Drone Attack Risk Assessment

Information Sciences and Technology

Edward Quinn, Ajay Kapur, Angela Romano,

Jong Jin Cho, Victor Lin, Iang Lin

Table of Contents

I. Introduction

Terrorism is not a new topic in today's society, as sad as it is to say that. Around the world, terrorism is a sore subject, but one that cannot be ignored due to the fact that terror attacks have become relatively more common. Terrorist attacks range from shooting to bombs to simply running people over with a car, and terrorism doesn't pick favorites nor sticks to one ethnicity, terrorism happens can happen to anyone at any given time. If we take a look throughout the year, we can highlight some of the most known terrorist attacks like the one that happened on October 31, 2017 when in New York 8 people were killed and 12 injured when an attacker drove his car onto a bike bath then proceeded to hit a school bus, killing some kids. Or we can look at the Las Vegas attack on October 1, where 59 were killed and over 500 injured when an attacker opened fire on a concert when he was in a hotel room with a vantage point. These are just simply two examples of attacks that happened just in the United State alone, with many more happening around the world.

Terrorism doesn't come from one ethnicity, according to the Oxford Dictionary the definition of terrorism is "the unlawful use of violence and intimidation, especially against civilians, in the pursuit of political aims". This is just one way to define terrorism due to the fact that we can take any kind of attack and claim it to be a terrorist attack. As technology changes and becomes more powerful, which can be viewed as good for the human race, you can also take the side that due to these technologies, terrorists can exploit this and use these technologies against us. For example, let's take a look at the typical car. Cars are used everywhere in the world and are very important in society. Cars help people get from location A to location B in a certain time frame. Typically most people don't look at cars as a type of weapon that terrorist can use, but as we look at recent attacks, terrorist can use a car to start running down pedestrians and cause a lot more harm than people would think.

In this risk assessment we take a look at new technology that has changed the way people perform certain tasks, we are talking about the Drone. Drones are new, they're the newest "big thing" in both the media and the news. Drone are considered unmanned aerial vehicles (UAV) that has a controller that the user uses to fly around the Drone. The uses of the Drone are very useful, they can help photographers capture aerial images, you can program a Drone to follow you so you take recordings while snowboarding, or skiing, or skateboarding, and many other uses that users find and make up along the way. The government has been trying to figure out how to control the use of the Drones as in where there should be do not fly zones, and the basic laws that should apply to users. Since this technology is so new, there isn't many rules or guidelines for the proper use of Drones.

This risk assessment takes a look at Drone, but in a terrorism perspective. Terrorist can get Drones easier than getting a gun, and since terrorist can easily control the Drone without being in the same areas as it, they can strap a bomb on it, or a toxin on it and fly it into a crowd of people and cause serious damage. Since there is a number of possible Drone terrorism attacks,

we are going to take a look at one in depth. We are looking at a drone terrorist attack on Beaver Stadium in State College, PA. On a typical home game at Beaver Stadium, the stadium can hold up to 107,000+ students, faculty, staff, parents, alumni, and grandparents at once, with another few thousand people outside the stadium tailgating and drinking, causing it to be a possible target for a attack.

The scenario we are evaluating in this report is as follows: it's a typical home game at Beaver Stadium and everyone's enjoying themselves and having a good time, then comes a suspicious person who starts to fly around a drone, pretending that he's recording a video for the school when in fact, he's strapped a bomb onto the top of the drone, just waiting for a time to send the drone inside the stadium to cause some harm. This risk assessment will go into deep details about what controls are in already in place, what controls should be in place, what controls are in place, how we went about defining vulnerabilities and what Beaver Stadiums vulnerabilities are.

A) Purpose

Conducting risk assessments is very crucial part of any industry, organization, or event. This is because risk assessments are meant to look at different scenarios that could possibly happen that could cause any sort of unwanted damage. The purpose of this risk assessment is to identify, deconstruct, and create preventative measures for a possible drone attack on Beaver Stadium. As a group we also aim to create certain controls that could be put in place in order to prevent any possible attacks. The use of these controls can also be changed slightly because the use of our scenario, Beaver Stadium, can also be changed for any type of sporting events or events with large crowds.

B) Scope of the Risk Assessment

The scope of any risk assessment is very important. This section is suppose to describe what the risk assessment looks at, what's included and what isn't included within the assessment. Our assessment takes a look at a scenario where a malicious person is controlling a drone with a possible bomb strapped to it. The scope of the assessment includes: Beaver Stadium, students, faculty, alumni, Beaver Stadium staff, police, State College Borough Police, and State College Community. The reason we selected these to be included in the scope is because as a group we looked at who would get impacted the most upon a possible attack taking place. What's not included in our scape is the university campus, the Bryce Jordan Center, and the other buildings and campus owned areas that surround Beaver Stadium.

