide or adding amendments to NSS 9, NSS 11-G, NSS 26-G, and NSS 27-G is how to properly assess a UAS threat from a benign recreational drone. Operators or facility personnel would follow protocol when spotting a drone up until a decision to neutralize or ignore the drone is made. Should a decision be made to attempt to neutralize a drone, options would be decided based on further protocol; however, the decision would need to avoid drawing attention to the material as best as possible if it was a single drone with no other adversaries nearby. The NSS documents could help in smoothing out this decision-making process for nuclear or radioactive material at a facility or in transport.

Disruptive Innovation Regulations

The toolkit introduced by Cortez shows promise when regulating UAS use in nuclear security. When combined, the four components of this toolkit could aid in developing some form of enforcement for the use of UAS technology in nuclear security. With the increasing trend of drone sightings near nuclear facilities around the world, the timing of a rule or regulation surrounding UAS technology would be beneficial for the security world. The timing of the regulation is crucial in preventing material from being stolen or a facility being tampered with which could have significant consequences.

The next step is how the technology would be handled in the regulation. This action would fall somewhere between the FDA and FCC examples previously presented. Empty threats against UAS technology could lead to the technology becoming uncontrollable in nuclear security. On the other hand, early and aggressive threats against UAS could significantly limit the potential uses of the technology in nuclear security. The responsible agencies (namely the FAA and NRC) for how to handle UAS technology in nuclear security would need to collaborate in developing a guidance for drones in the U.S. Additionally, these agencies would also benefit from discussions with the international community via the IAEA.

Applying the Disruptive Theory of Innovation to UAS

The final step for this analysis is to take the structure developed in Chapter Three and apply it to the collective information presented in the case studies. This analysis provides a qualitative approach for applying disruptive theory to nuclear security using UAS as the example innovation.

The very first step of the structure presented is simply identifying the innovation to be analyzed. UAS was chosen because it is a rising topic in nuclear security and has increased as a threat over the years. It may still be in the early stages of its place in nuclear security, but UAS has potential to make a big impact in the field for a variety of reasons. Its versatility, its almost annual performance improvements, and new aerial dimension can be beneficial to the field or act as a major adversary threat.

The time frame used for disruptive theory was the range of the case studies presented. This was from 2012-2019, offering nearly a decade of time to assess UAS technology. For disruptive innovations, the time they take to disrupt a market can vary. One factor for this would be the market, and while nuclear security is an evolving market, it does not necessarily occur

overnight. Some reasons technologies in nuclear security may not have immediate impacts are performance requirements and regulations.

Recognizing a potential disruptive innovation on the market is an important step to counter or mitigate the impact of the innovation. For facilities, quickly developing protocols and regulations on how to respond to UAS threats could help minimize any impact they may have in nuclear security. On the other hand, adversaries recognizing that nuclear facilities have begun utilizing a new technology could change their way of planning an attack. Regardless of the innovation of interest, early recognition and response to a new innovation can help lessen its impact and avoid negative outcomes for an incumbent. For nuclear security, this is important because if adversary UAS use becomes a widespread technique against facilities, the likelihood of future attacks could increase with disastrous consequences such as missing material or public panic.

As previously mentioned, UAS has attributes that are attractive to both nuclear facilities and malicious actors. This step of the theory looks at these attributes and answers the "why?" question for what draws the product to the consumer. UAS offers a new aerial characteristic that can be manually controlled or even autonomous and its performance capabilities have been significantly improving since they were brought on the market. From a nuclear facility perspective, this could allow for miles of surveillance and for quick response to a location of an ongoing security incident. For adversaries, this could also allow for a larger range of surveillance, but also a quick way to deliver an explosive payload to a location. These are just a few examples of why UAS may be an attractive product. Different uses and techniques may also be developed over time with this technology that have not been conceptualized yet.

