Narrowing the Grey Zone Conflict Margin

Narrowing the Grey Zone Conflict Margin

David A. Lemont

A Thesis in the Field of International Relations

for the Degree of Master of Liberal Arts in Extension Studies

Harvard University Extension School

November 2018

Abstract

Modern day conflicts are radically evolving by reducing target size, decreasing enemy footprint, increasing the global reach while most importantly increasing population concerns of potential local threat. Through the rapid development of technology and globalization, all levels of aggressive actions or conflicts have become of international interest. Prior to recent technological advancements, smaller level conflicts remained limited within a region.

Actions that do not quite fall under the clear definitions of "War" by lesser levels of aggressions are defined by Lauren Fish, writer of the *Small Wars Journal*, as "Grey Zone" conflicts. Not to be confused with traditional methods of "low intensity" conflicts between two opposing nation-states, Grey Zone conflicts are undeclared acts of international conflict that operate with an ambiguous approach that lack an acknowledged state of hostilities between established states. Grey Zone aggressors cannot be clearly identified as they do not immediately expose their motives and/or locations. Grey Zone conflicts have numerous methods of approach, including cyber-attacks, occupation of land, use of biological and chemical agents, small scale terrorism and hostage situations. The largest problems in dealing with Grey Zone conflicts are identifying the responsible actors and intent as well as justifying the proportionate level of response in a timely fashion before conflict evolves or escalates to war.

This thesis will identify Grey Zone conflict trends, consider future trends of enemy responses to respond to less familiar methodologies of conflict in order to narrow the margin between low-level, Grey Zone conflicts, and acts of war. By suggesting

guidelines for actions against Grey Zone conflicts, the US government and other governments will be able to appropriately respond in hopes of preventing war.

Dedication

To my father who passed during the writing of this thesis. His drive for success and his never quit attitude gave me the determination to advance my studies and achieve the honorable.

Acknowledgements

First, I would like to acknowledge my wife Karen as a staple for my success during the entire master's degree process. She kept me on track and motivated me to focus during trying times. Her dedication and support allowed me to focus on my studies while mitigating many external life stressors.

To Professor Doug Bond, my research advisor. His approach to the Harvard Extension School Master's Degree Program made my educational experience an enjoyable one. I am almost sad that it has ended. Almost.

Last, but not least, I would like to recognize Professor Tom Nichols. His lectures incorporating obscure "80's" movie references were amazing. Like all great educators, he made complicated subject matter easy to follow.

Thank you all!!!

Table of Contents

Dedication iv

Acknowledgements v

List of Figures ix

Chapter I. Defining the Grey Zone 1

Chapter II. Previous Views on Drone Use 8

Drone Technology: What is a Drone? 9

Radio Control 9

GPS 9

Autonomous 10

Chapter III. Views on Grey Zone Drone Warfare: Foreign and Domestic 12

Defining Military Drones 13

The Raven 14

Predator 15

Commercial Drones 15

Micro Drones 17

Non-Military Drone Based Cyber Threats 18

Drone Based CBRNE Threats 19

Chapter IV. NFL Super Bowl LIV 21

EMA Command and Control 23

Medical Services (ESF 8) 24

Evacuation Plans (ESF 1) 25

Transportation (ESF 1) 25

Agriculture and Natural Services (ESF 11) 26
Hazardous Materials Response (ESF 10) 27
National Disaster Recovery Framework (ESF 14) 28
External Affairs (ESF 15) 29
Chapter V. Ideas and Considerations 31
FAA Regulations 31
Drone Registration 32
Manufacturer Restrictions 33
Weapon/Counter-Weapons 33
Countering Drones with Drones 34
Chapter VI. Findings 36
When Can the Government Take Action? 37
The Bush Doctrine Concept Revisited 38
Chapter VII. Conclusion 40
General Overview and Important Contributions 40
Main Points 41
Ambiguity Reduction 43
References 45

List of Figures

Figure 1. Micro Drone Examples 17

Figure 2. Projected Drone Sales 18

Chapter I.

Defining the Grey Zone

Modern day conflicts are radically evolving away from traditional warfare toward asymmetrical methods. Recent acts of aggression are proving more successful when attacking smaller targets. Enemy forces such as terrorist groups have determined that large scale attacks result in a large-scale retaliation (Bensahel, 2017). Successful full scale retaliations delegitimize power of the terrorist organization as well as the purpose of the attack.

To avoid a military response, these groups operate below declared acts of war by creating large scale fear on smaller random targets. Although few large-scale attacks have followed the September 11th terror attack, vigilant observers disrupted terror attempts such as the Times Square bombing of 2010 through information sharing. As a result of public increased situational awareness, large scale attacks are difficult to plan and hide. With assistance from the general population, the proper authorities were able to collect credible intelligence to track the enemy and intent (Toure, 2017). Analysts identified that the terrorist organization responsible for the failed Time Square attack trained their members in Pakistan and sent them worldwide with the simple intent to destroy the Western culture.

Enemy organizations such as terrorists are minimizing their footprint by keeping training locations small, secluded and remote (Bindra, 2001). The proven success of their attacks is based on minimal numbers of personnel operating incognito. For example, small cell operations such as sleeper cells only rise to power when called to duty. With

today's technological advances, electronic communications such as cellular phones and internet have replaced the need to manually move forces in mass formations (Pekgozlu, Ozdemir, & Ercikti, 2007). Real time global communication gives enemy organizational leaders the ability to lead remotely.

Small cell operations have proven beneficial as they embed their teams among the population with the ability to hide in plain sight. Not only do they train for a specific mission, but they train to adapt to social norms within their environment. Enemy forces are within society, gaining intelligence and knowledge surrounding the mission. Without breaking the role of society, information shared in real time assesses and solidifies a plan of attack.

Attacks on targets that cause disruption and conflict within a population do not necessarily have to be large in scale to yield large effects. The ability to create a conflict by disrupting daily norms instills concerns among the population that any location and any person can be vulnerable. One effective way to reduce the public's confidence in the US is to cause a government disruption that divides the public opinion (Leahy, 2018). Smaller scale conflicts initiated by enemy forces achieve success when civil populations distrust government authority to retaliate or not.

The US media and news sources attempt to get news out to the public in the most expeditious manner. Information no longer remains local as internet and international television news feeds can relay local and global news in real time. The rapid ability to spread news about all levels of aggressive actions or conflicts can therefore generate international interest. Governments, from a global perspective, have personal interests in the success or failure of US. Democracy (Rogoff, 2007).

Traditional and conventional acts of war allow the US to initiate counter-actions increasing to military response. Less evasive but effective means, such as economic sanctions or diplomacy, resolve or contain low level acts of aggression. Although the US government is able to respond with various models of national power, the military is not prepared to combat modern-day asymmetrical warfare. US Army General H.R. McMaster has said, “There are two ways to fight the United States military, asymmetrically and stupid. Asymmetrically means you're going to try to avoid our strengths” (Schogol, 2014).

Asymmetric actions that don’t quite fall under the clear definitions of “War” by lesser levels of aggressions are defined as “Grey Zone” conflicts (Brands, 2016). Not to be confused with traditional methods of “low intensity” conflicts between two known opposing states, Grey Zone conflicts are deliberate acts of international conflict that operate with an ambiguous approach. These ambiguous attacks allow Grey Zone aggressors to operate in between the acts of war and low level conflicts while masking their identity as they do not immediately expose their motives and/or locations. Grey Zone conflicts operate below the threshold of military response requirements and also increase difficulty to provide a governmental mitigating response by the time all actions are complete (Brands, 2016). Grey Zone conflicts have a limitless method of approach. Most current Grey Zone conflicts execute through cyber, occupation of land, use of drones, biological and chemical disbursement, small scale terrorism including hostage situations.

An example of a recent Grey Zone conflict is the Russian occupation of Crimea. Prior to the 2014 referendum for Russia to acquire Crimea, activities of civil unrest and

de-legitimatization of the Ukraine government occurred. Paramilitary personnel created disruption within the Crimean Peninsula wearing black fatigue style uniforms with no affiliation insignias (Friedman, 2014). No countries claimed responsibility for the actions of the paramilitary soldiers, not even Russian President Putin. While Ukraine requested support from the UN to fight the paramilitary soldiers, no one came to their aid. The Ukraine government identified that the black uniformed militants were part of the Russian Military (Friedman, 2014). A quick occupation and low level conflicts deemed the Ukraine as incapable of protecting their land. Once the Ukraine government was de-legitimized and overpowered, the Russian Referendum overwhelmingly voted for the Russian Control of Crimea.

Another Grey Zone conflict example is the controversial US Presidential election process. Since the 2016 US Presidential election, news media sources from both liberal and conservative politically biased networks such as CNN and FOX News have argued for and against the amount of legitimacy that the electoral process maintained. Why is any corrupt presidential election a Grey Zone concern? Identifying and exposing vulnerable or corrupt systems delegitimizes the perceived governmental control (Michael Collins, 2018). Feeding the possibility of a corrupt system to the public delegitimizes the trust in governmental democracy. Adversaries try to disrupt democracy and try to expose governments as a non-effective method (dos.gov, 2006). Internal conflict among the US population can benefit other countries and organizations economically and politically. Who is responsible for tampering with the elections? CNN News broadcasts continue to question Russia's involvement within the US Presidential elections (cnn.com, 2018). Fox News reports all allegations of President Trump's involvement with the Russia collusion

were cleared (Schallhorn, 2017). This contradiction of information distribution is a method of Grey Zone concern. After multiple investigations and efforts to identify the source of corruption within the electoral process, no confirmed information can be applied to initiate offensive actions. To make the situation more confusing social media programs are no longer safe from corruption. These programs have been infiltrated with computer infested viruses known as "Bots" that automatically push politically slighted information to the mainstream through social media feeds, generating a rise of internal social conflict (Keohane, 2017).