II. Risk Assessment Approach

A. Student Biographies

Ed Quinn , Ajay Kapur, Angela Romano, Victor Lin, Jin, and Iang Lin have conducted this risk assessment. The students are in the College of Information Sciences and Technologies at The Pennsylvania State University.

Iang Lin is studying Information Science and Technology with the option of Integration and Application and also studying Supply Chain Management for minor. Iang's future career is focusing on IT consultant. Iang has worked in an education industries called KIPP DC during summer 2017 as Technical Support Associate. His main role in this internship was provide technical support to people with issue with the technology and worked on several technical project. Iang is a team player that like to organize the material and information for the project.

Ed Quinn is currently studying as a Security and Risk Analysis major Information Sciences and Technologies minor. Ed is working towards the Information & Cyber Security (ICS) option in SRA and looking for a focus in Incident Response and Digital Forensics. Ed is a team player who is motivated and hardworking as well as experienced in the Information Technology field. Ed has worked for three years at the Penn State Information Technology Services Help Desk and interned in the information security office at a small manufacturing company, New Pig, as well as a Pharmaceutical company, Allergan.

Ajay Kapur is also studying Security and Risk Analysis with a Information Science and Technology minor. Ajay had an internship at Nutrisystem at Fort Washington PA, under the role of Securities Intern during the summer of 2015 and worked as a Computer Support Technician at The College of New Jersey for a year. Someday Ajay hopes to build a career working in the cybersecurity field and hopes to be a CISO for a company one day. Ajay works great on a team, giving any input that he believes would be beneficial.

Victor Lin is currently majoring in Information Science and Technology in Design and Development and minoring in Security Risk Analysis. Victor's future career focuses on software development and software design. During the summer of 2017, Victor did an internship with Liberty Mutual Insurance, and he worked on server-web programming to improve his Java and coding skills. At the moment, Victor is the learning assistant/coach for IST 220: Network & Communications, and IST 230: Discrete Math. In the future, Victor hopes to use his skills and knowledge to building his own software company to help improve the lives of others.

Jong Jin Cho is currently double majoring in Security and Risk Analysis and Chinese, Minoring in History. Jong Jin Cho is currently looking for an internship. He can speaks native level of Korean and English, Intermediate level of Chinese. He can able to use Python and mySQL. Currently, Jong Jin Cho is working in Penn State Business and Auxiliary services as common desk clerk. He is looking for the opportunity to work in the United States government.

Angela Romano is currently majoring in Security Risk Analysis, with a concentration in Information Cyber Security. Angela is also minoring in Information Sciences and Technology. She is currently leaning towards a career with financial analyst. She can speak fluent English, and novice in the Italian and Spanish language. Angela is a hardworking, ethical, goal oriented person, who is passionate in the field of IT. Angela has had past IT experience through her employment with Penn State's IT Service Desk, for 2 years.

B. Hazard Identification Approach

For the risk assessment there was a three-part hazard identification process that was used. This approach involved a literature review, structured analytics, and a photographic investigation. First we investigated the protocols that are currently in place for identifying hazards such as drones before a hazard occurs. For example, we spoke with the Beaver Stadium Security Team and they currently don't have any process in place for identifying drones, seizing them, and getting individuals to safety for a malicious drone attack.

First, the literature review phase of the three-part hazard identification process relates to **Figure 1,** we found that there aren't any helpful tools at the moment that allow for drone tracking within a selected range. For example, if a home owner wanted to download a software onto a raspberry pi that is left always running and set up with notifications to notify the owner of the raspberry pi that there is a drone near his house, this is currently not an option. It would be a great way to identify the location of a drone so beaver stadium could set something like this up so they could monitor the area to make sure it is safe from drones.

Next, the structured analytics contributed to developing the risk factors involved with drone usage. Based on the literature review, there is no technology in place for drone monitoring to happen. This leaves the beaver stadium security team with using manpower, communication, and physical security protocols in order to keep the stadium safe during an event. It is not necessary to build from scratch an entire system for drone sightings, after speaking with the security team there is already multiple systems in place for different types of attacks and keeping the stadium visitors safe, and this can also be applied to drone attacks with little manipulation of the system.

The final process is a virtual site visit, which the analyzation of the stadium and brainstorming of possible drone related threats could occur to the stadium. The analyzation was done in figure 3, which shows the updated aerial view of the stadium.