Sustained innovations are developed as an attempt to improve upon current products and ignore any noise a disruptive innovation may be causing in the market. While use of the innovation may increase, sustained innovations by the incumbent almost ignore the development of a disruptive innovation to keep its use with a wide audience. For nuclear security, ignoring potentially disruptive technologies could carry significant consequences because even just one successful attack on a facility could spark a chain of future attacks until the innovation is better handled. From the facility perspective, adversaries may not see the benefit of using UAS on their own and instead prefer having additional ground forces when planning an attack. This would leave room for them to instead upgrade any weapons or traditional tools used by malicious actors. These sustained innovations by the adversary may or may not be sufficient to successfully attack a facility that utilizes UAS technology in its security design. For the adversary point of view, nuclear facilities may underestimate the potential for UAS use by malicious actors. In this case, they may just upgrade their current alarm or sensor systems to more state-of-the-art designs and not find the benefit of UAS at the facility. These traditional security measures implemented by facilities may not be sufficient in mitigating UAS threats and instead be nearly ineffective in countering this technology during an attack.

Budgeting resources to counter a disruptive innovation creates opportunities for the incumbent to plan for countering a disruptive innovation. The increasing trends of UAS spotted at high profile facilities has put UAS on the map as a security concern. It is likely that nuclear facilities have begun counter UAS measures and how to allocate resources to minimize the effects of this technology. Also, facilities may be in communication with the FAA and NRC to develop regulations that help structure responses to UAS threats at nuclear sites. On the adversary side, resources may be spent on tools to bring down UAS at nuclear facilities.

Alternatively, UAS may be used as a method for countering drones at a nuclear site. This could include distractions for ground forces or developing techniques to remove UAS with their own drones. Overall, the budgeting of resources may be dependent upon the current impact UAS has in nuclear security at any given time. If UAS is not deemed a big concern over an arbitrary time frame, fewer resources may be spent than if it is a high threat security concern. With limited information available, this step of the disruptive theory is difficult to assess, but some potential inferences can be made as to how resources may be budgeted to counter UAS from either perspective.

Because of the limited amount of information available to the public in the area of UAS, it is difficult to assess the final two steps of the disruptive theory of innovation as it pertains to security. Nuclear facilities may never truly fall behind when considering how to react to a newly developing threat such as UAS. There may be a time gap for when a regulation is developed to help create procedures on how to counter adversary threats using these emerging technologies, but they would never simply be ignored if they had potential to cause future security incidents. A limiting factor in this step for a nuclear facility may be the allocation of resources if UAS was not deemed a serious enough threat at that site. This would limit security measures designed to counter UAS and may open better opportunities for adversaries to utilize these tools in a quick enough time span to cause a significant impact in the nuclear security world. At the same time, adversaries may not necessarily give up their intentions because of the presence of UAS at a nuclear facility. Instead they may adapt or change their tactics when planning an attack to illicitly steal nuclear material. Again, resource budgeting to counter a potential disruptive innovation is critical for either side of the spectrum as this step lays out how they plan to work around emerging technologies such as UAS.

The final step of the structured disruptive theory is the incumbent succumbing to the disruptive innovation. The only case study presented that demonstrates an incident with major consequences was the attack on the Saudi Aramco oil refinery. During this incident, the incumbent, the refinery, was not sufficiently prepared for a drone attack of this proportion. While the drones used were military grade or close to it, swarming of smaller, publicly available drones could potentially still have had a similar impact if coordinated properly. Even though this incident was not a nuclear facility, a smaller scale attack done in a similar manner could still have severe consequences even with drones that do not have the same capabilities as a military grade one. It is uncertain if UAS has been used to successfully deter an adversary threat at a nuclear site. Regardless, if more incidents occur at nuclear sites and an adversary successfully obtains nuclear material or site information like the Dimona facility incident, it could reinforce this step for UAS becoming a disruptive innovation in nuclear security. Table 3 provides a summary to better visualize the structured steps of disruptive theory and how it can apply to nuclear security. For reference, the incumbent in the nuclear facility equivalent step is the adversary and the incumbent in the adversary equivalent step is the nuclear facility.

