SUBS, SWARMS, AND STRICKEN INFRASTRUCTURE:
THE VULNERABILITY OF THE UNITED STATES TO NON-TRADITIONAL TERRORIST THREATS

by
Patrick Collman

A thesis submitted to Johns Hopkins University in conformity with the requirements for the degree of Master of Arts in Global Security Studies

Baltimore, Maryland
May 2017

Abstract:

The lack of mass casualty domestic attacks in the United States, carried out by foreign fighters, since 9/11 should not be taken for a sign of future invulnerability. Major Islamic terrorist organizations have previously conducted attacks focused on splashy news headlines and high body counts. However, Al-Qaeda's original stated goal was to bankrupt the West, not kill everyone in it. Is the United States simply impervious to such an attack aimed at causing extensive financial or economic damage? Or is the United States vulnerable, and ultimately a sitting duck? This paper will argue the latter.

By examining the relationships between Islamic terrorist organizations and drug-trafficking organizations in Central and South America, and investing the use of advanced narco-submarines by the latter, the goal is to explore a viable means for inserting a group of armed, trained men undetected into the United States. Case studies examine the effectiveness of swarm-style terrorist attacks when compared to WMD and lone-wolf terror attacks. Further case studies seek to highlight extensive vulnerabilities within the U.S. energy and economic infrastructure that, if taken offline via terrorist attack, would result in long-lasting and immensely expensive consequences if attacked.

Were Al-Qaeda or another terrorist organization to decide that they wanted to hit America in the pocket book as opposed to racking up a body count, this paper seeks to show that they possess the means, the ability, and the opportunity to do so.

Advisors: Dr. Leslie Copeland, Dr. Jacob Straus, Dr. Sarah Clark

Acknowledgements:

For my family, and all those who fell in service to the Republic. Semper Fidelis.

Table of Contents

List of Figures

Thesis Introduction

In the aftermath of 9/11, there has not been another mass-casualty attack carried out by terrorist foreign fighters in the United States. Widespread changes and developments to intelligence collection and sharing, law enforcement and government coordination, and safety procedures have prevented another "Black Swan" like 9/11 from happening. It is also possible to argue that this lack in attacks is not due to interest or effort by Al-Qaeda or ISIS – one need only to look at the numerous attacks that have occurred in Western Europe in the last few years to see that Islamic terrorist still possess a fundamental desire, and indeed make it a primary goal, to strike at the West.

Interestingly, these mass-casualty attacks veer somewhat from the original path laid out by Al-Qaeda back in the early 2000s. Osama bin Laden and other senior Al-Qaeda leaders repeatedly stated that the ultimate goal was to bankrupt the West, and cause crippling financial damage which would hamstring the West's attempts to combat Islamic radicalism. However, the majority of terrorist attacks in recent years appear to focus on simply running up a body count, and financial impacts only come about indirectly. Why have Islamic terrorists not directly gone after a target which would have a direct and significant impact on a Western country's economy – is this due to a contradiction in dogma, focusing on body counts instead of hitting the enemy in the pocketbook? Or is it due to a lack of means or targets that could produce a significant financial impact?

It is important to investigate this apparent anomaly because the United States risks opening itself to another "Black Swan" attack potentially worse than 9/11 if the risk is ignored. This thesis aims to highlight how Islamic terrorist organizations, should they

wish to conduct a strike against the domestic U.S. that resulted in significant financial and economic impacts, possess the means, ability, and targets to conduct such an attack. Furthermore, should they do so, there is currently little the U.S. could do to prevent or effectively recover quickly from such an attack.

In Chapter 1, "SHADOWS IN THE DEEP: Narco-Submarines, Terrorism, and Domestic Security", I examine the nature and history of the relationships between Islamic terrorist organizations and drug-trafficking organizations in Central and South America, and explore the development and use of advanced narco-submarines by the latter to smuggle narcotics into the United States and elsewhere. The goal of this chapter is two-fold: first, to determine if strong business relationships exist between Islamic terrorists and drug-trafficking organizations, to the point that the latter may assist the former in achieving objectives inside the U.S.; and secondly, to explore the effectiveness of drug-running narco-submarines, if the U.S. is effectively interdicting them, and if drug subs are capable of smuggling more than just narcotics. My argument for this chapter is that the drug-trafficking organizations possess a means of clandestine transport and entry into the United States (narco-submarines) that Islamic terrorist organizations are capable of exploiting – a vessel capable of carrying ten tons of narcotics can just as easily transport armed men and materiel. Furthermore, I seek to highlight that drug-trafficking organizations have assisted Islamic terrorist organizations in the past, and thus are capable and willing partners in the future.

In Chapter 2, "THE STINGING SWARM: the Threat the United States Faces from Terrorist and Swarm Tactics", I examine the effectiveness of swarm-style terrorist attacks in comparison to WMD and lone wolf-style terror attacks. The purpose of this

chapter is to explore whether a swarm-style terror attack poses a greater threat to the domestic United States than a WMD or lone-wolf terror attack, in measuring the effects and casualties resulting from examples of each style of attack. I explore a number of case studies examining the effectiveness of swarm tactics in both military settings (real-world and training environments) as well as two actual terror attacks in which swarm tactics were employed (Mumbai in 2008 and Paris in November 2015). As a measurable comparison, I then compare the casualty tallies from WMD, lone-wolf, and swarm-based terror attacks in order to determine which yields the highest body count. Swarm attacks produce significantly more casualties, last longer, require greater law enforcement effort to end, and in both cases resulted in cities being, for all intents and purposes, shut down for the duration.

Lastly, Chapter 3, "SPOILING GOLIATH'S GARDEN: Determining the Vulnerability of U.S. Economic and Energy Infrastructure to Kinetic Attacks", explores centers of gravity within the U.S. economic and energy infrastructure that represent soft targets vulnerable to kinetic terrorist attacks. In particular, I chose to look at centers of gravity with the electrical and petroleum/economic industries, as these represent some of the most crucial enablers of everyday life. Examining these critical nodes through a series of case studies, the goal is to highlight their importance and vulnerability, as well as the ramifications of a successful terrorist attack on one or several of the examined cases. From key elements of the western U.S. electrical grid, to shipping, to the petroleum industry, the United States is replete with infrastructure that possess little in the way of defense from a determined kinetic attack. Drawing on real-world examples which manifested on a much smaller scale, the chapter explores the relative vulnerability of key

nodes to simple kinetic attacks, the difficulties faced in compensating for a lost node, and the secondary and tertiary economic, environmental, and societal effects of an attack on any of the examined case study subjects.

The overarching goal of this thesis is to lay out a clear blueprint, a "Road to Crisis" as to how an overseas Islamic terrorist organization could clandestinely infiltrate significant numbers of men and materiel into the United States; showcase tactics that maximize the effectiveness of a small number of armed individuals against a larger opponent; and pinpoint targets where terrorists could strike in order to cause extensive and long-lasting economic and domestic damage to the United States, not through killing Americans but through infrastructure and economic damage. Rather than exploring the probability, this paper aims to examine the *possibility* of such an attack on key infrastructure. In presenting a cohesive threat arc and providing real-world scenarios that illustrate the individual concepts on a smaller scale, the desired outcome of this thesis is to foster constructive dialogue and the development of effective counters to the threats examined herein.

Chapter 1: Shadows in the Deep

Terrorism, Narco-submarines, and Domestic Security

Introduction

In this chapter, I will address the following question:

Considering the developing relationships between international terrorist organizations seeking to attack U.S. interests and drug cartels in Central and South America, do narco-submarines pose a significant threat to U.S. domestic security?

Narco-submarines, also known as narco-subs and drug subs, are fully submersible naval craft operated by drug cartels in Central and South America. Used to transport narcotics in great quantities, in recent years they have proven to be a stealthy and effective means of penetrating U.S. coastal security measures. Utilized by the cartels in the Pacific Ocean, Gulf of Mexico, and Atlantic Ocean, in recent years their numbers have increased dramatically.

I would argue that narco-submarines *do* pose a distinct threat to the U.S. homeland, and I plan to do so in this paper using a two-step approach. First, I will explore current relationships between international terrorist organizations that may have an interest in conducting an attack on U.S. soil, and drug cartels operating narco-submarines to transport narcotics from Central and South America into the United States. Once the scope of this relationship is established, the second (and majority) section of the chapter will explore and assess the history, evolution, and capabilities of drug cartel narco-submarines.

My goal in this chapter is to show that, while not a concern to U.S. domestic security when operated by drug cartels, narco-submarines do pose a significant threat if acquired by a terrorist organization seeking to attack the United States at home. Furthermore, my intent with this paper is to not only shed light on this little-known

subject, but to spark further dialogue and research geared towards implementing a better defensive strategy for U.S. shores.

Literature Review

There is a dearth of academic literature specifically examining the domestic security threat posed by narco-submarines; even the U.S. government realized this and commissioned a study to be done in an attempt to develop a capabilities analysis and threat assessment of narco-submarines, which are deemed to be an "underconsidered/understudied topic"[1].

While unarmed, narco-subs possess the capability to transport tons of men and materiel just as easily as they transport narcotics. Initially crude, small and only semi-submersible, narco-subs are now large, fully-submersible, stealthy craft capable of accurate navigation and transporting tons of cargo for thousands of miles[2]. Current interdiction operations only succeed in catching roughly one of every four detected narco-subs[3]. Such an effective means of penetrating the U.S. border security apparatus represents a major threat to U.S. domestic security, particularly when considering the possibilities of a terrorist organization acquiring the use of a narco-sub and utilizing it to transport operatives and equipment (including "dirty bombs", biological agents, high explosives, and other weapons) to the United States undetected.

[1] Edited by Byron Ramirez and Robert J. Bunker, "Narco-Submarines: Specially Fabricated Vessels Used For Drug Smuggling Purposes", written for the Foreign Military Studies Office, 2014. PDF.
[2] Byron Ramirez, "Narco-Submarines: Applying Advanced Technologies to Drug Smuggling", Small Wars Journal. Posted 8 March 2014. Accessed 25 February 2016.
[3] Byron Ramirez and Robert J. Bunker, "Narco-Submarines: Drug Cartels' Innovative Technology", Center for International Maritime Security, 2 August 2014.

Discussion on Parallel Literatures

There are several literatures that run parallel to my arguments. These include:

- drug cartel capabilities and intentions
- counter-narcotics and drug-interdiction operations
- the existence and scope of ties between drug cartels and international terrorist organizations

Examining the cartels' capabilities and intentions will ideally provide me with both historical background and technical/performance details of the cartels as well as their narco-subs. With their primary purpose being the covert transport of illicit narcotics, narco-subs are a major target for attempts by U.S. agencies intent on stemming the flow of drugs into the United States. Literature examining current and potential business ties between cartel and terrorist groups will provide crucial support for my main argument.

Schools of Thought

Literature regarding drug cartel capabilities seems to agree on a number of points: narco-subs are becoming more sophisticated and capable; cartels are using them with dramatically-increasing frequency[4]; and they are almost impossible to locate and capture once launched. Most of the focus in this literature is on the transport of narcotics, however; little thought seems to be given towards other potential cargo (i.e. terrorists and weapons). Only two[5] sources[6] directly address the possibility of terrorists utilizing narco-subs for transporting something besides narcotics, and a third source[7] mentions the

[4] "Waving, Not Drowning". *The Economist*, 1 May 2008.
[5] Terrance G. Lichtenwald, Mara H. Steinhour, and Frank S. Perri, ibid
[6] Joseph Direnzo, "What the Semi-submersibles Mean: Transnational Gangs, Drugs, and Terrorism", *Defense Media Network*, 12 August 2010.
[7] Byron Ramirez and Robert J. Bunker, "Narco-Submarines: Drug Cartels' Innovative Technology", ibid

possibility in one brief paragraph. I intend to explore this concept in fuller detail and address this gap in the current field of analysis.