Grey Zone conflicts are difficult to identify due to the purposely unpredictable actions of unknown responsible actors and their intent for the US to justify the proportionate level of preemptive or preventive response in a timely fashion before conflict evolves or escalates to war (Betz, 2015). The backbone of military studies is that history repeats itself. Historically, various styles of traditional or conventional warfare could be predicted in preparation for the next conflict. The predictability of Grey Zone asymmetrical actions is less likely to be identified with little to no precedence to revert back to and study (Betz, 2015). Therefore, how must any government posture their countermeasures to prepare for the unknown Grey Zone?

To Grey Zone aggressors, laws of war do not apply. 19th Century Westerners conducted The Hague Conferences in the late 1800s and early 1900s to develop the Geneva and Hague norms (Yale). The Hague model limits any state's methods and means of waging war. The negotiations were dominated by the more powerful countries of those that were represented at the conferences. Middle East countries were not yet developed and therefore could not be well represented. The follow-on leadership development of the

Middle East countries do not feel obligated to adhere to The Hague norms because they do not feel that the settlements are a binding contract (PBS, 2008).

The US military is always preparing for the next war. With a low predictability within the Grey Zone, military reverts back to training against last known threats. Knowing and understanding the enemy helps shape preparation for countermeasures (Piddick, 2009). When one cannot identify the combatant or no one takes responsibility for the disruption, it is difficult to take appropriate action. The Grey Zone enemy no longer is identifiable by uniform and rank. Much like guerilla tactics, enemy actors conform their appearance to their surrounding environment. These small cell non-militant covert enemy forces act autonomously while ring leaders refuse to immediately claim responsibility.

The inability to apply military countermeasures against Grey Zone conflicts is causing confusion and complications that deter a timely and reasonable reaction to mitigate a potential threat. Action or inaction towards Grey Zone conflicts further separates the views and political opinions for a legitimate government. Should the US have gotten involved in the Russian/Crimea conflict? Was the US failure to act the result of Russian occupation? Concurrently, was the US's empty threat or failure to respond to Syrian forces the result of a successful chemical attack on the Syrian population?

Grey Zone conflicts have caused the US to be reactive rather than proactive in their response methods. Airport Security is the most obvious example. Post 9/11 security measures have increased, questioning personal invasion of privacy. X-ray machines that can clearly see shapes and sizes of human private anatomy have raised the question of intent. Constant increased security measures such as personal intrusion screening

techniques at an airport or personal privacy invasions via drone activities, have been emplaced to prevent similar attacks from happening in the future. Constant additions and layers of security measures in a response approach increase government and corporate control which change the definition of daily norms.

The US remains to be reactive in response to Grey Zone conflicts because these acts are uncharted concepts. Through trial and error, adversaries attempting Grey Zone conflicts exploit vulnerabilities by the evolution of attacks. Unless the concept has been attempted, no country could know to prepare for an "underwear bomber" passing through airport security. The post incident response for TSA was to add bomb sniffing devices to the X-Ray machines.

Currently, there are global concerns that involve violations to privacy oversite such as selling personal information collected on the internet, chemical and biological threats, cyber threats and how they all relate to today's global concerns (Broich, 2017). Additionally, media outlets publicly share concerns about how US foreign policies are being addressed in regard to handling or mitigating Grey Zone actions (Ignatius, 2017). Responses to Grey Zone attacks typically get delayed until the enemy is known. This is no longer an option in today's climate. Analyzing new case studies involving breakthrough concepts and ideas are important to generate an immediate response or countermeasure.

Chapter II.

Previous Views on Drone Use

This chapter further expounds upon the concerns of why US government needs to address a timely response according to the paradigm shift of ambiguous Grey Zone attacks. It is important for the US government to remain relevant and to evolve with current changes in warfare, especially when Grey Zone operations can disrupt national security prior to identifying an appropriate response. By increasing adversarial awareness of international concerns in conjunction with the will and capabilities to disrupt US diplomacy, the US government can implement the appropriate tools available to them to counter, prevent, and/or mitigate actions before an escalation to war.

The purpose of this study is to explain asymmetrical Grey Zone conflicts that can potentially cloud the US decision making process, while identifying preemptive methods to counter, mitigate and eliminate the potential for escalation to acts of war. This thesis will use the particular cases of drone and micro-drone warfare in the US as a way of studying weak regulations leading to weaponized procurement for terrorist type activities while instilling the ability to delegitimize the US Government. In order to prevent catastrophic Grey Zone events from occurring, this thesis will consider new measures to prevent conflict escalation by recommending improvements to technological awareness of drone capabilities, specialized homeland defense with emergency management measures, military training, adjusting, implementing regulations of military and civilian drone uses, while preparing for technological and legal countermeasures to minimize the "Grey" from the Grey Zone activity.

Drone Technology: What is a Drone?

What is a drone? Drones are "the monosyllabic catch-all for remote controlled unmanned aircraft" (Atherton, 2014). Historically, drones have been designed in all shapes, but mostly large in stature. Drones, also known as Unmanned Aerial Vehicles (UAVs) and Unmanned Aerial Systems (UASs), in the simplest terms are "unmanned flying robots." Drones have different controlling capabilities. They can be operated via remote control radio frequencies, pre-programmed flight patterns, or autonomously. This thesis will further discuss each operation as it is important to understand and identify countering measures.

Radio Control

All radio controlled devices share four similar main components incorporating a transmitter, receiver, motor and a power source. Radio controlled drone frequencies have the ability to remotely control flight patterns through a radio frequency identification (RFID) codes (Swedberg, 2017). The RFID specifically sends coded signals from a transmitter through the air to link the frequency to the specific drone's receiver. The receiver accepts the commands from the transmitter, controlling the function of the motor on the drone. The RFID also individualizes the signal from controlling other drones within the area (Swedberg, 2017).

GPS

Drones can also be controlled by a global positioning system or GPS. Drones that operate via GPS are preprogrammed to self-locate by sending and receiving signals from satellites (DroneOmega.com, 2017). By receiving signals from multiple satellites, each drone can triangulate its location. A GPS operated drone can also adjust its location to a predetermined flight pattern. This style of operation does not require a remote-control operator.

Autonomous

Another method of drone operation is known as autonomous control. This method does not require radio frequencies or satellite communications. Autonomous control removes any ability to maneuver the drone while in operation (Law360, 2018). An on-board computer internally controls all mechanical operations. Scientists and large scale investors such as Google and Amazon have continued to improve autonomously controlled drones for the use of package delivery and emergency evacuation platforms. Currently, a California based company "Zipline" is using Zip Drones which are autonomously controlled crafts to deliver medicine in remote regions of Africa (Foster, 2016). Zip Drones deliver over 40% of all blood transfusions in Ruanda.

All three methods of operation are important to understand as all are difficult to counter or defend without specific electronic, radar or jamming equipment. Even recent technological countermeasure equipment has become antiquated as these three anti-drone tools combat larger scaled aircrafts. Drones literally and figuratively fly below the radar.

In 2017, an article in the *Washington Post* discussed the transition of the use of drones from a commercially driven toy that increased from a nuisance to an immediate

threat of US National Security. The article referenced the 2015 commercial drone landing on the Whitehouse lawn (Drehle, 2017). A hobbyist flew a DJI Phantom commercial drone at 3am and lost control over the Whitehouse grounds resulting in a Secret Service lockdown within the immediate area (Hennigan, 2018). This mishap identified that a threat against the Whitehouse or any high-leveled security area is not necessarily an attack with an apparent weapon system. Despite the fact that the FAA has restricted flight areas, this incident proved that a commercial drone can fly in these same areas undetected. Identified as a race against time for an imminent drone attack, the US Government has agreed to invest $401.2 million in drone countering equipment and technology (Hennigan, 2018).

Chapter III.

Views on Grey Zone Drone Warfare: Foreign and Domestic

How can drone operations affect US National Security? Kirstjen Nielsen, the Secretary of Homeland Security, recognizes the importance and transformation of drone technology as both positive and negative (Nielsen, 2017). As e-commerce is dependent on this technology, critical infrastructure is becoming more vulnerable to attacks. The Department of Homeland Security is favoring legal authority to counter corrupt operators of aerial devices. Drone regulation development passed by congress addresses airspace with minimal understanding of drones as a weapon system (Nielsen, 2017).

Collectively, drone capabilities have the ability to disrupt entire nations. The smallest of attacks can have major results delegitimizing governance and society's sense of legitimate security (cia.gov, 2003). Nations such as China have already used cyber warfare as espionage against the US (Lindsay, 2015). As an example, to exploit the reduction of costs to replicate drones, the US spent many years and millions of dollars in the research and development of the F-22, B-2 Bomber, and the F-35 Stealth Fighter Jet (Mizokami, 2017). China was able to quickly replicate these fighter jets with only construction costs. They have also identified the US capabilities of these weapon systems in order to produce defensive counter measures (O'hare, 2016). It is also public knowledge that states such as China and those in the Middle East have used drones to gain intelligence on US soil.

Regulations for commercial or consumer drones for purchase are currently unrestricted. Anyone, anywhere can purchase drones at a local hobby shop for personal

(terrorist/espionage) use. Non-state actors such as ISIS are even more of a threat when it comes to drone warfare. The terrorist agenda is to disrupt and delegitimize the governmental control of large nations. ISIS does not have the same economical stamina as nation states. Therefore, they must operate on a budget (Smith, 2015). Drone and micro drone technology are easy to commandeer and inexpensive enough to add to their arsenal of effective weapon systems (Piore, 2013).

In 2016, ISIS implemented drones as a weapon system when combatting Special Operation Forces in Mosul, Iraq. ISIS incorporated drones with grenades and explosives in order to disrupt these forces by deploying multiple drones forcing soldiers to seek cover and concealment. General Raymond Thomas claimed that the drones also known as "Killer Bees" were effective enough to disrupt the coalition progression (Hennigan, 2018). Although no casualties resulted from these attacks, General Thomas claimed that counter-drone measures were "most daunting" because tankers and fighter pilots could not address a small weapon system (Hennigan, 2018). The countermeasures became limited to rifle shots in hopes of shooting the drones out of the sky.