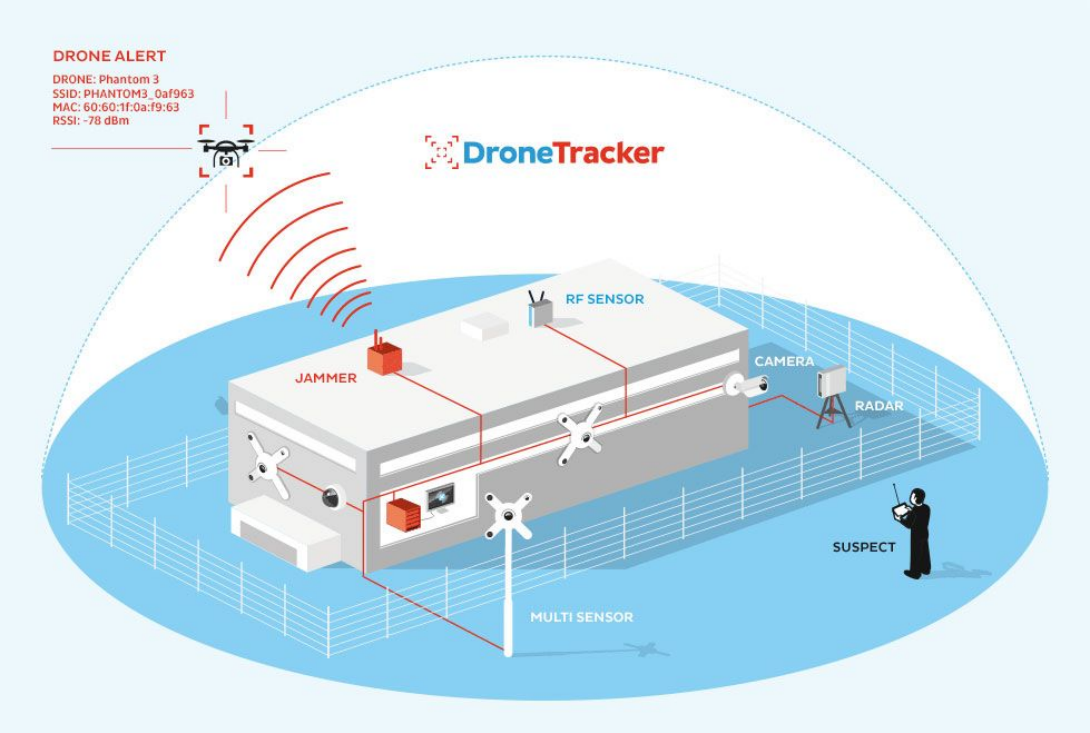

Figure 1: Drone tracker

Figure 2: Beaver stadium

C. Risk Matrix

Figure 3 is the risk matrix that will be used to evaluate each risk's impacts and their likelihoods. The X axis represents the probable impacts rated from one (being a low impact) to three (being a high impact), and the Y axis represents the likelihood, also rated from one (low likelihood) to three (high likelihood). Each cell multiplies the impact rating and the likelihood rating to come up with a number that'll then represent if there's a low, medium or high likelihood of happening. The green cells that are represented show low risk events, and has a numerical value of 1 to 2. The next color yellow, represents medium impact events and medium likelihood of happening and is represented by numerical values 3 to 4. These two incidences would each have a medium impact level but different likelihoods. Another part of the yellow is rare likelihood and high impact. These are numerically represented by the numbers 6 to 9. In this case, the likelihood of this happening is very rare, but in the event of this happening lives could be lost, and panic could increase which would make the situation worse. Finally, the red indicates very likely and a very high impact.

This figure is the basis of how we rated each scenario in the following sections. In further sections we use this matrix to compare the likelihood of each scenario to its risk. We then rate the likelihood based on impact level to decide which scenario would have the biggest impact.

Risk Matrix	Impact 1	Impact 2	Impact 3
Likelihood 3	3 * 1 = 3	3 * 2 = 6	3 * 3 = 9
Likelihood 2	2 * 1 = 2	2 * 2 = 4	2 * 3 = 6
Likelihood 1	1 * 1 = 1	1 * 2 = 2	1 * 3 = 3

Legend

6 – 9	High Risk
3 – 5	Medium Risk
1 – 2	Low risk

Figure 3

II. System Characterization

Our IPO model will be used for this risk assessment of drones and beaver stadium to help focus the threat/vulnerability and asset identification. In our risk assessment we will illustrate the drone scenarios input, system process, and the output. In our scenario a drone is within flying distance of Beaver Stadium. There are some precautions and certain procedures people can do during those situations.

There are many spots that drones attack given the amount of open space Beaver stadium has. For instance, there are a lot of open space below the stadium and a drone could just fly underneath. Should there be an incident of a drone flying around Beaver stadium is just an incident waiting to happen.

However, if the unlikely event of a drone attack were to happen there are some process that are in place that could help mitigate the situation. Based on research, during the November 2015 Paris attacks, a suicide bomber attempted to blow up the national stadium of France, Stade de France. After the bomb went off, people were confused and panic would ensue. However, with the help of stadium security and staff, they were able to help people to get to safety. During this moment, they asked the spectators to come to center field, and slowly in an orderly fashion escorted people out the stadium using the evacuation exits. However, this was a coordinated attack and, attacks were happening elsewhere simultaneously. Many of the bars and restaurants where targets and unfortunately there were many casualties and injuries. As the EMS were rushed to the scene, they had a steps and procedures to follow. By avoiding overcrowding the hospitals, EMS sent the seriously injured to the hospitals, and treated those with less serious injured on the streets. By do quick check ups on the victims and move on to the next.