Regarding counter-narcotics and drug-interdiction operations, there is a consensus that the most effective tactic to counter drug-subs is to capture them while still being assembled in their tropical workshops. In agreement with literature assessing drug cartel capabilities, parallel literature concerning drug interdiction operations emphasizes the difficulty of detecting drug subs once they have launched, although new technology and tactics are starting to bear fruit as well[8]. However, there is little discussion into how looming budget cuts will affect the effectiveness of current interdiction efforts. Nor is there any discussion on interdicting drug subs when they stop to offload cargo. This may be due to security concerns; nonetheless, any information will prove useful as I describe current efforts to interdict narco-subs, and why those efforts must be increased.

Literature on connections between drug cartels and terrorist organizations emphasizes a growing connection between drug cartels in Central and South America[9] and terrorist organizations hostile to the United States, including Al-Qaeda, the Taliban, Hamas and Hezbollah. The majority of the focus seems to be on terrorist organizations using drug trafficking as a means of income to fund other operations[10]. However, the sources also indicate that there is growing concern about potential cooperation between the two groups to smuggle terrorist operatives and accompanying weaponry into the United States[11]. This parallel literature will prove most efficacious to my thesis by

[8] Christopher Lagan, "Drug Subs 2.0", *Coast Guard Compass*, 13 July 2010
[9] Testimony by Steven C. McCraw, ADOIC-FBI before the Senate Judiciary Committee on 20 May 2003
[10] Michael Braun, "Drug Trafficking and Middle Eastern Terrorist Groups: A Growing Nexus?", *The Washington Institute*, 25 July 2008
[11] Michael T. McCaul, "A Line in the Sand: Countering Crime, Violence and Terror at the Southwest Border", Congressional Report before Congress, November 2012, p. 3-5.

providing proof of cooperation between drug cartels and terrorist organizations, and thereby validating the possibility of terrorists acquiring the use of a narco-sub.

Theory and Hypothesis

Narco-submarines are a newer technology, initially appearing the mid-90's and seeing a rapid increase in technology, sophistication, and usage. They have progressed from small, semi-submersible, short-range craft to vessels capable of transporting four tons of cargo from Ecuador and Honduras to Europe running entirely underwater[12], powered and operated by advanced technology despite being constructed in covert jungle workshops. Furthermore, U.S. operations have thus far proven very unsuccessful at interdicting these craft, even when their general routes and schedules are known[13].

I am in somewhat uncharted waters in exploring this subject: scant work has been done on this topic, and therefore there are few official theories to support or debunk. At best, scholars and researchers have made tentative statements[14] regarding the possibility of terrorist groups acquiring and using a narco-sub. The overwhelming majority of work concerning narco-submarines is focused on their drug-smuggling capabilities, even those also examining the applications of narco-sub technology[15] by terrorist groups. In the absence of more-formalized and institutionalized theories, I am left with my own: narco-submarines pose a significant threat to U.S. domestic security if one or more find their way into the hands of terrorist organizations.

[12] Byron Ramirez and Robert J. Bunker, "Narco-Submarines: Drug Cartels' Innovative Technology", Center for International Maritime Security, 2 August 2014.
[13] "Waving, Not Drowning". ibid.
[14] Byron Ramirez and Robert J. Bunker, "Narco-Submarines: Drug Cartels' Innovative Technology", ibid
[15] Terrance G. Lichtenwald, Mara H. Steinhour, and Frank S. Perri, ibid

Regarding the plausibility of terrorist groups acquiring a narco-sub, again there is no official theory around which to frame my argument. However, what is known is the extensive and still-developing[16] relationships[17] between terrorist groups and drug cartels[18]. Aiding and abetting one another in the transport and trade of narcotics, weapons, and terrorist individuals[19], my argument is that there exists a firm-enough line of communication and commerce that, should they so desire, terrorist organizations would be able to purchase passage or use of a narco-sub operated by a drug cartel in Central or South America.

Methodology

There are three concepts which underlie assumptions about the collection of relevant information during my research:

Data vs. Information:

- If "data" primarily implies numbers, then many elements of Global Security Studies, including my hypothesis, do not utilize data in the Statistics sense.
- My hypothesis cannot be supported by "data", as very little of it exists. It may exist in certain Top Secret echelons, although if I had access to it I would still be unable to use it due to its sensitive nature.

[16] Michael Braun, ibid
[17] Testimony by Steven C. McCraw, ibid
[18] Michael T. McCaul, ibid
[19] McCaul, p. 5

- My hypothesis utilizes what information is available, making use of the broader category of "information", which consists of estimates, observations, and trends reported by observers

Risk vs. Uncertainty:

- Information is used to determine **risk**, a numerically measurable concept as defined by the discipline of Statistics. It is useful for the "Law of Large Numbers", but not useful in predicting "The Next Event", which is the focus of my hypothesis.

Uncertainty:

- **Uncertainty** can be said to be an unquantifiable ignorance, defined by logical, psychological, or event-driven information or the lack thereof[20]. Uncertainty is what underlies my hypothesis. The information I will be using involves estimates reported by people giving their opinions, who themselves may have reasons to either de-emphasize or exaggerate their estimate.

To summarize: information is utilized to assess **risk**, which through the application of analytics produces conclusions/**probabilities** to indicate outcomes[21]. Information is also used to establish **uncertainty**; this uncertainty informs behavioral events, trends, and **possibilities** to indicate outcomes (the topic of this paper).

Research Method

My primary method in conducting the research for this chapter is the Sequential Exploratory Method (SEM). SEM consists of two stages: qualitative information

[20] www.businessdictionary.com/dictionary/uncertainty.html
[21] www.businessdictionary.com/dictionary/risk.html

collection and analysis, followed by quantitative information analysis that compliments or provides additional detail on the results of the first phase[22].The first phase is generally given the majority of emphasis and development, with data from the second phase serving to highlight and compliment key informative points from the first. This method will help answer my research question by giving me a simple, yet concrete, framework within which to conduct my research and frame an answer to my research question, while allowing for the presentation of both qualitative and quantitative information.

This method is excellent for answering my research question as "the primary focus of this model is to initially explore a phenomenon"[23]. It is also touted for being useful in "testing elements of an emergent theory"[24]. Since this body of work can be said to be exploring two different phenomena, and proposing an "emergent theory", this method seems well-suited for the type of research and goals that I have in mind.

Also, SEM is ideal due to its design. It is simple, linear, and uncomplicated: two phases of research, the second (quantitative) done with the goal of complimenting the results synthesized from the first (qualitative). Unlikely to confuse either the researcher or the researcher's audience, this method is ideal for answering a research question that seeks to explore and expand upon current qualitative information[25].

The dual focus of this method allows for a wide variety of data sources. For the first qualitative phase, I expect to draw from academic and strategic journal articles, newspaper and magazine articles, and military/government assessments. SEM will facilitate the collection of information regarding the nature of terrorist/drug cartel

[22] John W. Creswell, "Research Design: Qualitative, Quantitative, and Mixed Methods Approaches", Sage Publications, Inc., Thousand Oaks, CA, 2009, p. 211
[23] Creswell, p. 211
[24] Ibid., p. 211
[25] Creswell, p. 212

relations, the history and capabilities of narco-submarines, and interdiction methods past, present, and future. This is particularly important since the theoretical nature of my research question places the emphasis on qualitative information, and not necessarily quantitative data.

For the quantitative segments, I will look for sources focusing on technical, measurable data: government reports detailing success rates of interdiction efforts and technological advancements in narco-sub design, the numbers of narco-subs captured or lost, or the frequency and magnitude of interactions between terrorist organizations and drug cartels. If information from the first phase does not correspond to data collected from the other phase, or if the quantitative data does not confirm and build upon the information collected in the qualitative phase, then this will make an argument against my question. However, if information and data from both phases of SEM correlate with and support one another, then this will bolster the strength and validity of my research question.

The primary weakness of this method is the quality of the first phase - qualitative data collection and analysis. Incomplete or vague data collection here will compromise the subsequent quantitative research and analysis. Utilizing this method, I must collect information from as many qualitative sources (in terms of design, objective, and background) as possible, and seek out the common themes that run through them. I must also take care not to rely overly on the qualitative phase of my research. While the quantitative data is secondary in this method, it is no less important, and thus I must make a conscious effort to give sufficient attention to the research, analysis, and implementation of data derived from this phase.

Information

Terrorist and drug cartel relationships linked

The widely-held beliefs amongst key U.S. law enforcement agencies is that terrorism and drug trafficking are "inextricably linked"[26]. Long viewed as a key source of income, successful drug trafficking by terrorist groups is exemplified in Afghanistan's provision of the majority of the world's heroin under Taliban rule[27]. This is not a decreasing trend, either, and it is estimated that up to sixty percent of terrorist organizations are involved in drug trafficking[28].

Intensifying relationships

This growth has resulted in an increased presence of international terrorist groups in Central and South America. Hamas and Hezbollah, as well as Iranian forces, have been found cooperating with members of the Revolutionary Armed Forces of Columbia (FARC), and with drug traffickers in the tri-border area of Brazil, Argentina, and Paraguay[29] [30] [31] [32]. Al-Qaeda and the Taliban, responsible for approximately 70% of the world's heroin[33], also have a proven presence in Central and South America[34]. Above all other drug-trafficking groups in Central and South America, the Mexican cartels have grown exceedingly powerful, and developed extensive international business

[26] Testimony by Steven C. McCraw, ibid.
[27] McCraw, ibid.
[28] Braun, ibid.
[29] Braun, ibid.
[30] Rand Beers and Francis X. Taylor, "Narco-Terror: The Worldwide Connection Between Drugs and Terror", testimony before the Senate Committee on the Judiciary Subcommittee on Technology, Terrorism and Government Information, 13 March 2002
[31] McCraw, ibid
[32] McCaul, p. 7-13
[33] Beers and Taylor, ibid.
[34] McCaul, p. 11-12

relationships in transporting narcotics[35], including ties with Middle Eastern terrorist organizations.

The burgeoning relationships between terrorist groups and drug cartels have expanded beyond simple drug trafficking. Cartels and other drug trafficking organizations in Central and South America have facilitated the illegal entry[36] into the United States of suspected terrorists on several occasions[37], and known or suspected terrorists have been captured on numerous occasions attempting to cross the border into the U.S. illegally with cartel assistance[38]. On another occasion in 2011, an Iranian operative attempted to hire a Mexican cartel hit-man to assassinate the Saudi Arabian ambassador to the United States[39]. Representatives of Hezbollah have been captured attempting to orchestrate large-scale arms sales to FARC members in return for narcotics[40].

Current findings from U.S. federal law enforcement agencies such as the FBI, DEA, and CIA show that these business relationships are far from waning, or staying in the current configuration of narcotics and arms exchanges – rather, this trend is "growing at light speed"[41].

[35] McCaul, p. 15-17
[36] "Mexican Cartels Smuggle Terrorists into U.S. Through Rural Texas Border Region", *Judical Watch*, 29 July 2015. Accessed 22 October 2016.
[37] McCaul, p. 5-6
[38] *Border Surge Report*, Texas Department of Public Safety, 24 February 2015. Accessed 31 October 2016.
[39] CNN Wire Staff, "Iranian Plot to Kill Saudi Ambassador Thwarted, U.S. Officials Say," *CNN*, Oct. 12 2011. Accessed August 12, 2015
[40] McCaul, p. 10
[41] Braun, ibid.

Narco-submarines: history, development, abilities

The use of submarines to transport drugs was first explored by the Medellin Cartel in Columbia[42], in response to the rising interception of "go-fast" speed boats by naval and coast-guard forces. In an attempt to continue transporting narcotics and reduce the number of interceptions by law enforcement, Columbian drug cartels poured significant resources into the development of viable transport submarines. They brought in Russian naval engineers[43] to consult on design and technical issues.