Nielsen states that authorities from Congress and the Department of Defense have created legislative fixes to develop and counter drone attacks. She further explains that the same requirements are a viable and immediate need for a homeland defense response. W.J. Hennigan, a writer for *Time Magazine*, identifies that electronic eavesdropping laws prevent government retaliations against drones with the use of electronic signals (Hennigan, 2018). Senators have recently proposed a bill to the Trump Administration to use electronic jamming systems surrounding federal facilities. This bill is under review by Congress for an anticipation of approval by the end of 2018.

Defining Military Drones

Dating back to the mid 1800's, drones in the form of kites and hot air balloons were used as military training aids such as targets (Century-of-flight.net). It was not until World War I that the US incorporated drones into its arsenal (Arbuckle). Development of drones in the form of Unmanned Aerial Vehicles (UAV's) were game changers for aerial bombing and aerial photography to gain intelligence. Drones have been a part of the US military inventory ever since.

The US military has broken down enemy drone use into four categories. Direct, indirect, swarm and surveillance/observation (Sanders, 2017). Direct attacks incorporate flying a drone into contact with another object causing damage, injury or death. Indirect drone attacks carry weapon systems to project at a target from a distance. Swarming operations include hovering and surrounding an area disrupting frequencies or standard operations. Surveillance and observation operations allow drones to carry cameras that will report intelligence back to the operator. Below are examples of known drones that have been incorporated into military and governmental operations.

The Raven

When one hears of a military drone strike, the typical thought is the use of a large drone defined by the military as an Unmanned Aerial Vehicle (UAV) that replicates a full-sized aircraft." The most commonly known military drone is the Raven. The Raven is a $35,000.00, 4.6-pound hand launched drone that can be operated either by a ground

operator or autonomously using GPS. It can fly up to 6 miles at a 500-foot altitude. Its speed can reach up to 60 miles per hour (Army-technology.com, n.d.). The Raven's general mission is to conduct surveillance by utilizing a daytime as well as an infrared camera system. This Raven system has been adopted by many military forces.

Predator

The Predator is one of the older drone systems that the US government employed during the Bosnian, Iraq and Afghanistan conflicts. The Predator platform has had many modifications since the first employment in 1995. Its primary mission is surveillance and reconnaissance. With a 27-foot long body and a 55-foot wingspan, the $20 million Predator can achieve flight altitudes to exceed 25,000 feet with a range of 150 nautical miles (Monthly, 2012). As a surveillance craft, the standard Predator has camera systems with infrared capabilities. The mission of the Predator has extended to not only conduct surveillance, but also apply indirect damaging capabilities. Some of the improvements include adding four hellfire anti-armor missiles, laser guided systems to improve pinpoint accuracy, and satellite capabilities. The predator is limited to direct line of sight control. The other additions such as cameras and bombs can be controlled globally.

Commercial Drones

When discussing "backyard drones" the idea is the 4-propeller hovering toy. One of the more popular 2018 commercial drones on the market is the DJI Phantom. It is priced under $1,000.00. Although drones can vary in price, the Phantom is the average cost for a drone of quality. The Phantom weighs 4-pounds and is 11.5 inches wide by 7

inches tall. It has many advanced features similar to the technologically advanced military drones. The Phantom comes with high definition video resolution, and a dedicated remote control (DJI, n.d.). When the Phantom is out of sight from the operator, the drone has a "return to home" capability. The Phantom reverses its path until the signal is reconnected. The Phantom is also capable of GPS input to follow a predesignated waypoint path. Unlike the government-controlled drones, commercial drone operators are legally restricted to certain operations defined by the US Federal Aviation Administration (FAA).

Drone technology has catapulted so quickly that even FAA regulations are still trying to clearly define flight restrictions (FAA, 2016). The FAA has implemented some control measures by restricting weights and flight airspace. Unfortunately, many drones maintain the same or more dangerous capabilities to provide direct, indirect, swarming and surveillance capabilities. Modern drones have the lift capacity to carry a camera system that provides a direct feed back to the operator. The June 2018 *Time Magazine* cover was created by drones that received placement directions off of a central drone. The operator from the Intel Shooting Star team controlled one drone which fed spacing information to over 957 more drones placing each one in perfect alignment (Stangel, 2018).

With drone laws still evolving, the ability to identify the right to privacy remains in the courts. FAA regulations continue to battle the courts over legalities of operating in airspace along with private land right to privacy. Drone regulations are highly restrictive for those that obey the law. FAA restrictions focus on the operation of a drone in flight but fail to address the purchase of a commercial drone.

Micro Drones

Modern day drones are continuously getting smaller and more difficult to identify. The latest inception is known as the micro-drone. The FAA identifies micro-drones as drones that weigh less than 4.4 pounds. These micro drones can further mimic small insects and can become virtually unidentifiable. How dangerous could this actually be?

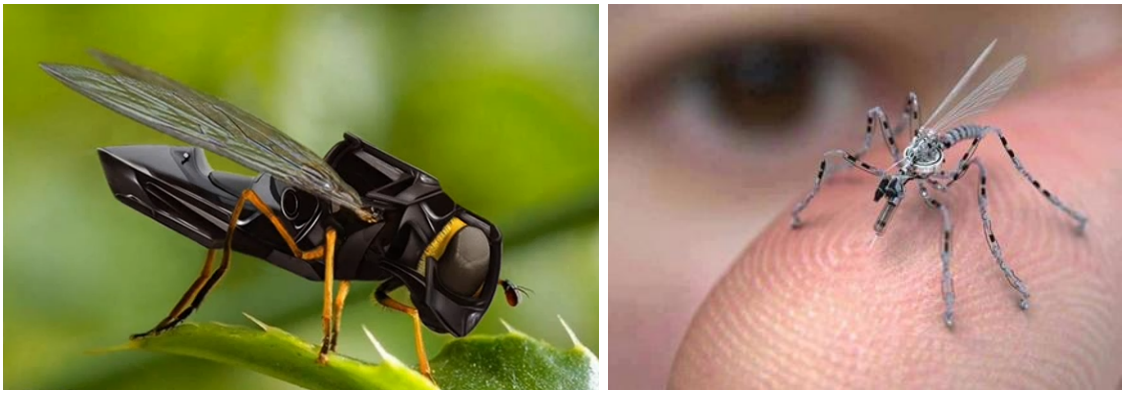

Figure 1. Micro Drone Examples

Calderone, 2016; Mikkelson, 2018

The dangers of these drones are limited only by the imagination. Many science fiction movies that depict the future incorporate drones as a common item. Drones have flooded the consumer market. As more advanced drone technology becomes available worldwide, developmental costs decrease, making it affordable to the public consumer.

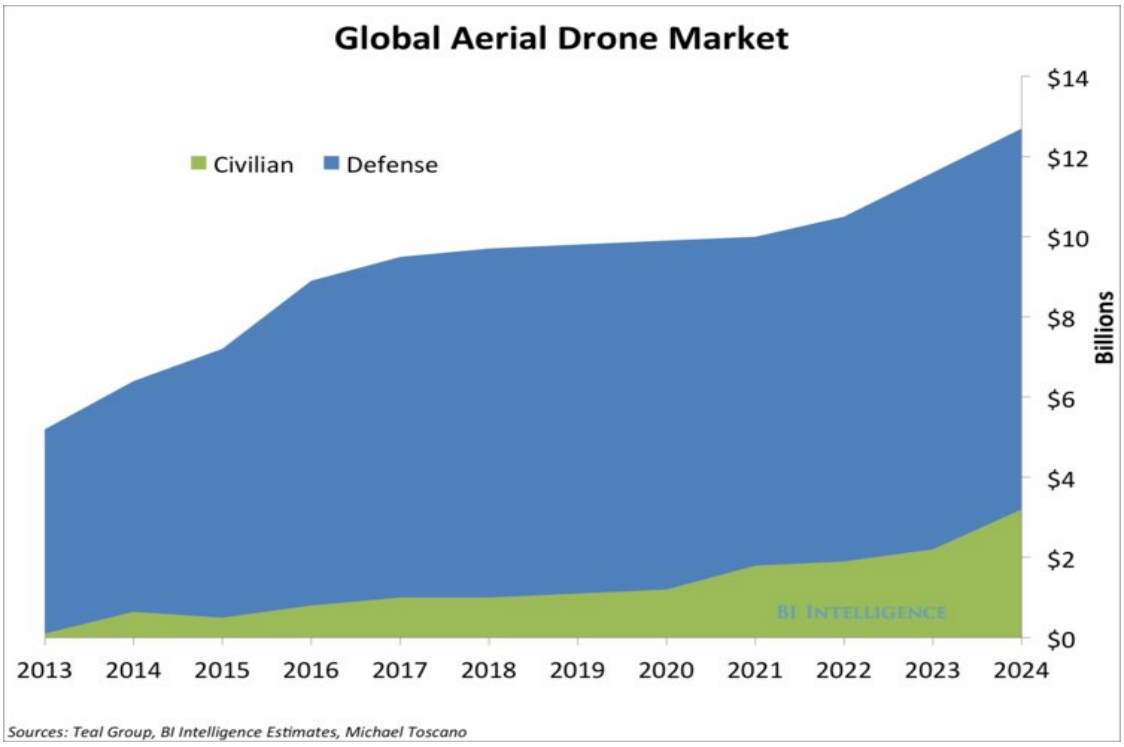

Figure 2. Projected Drone Sales

Ballve, 2014

The chart above is a study provided by the Teal Group, identifying the spending trends for purchasing drones. The prediction of both military and civilian spending continues to exceed 13 billion dollars by the year 2028. This is a forecasted increase of 10 billion dollars from the current year of 2018 (Ballve, 2014). The drone capability is only advancing and becoming more accessible to the public. The rising concern of drone operations in the Grey Zone parallel with the increase in sales.