We used this past event as an example because it involved sports event which had around 89,000 attendees. However, since our scenario involves drones, the procedure will be different. After the initial bomb, people should continue to be on high alert and report anything to authorities. Since there will be some who will be controlling the drones, the attacker could be mixed in with the other spectators. On top of which, the spectators should watch over the skies for any additional drones that may be around the area.

One of the best solutions, or outputs, that we came up with was to not allow the use of drones entirely. If there are drones that were brought near the stadium, authorities should confiscate them. In addition, there should be a message that reminds attendees to report any suspicious activities and to report any flying objects. The message should also remind people that drones are not allowed in the first place.

With a dangerous new world of drones, another solution would be to get mini drones and cheap ones off the sales markets. At Amazon, you can easily buy a tiny drone for $250. This can be manipulated and made to destruct instead of using it for recreational fun which is what it's

intended to be sold for. With the fairly low costs of drones, which is far cheaper than the costs of a fighter jet, armed drones will play a key role in future conflicts.

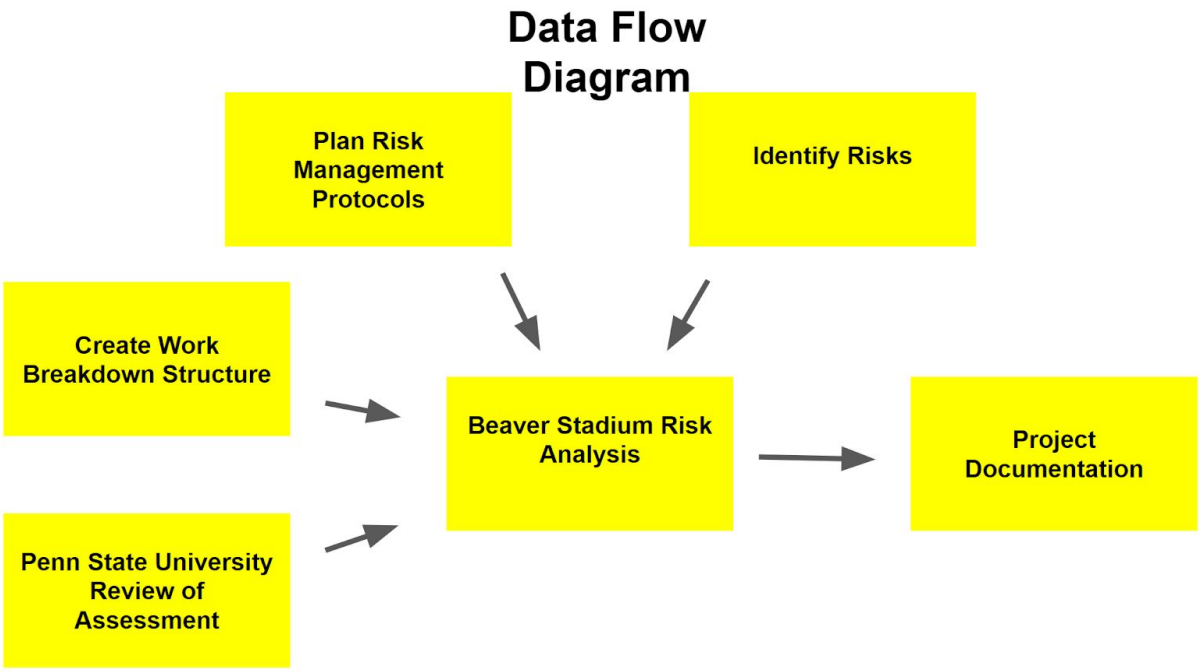

Figure 4 (Data Flow Diagram)

IV. Threat Statement

According to National Institute of Standards and Technology (NIST), In document defined threat as three ways. These are considered natural threat, human threat and environmental threat (NIST 800-30, 2002, pg. 13). Since the drone attack is intentional, it is considered as human threat. Currently, the Beaver stadium holds 110,823. it is significantly large amount of people will watch the game during the game day. This means the vulnerability and threat will hurt significant amount of people. In order to counter these human disaster, analysis on the threat is crucially important.