Initial narco-submarines were assembled in secluded swamps and tributaries, away from prying eyes and requiring all materials to be transported in by boat and by hand. The "subs" were actually semi-submersibles: small, with a limited range and capable of only partial submersion. Other models were capable of diving to shallow depths, but were still easily detectable via sonar and Magnetic Anomaly Detection (MAD). Yet others were "torpedoes" designed to be towed along underwater by other boats. These various designs met with limited success, as they were still vulnerable to interception and were incapable of carrying significant amounts of cargo. In addition, they proved to be extremely unreliable. However, narco-submarines have progressed through a dizzying array of designs and sophistication; from 2000-2007 submarine designs went through a relatively rapid "experimentation", "prototyping", and "standardization and design maturation" phases[44].

[42] Byron Ramirez, "Narco-Submarines: Applying Advanced Technologies to Drug Smuggling," *Small Wars Journal*, March 8, 2014. Accessed August 12, 2015
[43] ibid
[44] Byron Ramirez and Robert J. Bunker, "Narco-Submarines: Specially Fabricated Vessels Used for Drug Smuggling Purposes," for the Foreign Military Studies Office (FMSO), May 2014: 30. Accessed August 12, 2015

In 2010 a submarine was discovered in a Columbian coastal swamp that represented what many consider the pinnacle of narco-sub engineering. It was 74-feet long, with a hull of carbon fiber and Kevlar to avoid detection. The submarine was powered by both diesel and electric sources, with a range of 6800 nautical miles and a crew of four to six. It was able to run underwater for eighteen hours on electric power before needing to recharge its 289 lead-acid batteries, and the sub was capable of carrying nine tons of cocaine or other contraband[45]. Virtually silent when operating on electric motors and difficult to detect due to its hull materials, this sub represented a monumental leap forward for the cartels, especially since it was equipped with GPS, electro-optical periscope, an infrared camera, and other technical equipment to aid in navigation and operation. A similar sub was captured several months later, which confirmed that this leap in technology was not a one-off occurrence[46]. Bunker and Ramirez are quick to point out in their paper that "drug cartels today are much more organized, adaptive, and strategic"[47], and in a business where the profits reach into the billions, narco-submarines are seeing a significant amount of money, thought, and effort being put into their design and construction.

Current Interdiction Efforts

Attempts by U.S. Navy, Coast Guard, and Customs to interdict the narco-subs have met with limited success. General John F. Kelly, USMC, the commanding general

[45] Jim Popkin, "Authorities in Awe of Drug Runners' Jungle-Built, Kevlar-Coated Supersubs", *Wired Magainze*, March 29, 2011. Accessed August 12, 2015
[46] ibid
[47] Byron Ramirez and Robert J. Bunker, "Narco-Submarines: Specially Fabricated Vessels Used for Drug Smuggling Purposes," for the Foreign Military Studies Office (FMSO), May 2014: 9. Accessed August 12, 2015

of SOUTHCOM, testified that "last year, we had to cancel more than 200 very effective engagement activities", and due to a shrinking budget SOUTHCOM is unable to pursue 74 percent of suspected maritime drug trafficking[48]. When one considers that the 74-percent statistic is only involving "suspected" trafficking (i.e. observed trafficking) not being interdicted and does not factor in the *unobserved* trafficking that is taking place, it is safe to say that SOUTHCOM is missing far more than 74 percent of maritime drug trafficking operations.

The U.S. Coast Guard is struggling as well: despite capturing 129 tons of narcotics in 2011, they suspect they have missed another 500 tons, and Rear Adm. Charles D. Michel told the *New York Times* that "[his] staff watches multi-ton loads go by"[49]. 129 tons captured out of a suspected 629 tons – this comes out to an interdiction rate of 1 sub interdicted for every 6 that go by. Far lower than SOUTHCOM's purported 1 out of 4, and perhaps a more accurate overall reflection of the interdiction rate. There are no indicators that any part of this equation will change in the near future, with operating budgets for SOUTHCOM and the Coast Guard are being reduced and the cartels dumping more and more money, time, and effort into narco-sub R&D.

Strengths and weaknesses

The information presented in this paper on terrorist/cartel relationships and narco-submarines comes from a wide array of sources, including academic and strategic journal articles, official government testimonies, newspaper and magazine articles, and

[48] Claudette Roulo, "Budget Shortfalls Reversing SOUTHCOM Gains, Commander Says", *American Forces Press Service*, March 13, 2014. Accessed August 12, 2015
[49] Adam Clark Estes, "The Feds Can't Catch the Cartels' Cocaine-Filled Submarines", *The Wire*, September 9, 2012. Accessed August 12, 2015

government-commissioned studies. The sheer diversity of these sources is a major strength – exploring a concept and developing a theory from multiple perspectives allows for the creation of a thorough, well-rounded argument. While the less-academic nature of the newspaper and magazine sources is a weakness, the validity of the other sources allows for thorough fact-checking and validation.

Analysis

Considering the information collected on terrorist organizations, drug cartels, and narco-submarines, there are a number of conclusions I feel can be drawn from the results of the research presented.

As previously discussed in the Information section, research shows that there are relationships and channels of communication between international terrorist organizations (particularly those of Middle Eastern origin who seek to harm the United States and her interests) and drug cartels and traffickers operating in Central and South America. Furthermore, these relationships have developed well beyond simple transactions and transportation of narcotics and money. Exchanges of arms, military advice and training, and smuggling of individuals into the U.S. via the border have already occurred.

As these relationships develop and mature, as many U.S. law enforcement agencies agree, it is safe to assume as with the past growth of the occurrence of the *method* (submarines) the madness (these types of more dangerous transactions) will only increase in scale and occurrence. Considering the majority ownership of the world's supply of heroin by Al-Qaeda and the Taliban, the military acumen and hardware

possessed by Hezbollah, Hamas, and Iranian operatives, and the desire of Central and South American drug cartels to expand their respective spheres of influence and power within those spheres, coupled with the fact that the first group wants to attack U.S. interests at home and abroad and the latter group possesses the ability, via narco-sub, to infiltrate with great rates of success U.S. coastal protective measures, I would argue the risk is high that groundwork has been laid for an international terrorist organization to acquire passage on, or control of, a narco-submarine.

Regarding narco-subs, there are a number of conclusions that can be drawn which, in turn, address this paper's research question. First, as covered in the Information section illustrates, narco-submarines have experienced dramatic improvements in design, effectiveness, and capability in a relatively short amount of time. Initially only semi-submersible, or unmanned and towed submerged behind a larger craft, at present narco-submarines are witnessing tremendous growth in both design and numbers. Now capable of running fully-submerged over vast distances, able to transport cargo in quantities up to 10 tons, and guided by sophisticated re-purposed GPS and sonar equipment, narco-subs are capable of traversing great distances with excellent accuracy – gone are the days of pilots having to hug the shore or surface repeatedly to check their bearings. Furthermore, cartels are designing and coating narco-subs with materials to aid in reducing their signatures on both sonar and MAD (Magnetic Anomaly Detection), stealth improvements which make them even more difficult to detect. The subs are also cheap for the cartels to produce, costing only a couple million dollars each – cheap enough that the cartel crews often scuttle them at the end of their journeys, instead of attempting to return them. The shrinking price tag also means that smaller cartels and less formal operations will be able

to construct and operate their own drug subs. This will result in more drug subs in the water, and complicate interdiction efforts.

Second, findings in the Information section show that these technological advancements have resulted in U.S. interdiction efforts facing severe hurdles to curtail narco-sub traffic. Effectively invisible once launched, U.S. Navy, Coast Guard, and Customs forces are hard-pressed to detect and interdict these vessels. Attempts to capture these vessels before launch have shown some success, but not enough to stem the tide of narco-subs, approximately 75% of which are estimated to be slipping through U.S. coastal defensive measures. This is compounded by the fact that recent budget cuts and sequestration will negatively impact U.S. interdiction efforts, and the likelihood of a narco-sub being captured in transit will likely approach the old figures of just one in ten being caught. A decrease in narco-sub interdiction rates has potentially grave implications, in that such an astounding success rate will likely encourage cartels to continue to increase the number of narco-submarines being built and used. The increased number of drug subs will, in turn, feed a vicious cycle of increasing the stress on whatever interdiction forces are present, which means fewer narco-subs will be interdicted, which will lead to more being built – rinse, wash, repeat.

Third, considering the advances made by the cartels in narco-sub construction and operation, and the difficulties faced by U.S. forces in stopping them, it would be hard to find a more effective means of transporting cargo (including terrorists and their weapons) into the United States illicitly. Much effort has been put into making our land borders impermeable – those with terrorist connections will find themselves hard-pressed to make it through airport customs unmolested, and even crossing on foot across the U.S.-Mexico

border is not as easy as it once was. However, as shown in the Information section, a narco-sub is just as capable of carrying ten tons of terrorist operatives and their equipment (including small arms and explosives) as it is cocaine or marijuana, and at worst sees only a 25% chance of being interdicted before reaching U.S. coastal waters and offloading its cargo. The cheap cost of narco-subs and their increasing numbers would also allow a terrorist group to spread operatives and equipment out across several vessels; to do so would almost guarantee a majority, if not all, of a terrorist force reaching U.S. shores undetected. Should a terrorist group seek to infiltrate operatives and equipment into the United States, they will likely be drawn to the low-risk factors of discovery of purchasing passage on, or ownership of, a narco-submarine.

Counterfactuals

For all practical purposes, counterfactuals do not exist for this topic. There is no noteworthy argument that the likelihood of terrorist infiltration into the United States does not exist, that narco-submarines do not pose a distinct threat, or that the sophistication of the smugglers and their submarine capability is not increasing. One could argue that a counterfactual can be inferred by the lack of action taken by the government and law enforcement agencies; likewise the reduced monetary and personnel resources allotted for interdiction efforts. Another counterfactual might be the relative lack of energy spent on researching and assessing the threat posed by narco-submarines. These are, at best, indirect counterfactuals and do little to directly address my hypothesis. Failure to appreciate the severity of a threat does not diminish the likelihood or magnitude of that threat. Furthermore, the human tendency to ignore threats until negative outcomes have already occurred is a well-known short-coming of the species.

One of the consequences of developing what may be considered an emergent theory is that, in addition to finding scant source material, one cannot address the counter-arguments made by those who came before, and therefore must wait and allow one's own theory to be assessed and critiqued.

Conclusion

The purpose of this chapter was to determine an answer to the following question: *Considering the developing relationships between international terrorist organizations seeking to attack U.S. interests and drug cartels in Central and South America, do narco-submarines pose a significant threat to U.S. domestic security?*

As of the time of writing, there are no *known* attempts of a terrorist organization attempting to purchase transit on or ownership of a narco-sub. However, the past is not a predictor of the future. The purpose of this chapter is to determine not whether event has occurred, but the likelihood of an event occurring, and to assess the severity of the threat posed by narco-submarines to U.S. domestic security.

Taking into account the robust and still-developing relationships between terrorist organizations such as Al-Qaeda, the Taliban, Hamas, and Hezbollah (and through them Iran), and confronting the astounding success that narco-submarines see in transiting undetected into U.S. waters, I would argue that narco-submarines pose a distinct, serious threat to U.S national security. While themselves unarmed, their ability to transfer large amounts of men and materiel illicitly into the United States makes these drug subs a significant security threat that bares further investigation and effort to interdict. The

narco-subs only need to be right once in order to successfully infiltrate the United States – every sub missed has the potential to cause severe and long-lasting damage when one considers a cargo of armed terrorists instead of cocaine.

According to the National Ocean Service, the U.S. coastline extends over 95,471 miles[50]. Considering that narco-subs are known to be operating in both the Pacific and Atlantic Oceans, as well as the Gulf of Mexico, the overwhelming majority of that coastline falls within the operating range of those narco-submarines. So what can be done to try and mitigate this threat?