Non-Military Drone Based Cyber Threats

New developments from computer experts have significantly improved alternative cyber attacking techniques such as “Kill Sticks” (Whittaker, 2016). Kill Sticks can be inserted into any part of a computer network, fowling all software and destroying the

entire network beyond repair. One version of Kill Sticks can be identified as a small USB memory stick. Plugging this Kill Stick into a computer will apply a malware program corrupting the computer and its corresponding network (Whittaker, 2016).

Micro drones have the ability to support the weight of a Kill Stick and have the technology to enter secured areas with little to no detection. These micro drones can remotely fly into classified and secured areas and robotically insert the Kill Stick into any network, corrupting its information while bypassing cyber-security protection emplaced protocols.

Micro drones also have other network threatening capabilities. A swarm of drones hovering outside of a network system could electronically interfere with operations such as disrupting an electrical grid subsequently creating a power outage (Wagenseil, 2016). Another concerning threat is the compromising of computer networks through "Zombie" attacks. Zombie computers have many dangerous capabilities, such as spreading viruses throughout a network of computers, or denial of service to websites by creating an overabundance of flooding a particular website (Strictland, n.d.). Strategically placed micro drones with Zombie capabilities are able to covertly enter a network while controlling and manipulating operations without detection (Strictland, n.d.).

Drone Based CBRNE Threats

Toxic WME agents related to CBRNE are also threats that military training attempts to counter or prevent. Performing maneuvers in protective gear such as protective masks is a standard practice for today's military (Spellman, 2010). Training consists of a basic understanding of operating in and decontamination from blood,

nerve/agents and other chemicals alike. Concerns in 2003 identified the threat of Iraq dispensing chemical agents via large scale drones (Burns, 2003). Valid threats of CBRNE warfare forced the US military and allied forces to incorporate training and equipment carrying precautions. CBRNE WMEs have the ability to be contained in an aerosol spray dispensing the contents via the use of drones.

Nation states following the Geneva Protocol have self-imposed control restrictions on CBRNE WME substances with an understanding of chemical uses under the laws of war (state.gov, n.d.). Violations of the Geneva Protocol may be an act of war by nation states using CBRNE related WMEs. Unfortunately, non-state actors and terrorist groups don't adhere to the laws of war because the laws of war were written by and for states. These groups would argue that this kind of attack is an equalizer against states who've rigged the system to be only about states. The ability to make homemade WME's is closer to home than one may realize. Fentanyl, as an example, is a synthetic opioid created for use as a pain killer. It could be repurposed to be used as a lethal, low detection risk WME. Even stronger strands of synthetic opioids such as a grain of car-fentanyl, comparable to a granule of powdered sugar, would render a lethal dose for an adult (Corbin, 2018). Hidden syringes on micro drones easily have the capability to transport and administer a lethal dose of a chemical or biological agent. The significant increase of drone usage for transport as identified in the Ruanda blood example simultaneously generates cost efficiency and timeliness as well as a concern for national and international threats.

Chapter IV.

Super Bowl LIV

Imagine the date is February 2, 2020, when the New England Patriots compete against the San Francisco 49ers for the NFL Super Bowl LIV Championship in Miami Florida. Predicting ticket sales prices based on the 2018 Super Bowl, the 2020 ticket sales have increased to $5000.00 for a budget seat and $50,000.00 for prime seating. Although many people world-wide will be watching this game from a television, the main event attracts those that have the ability to afford tickets. Movie stars, politicians, company CEOs, and other established persons of wealth will participate in the audience by not only cheering for the multi-million-dollar contract football players and staff, but also the halftime performers. This annual event may arguably be the largest collection of per capita income in one relatively compact location.

Along with the athletes, audience, performers and support staff, the stadium is filled with increased and high level security. Strategic police positioning, pre-event security sweeps, bomb sniffing dogs, X-ray machines, and random pat down checks are conducted to prevent any undesirables inside the venue. The Goodyear Blimp is overhead filming the game, advertising those companies willing to pay for space.

Deliberate risk assessments have been analyzed by local and federal emergency managers to mitigate any ground threats. Where is the most overlooked vulnerability of this event to cause disruption? The 188’ high stadium is not enclosed (Yousefi, 2016). All mitigation factors surround the ground environment. Aerial mitigation factors are equally important to consider as a need to respond as ground threats.

In this scenario of the Super Bowl LIV, a terrorist group is attempting to conduct a mass fatality event that instills fear and distrust in the US government to handle a crisis in the public sector. In doing so, the terrorist group has devised a plan to disperse a chemical agent to the crowded stadium. The disbursement method is through autonomously operated drones. The terrorists have programed these drones to congregate over the stadium and fall into the various areas within the crowds. Upon contact, the drones will dispense a life threatening chemical agent causing fatalities and mass casualties.

As a result, the non-fatality population within the stadium will either attempt to escape, seek medical treatment, or fall to be incapable of self-evacuation. The exits become overcrowded. The parking areas become congested. Medical emergency egress routes are blocked. Contaminated personnel will be directed to consolidate in a dedicated area, but some scared and unaware victims expand the contaminated area by vacating the premises. Once on scene, specialists collect the fatalities with proper protective equipment to a consolidated collection point.

The success or failure of the attack will depend on a number of variables. First, how many fatalities were there? How many casualties? How quickly and effectively did the authorities react to control the attack? Were the responders able to diagnose and treat the victims? Was the media able to control the news flow in an accurate manner? The objective of the terrorists is that the response will be chaotic and incompetent. Failure to respond properly can turn the public away from supporting the government and redirecting their frustration internally rather than the actual attack. The terrorist group will exploit the US failures as weakness while self-promoting their strengths. In the end the terrorist group gains legitimacy world-wide as those that can cripple the US

government. Conversely, quick agency responses and actions taken to properly mitigate the attack will further strengthen the US government legitimacy by reducing the Grey Zone and identifying the actors and purposes.

EMA Command and Control

The primary focus of Emergency Management Agencies (EMA) is to prepare for a large-scale mass casualty event improving human security (FEMA, 2018). Can hospitals local to the Miami Stadium successfully respond to a mass casualty event? What additional assets are available to mitigate a mass casualty leading to fatality?

State and Federal EMA leadership organizes and identifies response agencies for a variety of disaster management scenarios. EMA is not a governmental response organization in itself. They are the overseers of complimenting agencies that respond specifically to the emergency. They are the command and control headquarters. EMA as an orchestrator identifies, understands and implements the local and higher capabilities to function under one supervising organization. In order to be successful in cross coordination, training events of predictable scenarios create procedures and assign responsibilities. Much like the role of the nuclear and radiation identification Counter Terrorism Operations Support (CTOS) team, EMA will collect pre-incident information such as plume modeling to help determine the affected area based on wind and potential threats. Radiation and nuclear plumes are significantly greater than an unknown chemical or biological substance, but it is important to understand the drift patterns in order to safely release non-contaminated areas. It is also important to pre-identify a shelter in place safe zone to clear areas.

In the Fukushima incident of 2011, nuclear power plant safety was compromised by leaking radiation due to a tsunami strike. Media sources released radiation plume models to the public inferring that radiation drifted as far as California (Campisi, 2018). Although the plume models created by CTOS and other modeling agencies were accurate, the amount of radiation was less than significant at that distance (Zaveri, 2018). The individual particles were spread apart and had rendered no radiological threat. Similarly, Chernobyl identified a wide area of contamination. Although the danger area was not as significant in size, the population had already lost the trust of the government to move back into the area (Carl Willis, 2018).

Scenario based training events also identify Emergency Support Function (ESF) responsibilities to apply to a given scenario. Each ESF is separated by its specialty, whether it is sheltering, water supply, personnel mass decontamination, communications, evacuations or other necessary responses.

Medical Services (ESF 8)

There are many first responder agencies and organizations such as police, fire, hazmat, EMA and hospitals that work together to respond to a mass casualty event. A mass casualty event is not defined by a specific number of casualties, but the concern that the victims outweigh the resource capabilities. One of the most critical responders is the local hospital. Space availability within a hospital is concerning due to limited rooms and beds. It is also a concern of the number of caregivers available during the time of the incident.

Currently, there are 5 hospitals in the surrounding area of the Hard Rock Stadium in Miami, Florida. The bed capacity of each hospital varies, but is usually occupied with patients from other injuries and illnesses. If a patient from a mass casualty event is contaminated, the hospital's contaminated area bedding availability significantly drops. Every major hospital is trained and equipped with decontamination areas and processes for known contaminated patients. In many cases during a mass casualty event, an incident commander will identify multiple predetermined hospitals to transport victims.

Evacuation Plans (ESF 1)

The Hard Rock Stadium was opened in 1987 to seat almost 65,000 patrons. The structure itself is durable to withstand the east coast hurricanes and tropical storms. With much of the area exposed to open sky, the covered space is limited. Parking for a significant event is plentiful. The stadium has over 140 acres of dedicated parking areas. One identified vulnerability is that the stadium has dedicated only one helipad for emergency landings and transport. Planning considerations must include alternate landing areas for airlift emergent evacuations.

Transportation (ESF 1)

Miami is a densely-populated area with congested roads regardless of any scheduled major events. The highways are crowded with both commercial and residential traffic. In the event of any emergency ground evacuation, the roads will exceed normal traffic patterns by scared affected and non-affected civilians trying to escape the area. The Department of Transportation is overall responsible for traffic patterns and can create

road travel restrictions for emergency vehicle access. As all agencies argue personnel shortages, law enforcement or first responders under the command and control of the EMA typically provide this service. In the immediate and surrounding areas of the stadium, successful traffic and crowd control is important to mitigate the casualties and fatalities.