One of the human threat is chemical terror attack which attach the drone. The variety of Chemicals can be used for this attack. these chemicals are extremely toxic. The chemicals such as sarin gas, VX gas extremely dangerous threat large environment such as Beaver Stadium. In April 2 2017, The syrian Assad regime dropped the Sarin gas bomb and it hurts at least 250 people in 10 mins. if these bomb was dropped closed environment such as beaver stadium, the casualties will abruptly high. Historically, Sarin gas was widely used Kurdish Massacre (1991), Tokyo subway terror attack by Aum Shinrikyo(1995). These events provide crucial information that these gases can kill large amount of people during short period of time. another gas attack is

VX gas attack. VX gas is also considered as nerve gas however, it is less toxic compared to sarin gas. this gas is widely used because it is very easy to portable. For instance, 13 February 2017 North Korean spies killed Kim Jong Nam in Malaysia Kuala Lumpur international airport departure terminal. This case shows that how much this chemical weapon is easy to portable. these research shows that chemical drone attack will make disaster in the Beaver Stadium.

Second of the human threat is bomb dropping in the Beaver Stadium. According to the Federal Bureau Investigation, the one drone bomb drop could kill up to 116 civilians. large surface such as Beaver Stadium, the number will be increasingly high. it will hurt significant amount of people. For instance, if this is an IED, which made by pressure cooker. Double amount of people will die. For instance, during Boston Terror attack 3 people died and 264 people are injured. the pact Beaver Stadium will be larger casualties than Boston Terror attack.

Last human threat is suicide bombing through drone in the Beaver Stadium. which has most likelihood. Currently, FAA mandate that all the drone has to be registered by FAA. FAA can able to track the drones. the suicide bombing is very threatening because the attack it self is very sudden. It is very hard to predict. So this attack is most commonly method that terrorist might use many times. Because it is very costless and make significant damage in the Beaver Stadium and thus these vulnerability has to completely solved.

V. Risk Assessment Results

A. Vulnerability Analysis

A vulnerability can be defined differently depending on in which context it is being looked at, but there still is a generic definition that defines it in its simplest terms. vulnerability in essess is the quality or state of being exposed to the possibility of being attacked or harmed, either physically or emotionally. If we look at the term in an information security aspect it is a system can be attacked, whether it being an OS vulnerability(penn testing) or a human vulnerability (social engineering). In the terms of this assessment we look at vulnerability as all of the fan at a Penn State football game, the facility Beaver Stadium and anything else that can be damaged from a drone attack. The reason we take this as a definition of vulnerability is because during a PSU football game, no is thinking about a terror attack hence them becoming a vulnerability.

Throughout this assessment and during the creation of this assessment our group went through what vulnerabilities there are during a football game. As this is a general statement, there can be many vulnerabilities found. Since this is the case, as a group we figured out and raked some of the most important vulnerabilities that we thought needed addressing.

B. Existing Risk Controls

The existing risk controls that we have in place here at State College are the police force, fire department, and EMS. Events such as home games at Penn State, will have security to keep everyone safe and in order. The police will help people evacuate Beaver Stadium using each of the designated evacuation routes for each seating area as described in **figure 5**. The fire

department can check on structure integrity after a bombing. EMS and other medical teams are on standby inside and outside of the stadium. Other existing risk controls are metal detectors to help prevent people from carrying large metal objects into the stadium.

Figure 5: Beaver stadium evacuation()

C. Scenarios likelihood

Our risk assessment looks at three scenarios that can possibly happen. The first is a drone flying around and drops a physical bomb on or around the crowd. The second is a drone flying around that is the bomb, and the drone is like a suicide bomb going into the crowd. The last scenario is a drone flying around releasing a chemical gas in the air either in small doses as it flies around or all at once in a highly populated area. These Scenarios may seem like they're very unlikely to happen, but with the amount of terror attacks going on in the world, anything can happen. When we compare our scenarios to the risk matrix, we can rank which scenario has the greatest likelihood of happening and then in the later sections we will address the impacts of each likelihood happening.

After the analysis of the three scenarios and their respective likelihoods, we found that the most likely scenario to happen is a drone suicide bombing into the crowd. The reason this came out as a high likelihood is because suicide attacks are one of the most common attack methods in terror attacks. We also thought that if a drone does a suicide attack, that means less evidence of the drone can be found leaving only the controller still in tact. The second most likely to happen

was the drone dropping a bomb onto the crowd. The reason this was rated as a medium likelihood is because a bomb threat is common but the attacker would have to configure the drone so that he can drop the bomb and detonate it when the attacker wants to. There are some attacks that happened where some level of engineering takes place, but this usually isn't what happen. Because of this reason, we found that this scenario is less likely to happen. Finally, we found that the drone releasing a chemical has a low likelihood. Comparing most terror attacks, most attacks are usually done with bombs or weapons of sorts, only a few attacks in history include a chemical weapon. Although this attack can still certainly happen, we rated this risk as a low likelihood.

Figure 6 shows the scenario and likelihood that was found based on the results of **figure 3**, the risk matrix. We cross referenced these two figures to decide where each scenario falls in accordance to one another and which ones are most likely or not.