Threat mitigation

Firstly, more research must be done. Narco-submarines have received precious-little attention academically or militarily; several of the sources used in this chapter came from one or both of the same two authors, Byron Ramirez and Robert Bunker. To paraphrase Sun Tzu: "if you know yourself, and you know your enemy, you will never suffer a defeat". Sun Tzu would be disappointed in current U.S. efforts to understand and learn about narco-submarines. In regards to narco-subs specifically, we currently know much about ourselves and very little about the enemy. A clear indicator of this lack of intelligence is the fact that only rough estimates on the number of subs making the passage into U.S. waters are available, and that no sort of firm count has been attempted. Likewise, a better understanding of the nature and scope of relationships between terrorist organizations and cartels is required; absent this, effective means of countering this working relationship will be difficult to design and implement. In order to effectively combat this threat, better intelligence and greater research is needed. Only once a clearer

[50] NOAA website, http://oceanservice.noaa.gov/facts/shorelength.html

picture is established, and better intelligence collected, can effective steps be taken to counter the threat posed by drug subs and their acquisition by terrorist groups.

Secondly, efforts must be intensified where interdiction efforts have proven effective; in particular, attempting to interdict the subs prior to launch. U.S. forces operating in conjunction with local law enforcement have seen success in locating and raiding fabrication sites in Central and South America – further manpower and funding should be steered towards facilitating and increasing the scope of these operations. In order to dissuade the cartels from building and operating narco-submarines, U.S. and local law enforcement agencies must make narco-subs either cost- or risk-inefficient. While making the building process too costly and interdicting the majority of subs at sea are proving difficult strategies to implement, what can be done is to make the construction process too difficult to undertake. If the cartels see more and more construction sites being raided before the subs are completed, and more subs are seized than are launched, then the cartels will be pressured to seek out a new method of smuggling narcotics. If the cartels are less-inclined to build narco-subs, this in turn will lessen the likelihood of one being acquired by a terrorist organization seeking a means to infiltrating the United States undetected. All of this can be achieved by increasing the scale and scope of land-based interdiction operations. Furthermore, this might prove to be more cost-efficient than operating at-sea interdiction elements, which in today's era of sequestration and diminishing budgets cannot be overlooked.

Finally, it is necessary to implement a plan closer to home in order to interdict subs that do manage to launch. Particularly in the region of Southern Command (SOUTHCOM), U.S. Navy and Coast Guard operations have produced results, albeit

modest ones[51]. Despite budget cuts across government agencies, curtailing these operations only harms interdiction efforts. At best, a cheaper alternative must be sought if current successful tactics cannot be bolstered. If constantly patrolling vessels and aircraft are too expensive to maintain, perhaps implementing some sort of passive listening array in key areas to serve as an early-warning tripwire could prove effective. During the Cold War, the Sound Surveillance System (SOSUS) positioned to cover the Greenland-Iceland-United Kingdom (GUIK) gap proved effective at detecting Soviet submarines, particularly when paired with toward sonar systems[52]. These passive measures could decrease operating costs, while ensuring that approaching narco-subs were still detected in time for U.S. Navy or Coast Guard forces to interdict them.

Another option lies in the technology of surface and underwater drones that the U.S. Navy is developing. Far smaller and cheaper to operate than a Coast Guard cutter or Navy destroyer, as this technology is developed and put into service, perhaps an application can be developed to use these drones in counter-sub operations in the Gulf of Mexico and other potential narco-sub transit areas. In conjunction with a SOSUS-like system, this networked system could provide the Coast Guard, Border Patrol, and U.S. Navy with accurate detection and targeting capabilities, and would subsequently improve interdiction rates.

Ultimately, a solution to the threat posed by narco-submarines is beyond the scope of this chapter. My purpose in writing is to highlight the threat posed by these vessels, and the definitive potential for terrorist groups to access and utilize one of these craft to assist in conducting a terrorist attack on the United States. Ideally, wiser and

[51] Jim Popkin, "The High Seas", *Slate.com*, 8 Oct. 2013
[52] *"SOSUS The "Secret Weapon" of Undersea Surveillance". Undersea Warfare, Vol. 7 no. 2 (US Navy). Winter 2005*

more powerful heads than mine will agree, and seek a means of effectively countering this threat.

Chapter 2: The Stinging Swarm

The Threat the United States Faces from Terrorists and Swarm Tactics

Introduction

"Float like a butterfly, sting like a bee!"[53]

Widely known amongst boxing and sports fans, Muhammed Ali's titular quote has applications outside the boxing ring. For example, such tactics were used by Afghan and Chechen fighters against the Soviets and Russians in the 1980s and 1990s, insurgents from Afghanistan and Iraq against the United States in the last two decades, and numerous terrorist attacks during the same period. In order to survive against a more numerous, better-armed foe, a fighter must remain light and agile, striking quickly and withdrawing before a punishing retaliatory blow can land.

Since the attacks on 9/11, the United States has made concentrated efforts to protect itself against further terrorist attacks. However, events like the anthrax letters, the Boston Marathon bombing, the Fort Hood massacre, the Chattanooga recruiting office attack and the Orlando nightclub shootings show that the U.S. in still extremely vulnerable. These attacks were textbook examples of attempted Weapons of Mass Destruction (WMD)- (anthrax letters) or lone wolf-styled (Boston, Fort Hood, Chattanooga, Orlando) attacks. Based on proven effectiveness of recent examples I would argue that there exists an even greater threat than WMD or lone-wolf attacks to U.S. homeland security: a small-group, "swarm"-based terror attack.

In this chapter, I examine four separate cases: an asymmetrical conflict, a U.S. military exercise, and two terrorist attacks. These cases highlight the threat posed by and

[53] The late Muhammed Ali, in his press interview before fighting Sonny Liston in 1964. Ali would go on to win the fight, despite being the underdog. "Muhammad Ali's Most Memorable Quotes", ABC News, 4 June 2016. Retrieved 5 June 2016.

the effectiveness of a "swarm"-styled terrorist attack. WMD- and lone wolf-based attacks do pose a threat to domestic security in the United States; however, I intend to show that the greatest threat, capable of producing the more damaging result inside U.S. borders and easier to pull off, does not come from a suitcase nuke, dirty bomb, or from a lone fanatic, but from a small, coordinated group of motivated individuals: the swarm.

.

"Swarming"

Swarming is a military tactic to overwhelm a target through multiple, simultaneous attacks by small, loosely-coordinated groups. In other words, while "swarming is seemingly amorphous, … it is a deliberately structured, coordinated, strategic way to strike from all directions, by means of a sustainable pulsing of force and/or fire, close-in as well as from stand-off positions."[54] From this broad definition, scholars have focused more closely on swarming as a military tactic. For example, one study defined swarming as occurring "when several units conduct a convergent attack on a target from multiple axes…. Attacks can either be long range fires or close range fire and hit-and-run attacks."[55] The use of swarming, according to this definition, can be found in many historic conflicts including during the Chechen Wars, by the Mongols, by the Russians during Napoleon's retreat, by the Finns during the Winter War against the Russians, and by the Afghans against the Soviets in the 1980s.[56] In fact, "against a conventional adversary…the swarming of directed fires should have devastating

[54] John Arquilla and David Ronfeldt. *Swarming & the Future of Conflict*. Santa Monica, CA. RAND, 2000, p. vii. Retrieved 06.18.2016.
[55] Sean J. A. Edwards. *Swarming and the Future of Warfare*. Santa Monica, CA. RAND, p. xvii. Retrieved 06.18.2016.
[56] William D. Shannon. *Swarm Tactics and the Doctrinal Void: Lessons From the Chechen Wars*. Naval Postgraduate School, 2008, p. 4-9. Retrieved 06.18.2016.

effects."[57] This paper intends to highlight the lethality, and emphasize the threat posed to the United States by a domestic terrorist swarm attack.

Literature Review

The threat of WMD-oriented terror attacks

Some domestic security professionals consider it unlikely that a terrorist group will use a WMD against the United States for the foreseeable future. In fact, a 2012 study by the Nuclear Threat Initiative (NTI) examined the possibility of a WMD attack and concluded that "in the past decade, there is no evidence that jihadist extremists in the United States have acquired or attempted to acquire material to construct CBRN weapons."[58] Another study points out that more lives were claimed in a conventional bombing (Oklahoma City) than in a WMD attack (Tokyo subway Sarin gas attacks), and goes on to emphasize that WMDs also pose a serious threat to the terrorist group trying to construct them.[59]

However, a (contradictory) study published by NTI illustrates how it is possible to fabricate and deploy bio-weapons with only a college-level understanding of microbiology and basic lab equipment,[60] and thus a WMD terrorist attack should not be considered outside the realm of possibility. A report published by Harvard's Belfer Center found that "despite the non-occurrence of a WMD attack in the U.S. up until now, it would be foolish to discount the possibility that such an event will occur in the

[57] Arquilla and Ronfeldt, p. 5
[58] Peter Bergen and Jennifer Rowland, from the New America Foundation, in an article posted on CNN's website on 08.08.2012. Quote retrieved from the Nuclear Threat Initiative website on 06.18.2016.
[59] Steve Bowman. *Weapons of Mass Destruction: The Terrorist Threat*. CRS Report for Congress, published 03.07.2002. Retrieved 06.18.2016.
[60] Rachel Oswold. "Despite WMD Fears, Terrorist Still Focused on Conventional Attacks". Nuclear Threat Initiative website, 04.17.2013. Retrieved 06.18.2016.

future."[61] This back-and-forth appears endemic to the debate, with no one able to present concrete evidence of the WMD capabilities of terrorist organizations.

Ultimately, there seems to be little consensus in the unclassified literature available to either support or deny the likelihood of a pending, successful WMD terror attack in the United States by terrorist organizations – purportedly, they lack the necessary infrastructure and technical requirements[62], yet others claim that the technology and ability is within their reach. Given that WMDs are a low-probability, maximum-impact event, trying to prevent one can theoretically take the entire economic output of a country with little discernable improvement in actual prevention.

The threat of lone wolf-oriented terror attacks

According to the National Security Critical Issue Task Force (NSCITF), there is no official U.S. government definition of "lone wolf attack."[63] The NSCITF defines a lone-wolf attack as:

> the deliberate creation and exploitation of fear through violence or threat of violence committed by a single actor who pursues political change linked to a formulated ideology, whether his own or that of a larger organization, and who does not receive orders, direction, or material support from outside sources.[64]

Examples of recent lone wolf attacks in the United States include shootings in Chattanooga, TN[65]; Fort Hood, TX[66]; and Orlando, FL[67]; and the attempted bombing in

[61] Rolf Mowatt-Larssen. "Al Qaeda Weapons of Mass Destruction Threat: Hype or Reality?". Belfer Center, Harvard. Published January 2010, retrieved 06.18.2016.
[62] Gavin Cameron, "WMD Terrorism in the United States: The Threat and Possible Countermeasures". Published in *The Nonproliferation Review*, Spring 2000, p. 169. Retrieved 06.19.2016.
[63] Security Studies Program, *Report: Lone Wolf Terrorism*. National Security Critical Issue Task Force; Georgetown University. 06.27.2015, p. 9. Retrieved 06.19.2016.
[64] Ibid, p. 9
[65] Catherine Shoichet and Gary Tuchman, "Chattanooga shooting: 4 Marines killed, a dead suspect and questions of motive", CNN, 17 July 2015. Accessed 10 August 2016.