Table 3. Structured disruptive theory of innovation process as applied to nuclear security

Business Step	**Nuclear Facility Equivalent Step**	**Adversary Equivalent Step**
Identify the innovation to analyze	UAS is the chosen innovation	UAS is the chosen innovation
Determine the time frame of reference	2012-2019	2012-2019
Recognize the potential disruptive innovation by the incumbent in the market	Adversary changes tactics to attack a facility that uses UAS	Facility develops protocols or regulations to systematically respond to UAS threats
Identify what attributes the product offers to consumers	Autonomous, aerial characteristic with wide range surveillance	Autonomous, aerial characteristic with wide range surveillance, quick payload delivery
Continue to develop sustaining innovations	Adversary weapons or equipment upgrades	Current security system upgrades at the facility
Budgeting resources to spend on developing a product to match the disruptive innovation	Investment in tools or techniques to disable UAS at nuclear facilities	Facilities invest in counter UAS measures
Failure to catch up to the disruptive innovation	Adversaries do not effectively adapt to UAS use at facilities	Lack of regulations or facility does not have sufficient security systems to counter UAS
Incumbent succumbs to the disruptive innovation	Adversary threats are constantly mitigated through use of UAS technology	Material is stolen, significant socioeconomic events occur

CHAPTER FIVE:
CONCLUSIONS AND RECOMMENDATIONS

Conclusion

The disruptive theory of innovation was introduced as a way of evaluating the impact of an emerging technology in nuclear security. UAS has become an emerging threat at nuclear facilities. Sightings have increased over the past decade which has drawn attention to the technology. Because UAS is a potential tool for both facilities and its adversaries, both perspectives were considered and addressed to better demonstrate the disruptive theory of innovation's potential for the nuclear security world.

UAS is attractive to both ends of the nuclear security spectrum because it adds a new dimension to security by opening an aerial opportunity to either protect or threaten a nuclear facility. Aerial mobility allows for UAS to travel to a specified location within a short period of time. For facilities, this allows for a very quick response to a security incident. This quick response is vital should the incident be significant and not a false alarm.

On the other hand, UAS allows for distant and subtle surveillance with a 360^{o} view for adversaries. While surveillance is a common tactic, UAS can also be used to distract a facility and open up ground opportunities for ground forces. Additionally, IEDs, RDDs, or other explosives may be attached to UAS to deliver a payload and significantly disrupt a nuclear facility. Swarming of UAS with or without payloads can also have a severe impact against nuclear facilities. Large numbers of weaponized drones could prove difficult to mitigate if a nuclear site was not sufficiently prepared for an attack of this nature.

The case studies presented all had one common theme – a lack of handling a drone while near a nuclear facility. While Israel eventually shot down the drone 10 miles from the Dimona

nuclear research center, it still allowed the vehicle to photograph critical areas of the facility. The uncertainty of whether the pictures or video feed were transmitted or not is alarming as valuable data could end up in the possession of a malicious group. France had several occurrences between 2014 and 2018. One of these instances involved a UAS actually breaching a power plant's walls and making contact with a concrete wall. Although there was no harm to the personnel or facility, the fact a drone was able to get as close as it did to a key part of the power plant raised concern. In the United States, multiple drones were spotted over the SRS. The intent of these was unknown, but an increase in UAS incidents could indicate that they will play a role at nuclear facilities and cause security threats in the future.

Disruptive theory was laid out in a more rigid structure to help assess the impact of UAS over the past decade. The cases presented help show the beginnings of how a disruptive innovation can disrupt a market. UAS technology has grown in trends and since 2012 has been increasingly spotted around nuclear facilities. It is possible that there are even more instances of this, but information may not have been made available to the public so this cannot be confirmed. Even if information is upheld, it is critical that the UAS technology be carefully analyzed to assess its impact on nuclear security. Vulnerability assessments can help greatly with this, but disruptive theory can provide a more systematic approach to how a facility views the technology over time. A combination of these two methods could help prevent a significant future attack on a nuclear facility or material in transport and help bolster the fundamentals of security against future emerging technologies.

The structure that was developed to provide a more systematic approach to using the disruptive theory of innovation. The eight-step process presented allows for analysis at various phases of the disruptive process. Clear designation of the innovation and supporting evidence

during each step is critical when applying the disruptive theory of innovation to a different field other than business. For nuclear security, both the facility and adversary perspectives gave various levels of impacts because of the case studies presented. There was minimal information about their use at facilities, but UAS has been used in adverse or suspicious ways in the past with an increasing trend over the years.

Recommendations

The information presented above was meant to help utilize a different methodology when assessing various aspects of nuclear security. Effectively using the disruptive theory of innovation and learning the full impact of an innovation can aid in the distribution of resources around a nuclear facility to prevent the threat of an emerging technology. This can help to establish different threat levels of different technologies in various areas of the world.