Time is critical to ensure a maximum effort to prevent fatalities. Therefore, the less critical contaminated personnel will be waiting for medical support or clearance. During this time, all personnel will be treated as displaced civilians. They need sustenance and sheltering while the more critical people are being treated and evacuated. Again, sustenance and sheltering are separate ESF functions controlled and directed by EMA.

Agriculture and Natural Services (ESF 11)

Water and food supply may be self-sustaining for a limited time as the arena provides food and drink. The Department of Agriculture stockpiles water for catastrophic emergencies that would have to be transported to the location. For standard emergencies such as a hurricane or a tornado, the National Guard, Red Cross, and other nonprofit agencies would take responsibility to transport food and water. In this case, sending these agencies without the proper protective equipment into a contaminated area would only add to the total number of contaminated personnel. Special considerations of protective equipment such as fully encapsulated suits with self-containing breathing apparatuses and decontamination would prevent further contamination. Once identified, the level of preventive equipment can decrease to the appropriate level. By decreasing within the threshold of the contaminants, first responders may not need to operate on compressed

air. This increases the amount of time to operate within the contaminated area because air tanks have limited air consumption. In addition, anyone who goes on air is required to be medically monitored for twice the amount of time on air.

The initial plan for sheltering during an emergency is to shelter in place. This is the safest way not to increase the contaminated area. Access to bathroom facilities and overhead cover is limited. As time elapses and the critical evacuations are ongoing, the further separation of contaminated personnel are further segregated, decontaminated and evacuated. Areas of safe refuge are created in order to evacuate and segregate potential patients out of constant exposure.

Hazardous Materials Response (ESF 10)

Containing the contamination whether it is personnel or equipment such as personally owned vehicles is difficult. In order to properly isolate the contamination, designated areas must be assigned to separate and categorize the level of threat. Direct contamination is the most severe category. Those that were directly contaminated are in the greatest threat of becoming a fatality. Those that feel ill but have had less or indirect exposure should be separated from both the critical and the non-exposed population. At no time during this process should anyone be released on their own accord. Just because they don't feel sick, doesn't mean that they can't be exposed while evacuating. Any of the thousands of drones that were released could have fallen short and ejected their contaminants onto a vehicle, door knob or any area that would be vulnerable to touching skin.

Overseen by the Environmental Protection Agency (EPA), decontamination teams such as the US National Guard's Chemical, Biological, Radiological, Nuclear and High Yield Explosive (CBRNE) Enhanced Response Force Package (CERFP) will conduct mass decontamination processes in order of precedence. Further medical evaluations will be required even after decontamination. Therefore, the decontaminated personnel will be transported to emergency shelters as the hospitals are overcrowded and going home is not an option. EMA identifies local sheltering areas such as schools, churches, arenas and other large facilities out of the danger zone.

Mass decontamination processes typically average about 100 people per hour per team, based on the level and type of contamination. This does not include decontamination of the area and other items. The drone driven scenario would have expended and non-expended drones within the area. The danger of stepping on one to expend its contents is still a danger to the immediate area. Areas of isolation must be screened for remaining drones and contamination to ensure residual attacks do not occur. This would mean that parking lots would be off limits until screened and rendered clear. The decontamination line is outside the threat area so that once a person is rendered decontaminated, medical professionals can treat the patients without going into the danger area. This also requires logistical support of medical resupplies. All equipment brought to the site will remain as part of the crime scene.

National Disaster Recovery Framework (ESF 14)

The EPA is responsible for the long term clean up. The most detrimental action the EPA deals with is mortuary affairs. They collect, identify and remove fatalities from the

contaminated area. Rendering a stadium, people, structures equipment and vehicles safe for use will take time and additional resources. Regardless of the timeframe, there will be significant loss. Along with the removal of fatalities, permanent damage casualties, other recoverable casualties, personal possession loss, and criminal activities (stealing, fighting) within the area of contamination are collective efforts to manage by the EPA and other first responders.

External Affairs (ESF 15)

The Department of Homeland Defense (DHS) is responsible for the coordination of the post scenario information distribution. Information sharing to the public has its complications with the amount of information that should release without compromising any follow-on investigation. The Federal Bureau of Investigations (FBI), the Defense Intelligence Agency (DIA), and other agencies investigate the crime scene in which technology and pattern identification can lead to a specific terrorist organization. Without public media from the responsible terrorist group admitting to the attack, it is up to these agencies to identify the actors.

Releasing any information prematurely could allow the terrorist group to further hide within plain sight. Not releasing enough information will falsely allow the public to generate their own ideas. If there is a significant amount of evidence leading to a specific terrorist organization, the government will research their background for reasons to initiate this attack. Inconclusive evidence from the investigation cannot clearly provide recommendations for actionable decisions for the senior government officials to act.

The above scenario would be more complicated with the crossover of interagency concurrent actions. This example of a response shows that an attack by one person and some basic technology could trigger a response of thousands of responders. Even if all agencies control the situation to the best of their ability, the Grey Zone attack may still be successful. The public may still disagree on the source of the attack, making it difficult to support a retaliation. The imposed complication of a Grey Zone attack causes public indecisiveness, splitting opinions of proper response methods. Inconclusive and delayed decisions typically result in no action. The attack remains a victory for the terrorist.

Chapter V.

Ideas and Considerations

Increasing awareness of drone capabilities creates a demand for preventive and countermeasure research. A collaboration of government regulation in conjunction with manufacturing ownership are baseline deterrents for preventing the misuse of drones. The following ideas and considerations are important for determining Grey Zone dangers of drone use in order to identify the potential strengths and weaknesses allowing or preventing a catastrophic event.

FAA Regulations

Directed by US Congress, aviation safety regulates through the Federal Aviation Administration (FAA). In June of 2016, The FAA released new policies and regulations pertaining to drone (UAV) operations (FAA, 2016). The FAA also mandates that local and state governments do not permit or regulate any type of aircraft or navigable airspace. Updated FAA Regulations further define methods and allowances of operations. All operators must be at least the age of 16. The only means of radio control operations must include a visual line of sight. This means that the drones must not exceed a distance or coverage beyond the view of the operator. To help mitigate this issue, some manufacturers have incorporated an auto return if the drone loses signal or exceeds a certain distance. This automatically backtracks the drone to the point of origin until the transmitter and receiver have reconnected.

All drone operations have regulated time and lighting restrictions as well. All drones can operate during daylight hours. Drones that have specially approved lighting systems may operate during twilight hours. Regulations also restrict the max speed of a commercial drone. The speed is not to exceed a groundspeed of 100 miles per hour. To operate any drone, the operator must be a registered or licensed operator. The drone operator provides the FAA personal information as well as the drone identification information.

Drone Registration

Drone registration has been a topic of conflict during the evolution of the US Congress Modernization and Reform Act in 2012. This act overturned the FAA's original decision to mandate non-commercial hobbyists to register their drones. The reversed requirement fought in January of 2016, resurfaced in 2017. As of 12 December, 2017, the US Government has reinstituted a "mandatory" registration requirement for all drones that weigh between 0.55 and 55.0 lbs. This registration process is a designed web-based program completed through the non-affiliated Federal Drone Registration Website. The FAA Website identifies that the FAA has already issued over 1 million Remote Pilot Certifications (Hennigan, 2018). With over 3 million drones estimated sold in 2018, the number of registrations remains to be a small percentage.

In order to ease the registration process, the NoFlyZone.org database provides an online registration form. This website tracks new and existing drone pilots to comply with FAA regulations. The website processes personal information along with drone

serial numbers in case a drone goes astray. A federally commandeered drone that violated air restrictions can trace back to the operator.

Manufacturer Restrictions

In order to remain compliant with FAA safety regulations, many of the leading drone manufacturers such as DJI Innovations are incorporating Geofencing technology into each drone (Newman, 2015). Geofencing is an internal blocking mechanism that creates a geographical boundary to prevent a drone from flying into a no-fly zone or restricted air space. The drone will have a turnaround and return to base capability if the drone reaches a restricted area or in some cases travel out of immediate eyesight. Geofencing programs work with both GPS and radio frequency.

Weapons/Counter Weapons

The US government currently possesses equipment to counter military grade drone operations. Unfortunately, enemy attacks have the ability to use consumer grade drones which can operate undetected and uninterrupted by radar. In the interest of national security, the US government and major corporations should invest in more modern drone countering equipment. Unlike Geofencing, developments such as “DroneShield” are an external acoustic technology to identify, mitigate and protect areas from drone operations (DroneShield). Although US interests involve the safety and security of its citizens, no matter their location, the decision to remain in a defensive posture is not feasible. Homeland attacks can cause the defensive mechanism reaction transitioning the US model of freedom into overregulated security measures.

Large scale events such as the aforementioned Super Bowl scenario, Boston Marathon, or MLB World Series are "hardened targets" or targets more difficult to penetrate due to the increased security measures on the premises. These large-scale events still retain vulnerabilities, but actions and risk assessments have been studied to harden the risk, providing a safer environment. Before any executed events, law enforcement agencies along with emergency managers and first responders identify vulnerabilities and try to mitigate potential risks. Security measures must now incorporate the threat of drones and mitigate the potential dangers. Drone control can operate from miles away without any human presence in the immediate vicinity. Counter measures such as DroneShield cannot cover 26.2 miles of a marathon route but can cover highly populated areas such as a finish line.

Countering Drones with Drones

This research identifies two specific drone threats with a variety of drone capabilities that have the potential to spearhead a new breakthrough to modern warfare. US military Special Operations Forces (SOF) continue to fight by unconventional and asymmetrical means. SOF are the most familiar of all the US armed forces that operate similarly to Grey Zone warfare. Drones have the ability to disrupt but also support the unconventional war fight. SOF needs to embrace new technology while creating, exercising and solidifying countermeasure training.