Times Square, New York City. Internationally, the 2011 attacks in Norway carried out by Anders Brevik and the 2015 Hyper Cacher kosher market attack in France are considered to be textbook examples of a lone-wolf attack. Profiling and detecting individuals planning lone-wolf attacks can be exceedingly difficult.[68] In fact, "there is no standard profile for the American lone wolf terrorist."[69] This difficulty in creating a profile means that it can be very hard to detect and interdict a lone-wolf terrorist before he or she commits their attack. Despite the nebulous nature of both the definition of the attack and profiling of the executors, as a strategy lone-wolf attacks provide an excellent means for Islamic terrorists to "terrorize the West…asymmetrically."[70]

Despite several high-profile incidents, lone-wolf attacks by terrorists in the United States are not on the rise,[71] and are not one of the most significant threats to public safety.[72] In fact, between 2009 and 2012, cases of lone wolf terrorist attacks in the U.S. declined overall, although they did see a slight increase from 2012 to 2014[73]. While the frequency of lone-wolf attacks seems to be in doubt, the common consensus is that these attacks typically do not kill many people.[74] One of the few exceptions to this is the attack carried out by Anders Brevik, who killed 77 people.[75] Lone-wolf attacks might be effective in certain settings, but they are not generally seen as a viable tactic for Islamist

---

[66] "Gunman kills 12, wounds 31 at Fort Hood", NBC News and msnbc.com, 5 November 2009. Retrieved 10 August 2016.
[67] Ralph Ellis, Ashley Fantz, Faith Karimi and Eliott C. McLaughlin, "Orlando shooting: 49 killed, shooter pledged ISIS allegiance", CNN, 13 June 2016. Retrieved 10 August 2016.
[68] Ibid, p. 16
[69] Mark S. Hamm and Ramon Spaaij, *Lone Wolf Terrorism in America: Using Knowledge of Radicalization Pathways to Forge Prevention Strategies*. Indiana State University, February 2015, p. 6. Retrieved 06.19.2016.
[70] Naina Bajekal, "The Rise of the Lone Wolf Terrorist." Time Magazine, 10.23.2014. Retrieved 06.19.2016.
[71] Hamm and Spaaij, p. 2.
[72] Security Studies program, p. 15-16
[73] Ibid, p. 16
[74] Bajekal, "The Rise of the Lone Wolf Terrorist".
[75] Ibid

terrorist groups to create mass-casualty events. Instead, the main strength of lone-wolf attacks seems to lie in their ability to create a major psychological impact with relatively little actual violence to the general population or to physical infrastructure.

The threat of swarm-oriented terror attacks

Literature on this subject covered a wide range of arenas, from academia to government, books to news articles. There is markedly little dissent on the continued threat posed by a swarm-style terrorist attack.[76] In analyzing the case studies presented in this chapter, I attempt to draw on as wide a range of material as possible.

One of my prime sources, written for a government think tank, has served as a cornerstone for numerous works concerning the use of swarm tactics in a military or terrorist setting, including two of the case studies in this paper. Written to study the benefits, costs, and risks of engaging in swarm tactics, [77] the authors also examine the role of technology in enabling swarming as a tactic.[78] They argue that swarming is the "fourth form" of warfare, the next step following the previous three: the melee, massing, and maneuver warfare.[79] Pertaining to terrorist attacks, this source emphasizes several characteristics of swarming: "autonomous or semi-autonomous units engaging in convergent assault on a common target" and "many small, dispersed, 'internetted' maneuver units."[80] This source also highlights the fact that "when swarming works, it

[76] Cerwyn Williams, "The Threat from Swarm Attacks: Case Studies from the North Caucasus", published in the *CTC Sentinel*, May 2012, Vol. 5, Issue 5, p. 25. Retrieved 06.19.2016.
[77] Arquilla and Ronfeldt, p. vii
[78] Ibid., p. 7
[79] Ibid, p. 10-20
[80] Ibid, p. 21

[works] very well, [and often acts] as a force multiplier."[81] It is also quick to warn that the U.S. will "increasingly face swarming by adversaries," from nation-states as well as terrorist and transnational criminal organizations.[82]

Another think-tank report observes that "insurgents are employing swarming as a form of asymmetric warfare against superior conventional armies from the mountains of Afghanistan to the cities of Iraq."[83] The report also points to one the most effective aspects of swarm tactics that is that "swarms must be offensive at the tactical level."[84] This is true both in military and terrorist applications of swarm tactics, and is seen in both case studies I present involving terrorist attacks (Mumbai in 2008 and Paris in 2015). The report also concludes that "suicide swarms" (swarms where the members are willing to fight to the death) "also seek devastating results in a short amount of time"[85].

The rest of my sources range from think-tanks such as The Washington Institute, articles published in *Foreign Policy* and *The New York Times* and other news sources, government-sponsored studies, and academic and journalistic essays. Overwhelming, these sources discuss the effectiveness of swarming, particularly when used against larger opponents. There is very little literature that I have found that argues *against* the effectiveness of swarming as a tactic. Whether the lack of arguments against swarming's effectiveness is due to lack of effort on the part of academia or the fact that swarming is undeniably effective, I am not certain. I feel that this lack of counter-arguments strengthens my argument – whereas the literature regarding WMD and lone-wolf attacks is at best ambiguous regarding the efficacy, impact and likelihood of those tactics, the

[81] Ibid, p. 40
[82] Ibid, p. 43
[83] Edwards, p. xvii
[84] Ibid, p. 101
[85] Ibid, p. 105

opinions surrounding the effectiveness of swarming as a tactic are unanimous in their affirmation.

While there is an abundance of literature regarding the effectiveness of swarming as a tactic, the majority of sources focus on its applicability in a military setting. Swarming as an effective terrorist tactic has received relatively little attention, which is an issue I hope to address in this paper. The case studies I present, in conjunction with the sources I have found on swarming, will demonstrate why the United States should fear a swarm-style terrorist attack within its borders.

Methodology

The overall purpose of this paper is to illustrate the effectiveness of swarming when compared to WMD and lone-wolf tactics, by examining cases of swarm-tactic implementation in a variety of real-world scenarios. This paper utilizes four case studies to examine recent historical events in which swarming was used as a decisive tactic. These are:

- the First Chechen War, specifically the Battles of Grozny in the mid-1990s, in which Chechen separatists repelled a larger, better-equipped Russian army and utilized swarming tactics to inflict catastrophic casualties;
- the 2002 U.S. military exercise Millennium Challenge, where a simulated U.S. carrier group was sunk in the opening minutes of the exercise by a wily Marine general employing swarm tactics on a tactical and strategic level;
- the 2008 terror attack in Mumbai, when ten members of Lashkar-e-Taiba staged a commando-style sea raid and used swarm tactics against targets in the bustling

Indian city of Mumbai, instigating an assault that would last several days and require military intervention to end;

- the 2015 terror attack in Paris, where seven supporters of Islamic State of Iraq and the Levant (ISIL) staged a swarm attack against cafes, restaurants, a sports stadium, and a theatre in the middle Paris that, despite lasting only a few hours, caused a similar number of casualties to the attack in Mumbai several years prior.

Case studies as a methodology are advantageous since they allow for the researcher to conduct comparisons on a variety of levels. I can compare not only between the actual outcomes of events and theories proposed by existing literature, but also examine the effectiveness of swarming on a case-by-case basis. This multi-faceted examination allows for the construction of a thorough examination of the effectiveness of swarming from both theoretical and real-world applications.

The literature on terrorist attacks provides little in the way of methodology comparison – at no point was I able to find a study which broke down how various tactics used by terrorists to conduct an attack compared against one another. The literature on WMD and lone-wolf attacks by terrorists is extensive, discussing both past events and future implications, but I was unable to find a direct "X tactic has been proven to kill more people than Y tactic" discussion anywhere. This paper will hopefully provide that missing component, examining swarming across a number of case studies and then comparing the real-world results against those from WMD and lone-wolf terrorist attacks.

All four case studies involve the use of swarming by a numerically- and technologically-inferior participants. While the first two case studies focus on military actions (Battles of Grozny and Millennium Challenge 2002), the latter two case studies

examine swarming tactics in recent terrorist attacks (Mumbai in 2008 and Paris in 2015). As my thesis posits that a swarm-style terrorist attack poses a greater threat to U.S. domestic security than a WMD or lone-wolf attack, these final two cases studies will prove to be especially important in validating my argument.

The main downside to case studies as a methodology is favoritism – picking cases that only highlight the specific points desired by the author. To counter this, cases have been chosen that examine the use of swarming in military conflicts and where swarming was used to conduct terrorist attacks. In doing so, the versatility and effectiveness of swarming in both military and terrorist applications is demonstrated.

Case Studies

Case Study #1 – The First Chechen War: The First and Second Battles of Grozny

Background

With the collapse of the Soviet Union, former satellite countries declared their independence from the former superpower. One of these was the Chechen Republic of Ichkeria (Chechnya). In the years following its establishment, thousands upon thousands of non-Chechen citizens fled the country, claiming violent discrimination and persecution.[86] This led to a civil war within Chechnya. The Russians initially provided covert support to pro-Russian Chechen groups, but when diplomacy failed, the decision was made to send Russian military forces into Chechnya to quell the conflict.[87]

[86] Sebastian Smith, "Allah's Mountains: The Battle For Chechnya", Nov. 2005, Taurus Park Publishing; Akron, OH. Kindle Edition

[87] William D. Shannon, "Swarm Tactics and the Doctrinal Void: Lessons From The Chechen Wars", June 2008, Naval Postgraduate School, p. 35. Accessed 07.01.2016.

Recognizing their disadvantages, the majority of Chechen forces withdrew to the capital city of Grozny and prepared for battle.[88]

The Battles for Grozny

While both Chechen and Russian forces had similar small- and medium-arms and equipment, the Chechens faced a decided disadvantage in air power, armor, and heavy weapons. To maximize their effectiveness, Chechen fire-teams consisting of three to four men would operate in loose conjunction, attacking Russian armor and infantry columns from a variety of directions and angles (basement, middle stories, rooftops) at the same time.[89] These simultaneous, multi-pronged attacks allowed the Chechens to inflict massive casualties upon the Russian forces, who found that "against the swarm, their tactics were still mostly ineffective."[90] Even Russia's special operations troops were challenged. By the time the second battle of Grozny commenced, Russian military forces were almost helpless before the swarming Chechen fighters.[91]

The use of swarming tactics by Chechen forces permitted them to deal Russia some of its worst military losses since World War II. For example, in one instance, a brigade consisting of over 1000 men and approximately 142 armored vehicles was completely wiped out in only sixty hours.[92] The Chechens would claim to have destroyed over 400 Russian tanks and Armored Personnel Carriers (APCs) by the end of the New Year's Eve battle.[93] Swarming also allowed small Chechen fire teams to bog down much

[88] Shannon, p. 36
[89] Carlotta Gall and Thomas de Waal, *Calamity In The Caucasus*, NYU Press, New York City, Kindle edition
[90] Shannon, p. 40
[91] Gall and de Waal, Kindle edition
[92] Ibid
[93] Smith, Kindle Edition

larger Russian forces within Grozny, while other Chechen units simultaneously attacked Russian logistics and support forces outside the city, which severely impacted Russian morale (not to mention logistics for the troops in the city).[94]

The First Chechen War, during which the First and Second Battles of Grozny were waged, ended with Chechen forces still in control of Grozny, despite an overwhelming numerical and materiel advantage held by the Russians. While many reasons have been offered as to why the Russians lost (poor training, low morale, conflicting chains of command), a major cause of the Russian loss was the use of swarming tactics by Chechen forces.[95]

Case Study #2 – Millennium Challenge 2002 (MC02)

Background

Millennium Challenge 2002 (MC02) was a joint military exercise conducted by the United States military that, at the time, was the largest war-game ever conducted by the U.S.[96] It involved over 13,500 soldiers, sailors, airmen, and Marines, and aimed to "assess the ability of a Joint Task Force (JTF) to execute the Rapid Decisive Operations (RDO) war-fighting concept."[97] In the exercise, the U.S. task force (the Blue team) would face off against an unspecified Middle-East-based country (the Red team, purported to be Iran).[98]

---

[94] Shannon, p. 40-41
[95] Ibid, p. 41
[96] *U.S. Joint Forces Command Millennium Challenge 2002: Experiment Report*, USJFCOM, 4 Aug. 2002, p. iii. Retrieved 10 July 2016.
[97] Ibid, p. v
[98] Brett Davis, "Learning Curve: Iranian Asymmetrical Warfare and Millennium Challenge 2002", Center for International Maritime Security (CIMSEC), posted 14 Aug. 2014. Retrieved 9 July 2016.