One way to strengthen the use of disruptive theory in nuclear security would be to quantify the findings of an assessment. As it currently is, the theory is more of a qualitative approach to addressing an innovation. Quantification of the methodology could help visualize the overall evaluation to more easily interpret the data. A chosen threshold could be used to determine risk levels for a technology by evaluating the theory at given steps and eventually as a whole after a given period of time has passed.

While the theory does have potential in nuclear security, another way it can be improved is by defining the last step, succumbing to the innovation, to a more universal definition. As it currently stands, succumbing to UAS could range anywhere from a picture taken from the drone or coordinating a full attack on a facility and material being successfully stolen. Another way a facility could succumb is if it uses more resources to remove a threat than an adversary used on its UAS. Having a firmer definition of what it means for a facility to succumb to an innovation

could improve the overall effectiveness of the theory in nuclear security for any innovation of interest.

Another way the disruptive theory of innovation could be improved for nuclear security is determining how many times a facility must succumb in order for the innovation to be considered disruptive. A single instance of material successfully being stolen could have severe socioeconomic effects, but a single picture of a facility may not be considered as significant as material being stolen. In this case, multiple instances of surveillance could be required in order to even consider UAS being disruptive. The quantification or creation of a standardized index could help coordinate the significance and recurrence of UAS incidents when determining if the technology is firmly considered disruptive.

Because UAS involves communication via cyber networks, it is vulnerable to cyberattacks. This could alter the level of disruption UAS has in nuclear security because if facilities have drones that are turned against through virtual adversary control, they could be utilized by actors in different ways to gather more information at a facility or distract/interfere with guards or facility operations. Alternatively, cyber could be considered an entity of its own for analysis using disruptive theory. Other areas of cyber such as

Finally, to aid in regulating UAS technology use and neutralization of threats, the IAEA could also begin developing a technical guidance centered around drones. These differ from an implementing guide like NSS 9-G (Rev. 1), NSS 11-G, NSS 26-G, and NSS 27-G in that technical guides provide information and guidance in a more specific area compared with an implementing guide. Alternatively, a technical guide could be developed for all emerging technologies in nuclear security.

Nuclear security is an everchanging system with more and more complexities developing within the realm. Technologies are constantly developing and being used in different and innovative ways to either protect material or plan to steal it. The current methodologies within nuclear security are more for a fixed-point assessment. The disruptive theory of innovation allows for a collection of these methodologies to systematically evaluate innovations are involved with vulnerability assessments or tabletop exercises over a range of time. While it may have its flaws just like any evaluation method in nuclear security, the disruptive theory of innovation can provide a different perspective to assess the impacts of technologies in the past and potentially predict the impact it may have in the future. It is vital that nuclear material does not get in the wrong hands. The disruptive theory of innovation can be used to help minimize adversaries' chances of illicitly obtaining this material or causing severe socioeconomic events for malicious use by better preparing facilities against emerging technologies against those sites.

REFERENCES

Aaron, A., Anderson, K., & Fialkoff, M. (2018). *Unmanned Aerial Systems as an Enhancement and Threat to Material Transport and Physical Security.* Vienna: International Atomic Energy Agency.

Alkobi, J. (2019, January 15). *The Evolution of Drones: From Military to Hobby to Commercial*. Retrieved from https://percepto.co/the-evolution-of-drones-from-military-to-hobby-commercial/

Araújo, K., & Gomera, J. (2016). *Disruptive Change in Unmanned Aerial Systems, Nuclear Facilities, and Radiological Protection: A Review of U.S. and French Developments.*

Christensen, C. (2006). The Ongoing Process of Building a Theory of Disruption. *The Journal of Product Innovation Management*, 39-55.

Christensen, C., McDonald, R., Altman, E., & Palmer, J. (2018). Disruptive Innovation: An Intellectual History and Directions for Future Research. *Journal of Management Studies*, 1043-1078.

Christensen, C., Raynor, M., & McDonald, R. (2015). *What is Disruptive Innovation?* Harvard Business Review.

Cortez, N. (2014). *Regulating Disruptive Innovation.*

FAA, F. A. (2016). *81 FR 42063*.