Offensively, drone capabilities improve operations within any Military arsenal. Various small scale drones cover a larger footprint with enhanced intelligence benefits. Operated at the group level, micro drones can provide enhanced visibility of an area of

interest without compromise. The US military can also shut down power grids in support of kinetic strike missions. Offensive drone usage would enhance the ability to strike and counterstrike various styles of Grey Zone operations by reducing human exposure, blocking enemy communications, while concurrently increasing military intelligence.

On July 4, 2017, inmate Jimmy Causey escaped from the Lieber Correctional Institution in South Carolina. Law enforcement officials captured Causey, initiating an investigation. The investigation determined that Causey had a pair of wire cutters flown into the prison grounds by way of a commercial drone (Hennigan, 2018). Prison breaks are now potential threats incorporating commercial drone use. In May of 2018, South Carolina law enforcement agencies introduced new drone equipment to the media sharing the ways prisons will combat the threat of future drone assisted prison escapes (Hennigan, 2018). This is the first time where prison systems incorporate drones against drones.

Chapter VI.

Findings

This thesis identifies and discusses the multitude of challenges that drone operations bring to the Grey Zone. The Grey Zone is not only a local, state and federal concern, but also an international one as well. The misperception of communication and cooperation among departments, agencies, and countries is greater than the common public may realize.

Grey Zone operations such as the example above can generate a mass response from individuals, local, state, federal, non-governmental organizations as well as international agencies to react to a catastrophe. To identify a threat of an unusual nature requires clear communication. Common terminology facilitates communication with regulations and doctrine. Predetermined definitions within updated regulations and doctrine allow the government to expedite a response rather than just a reaction. Today's technology enables the population to communicate in real time. Communication at all levels shapes the scope of the event.

In order to overcome some of the communication difficulties, host agencies create war gaming scenarios. Scenario based programs further discuss the roles and responsibilities of each agency. Through cooperation and discussion, each agency better understands the roles of other organizations to achieve a streamlined response process. Given specific exercise scenarios also achieve command and control authorities in order to discuss required information needed to share among all agencies. Common language, definitions, and trust are essential to create interagency cooperation.

Accurate information sharing is key to expedite a reaction and a timely appropriate response, but interagency cooperation remains a concern. Extracting information for a common goal is difficult for an individual agency to relinquish. Recognition and credit validates future budget requirements. Historical US National Security Strategies collectively identify that the whole of government approach should unify organizations to create a cohesive system. Collective training events take away from individual agency training funding and time.

Tabletop exercises are the most effective way of predetermining interagency cooperation. Many exercises focus on natural disasters. An exercise incorporating a drone attack would change the dynamic for a change in potential threats. Much like CONPLAN 8888, the Pentagon's "Zombie Apocalypse Exercise Scenario," developing a collaboration for a drone attack would create a dialog for an overall understanding in agency requirements toward participation. The government's premise behind the Zombie Apocalypse was to create a new scenario to conduct joint planning among participating agencies. It is a new approach to interagency cooperation that forces a different level of thinking also known as the Grey Zone mindset. Unlike the Zombie scenario, the drone attacks are potentially a legitimate threat that would identify the need for improved organization for Grey Zone planning.

When Can the Government Take Action?

Article 5 of the Washington Treaty identifies the multinational response agreements if any attack were to occur against Europe or North America. An attack on one NATO ally location transitions to an attack on all. NATO in turn created a

multinational alliance to combat any attack. Each ally may assist to restore a secure North Atlantic Region. If a Grey Zone attack occurs with uncertain origin, the United States may respond independently. It is up to the NATO allies to decide whether or not to support a retaliation. Grey Zone conflicts cause a hesitation to respond on multiple levels. NATO allies need clear justification for initiating support. Without clear justification of who initiated a Grey Zone attack, with a lack of response or support, NATO allies do not violate Article 5.

On 3 August 2018, the Pentagon granted and released a new budget in the Defense Bill of $10 million per year for 3 years specifically designed to counter Grey Zone conflicts (Aftergood, 2018). SOF operational monies can be used for foreign fighters that are aligned with US interests. Similar to the State Partnership Program designed after the Marshall Plan for International Relations, the commander of the US SOF will initiate ways to work with foreign countries to train and equip military members to better prepare for a Grey Zone fight. The funding will better prepare forces to react in an expeditious manner and with self-sufficiency.

The Bush Doctrine Concept Revisited

The Bush Doctrine was a Post-Cold War attempt to react to those rogue states that don't adhere international laws. The doctrine refers to the "Axis of Evil" as being the greatest concern to US National Security (Record, 2003). The Axis of Evil consists of the dangers and potential threats of Iran, Iraq and North Korea. The new approach targets this Axis by focusing on combating terrorism, those that harbor terrorist groups, and states that may have radical ties to terror. The Bush Doctrine recognized that the same policies

can't apply to those states that don't follow Western Laws. Sanctions, embargos and the threat of combat are meaningless to those that don't value western beliefs. The Bush Doctrine attempted to reassure that any threat to the United States could provoke a unilateral response yielding consequences of unknown magnitude. The doctrine displayed vagueness in order to have the maneuverability to respond or react to Grey Zone warfare.

Michael Doyle, author of *Striking First* suggests that the Bush Doctrine was too vague to make a reasonable offensive decision. He believes that before any state operating unilaterally or multilaterally, any threat must meet four criteria to receive approval from the UN Security Council. The four criteria are lethality, likelihood, legitimacy, and legality (Doyle, 2008). These standards represent jurisprudence or a legal concept to provide guidelines with flexibility. A globalized acceptance or denial creates unity and backing in the decision to initiate preventive or preemptive actions.

Countering the thought of Doyle's concept, President Bush addressed students at West Point claiming, "If we wait for threats to materialize, we will have waited too long" (Dolan, 2004). Similarly, if the US waits for UN Counsel's approval, then time will pass the opportunity to retaliate. The freedom of regulation and policy interpretation must encompass responsibility to act in a timely fashion.

Chapter VII.

Conclusion

Grey Zone conflicts are new norms that prove effective against strategists with a traditional mindset. Because technology is evolving faster than government regulation, adversaries are rapidly evolving in the same manner. The implementation of commercial off the shelf (COTS) products as WME threats is a new and innovative method to undermine traditional countermeasures.

This thesis recognizes three important paradigm-shifts or fundamental changes in approach to predict, prepare for and counter future Grey Zone conflicts. The first paradigm shift identified is to eliminate the comfortability that perception is reality in regard to matters of national security. Second, a Grey Zone mindset is imperative to combat Grey Zone attacks. The last paradigm shift identified is the reduction of legal ambiguity narrowing the adversaries' Grey Zone margin to operate with impunity.

General Overview and Important Contributions

- Define Grey Zone Conflicts
- Define Drone Technology
- Identify How Drones Affect US National Security: Foreign and Domestic
- Application of CBRNE Threats with Drone Capabilities
- Identify Need and Requirements for Improved Interagency Cooperation
- Identify Gaps in Drone Regulations
- Identify Recommendations for Reducing the Grey Zone

Main Points

Since the initiation of this thesis, many significant drone attacks have made news headlines. The event that validates this research is the August 4, 2018 drone attack on Nicolás Maduro, the president of Venezuela. Instead of chemical dispersion identified in the aforementioned Super Bowl scenario, each of 2 drones carried a kilogram, totaling over 4 pounds of explosives (Kelly, 2018). Fortunately, the attack failed, but many of the concerns mirror the relevancy and urgency within this thesis. The specified drone attack failed to reach the President due to electronic military precautionary countermeasures.

The pervasive social acceptance of the expression that perception is reality leads to a false sense of security. This thesis concludes that perception is perception and reality is reality. For example, the perception that drone registration will provide ownership and responsibility for regulated drone use, hence the perception of drone identification. The reality is that of the millions of drone owners, only 1 million operators have registered authentically under the FAA requirement proving that not all drone users follow the law (Hennigan, 2018). Malicious drone use is outpacing the expertise needed to use and regulate that technology.

Currently, all levels of terrorist organizations stockpile drones for the purpose of weapon systems. The Joint Improvised Threat Defeat Organization (JIDO) has focused on two methods for countering drone attacks. JIDO Director LTG Michael Shields understands that there is no "silver bullet" to stop illegal drone use (Hennigan, 2018). He further identifies the development of the multifaceted flexibility of both soft and hard kill processes. Soft kill drone countermeasures such as electronic methods enable the capture

of drones without damaging the system. Hard kill countermeasures damage the drones denying continuous operations.

Collectively, military and civilian innovator experts, identify the need for drone countermeasures. “The Bard College Center for Study of the Drone” collected data on drone countermeasure products. This study concluded that there were in excess of 230 products designed to counter malicious drone operations (Hennigan, 2018).

In order to be proactive with a Grey Zone attack, the preparation for potential retaliations must come from a Grey Zone mindset. The Grey Zone mindset must operate under rules with flexibility. Identification of what a weapon is has expanded from the conventional term. September 11, 2001 identified an airplane as a weapon. Following the attacks of 9/11, weapons development evolved throughout the times of Iraq. Vehicle Borne Improved Explosive Devices (VBIEDs) became a new threat. The technological use of cell phones garage door openers and other electronic devices to detonate explosives from a remote location also followed (Drehle, 2017).

As modern technology has become the new platform for terrorist use, this concept is foreign and difficult for conventional strategists to navigate. A drone with a warhead is easily identifiable as a weapon, but following the Grey Zone mindset, a drone with no luggage can also be a weapon. Drones intended to fly directly into jet intakes of an airborne aircraft is an “in-flight” attack with a weapon. The identification of atypical weapons is paramount when identifying the Grey Zone attack. Grey Zone operations must remain regulated without ambiguity within context of the threat. Adversaries must accept instant consequences as a legitimate threat in order to deter such attacks. Political correctness and diplomatic debates must not interfere with realistic threat assessments.