While the U.S. force involved a carrier battle group, augmented with a Marine amphibious detachment, the Red team was severely behind the curve in regards to technology, capabilities, and armament.[99] The exercise was designed to be a free-play exercise; however, either team was capable of winning.[100]

MC02

The exercise started when the Blue Team issued the Red Team an ultimatum communication demanding their surrender within 24 hours; Lieutenant General Paul Van Riper, commander of the Red Team, decided to exploit Blue Team's false perception that they had "a monopoly on perception."[101] In order to foil Blue Team's advanced signal-gathering and communications-jamming equipment, Van Riper had dispersed his forces and utilized motorcycle messengers, light signals, and messages broadcast from mosque minarets to signal to his disparate forces. Able to communicate without interference, once the U.S. carrier group came into range LtGen Van Riper initiated his attack.

Aware of U.S. military defensive capabilities and his own inability to match them conventionally, LtGen Van Riper implemented a sweeping swarm-style attack against the U.S. carrier group.

> "Riper's forces unleashed a barrage of missiles from ground-based launchers, commercial ships, and planes flying low and without radio communications to reduce their radar signature. Simultaneously, swarms of speedboats loaded with explosives launched kamikaze attacks."[102]

[99] Micah Zenko, "Millenium Challenge: The Real Story of a Corrupted Military Exercise and its Legacy", submitted to War on the Rocks, posted 5 Nov. 2015. Retrieved 10 July 2016.
[100] PBS interview with LtGen Paul Van Riper, USMC (ret.), commander of the Red Team during MC02. "The Immutable Nature of War", NOVA interview, PBS, posted 4 May 2004. Retrieved 10 July 2016.
[101] Ibid.
[102] Zenko, for War on the Rocks

The carrier battle group found itself completely overwhelmed: 19 U.S. ships were sunk, including a carrier, several cruisers, and five amphibious ships.[103] In an interview afterwards, LtGen Van Riper admitted after the exercise that "the whole thing was over in five, maybe ten minutes."[104] Despite being drastically outnumbered and lacking in both resources and technology, in the opening move of the exercise LtGen Van Riper's swarm attack had pre-empted a U.S. strike, decimated one of the most powerful naval formations in existence, and inflicted thousands of casualties. When asked about his actions after the exercise, LtGen Van Riper stated "if it was going to be a fight, I was going to get in the first blow."[105] The use of swarm tactics allowed for the first blow to be a decisive one that shocked everyone involved in the exercise.[106]

Case Study #3: 2008 Terrorist Attack in Mumbai

Background

In November 2008, ten terrorists conducted an attack in the city of Mumbai, India that lasted nearly three days and "set a gold standard for how a small group of suicidal fanatics can paralyze a major city, attract global attention, and terrorize a continent."[107] In the aftermath of the attack, concrete ties linking the ten terrorists to Lashkar-e-Taiba (LeT) in Pakistan surfaced.[108] Prior to the

[103] Micah Zenko, *Red Team: How to Succeed by Thinking Like the Enemy*, Basic Books, 3 November 2015, Kindle edition
[104] Zenko, *Red Team*, Kindle edition
[105] PBS interview
[106] Zenko, for War on the Rocks
[107] Bruce Riedel, "Modeled on Mumbai? Why the 2008 India attack is the best way to understand Paris", The Brookings Institute, posted 14 Nov. 2015. Retrieved 10 July 2016.
[108] *Mumbai Attack Analysis*, N.Y.P.D. Intelligence Division, 4 Dec. 2008, p. 5. Retrieved 10 July 2016.

attack, an initial group of approximately twenty-five terrorist operatives received training (including weapons, tactics, assault, and amphibious raiding[109]) at an LeT camp in Pakistan.[110] Three senior LeT operatives took command of the seven trainees who passed, and the group divided into five pairs, with each pair receiving a different target around South Mumbai's waterfront.[111] Site reconnaissance by spies and Google Earth presented the terrorists with a detailed, in-depth assessment of the area, which allowed the terrorists to achieve familiarization with the environment well before the attack. [112]

60 Hours

In order to infiltrate the city of Mumbai, the attackers hijacked an Indian fishing boat, from which they launched two rubber dinghies to reach the shoreline along the Mumbai waterfront.[113] Once ashore, the group divided into their pre-determined teams and made their way to their initial targets. These included: the Chhatrapati Shivaji Terminus (Victoria Station) Rail Station, the Leopold Café and Taj Mahal Hotel, the Oberoi Trident Hotel, and the Narimann (Chabad) House (a Jewish community center). [114] The attackers also placed numerous time-delayed bombs in cabs and at target locations prior to and during the attack in order to sow further confusion.

---

[109] David Kilcullen, *Out of the Mountains: The Coming Age of the Urban Guerrilla*, Oxford University Press, 2013, Kindle edition
[110] NYPD report, p. 9
[111] David Kilcullen, *Out of the Mountains*
[112] Ibid
[113] NYPD report, p. 9
[114] Ibid, p. 17

Once the attack began, the terrorists exploited the initial chaos and moved rapidly from target to target, leaving first responders behind.[115] The terrorists struck several locations at once, and in conjunction with their mobility prevented first responders from developing an accurate picture of the situation.[116] This overwhelmed Indian law enforcement, which was not equipped nor trained to handle a swarm-style attack of this magnitude. The attackers were thus able to make their way towards their ultimate objectives (the Taj Mahal Hotel and the Narimann (Chabad) House) and gain entrance with relative ease. Only once they were ensconced in these redoubts, and the attack shifted from an urban swarm attack to an urban siege, were Indian law enforcement and military forces able to commence operations to bring the attack to a close. By the time law enforcement ended the siege and brought the attacks to a close, 166 people were dead, and over 600 wounded in the attack.

Case Study #4: 2015 Terrorist Attack in Paris

Background

As 2015 drew to a close, the security situation in France was tense. Terrorist attacks in January, committed by ISIS supporters, had killed seventeen people and wounded another twenty-two, which resulted in heightened security posture and increased border checks in France.[117] Nine attackers participated in the attack; all were EU citizens who entered France despite being known

[115] *Lessons from the Mumbai Terrorist Attacks – Parts I and II*, Hearing before the Committee on Homeland Security and Governmental Affairs – United States Senate, January 8 and 28, 2009, p. 9. Retrieved 10 July 2016.

[116] Angel Rabasa, Robert D. Blackwill, Peter Chalk, Kim Cragin, et al., *The Lessons of Mumbai*, RAND Corporation, 9 Jan. 2009, p. 9. Retrieved 8 July 2016.

[117] *Eric Randolph & Simon Valmary, "More than 120 people killed in Paris 'terror' attacks". Yahoo! News. Agence France-Presse, 13 Nov. 2015. Retrieved 11 July 2016.*

terrorism suspects.[118] Based in Belgium, the attackers brought explosive belts and automatic weapons into Paris with them, despite the strict border control measures in place by the French.

"On est parti on commence"[119]

As in Mumbai, the attackers launched near-simultaneous attacks on separate targets to begin their assault, just after 9 PM.[120] The attackers operated in three separate teams to maximize effectiveness and strike the greatest number of targets.[121] Targets included a sports stadium, restaurants and cafes, and a concert hall.[122] Moving quickly from target to target, the attackers also utilized suicide bombings in conjunction with automatic weapons in order to create the greatest number of casualties and heighten confusion.[123] The focal point of the attack became the Bataclan theatre, where three attackers opened fire on a packed concert hall, before taking dozens of hostages and beginning an urban siege.[124] Unlike Mumbai, however, within four hours seven of the attackers would be dead (the remaining two would be killed in a police raid several weeks later), but

---

[118] *Ian Traynor, "EU ministers order tighter border checks in response to Paris attacks". The Guardian, 20 Nov. 2015.* Retrieved 12 July 2016.

[119] "Let's go, we're starting" – a text message discovered on a cell phone belonging to one of the Paris attackers. Contrary to statements made in the aftermath of the attack, the attackers used no encrypted devices or other covert means of communicating. Only simple phrases, sent in the clear. Cyrus Farivar, "Paris police find phone with unencrypted SMS saying "Let's go, we're starting"," Ars Technica, posted 18 Nov. 2015. Retrieved 10 July 2016.

[120] The New York Times, "Three Hours of Terror in Paris, Moment by Moment", The New York Times, posted 15 Nov. 2015. Retrieved 12 July 2016.

[121] *Alicia Parlapiano, Wilson Andrews, Haeyoun Park and Larry Buchanan, "Unraveling the Connections Among the Paris Attackers", The New York Times*, 17 Nov. 2015. Retrieved 12 July 2016.

[122] Ibid

[123] Bruce Riedel, "Modeled on Mumbai?" Brookings Institute.

[124] Adam Nossiter and Andrew Higgins, "'Scene of Carnage' Inside Sold-Out Paris Concert Hall", The New York Times, 13 Nov. 2015. Retrieved 12 July 2016.

despite lasting less than four hours, the Paris attacks would still result in 130 victims killed, and another 368 wounded.

Analysis

The four case studies provide definitive examples where swarming allowed for a numerically- and technologically-disadvantaged force to inflict severe, in some cases catastrophic, casualties on the opposing force. The battles for Grozny and 2002's Millennium Challenge illustrated swarming's effectiveness in a military setting – the former involved the Russian military suffering its worst defeat since World War II, while the latter involved a military exercise designed to last two weeks coming to an abrupt halt within the first fifteen minutes due to catastrophic simulated losses to the U.S. forces. The Chechen rebels and LtGen Van Riper both utilized swarming tactics to compensate for their numerical and technological disadvantages to confuse, out-maneuver, and overwhelm their respective opponents. Their opponents, despite having almost every perceivable advantage, were unable to mount an effective defense or counter-attack. Considering the results, these two case studies leave little doubt about swarming's efficacy in a military setting.