Risk Scenario	Likelihood
Drone Dropping bomb	Medium
Drone suicide bomb	High
Drone releasing chemical	Low

Figure 6

D. Scenario Impact

We evaluated our threat identification and ran it through our risk matrix in order to come up with a risk score and determine the possible impact of a given scenario. The first, dropping a bomb through a drone is a small partial threat of casualties and it would be similar to any other type of air strike so the impact is low because there are already bomb procedures in place and beaver stadium security would be able to follow those protocols in order to keep the visitors safe. Next, is a suicide bombing using a drone. This scenario is the highest likelihood the highest impact because it is easiest for the attacker to go about one of these attacks. The attacker can be nearly anonymous and far away from the scene and be safely away from the scene while suicide bombing the stadium. Lastly, a chemical gas threat through a drone is a large possible threat because of the ease to go about the attack. Drones are portable and have the highest and likelihood of this attacks results are because of the ability of one of these attacks to kill a significant amount of people in the area of beaver stadium while the attacker can be far away and

safe from the chemical gas. This type of attack is easy to create and has the highest likelihood a well as the highest impact according to our findings.

Additionally in order to strengthen our results and make it easy to understand for any person looking at our model we also rated a few other common occurrences that we are all aware of through our risk matrix so we can familiarize the public about how these types of attacks compare to current threats that we are aware of.

E. Risk Rating

Drone dropping bomb has a medium likelihood, but it has a high impact. Drone suicide bombing has a high likelihood, and it also has a high impact. Drone releasing chemical has a low likelihood, and it also has a high impact. All of these scenarios of drone attack can high impact because each of these scenarios can cause damages, injuries, or even injuries, if any of these scenarios actually happened. While the likelihood is about the level of risk and the situation. Bombing scenario is probably the most well known when there is a terrorist attack. The reason why drone suicide bombing has a higher likelihood because suicide attack would means that there won't be any evidence left when the drone attack actually happened because the drone is most likely completely destroy therefore it is harder to track who was controlling the drone. Normal drone bombing requires some configuration on the drone and where some level of engineering takes place, but this isn't usually what happened. Finally, the last scenario is drone releasing chemical weapon, which has low likelihood because most terror attacks are done by using bombs. Only a few attacks was conducted by using chemical weapon and that is why it is low likelihood compare to the bombing scenario.

F. Recommended Treatments/Controls

Since the Drone is very recently developed, it is hard to counter threat against the Drone attack. Currently, FAA mendataize the regulation that all the drone has to be registered by the federal government. however, it is big debate between which one is considered as toy or actual drone. For Instance, Singer v. City of Newton (Singer, 2017) case. City of Newton mandetaize the drone that all the drones has to be registered by the city council. however, the Massachusetts state court decide that the drone it self is considered as toy, therefore it is can't be enforce to register by the state. The law of Drone is very complicated. because there are two type of law is exist for the drone. The state law can be very different than the federal law. In order to successfully counter these threats, the law has to be joint compromised and successfully enforce the law. The law will make successfully counter threat against the law.

The technology has to be also important to counter threat against drone attack. currently, the rader is only can be dictated certain level of altitude however, the radar technology is currently developing for the drones. especially, low altitude radar has significant expectation to defend

those kind of threats. The establishing the drone radar will be good treatment and control against the drone threat.

G. Technology to Counter Drone Attack

There are many technologies to defend against drone attack, but there are a few of them that it can be effective in our scenario at the Beaver Stadium. One of the technologies that we can use to defend against drone attack at Beaver stadium is the Geo-fencing or no-Fly Zone. This pretty much create an area that stop the drone from trespassing the property. The Geo-fencing can provide service to cover the entire Beaver stadium and beyond the expectation. This technology can stop drone from trespassing no matter what is on the drone. For example, if the drone has a bomb on it, the Geo-fencing can set it to several miles away from the Beaver Stadium so the drone won't be able to reach Beaver Stadium and even if it detonates, it will be several miles from the Beaver Stadium, which means it will be safe from drone attack. The downside of this technology is that in order to maintain a service area of the size of Beaver stadium and several miles bigger can be expensive. Also Penn State has to make sure that the technology that they use to support the Geo-fencing service needs to be stable at all time. If the Geo-fencing area isn't stable, it creates an opportunity for the drone to pass the Geo-fencing and attack the Beaver Stadium. However, this technology is only useful when the drone that the drone attacker used compliant with the update and the security. So if the drone attacker configure the drone or maybe jailbreak it then this technology won't work. This is why there will be other technologies are available to stop drone attack.