Gardiner, T. (2016). *Eighth drone spotted in SRS skies.* Retrieved from Aiken Standard: http://www.aikenstandard.com/article/20160706/AIK0101/160709671

Gliadkovskaya, A. (2018). *Greenpeace Activists Pilot and Crash Drone into French Nuclear Plant's No-Fly Zone.* Retrieved from https://www.euronews.com/2018/07/03/greenpeace-activists-pilot-and-crash-drone-into-french-nuclear-plant-s-no-fly-zone

IAEA. (2018). *Physical Protection of Nuclear Material and Nuclear Facilities.* Vienna: International Atomic Energy Agency.

IAEA. (2019). *Security of Radioactive Material in Use and Storage and of Associated Facilities.* Vienna: International Atomic Energy Agency.

IAEA. (2020). *Security of Radioactive Material in Transport.* Vienna: International Atomic Energy Agency.

IAEA, I. A. (2015). *Security of Nuclear Material in Transport.* Vienna: International Atomic Energy Agency.

Kagan, F. (2019). Attribution, Intent, and Response in the Abqaiq Attack.

Kallenborn, Z., & Bleek, P. (2018). Swarming Destruction: Drone Swarms and Chemical, Biological, Radiological, and Nuclear Weapons. *The Nonproliferation Review*, 523-543.

King, A., & Baatartogtokh, B. (2015). How Useful is the Theory of Disruptive Innovation? *MIT Sloan Management Review*.

Krane, J. (2020). Security Amid Instability: Oil Markets and Attacks in the Persian Gulf. *Georgetown Journal of International Affairs*, 120-128.

Lochbaum, D. (2015). *Drones at Nuclear Power Plants: Enemies or Helpers?* Retrieved from Bulletin of the Atomic Scientists: https://thebulletin.org/2015/03/drones-at-nuclear-power-plants-enemies-or-helpers/

Martin, P., Tomkinson, N., & Scott, B. (2017). The Future of Nuclear Security: Commitments and Actions - Power Generation and Stewardship in the 21st Century. *Energy Policy*, 325-330.

Meola, A. (2017). *Drone Market Shows Positive Outlook with Strong Industry Growth and Trends.* Business Insider.

Phillips, C., & Gaffey, C. (n.d.). *Most French Nuclear Plants 'Should Be Shut Down' Over Drone Threat.* Retrieved from http://europe.newsweek.com/most-french-nuclear-plants-should-be-shutdown-over-drone-threat-309019

Roth, N. (2020). *The Risks and Rewards of Emerging Technologies in Nuclear Security.*

Schmidt, G., & Druehl, C. (2008). When is a Disruptive Innovation Disruptive? *The Journal of Product Innovation Management*, 347-369.

Solodov, A., Williams, A., Al Hanaei, S., & Goddard, B. (2018). *Analyzing the Threat of Unmanned Aerial Vehicles to Nuclear Facilities.*

Times-Dispatch Staff. (2012). *Hezbollah Drone Sent to Scout Nuclear Facility, Israel says,*. Retrieved from http://www.richmond.com/news/hezbollah-drone-sent-to scout-nuclear-facility-israelsays/article_3490daec-c584-53a7-b1af-24e7e3a397d0.html

Warrick, J. (2017). *Use of Weaponized Drones by ISIS Spurs Terrorism Fears.* Retrieved from The Washington Post: https://www.washingtonpost.com/world/nationalsecurity/use-of-weaponized-drones-by-isis-spurs-terrorism-fears/2017/02/21/9d83d51e-f382-11e6-8d72-263470bf0401_story.html?Utm_term=.f6742c6fd459

VITA

Jason Karcz is currently a master's candidate for the degree of nuclear engineering at the University of Tennessee Knoxville. He is a sub-contractor supporting transportation security projects at Oak Ridge National Laboratory. In this capacity, he works on projects related to emerging technologies to transport security and supports regulatory development efforts for countries drafting transport security regulations. Prior to his work in transport security, Mr. Karcz worked on dynamic modelling for the nuclear lifecycle with emphasis on the PUREX process for fuel reprocessing. He holds a Bachelor of Science in Chemical Engineering from Virginia Polytechnic Institute and State University.