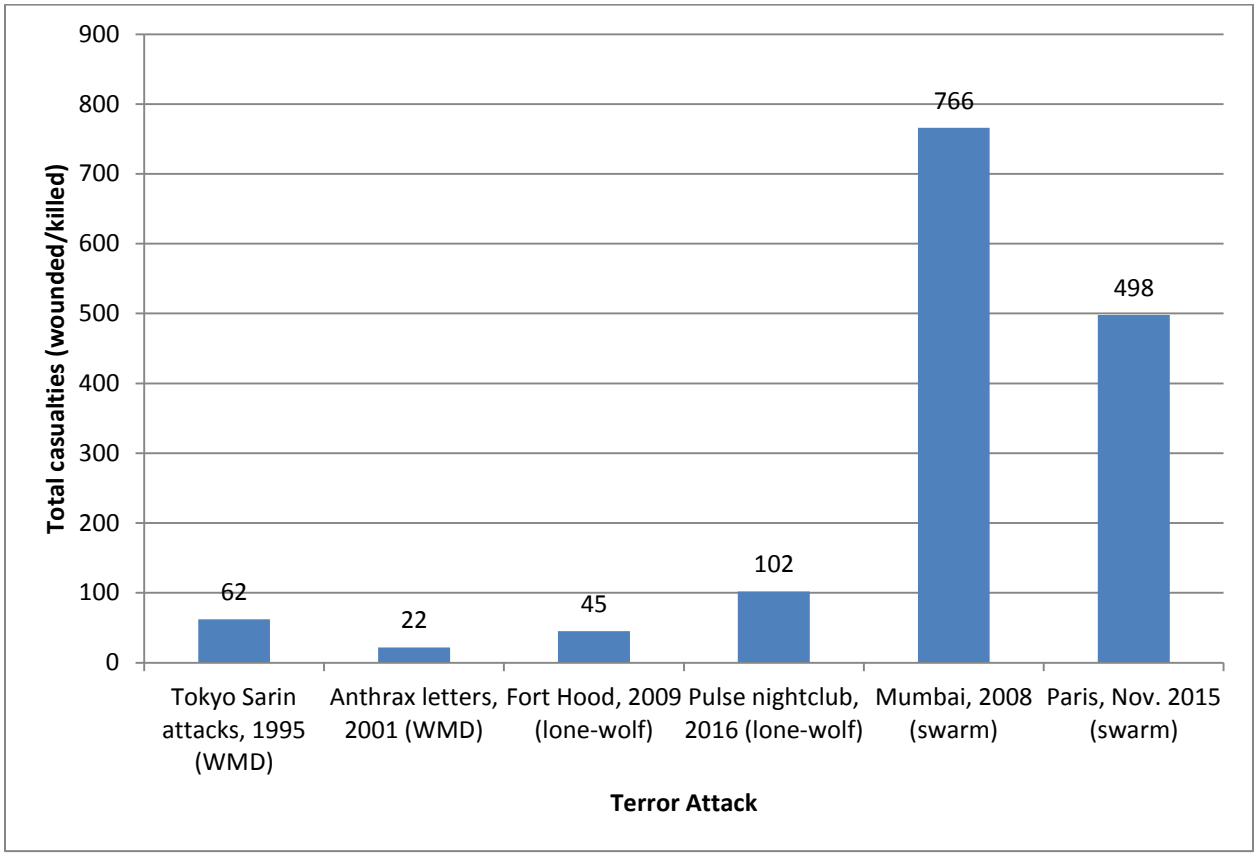
The second two case studies examine swarming not in a military context, but in the arena of terror attacks. These case studies, which examine the attack in Mumbai in 2008 and the attack in Paris in November 2015, are particularly important for my thesis as I attempt to show that a swarm-style attack poses a far greater threat to U.S. domestic security than a WMD or lone-wolf attack. In both cases, less than a dozen men managed to inflict several hundred casualties and shut down major cities. Both cases illustrate the

brutal effectiveness of swarm-based tactics in an urban environment – occurrences that will likely become more common as more of the population shifts towards urban centers.[125]

To further illustrate the effectiveness of swarm-based attacks by terrorists, Figure 1 shows the total casualty tally in selected terrorist attacks. These include the casualties from two WMD (one chemical warfare, the other biological warfare) attacks, two lone-wolf style attacks (one on an Army base in Texas, the other a nightclub in Florida), and two swarm-style attacks (in two modern international cities). Casualty tallies on the graph include both killed and wounded, and do not include the deaths of the attackers in the tally[126].

[125] Kilcullen, *Out of the Mountains*
[126] Casualty totals are drawn from acknowledged press reports released after each incident

Figure 1 – Terror Attack Casualty Comparison



As Figure 1 shows, a large disparity exists between casualties for WMD, lone-wolf, and swarm attacks. More than twice the people were killed and injured in the Paris November 2015 attacks than in all the non-swarm attacks listed. Even when the number of attackers in each of the swarm-based attacks is factored in (ten in Mumbai, seven in Paris), each attacker inflicts an average of 76.6 casualties in Mumbai and 71.1 casualties in Paris – far more casualties than many lone-wolf style attacks have inflicted.

WMD, lone-wolf, or swarm?

As discussed previously, while there is little consensus on the likelihood of a terrorist attack involving a nuclear weapon in the United States, there was agreement that

violent non-state actors appear to be far from acquiring the technological and engineering expertise necessary to fabricate, transport, and detonate a nuclear device[127]. A similar situation appears to exist for chemical and biological weapons. The perceived unlikelihood that a terrorist group would use a nuclear, chemical, or biological weapon exists because of the relatively high barrier of entry of WMD attacks[128]. They can be very complicated to manufacture, transport and deploy.

Lone-wolf attacks are easier for terrorist groups to motivate and execute. All that is required is an individual willing to kill and possibly be killed. As mentioned earlier, these individuals are hard for law enforcement to detect and therefore prevent[129]. As lone-wolves, however, they are capable of executing attacks of significant impact. Ultimately, they are constrained because law enforcement must stop only a sole operator and one man can only do so much to wage a terror attack.

Swarm tactics implemented by a small group of individuals, while more complex to organize, are shown in the case studies of this chapter to be a force multiplier, whether they are used by military units or terrorists. Some critics might argue that the necessary training, and potentially smuggling a trained group of individuals with equipment into a target country, might serve as a barrier to entry and inhibit these sorts of attacks from happening. Yet in both Mumbai and Paris these supposed difficulties proved to be insufficient to stop the terrorists. In Mumbai, the attackers received extensive training, conducting mock amphibious raids and practicing commando tactics before covertly infiltrating Mumbai by sea. In Paris, several of the attackers had previously travelled to Syria to fight alongside ISIS, and French intelligence flagged all of them as terror

[127] Cameron, "WMD Terrorism in the United States", p. 169
[128] Bowman, *Weapons of Mass Destruction: The Terrorist Threat*, CRS Report for Congress
[129] Bajekal, "The Rise of the Lone Wolf Terrorist", Time Magazine

suspects; despite this, they re-entered the EU and passed through heightened French border security with military-grade small arms and explosive suicide belts. In both Mumbai and Paris, these small groups used swarm-style tactics to create a level of destruction that no WMD or lone-wolf attack has been able to approach.

Conclusion

In the last two decades, the United States has faced an increased threat of domestic terror attacks. The goal of this paper was to argue that swarm-tactic terrorist attacks pose a greater threat, and can result in greater damage, than WMD or lone wolf-based terror attacks.

At the time of writing, there have been no swarm-tactic terrorist attacks conducted within the United States. There has been one chemical WMD attack (the anthrax letters in late 2001) and numerous lone-wolf attacks conducted in the U.S. since 2001. However, the absence of a terrorist swarm-attack thus far does not obviate the clear and significant risk such an attack poses. I examined four case studies in this chapter where swarm tactics proved decisive: the Russian siege of Grozny, Chechnya in the 90s; the U.S. military exercise Millennium Challenge 2002; and two real-world terror attacks, in Mumbai in 2008 and Paris in 2015.

The Chechens in Grozny utilized swarm tactics to counter the decisive armor and numerical advantage held by the Russian military forces seeking to seize Grozny – the battle ended in a Chechen victory, with the Russian forces suffering their worst losses since World War II. In Millennium Challenge 2002, the commander of the "Red" opposing force applied swarm tactics to missile, small-boat, and aviation assets – this led

to the attacking U.S. carrier battle group suffering almost total destruction in the first fifteen minutes of the exercise. In Mumbai in 2008 and Paris in 2015, trained groups of attackers equipped with small arms and explosives infiltrated bustling urban centers and conducted devastating attacks on multiple targets using swarm tactics, overwhelming local law enforcement; the attack in Mumbai lasted nearly three days, the attack in Paris over in a matter of hours due to the rapid use of explosive suicide vests by the attackers.

Comparing recent WMD, lone-wolf, and swarm-tactic terrorist attacks, the disparity in casualties between the first two types of attack compared to swarm-tactic attacks is utterly lopsided. Compared to the *least* deadly terrorist swarm attack (Paris in 2015), the most deadly WMD attack (Sarin attacks in Tokyo, 1995) resulted in approximately one-tenth the number of casualties of the (62 killed/wounded versus 498 killed/wounded); the most deadly lone-wolf attack (Pulse nightclub attack, 2016) only produced one-fifth the number of casualties (102 killed/wounded in Orlando versus 498 killed/wounded in Paris). When one considers that most lone-wolf attacks result in significantly fewer casualties than the cases presented in this study, the gap in "effectiveness" (casualties resulting from the attack) only widens.

While there is little disagreement that a successfully-employed WMD terrorist attack could result in catastrophic casualties, there is little consensus on the likelihood of such an attack occurring, and little evidence to support a pending attack in the future. Chemical, biological, radioactive and nuclear improvised devices required tightly-controlled, regulated, and tracked materials; constructing and moving such a device into the United States poses another set of problems to a potential terrorist. Overall, the barrier

to entry for terrorists to commit a WMD attack is well outside the reach of most terrorist groups.

Far more likely, and easier to orchestrate, are lone-wolf terrorist attacks. The U.S. and Western Europe have experienced dozens of these attacks in the last few years. It is agreed-upon by those involved that locating and interdicting lone-wolf terrorists before they commit their attacks is difficult, if not impossible. While far more frequent in their occurrence, lone-wolf attacks are often limited by the fact that only one individual is involved. While occasionally resulting in significant casualties (Norway attacks, 2011; Pulse nightclub shooting in Florida, 2016; Nice, France in 2016), more often lone-wolf attacks results in far fewer casualties[130]. While lone-wolf attacks are increasing in frequency, they are not as damaging as attacks conducted by groups.[131]

Critics might argue that the main weakness in swarm-based terror attacks is their reliance on groups of trained, equipped individuals. However, the attacks in Mumbai and Paris show that this is not the barrier some perceive it to be. The Mumbai attackers trained for months in Pakistan before conducting a covert, seaborne entry into Mumbai with all their equipment. Several of the Paris attackers fought in Syria, all were known to French intelligence agencies and were flagged for terrorist affiliations, and yet they were able to enter Europe and then France unimpeded, even though France's border security was on a heightened security footing due to terror attacks in January of 2015.

---

[130] Boston Marathon bombings, 2013 - 4 dead;
Bavarian train attack, 2016 - 0 dead;
Chattanooga shootings, 2015 - 8 dead;
Ottawa attacks (2), 2014 - 2 dead;
University of North Carolina car attack, 2008 - 0 dead

[131] Daveed Gartenstein-Ross, "What Does the Recent Spate of Lone Wolf Terrorist Attacks Mean?", for *War on the Rocks*, 27 October 2014. Retrieved 1 August 2016.

Furthermore, despite strict weapons restrictions within Europe, the attackers were able to bring military-grade small arms and explosive vests with them into France.

With the extensive U.S. coastline, a porous border with Mexico, and the longest international border in the world between Canada and the U.S., it would be naïve and dangerous to believe that a group similar to those from Mumbai and Paris would be unable to enter into the United States covertly. Particularly vulnerable is the U.S. coastline: drug cartel narco-submarines reach it almost unimpeded; the U.S. Coast Guard, Navy, and Border Patrol interdict only 10-25% of all submarines which operate in the Pacific, Gulf of Mexico, and Atlantic (see Chapter 1 of this thesis for a more detailed analysis of these subs and cartel-Islamic terrorist group nexuses). These subs can transport up to 10 tons of cargo, which can consist of men and materiel should an Islamic terrorist group intent on conducting a swarm attack in the U.S. purchase use or transit on a cartel narco-sub. Once making landfall, the only challenge remaining to such a group would be movement to the target and execution of the attack.

How to beat the swarm?

Determining detailed counters to potential swarm-based terror attacks could quite possibly fill at least one book, if not several. However, I feel it necessary to provide several potential ways the United States may be able to lessen the likelihood and severity of a terrorist swarm attack.

First, construct a more robust maritime security apparatus, particularly to counter the threat posed by narco-submarines and potential underwater infiltration by attackers. Efforts to interdict narco-subs while they are being constructed, increased patrols and

passive surveillance/detection measures by U.S. assets in the region, and increased interagency cooperation in the U.S. and abroad could ultimately result in fewer narco-submarines in operation and greater interdiction rates. This would remove a key means of terrorist operatives infiltrating the U.S. covertly and increase the risk of capture if terrorists sought to use narco-submarines to enter the U.S.