Other technologies that can be consider is to hack into the drone and disable the a certain feature of the drone such as disable the camera of the drone so the person who is controlling the drone won't be able to see what is going on. This technology requires somewhat high level knowledge of coding as they need to create codes for it and have to make sure the database of these code is safe from the attack. Another option is to use net to catch smaller hostile drone. This is the easiest and cheapest technology that we have. However this technology can only be limited when the drone is outside the Beaver Stadium because if we caught a drone while it is in the middle of the Beaver stadium then the drone will drop to someone, which can seriously injure them and safety is a top priority. This means that the Beaver Stadium can use all the technologies that we just mentioned to give the best protection for the audience since there isn't a single technology that can totally prevent a drone attack. Beaver stadium needs more than one technology to prevent drone attack just in case one technology doesn't work.

Another technology that can be used alternatively at the Beaver Stadium is GPS spoofing. Drone navigates to its destination by following the GPS coordination that the drone's user set on the drone or the control. So GPS spoofing masquerade as GPS satellites and send misleading signal such as changing the GPS coordination. This technology might sound like something that people would use for wrongdoing, but it can also prevent drone attack. There is a test conducted by University of Texas on GPS spoofing. The test showed that they were successfully hijack a drone that was 620 meters away. The setup was simple as well, it needs a receive antenna, an external reference clock, a transmit antenna, a computer, and a civil GPS spoofer with internet. As of right now, FAA has outlined a plan for allowing commercial drone using unencrypted GPS

signal to fly in the United States so this technology is allow. If FAA has any changes about this plan then we might not be able to use this technology at the Beaver Stadium. So this technology can only count as an alternative technology.

There is also technology called DroneWatcher APP and RF and Harrier DSR. DroneWatcher APP used small drones finder that detects, tracks, and records information on consumer and prosumer drones with a range of up to ¼ to ½ miles. It captures information about the drone such as the drone type, ID, and other information that can be used to support apprehension and prosecution by local law enforcement. For the size of the Beaver stadium, it requires multiple device to cover the whole stadium with real time web based awareness and automatic warning when it detects unauthorized drones. DroneWatcher RF can detect over 95% of the commercially-available, consumer, and prosumer drones and is very similar to DroneWatcher APP except it has with a range of 1 - 2 miles. Harrier DSR is primarily used to detect drones in clutter environment and it can detect drones that are not detectable by DroneWatcher APP and RF. It also has a longer range of detection with 2+ miles with a longer range for larger drones. However for Harrier DSR, it needs to build a radar that can cost a lot of money and time to build the radar. Depends on the financial situation of Penn State, Penn State may or may not consider the Harrier DSR and uses DroneWatcher. These three systems don't need to be used simultaneously. Each of them can be used individually, but using all three of them will provide the best detection defense for the Beaver stadium. Since these technologies is for detection only, it doesn't really have a way to prevent the drone attack. So what these technologies can do is to notify Penn State about the drone attack ahead of time so Penn State can evacuate the people in the Beaver Stadium before any injury or casualty or if Penn State has another plan to prevent drone attack, these technologies can give them time to set up their plan.

Some technologies that won't be considered in this project is to use laser beam to shoot down the drone. This technology is only limited to the military because it is very dangerous to use it. Without the authorization from the government or anybody to operate the laser weapon, this technology won't be consider to defend a location such as Beaver stadium. Also jamming the drone won't be consider as well because jamming the drone can create the situation similar when you use net to catch the drone. If you jam the drone in the stadium then it can also fall and injure somebody. The major difference between jamming the drone and using the net is that jamming the drone is actually illegal in the U.S. so that is the main reason why we can't jam the drone, but consider to use net to catch the drone, but of course, the net will only be used when the drone is outside the Beaver stadium.

Overall, the easiest way, but also the crudest way to counter drone attack is to "shoot it down." This is the most effective way to counter a drone attack, but it will create collateral damage when the drone falls as it creates massive lawsuit and injury. Since shooting it down isn't an option, using the net can decrease the damage and still stop the drone attack. However, it doesn't reduce the collateral damage to zero so that is why this technology will be use while the drone is still outside the Beaver Stadium so it won't create any injury to people. The most prefer method is by spoofing or preventing the drone's control links. This is where Geo-fencing and GPS spoofing can be used. Geo-fencing is the most popular way to counter drone attack by

creating an area that prevent drone from trespassing this area. However this technology can only be used if the drones are compliant with the update and security of the drone regulation. GPS spoofing changes the GPS coordination or send the wrong signal to the drone so the drone will go to another destination. An issue about Geo-fencing and GPS spoofing is a regulation by the FCC. Since most drones uses Wifi frequencies, signal jamming defined by FCC regulation is illegal in the United States because it would interfere with other frequencies such as ambulance frequencies, police radio, and civil devices. Detection technologies such as DroneWatcher APP and RF and Harrier DSR doesn't provide protection against drone attack, but it can give time for Penn State to execute any of their plan about drone attack. Since there are many regulation and other consideration such as collateral damage and hack proof, there isn't one technology that can fully counter drone attack so there should be multiple technologies available to prevent the drone attack at the Beaver Stadium.