Ambiguity Reduction

Drone operations within the Grey Zone have the ability to create the next societal change for and against US National Security. In order to reduce ambiguity within the Grey Zone, regulations must remain current and viable to adjudicate violations. In addition, government regulations must also adhere to the punitive response to re-enforce the legitimacy within these regulations.

Reactions to small scale attacks at large scale venues, continue to delegitimize US security. US Government remains reactive to counter Grey Zone attacks by implementing additional security measures to mitigate future attacks. For example, airport security checks have become more stringent based on the September 11th attacks. The follow-on attempts of passing security checkpoints with shoe bombs have further added security measures that require arguably excessive removal of garments and the controversial increase of X-Ray imaging of each airport traveler. These increased methods of security checks infringe on some travelers right to privacy during the screening process. Small scale terrorist attacks therefore have successfully changed US freedoms.

"Those who would give up essential liberty to purchase a little temporary safety, deserve neither liberty nor safety." ― Benjamin Franklin (Volokh, 2014)

Although this thesis incorporates futuristic concepts, this research is not to prepare under the "doomsday prepper" philosophy. The answer is not to create individual "safe-zone bubbles" for each person in preparation for global destruction. It is in fact to identify

that US National Security is especially vulnerable to drone capabilities from our state and non-state adversaries alike.

This study identified that any significant foreign Grey Zone attack on US soil incorporates multilateral agency responses in order to gain intelligence for processing. It also identifies that communication and information sharing is not occurring as efficiently and effectively as it should. Whether local, state, federal, or NGO agencies participate, common terminology for information sharing must improve. Agency leads must embrace the whole of government approach to render the quickest results. Military training, awareness, mitigation research and offensive development must evolve collectively among state actors to keep pace with the rapid technological growth of Grey Zone operations.

"Military failures in a complex world are a result of three things. Failure to learn, adapt, and anticipate." – General David Perkins (Ulibarri, 2015)

References

Aftergood, S. (2018, August 21). *Secrecy News: Pentagon Moves to Support War in the Grey Zone.* Retrieved from Federation of American Scientists: https://fas.org/blogs/secrecy/2018/08/dod-grey-zone/

Arbuckle, A. Q. (n.d.). *1914-1918 Balloons of World War I.* Retrieved September 10, 2018, from Mashable: https://mashable.com/2016/03/02/wwi-balloons/#D0LkFJoPC8qX

Army, U. (n.d.). *FM 3-09: Field Artillery Operations and Fire Support.* Washington, DC, USA: US Army.

Army-technology.com. (n.d.). *RQ-11 Raven Unmanned Aerial Vehicle*. Retrieved September 10, 2018, from Army Technology: https://www.army-technology.com/projects/rq11-raven/

Atherton, K. D. (2014, November 24). *The History of Drones in 9 Minutes.* Retrieved September 9, 2018, from Popular Science: https://www.popsci.com/watch-brief-history-drone

Ballve, M. (2014, October 13). *COMMERCIAL DRONES: Assessing The Potential For A New Drone-Powered Economy*. Retrieved September 10, 2018, from Business Insider: https://www.businessinsider.com/the-market-for-commercial-drones-2014-2

Bensahel, N. (2017, February 13). *Darker Shades of Grey: Why Grey Zone Conflicts Will Become More Frequent and Complex.* Retrieved August 12, 2018, from Foreign Policy Research Institute: https://www.fpri.org/article/2017/02/darker-shades-gray-gray-zone-conflicts-will-become-frequent-complex/

Betz, D. (2015). *GRAY ZONE CONFLICTS MAY BE THE NEW NORMAL, BUT WILL HAVE THE SAME MARGINAL SUCCESS.* Retrieved September 3, 2018, from Small Wars Journal: http://smallwarsjournal.com/jrnl/art/gray-zone-conflicts-may-be-the-new-normal-but-will-have-the-same-marginal-success

Bindra, S. (2001, September 19). *India identifies terrorist training camps.* Retrieved August 18, 2018, from CNN.com/World: http://www.cnn.com/2001/WORLD/asiapcf/central/09/19/inv.afghanistan.camp/

Brands, H. (2016, February 5). *A Nation Must Think Before It Acts.* Retrieved August 15, 2018, from Foreign Pilocy Research Institute: https://www.fpri.org/article/2016/02/paradoxes-gray-zone/

Broich, J. (2017, January 26). *2017 isn't '1984' – it's stranger than Orwell imagined*. Retrieved October 7, 2017, from The Conversation: http://theconversation.com/2017-isnt-1984-its-stranger-than-orwell-imagined-71971

Burns, J. F. (2003, March 13). *THREATS AND RESPONSES: IRAQI WEAPONS; Iraq Shows One of Its Drones, Recalling Wright Brothers*. Retrieved September 10, 2018, from The New York Times: https://www.nytimes.com/2003/03/13/world/threats-responses-iraqi-weapons-iraq-shows-one-its-drones-recalling-wright.html

Calderone, L. (2016, December 16). *Was that an Insect or a Drone.* Retrieved September 10, 2018, from Robotics Tomorrow: https://www.roboticstomorrow.com/article/2016/12/was-that-an-insect-or-a-drone/9265/

Campisi, J. (2018, July 26). *There may be traces of radioactive particles from Fukushima in your California red wine*. Retrieved September 10, 2018, from CNN: https://www.cnn.com/2018/07/23/health/california-wine-radioactive-fukushima-trnd/index.html

Carl Willis. (2018, April 16). *Will people ever move back to Pripyat when most of the radiation is gone?* Retrieved September 10, 2018, from Quora: https://www.quora.com/Will-people-ever-move-back-to-Pripyat-when-most-of-the-radiation-is-gone

Century-of-flight.net. (n.d.). *Century of Flight.* Retrieved September 10, 2018, from Military Baloons 1850 - 1900: http://www.century-of-flight.net/new%20site/balloons/Military%20balloons%201850.htm

cia.gov. (2003). *National Security for Combating Terrorism.* Strategic, Central Intelligence Agency, Central Intelligence Agency.

cnn.com. (2018, July 18). Retrieved August 22, 2018, from CMM Politics: https://www.cnn.com/2018/07/18/politics/trump-russia-targeting-us-cabinet-meeting/index.html

Corbin, C. (2018, April 11). *Run-ins with Carfentanil: The opioid 5,000 times more potent than heroin*. Retrieved September 10, 2018, from Fox News: http://www.foxnews.com/us/2018/04/11/run-ins-with-carfentanil-opioid-5000-times-more-potent-than-heroin.html

DJI. (n.d.). *Phantom1 Specs*. Retrieved September 10, 2018, from DJI.com: https://www.dji.com/phantom

Dolan, C. (2004). *Striking First: The preventive War Doctrine and Reshaping of US Foreign Policy.* Retrieved July 22, 2017, from Google Books: https://books.google.com/books?id=_24YDAAAQBAJ&pg=PA16&lpg=PA16&dq="If+we+wait+for+threats+to+materialize,+we+will+have+waited+too+long."&source=bl&ots=JR5ZnkIdT8&sig=-5Tk5gJzAH1lKkfCQ59W8UYSEcI&hl=en&sa=X&ved=0ahUKEwjZgfKJ5qDVAhVs0FQKHTmcCg0Q6AEILzAC#v=onepage&q="If%20we%20wait%20for%20threats%20to%20materialize%2C%20we%20will%20have%20waited%20too%20long."&f=false

dos.gov. (2006, September). *US Department of State.* Retrieved September 9, 2018, from National Strategy for Combating Terrorism: https://2001-2009.state.gov/s/ct/rls/wh/71803.htm

Doyle, M. (2008). *Striking First: Preemption and Prevention in International Conflict.* (S. Macedo, Ed.) Princeton, NJ: Princeton University Press.

Drehle, D. V. (2017, September 29). *The security threat we've been ignoring: Terrorist drones*. Retrieved October 5, 2018, from The Washington Post: https://www.washingtonpost.com/opinions/the-security-threat-were-ignoring-terrorist-drones/2017/09/29/3fbd1374-a51f-11e7-b14f-f41773cd5a14_story.html?noredirect=on&utm_term=.827ff233e13f

DroneOmega.com. (2017). *Drone Omega.* Retrieved September 10, 2018, from How GPS Drone Navigation Works: https://www.droneomega.com/gps-drone-navigation-works/

DroneShield. (n.d.). *DroneShield.* Retrieved September 10, 2018, from DroneShield: https://www.droneshield.com

FAA. (2016, August 29). *The FAA's New Drone Rules Are Effective Today.* Retrieved September 10, 2018, from Federal Aviation Administration: https://www.faa.gov/news/updates/?newsId=86305

FEMA. (2018, March 26). *FEMA*. Retrieved September 10, 2018, from About the Agency Mission Statement: https://www.fema.gov/about-agency

Foster, T. (2016, December 14). *10 Ways Drones Are Changing Your World*. Retrieved from Consumer Reports: https://www.consumerreports.org/robots-drones/10-ways-drones-are-changing-the-world/

Friedman, U. (2014, March 2). *Putin's Playbook: The Strategy Behind Russia's Takeover of Crimea.* Retrieved August 22, 2018, from The Atlantic: https://www.theatlantic.com/international/archive/2014/03/putins-playbook-the-strategy-behind-russias-takeover-of-crimea/284154/

Hennigan, W. (2018, May 31). *Experts Say Drones Pose a National Security Threat — and We Aren't Ready*. Retrieved October 5, 2018, from Time: http://time.com/5295586/drones-threat/

Ignatius, D. (2017, September 21). *Some Ways to Deal With North Korea*. Retrieved Octobet 7, 2017, from The Washington Post: https://www.washingtonpost.com/opinions/some-creative-ways-to-deal-with-north-korea/2017/09/21/239585dc-9f0c-11e7-9c8d-cf053ff30921_story.html?utm_term=.a6c520064859

Kelly, E. (2018, August 6). *USA Today.* Retrieved from Venezuela Drone Attack: Here's What Happened to Nicolas Maduro: https://www.usatoday.com/story/news/politics/2018/08/06/venezuela-drone-attack-nicolas-maduro-assassination-attempt-what-happened/913096002/

Keohane, J. (2017, February 16). *WHAT NEWS-WRITING BOTS MEAN FOR THE FUTURE OF JOURNALISM.* Retrieved September 3, 2018, from Wired : https://www.wired.com/2017/02/robots-wrote-this-story/

Law360. (2018, February 16). *Autonomous Drones: Set To Fly, But May Not Comply.* Retrieved September 10, 2018, from Wiley Rein LLP: https://www.wileyrein.com/newsroom-articles-Autonomous-Drones-Make-It-Easier-to-Fly-But-Harder-to-Comply.html

Leahy, R. L. (2018, February 18). *How to Think About Terrorism.* Retrieved September 2, 2018, from Psycology Today: https://www.psychologytoday.com/us/blog/anxiety-files/201802/how-think-about-terrorism

Lindsay, J. R. (2015, May). *Exaggerating the Chinese Cyber Threat*. Retrieved September 10, 2018, from Harvard Kennedy School Belfer Center for Science and International Affairs: https://www.belfercenter.org/publication/exaggerating-chinese-cyber-threat

Maddox, S. (2015, February 24). *Drones in the US National Airspace System: A Safety and Security Assessment.* Retrieved February 23, 2018, from National Security Journal: http://harvardnsj.org/2015/02/drones-in-the-u-s-national-airspace-system-a-safety-and-security-assessment/

Michael Collins, N. G. (2018, July 18). *Congressional GOP leadership: No doubt that Russia meddled in 2016 presidential election.* Retrieved August 22, 2018, from USA Today: https://www.usatoday.com/story/news/politics/2018/07/17/paul-ryan-really-clear-russia-meddled-presidential-election/791541002/

Mikkelson, D. (2018, May 2). *Insect Spy Drone*. Retrieved September 10, 2018, from Snopes: https://www.snopes.com/fact-check/insect-spy-drone/

Mizokami, K. (2017, March 14). *This Chart Explains How Crazy-Expensive Fighter Jets Have Gotten.* Retrieved September 10 2018, from Popular Mechanics: https://www.popularmechanics.com/military/weapons/news/a25678/the-cost-of-new-fighters-keeps-going-up-up-up/

Monthly, M. H. (2012, May 11). *Predator Drone Specifications*. Retrieved September 10, 2018, from Military History Monthly: https://www.military-history.org/articles/predator-drone-specifications.htm

Newman, L. H. (2015, February 10). *Here's How to Set Up a No-Fly Drone Zone Over Your House.* Retrieved from Future Tense: http://www.slate.com/blogs/future_tense/2015/02/10/noflyzone_org_lets_you_geofence_the_area_over_your_house_for_drones_to_avoid.html

Nichols, T. (2013). *No Use.* University of Pennsylvania Press.

Nichols, T. (Producer). (2017). *Harvard Lecture* [Motion Picture]. USA.

Nielsen, K. M. (2017, July 4). *The U.S. isn't prepared for the growing threat of drones*. Retrieved October 5, 2018, from The Washington Post: https://www.washingtonpost.com/opinions/the-us-isnt-prepared-for-the-growing-

threat-of-drones/2018/07/04/30cc2a76-7eef-11e8-b9f0-61b08cdd0ea1_story.html?utm_term=.8066bfd7d2b6

O'hare, R. (2016, November 1). *China proudly debuts its new stealth jet it built 'by hacking into US computers and stealing plans'.* Retrieved September 10, 2018, from Daily Mail: https://www.dailymail.co.uk/sciencetech/article-3893126/Chinese-J-20-stealth-jet-based-military-plans-stolen-hackers-makes-public-debut.html

PBS. (2008, May 11). *The Geneva Conventions: The Geneva Conventions: To Whom Do the Conventions Apply?* Retrieved August 22, 2018, from PBS/WGBH: http://www.pbs.org/wnet/wideangle/uncategorized/the-geneva-conventions-to-whom-do-the-conventions-apply/615/

Pekgozlu, I., Ozdemir, H., & Ercikti, E. (2007). *Communication Methods in Terrorist Organizations: A Case Study of Al-Qaeda Connected Terrorism in Turkey* . Retrieved September 2, 2018, from National Criminal Justice Reference Service: https://www.ncjrs.gov/App/Publications/abstract.aspx?ID=247416

Piddick, R. (2009). *THE NEED FOR CONVENTIONAL WARFARE AS THE US MILITARY ADDRESSES THE ENVIRONMENT & THREATS OF THE 21ST CENTURY.* Retrieved September 3, 2018, from USMC Master of Military Studies: http://www.dtic.mil/dtic/tr/fulltext/u2/a509847.pdf

Piore, A. (2013, July 11). *How I Tried Turning My Off-The-Shelf Drone Into A Weapon*. Retrieved September 10, 2018, from Popular Science: https://www.popsci.com/technology/article/2013-06/flight-fringe

Record, J. (2003). *The Bush Doctrine and War with Iraq*. Retrieved July 22, 2017, from US Army War College: http://ssi.armywarcollege.edu/pubs/parameters/articles/03spring/record.pdf

Rogoff, K. (2007, June 26). *Foreign Holdings of U.S. Debt: Is Our Economy Vulnerable?* Retrieved August 28, 2018, from Brookings: https://www.brookings.edu/testimonies/foreign-holdings-of-u-s-debt-is-our-economy-vulnerable/

Sanders, A. W. (2017). *Drone Swarms.* White Paper, US Army Command and General Staff College.

Schallhorn, K. (2017, July 13). *Trump and the Russia investigation: What to know.* Retrieved September 3, 2018, from Fox News Channel: http://www.foxnews.com/politics/2018/07/13/trump-and-russia-investigation-what-to-know.html

Schogol, J. (2014, September 11). *'American War Generals' a sobering reflection on U.S. failures in Iraq.* Retrieved February 20, 2018, from Military Times: https://www.militarytimes.com/off-duty/movies-video-games/2014/09/11/american-war-generals-a-sobering-reflection-on-u-s-failures-in-iraq/

Smith, S. V. (2015, December 10). *Leaked Budget Document Provides Glimpse Into How ISIS Makes Money*. Retrieved September 10, 2018, from National Public Radio: https://www.npr.org/2015/12/10/459249994/leaked-budget-document-provides-glimpse-into-how-isis-makes-money

Spellman, L. (2010, April 20). *Battalion NBC NCO hones skills by training others*. Retrieved September 10, 2018, from US Army: https://www.army.mil/article/38295/battalion_nbc_nco_hones_skills_by_training_others

Stangel, J. (2018, May 31). *TIME's Drones Issue: Go Behind the Cover.* Retrieved September 10, 2018, from TIME: http://time.com/longform/time-drones-behind-cover/

state.gov. (n.d.). *Protocol for the Prohibition of the Use in War of Asphyxiating, Poisonous or Other Gases, and of Bacteriological Methods of Warfare (Geneva Protocol)*. Retrieved September 10, 2018, from US Department of State Diplomacy in Action: https://www.state.gov/t/isn/4784.htm

Strictland, J. (n.d.). *How Zombie Computers Work*. Retrieved September 10, 2018, from How Stuff Works: https://computer.howstuffworks.com/zombie-computer.htm

Swedberg, C. (2017, September 6). *RFID Journal.* Retrieved September 10, 2018, from Lightweight Relays Enable Small Drones to Read RFID Tags Indoors: https://www.rfidjournal.com/articles/view?16560

The Geneva Conventions: The Geneva Conventions: To Whom Do the Conventions Apply? (2008, May 11). Retrieved September 3, 2018, from WGBH: http://www.pbs.org/wnet/wideangle/uncategorized/the-geneva-conventions-to-whom-do-the-conventions-apply/615/

Toure, M. (2017, December 11). *Suspect in Custody After 'Attempted Terrorist Attack' Near Times Square.* Retrieved September 1, 2018, from Observer: http://observer.com/2017/12/attempted-terrorist-attack-times-square-nyc/

Ulibarri, S. (2015, March 31). *US Army*. Retrieved March 12, 2019, from Perkins outlines how and why to 'Win in a Complex World': https://www.army.mil/article/145638/perkins_outlines_how_and_why_to_win_in_a_complex_world

Volokh, E. (2014, November 11). *The Washington Post*. Retrieved March 12, 2019, from Liberty, safety, and Benjamin Franklin: https://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/11/11/liberty-safety-and-benjamin-franklin/?noredirect=on&utm_term=.ac59104a3337

Wagenseil, P. (2016, August 9). *How a Drone Could Take Out a Power Plant*. Retrieved September 10, 2018, from tom's guide: https://www.tomsguide.com/us/drone-jamming-attacks-bh2016,news-23146.html

Whittaker, Z. (2016, September 8). *Now you can buy a USB stick that destroys anything in its path.* Retrieved September 10, 2018, from ZDNet: https://www.zdnet.com/article/now-you-can-buy-a-usb-stick-that-destroys-laptops/

Yale. (n.d.). *The Avalon Project.* Retrieved from Yale Law School: http://avalon.law.yale.edu/20th_century/hague04.asp

Yousefi, R. (2016, August 8). *Everything You Need to Know About the Dolphins' $500 Million Stadium Renovation*. Retrieved September 10, 2018, from Miami New Times: https://www.miaminewtimes.com/news/everything-you-need-to-know-about-the-dolphins-500-million-stadium-renovation-8659288

Zaveri, M. (2018, July 20). *Fukushima's Nuclear Imprint Is Found in California Wine (Drinkers, Don't Panic)*. Retrieved September 10, 2018, from The New York Times: https://www.nytimes.com/2018/07/20/science/fukushima-radiation-levels-california-wine-nyt.html