VI. Summary

Our risk assessment is based on bomb scenario of drone attack. Our location is focus on the Beaver Stadium. We did the hazard identification process to conduct a literature review, a structured analytics, and a photographic investigation. There is a protocol in place for identifying hazards such as drones and it can identify the location of a drone in order to monitor the area. The structured analytics result is that there is any technology in place against drone attack, which means some kind measures must be placed in order to prevent a drone attack. The photographic investigation has a photo of aerial view of the stadium to see the surrounding of the Beaver Stadium. Potential threats that we had identifying are chemical attack, bomb dropping, and suicide bombing. There are scenarios of these type of threat that happened before already, but the difference will be that these attacks will be conducted by using drones.

Existing risk controls that we have at the Beaver Stadium are the police force, fire department, and EMS. There is excavation plan in case of emergency and also no bag policy, small bag check, and metal detectors. We found three scenarios for Beaver Stadium. One scenario is the drone dropping bomb with medium likelihood and a high impact. Another scenarios is the drone suicide bombing with high likelihood and a high impact. The last scenario is drone releasing chemical with low likelihood and a high impact. All three scenarios can cause serious damage, injury, and casualty, which is why there are all have high impact. Drone suicide bombing can leave little to no evidence because most likely the drone will be destroy after the suicide bombing, which can be hard to track who was controlling the drone. According to previous scenarios, most terror attacks were using bomb and a few attacks were using chemical weapon, which makes it a low likelihood.

The system characterization is where we discussed the inputs, process, and outputs of a given system. In our case, which is a drone that is flying within the area of Beaver stadium and it is carrying dangerous materials. Given that there are standard procedures and protocols that first

responders follow, there additional steps that the civilians could do to protect themselves as well. For instance, the spectators should always keep in mind that drones are prohibited anywhere near Beaver stadium. Anything suspicious people should be reported immediately to the authorities. During the game it might be difficult for spectators to be on the lookout. Instead, extra security people could be positioned at the top of stadium to keep a look out for flying objects. Another output would be playing a message to the entire area of Beaver stadium to remind people that drones are not allowed, and to remind them to report any suspicious activities.

Recommend control that we found is the law enforcement for drone need to be joint compromised an successfully enforce the law because right now, the law for drone is complicated and state law, and federal law are very different. here are several technologies that can be considered to counter drone attack. One technology is geofencing, which is to set up a service area so drone won't be able to trespass it, but this technology only works against drone that the drone user didn't configure and compliant with update and security. So if the drone user jailbroken then this technology won't be able to stop the drone. Another technology is GPS spoofing, which is to change GPS coordination of the drone so the drone will go somewhere else. Right now, FAA doesn't have any plan against this technology, but since the drone law isn't stable yet, there might be changes about this plan in the future. The last technology is to use DroneWatcher APP & RF and Harrier DSR that are used for detection so this technology won't be able to stop the drone attack, but it can give times for State College to carry out their own plan such as the evacuation plan. There isn't a perfect technology that is available and legal to prevent drone attack so that is why these technologies are only for suggestion.

Reference List

Euchner, J. (2014). Occupational hazards. Research Technology Management, 57(2), 9-10. Retrieved from http://search.proquest.com/docview/1507798819?accountid=13158

Drone Detection & Defense Systems. (n.d.). Retrieved December 10, 2017, from http://detect-inc.com/drone-detection-defense-systems/

Drone Hack: Spoofing Attack Demonstration on a Civilian Unmanned Aerial Vehicle. (2015, May 13). Retrieved from December 10, 2017, from http://gpsworld.com/drone-hack/

Irving, C. (2016, February 24). Will ISIS Launch a Mass Drone Attack on a Stadium? Retrieved December 10, 2017, from https://www.thedailybeast.com/will-isis-launch-a-mass-drone-attack-on-a-stadium

McComb, S. D. (1932). HAZARDS. Marine Engineering & Shipping Age (1923-1935), 37(12), 514. Retrieved from http://search.proquest.com/docview/855857303?accountid=13158

Penn State. (2014, September 6). Beaver Stadium Evacuation Plan. Retrieved December 11, 2017, from http://news.psu.edu/photo/325330/2014/09/06/beaver-stadium-evacuation-plan

Staff, C. (2017, August 17). How to Stop a Drone Attack. Retrieved December 10, 2017, from https://www.campussafetymagazine.com/public/how_to_prevent_drone_attacks/

Singer, M. (2017, September 21). Singer v. City of Newton-(Case Declaring Local Drone Law Illegal). *Singer v. City of Newton-(Case Declaring Local Drone Law Illegal)*. doi:https://jrupprechtlaw.com/michael-singer-v-city-newton