In the domestic arena, I see at least two key areas for focus. First, law enforcement and first responders should drill to combat a swarm-style attack. In particular, the drills should focus on reacting to multiple swarm attacks rapidly following one another, such that law enforcement itself does not swarm the first attack, thereby depriving nearby areas of protection. One of the primary reasons the attack in Mumbai lasted sixty hours was law enforcement's lack of experience in dealing with such an attack, and coordination issues between law enforcement and military agencies. French anti-terrorism units, on the other hand, were quick to respond and contain the attackers in Paris, which helped restrict their movement (a key facet of a successful swarm attack) and limit casualties. U.S. law enforcement agencies should drill not only to respond to simultaneous attacks in multiple locations, but also to practice coordination and communication between local, state, and federal law enforcement agencies – an activity worth practicing regardless of the type of event that might occur. Developing "swarm-gaming" exercises, in conjunction with hostage, active shooter, and other scenarios faced by law enforcement, could also prove to be a critical tool in training to respond to swarm-based terror attacks.

Second, continual assessment of security measures at potential targets by the U.S. security apparatus should continue. Physical pat-downs at the Stade de France in Paris

prevented attackers wearing suicide vests from entering during a crowded international soccer match in 2015, forcing the bombers to detonate outside the stadium. The attackers in Mumbai and Paris also targeted popular hotels, cafes and a concert hall. To counter swarm attacks, it is likely necessary to consider re-vamped security procedures for venues such as these. Furthermore, critical infrastructure can also be vulnerable to swarm attacks. Continual assessments of U.S. critical infrastructure to determine which assets require hardening and additional defensive measures could be important. The key emphasis here is not necessarily in implementing more defensive measures, but *more effective* defensive measures.

To conduct these assessments, the agencies tasked with the protection of key infrastructure can serve as a Red Team, planning and conducting swarm-style attacks on potential targets. This would likely allow law enforcement to assess current defense measures in place as well as learn how potential terrorist groups may attack the facility. Serving as the attacking force allows law enforcement to get inside the minds of potential attackers, and can provide valuable feedback to develop defensive and attack-response measures. Alternatively, the development of an AI/simulation program to practice theoretical "swarm-gaming" and simulate attacks against various facilities could provide a valuable tool, and potentially spot weaknesses that human observers had missed.

While the *potential* damage of a WMD attack and the rising frequency in lone-wolf terror attacks is undeniable, neither is the fact that swarm-style terror attacks are far more destructive and thus pose a far greater threat to U.S. domestic security than either WMD or lone-wolf attacks.

Chapter 3: Spoiling Goliath's Garden

Determining the Vulnerability of U.S. Economic and Energy Infrastructure to Kinetic Attacks

Introduction

The last two decades have seen countless high-profile terror attacks around the world – the attack on the World Trade Center in New York and the Pentagon in Washington, D.C. in 2001; the Mumbai urban siege in 2008; the attack in Paris in November 2015; the Bastille Day truck attack in France in 2016. One of the common themes linking all these attacks is that they focused on "impact" targets – public institutions and gatherings, theatres, hotels, athletic stadiums – with the attackers placing a premium on body count and global visibility. With the exception of the Pentagon in 2001, none of the targets struck were military; almost all of those killed in these high-profile terror attacks were civilians or law enforcement.

Since then, the countries that fell victim to these terror attacks have taken dramatic measures to lessen the viability of these attacks and prevent them from becoming a recurring nightmare. Increased security personnel during public gatherings and intensified security protocols around large public gatherings have served to harden these once-soft targets. Law enforcement agencies in major cities have trained to be far more adept at responding to burgeoning terror attacks, becoming more agile and efficient in their responses. While there is still a possibility of terror attacks against "soft" targets in large cities, such as theatres, sports arenas, and hotels, the probability of terrorists achieving a similar successful high-visibility, high-body count attack appears to be decreasing.

However, what if terrorists planning a kinetic attack which sought to achieve a goal outside of a high body count and extensive press coverage? What if the goal is to

conduct an attack that resulted in fewer bodies on the ground initially, but has the potential for significant, or catastrophic, long-term economic and environmental effects? Such an attack would be a marked change in strategy to past terror attacks.

In this paper I will seek to answer the following question: does the United States possess specific weaknesses or chokepoints within key energy and economic infrastructure that terrorists could target with a kinetic attack to cause massive economic, energy, and/or environmental damage? While such an attack might not create the same high body count and terror as some of the aforementioned attacks, I believe the results of a successful terrorist attack on a key infrastructure target make these viable targets worth examining, and protecting.

Literature Review

Broadly speaking, the literature concerning U.S. critical infrastructure vulnerability to terrorist attack highlights two main sources of threats: cyber-attacks, and kinetic attacks. Within each there is further discussion on the vulnerability of various sub-sectors of the national infrastructure: water[132], electricity, petroleum, economy, transportation.

Cyber-attacks seem to take the lion's share of the attention and concern: the U.S. Army Training Command's Deputy Chief of Staff for Intelligence (DCSINT) Handbook No. 1.02, Critical Infrastructure Threats and Terrorism mentions cyber-attacks in the opening pages of the Handbook[133]. The discussion on cyber-attacks then proceeds to

[132] Claudia Copeland, *Terrorism and Security Issues Facing the Water Infrastructure Sector*, Congressional Research Service, 15 December 2010.
[133] Deputy Chief of Staff for Intelligence, *Critical Infrastructure Threats and Terrorism: Handbook No. 1.02*, 2006, p.2-3

consume the majority of the remainder of the handbook, receiving three sections' worth of attention to the one chapter on physical attacks. The Department of Homeland Security's (DHS) webpage on Critical Infrastructure Security also provides a robust discussion on cyber-security and the risk of cyber-attacks to U.S. infrastructure[134]. DHS' *Energy Sector-Specific Plan 2015*[135] and *Dams Sector-Specific Plan 2015*[136] both discuss the threat posed by cyber-attacks. ICF International released a report in June 2016 examining the security and resilience of the U.S. electrical grid; cyber-attacks receive a length analysis in this report as well[137]. Numerous recent[138] news[139] reports[140] also devote significant[141] discussion[142] and analysis[143] to the threat posed by cyber-attacks to U.S. critical infrastructure.

The threat of physical attacks to key infrastructure seems to have taken a back seat to the threat posed by cyber-attacks. In several of the aforementioned sources (Handbook No. 1.02, DHS' *Energy-Sector Specific* and *Dam-Sector Specific* plans) physical attacks receive noticeably less discussion and analysis than cyber-attacks. ICF International's report pays equal attention to both threats, but my research showed far less discussion, and thus concern, of physical attacks posing a significant threat to key U.S. infrastructure. Similarly, there is little discussion or analysis of current physical security

[134] https://www.dhs.gov/topic/cybersecurity
[135] Department of Homeland Security, *Energy-Specific Sector Plan 2015*, 2015, p. 4-5, 26-28.
[136] Department of Homeland Security, *Dams-Specific Sector Plan 2015*, 2015, p. 9, 19-25.
[137] ICF International, *Electric Grid Security and Resilience: Establishing a Baseline for Adversarial Threats*, 2016, p. 18, 36-51.
[138] "Cyber Attack on Nation's Critical Infrastructure", ABC News. Accessed 13 January 2016.
[139] Michael Assante, "America's Critical Infrastructure is Vulnerable to Cyber Attacks", *Forbes.com,* 11 November 2014.
[140] Tony Kovaleski, Liz Wagner, and Mark Villarreal, "Critical Infrastructure Vulnerable to Cyber Attack, Experts Warn", *NBC Bay Area*, 1 February 2015.
[141] Ben Frankel, "Cyber attacks on critical infrastructure reach U.S.", *Homeland Security News Wire*, 21 November 2011.
[142] Steve Reilly, "Records: Energy Department struck by cyber attacks", *USA Today*, 9 September 2015.
[143] Cory Bennett, "Critical infrastructure cyberattacks rising, says official", *The Hill*, 13 January 2016.

measures – this is logical considering the sensitive as well as public nature of several of the examined installations, but the author's personal observations of security personnel and protocols at several of the discussed locations gives the impression of minimal, predominantly passive security measures.

Furthermore, a trend amongst all literature found is a lack of specific discussion regarding vulnerabilities. General discussion of the vulnerabilities of various infrastructure sectors to cyber and physical attacks abounds – however, there is little in the way of specificity in discussing these vulnerabilities. Nor is there much discussion regarding prioritizing infrastructure sectors; only DCSINT's Handbook 1.02 places primacy on one specific infrastructure sector (energy)[144]. Also, protection from natural disasters is a common thread of discussion, occurring concurrent with analyzing threats from cyber and physical attacks in much of the literature; ICF International's report is the only one which focuses specifically on "adversarial threats"[145] to critical infrastructure.

Worth examining is also the literature of those who might seek to strike at the United States. In November of 2004, Al-Jazeera released a transcript of Osama bin Laden's most recent tape – in it, the then-leader of Al-Qaeda highlighted that one of Al-Qaeda's primary goals was to "[continue] this policy in bleeding America to the point of bankruptcy."[146] In the video transcript, Bin Laden also goes on to observe that "every dollar of Al Qaeda [defeats] a million dollars [of the United States]", causes job loss, and that the "real loser…is the American people and their economy"[147]. Bin Laden's focus was not on killing Americans per se – that simply provided a means to an end, which in

[144] DCSINT, *Handbook 1.02*, p. II-6.
[145] ICF International, p. 1.
[146] "Bin Laden: Goal is to bankrupt U.S.", *CNN.com*, 1 November 2004. Accessed 10 February 2017.
[147] Ibid

Bin Laden and Al-Qaeda's aim was to provoke a military response from the United States, and force the U.S. to commit significant time and treasure towards fighting Al-Qaeda. Al-Qaeda and those sympathetic to Al-Qaeda can easily continue this "bleed-until-bankruptcy"[148] plan by striking not at people, but at key economic and energy infrastructure nodes within the United States, and using the resulting economic and environmental damage to force the United States to spend money that might elsewise go towards counterterrorism operations overseas.

The dearth of successful examples of terrorist-lead cyber-attacks, coupled with successful physical attacks against U.S. infrastructure in the past[149] and the former leader of Al-Qaeda emphasizing the focus on financially damaging the United States, leads this author to focus on kinetic attacks as the primary threat facing U.S. critical infrastructure. The purpose of this paper is to highlight specific cases within the U.S. energy, environmental, and economic infrastructure that are uniquely vulnerable to kinetic terrorist attacks that, if damaged, would create significant and long-lasting economic and environmental impacts whose financial costs would place a significant burden on the U.S. economy and the average American. By highlighting specific cases of infrastructure vulnerability, the goal is to force accountability and drive discussion of counters to potential kinetic attacks, and ideally precipitate effective action in addressing these weaknesses.

[148] Ibid

[149] Jared Ferris, "Terrorist Attack Shows Vulnerability in Critical Infrastructure", *The Daily Signal*, 19 February 2014. Accessed 29 December 2016.

Methodology

This paper uses four separate case studies to analyze targets across the U.S. domestic infrastructure and economic spectrum to highlight key nodes which present themselves as targets to a kinetic terrorist attacks. These are:

- The Hoover and Glen Canyon Dams, located in Arizona and Utah respectively. Both straddle the Colorado River. Their vulnerability lies not in terrorists attempting to breech the dams themselves; instead, the weakness in both these facilities from a counterterrorism standpoint lies in their transformers – large, custom-built pieces of equipment that sit exposed at the bases of the dams, take months to replace, and without which the dams are incapable of producing electricity.
- The Ports of Houston and Corpus Christi. These are two of the busiest ports in the United States, and key locations for the majority of the U.S. petroleum refining and unloading facilities. Their vulnerability to kinetic attack lies in both the refinery facilities, and the anchored petroleum tankers waiting to offload.
- The Louisiana Offshore Oil Port. Located just off the coast of Louisiana, this complex is responsible for offloading petroleum tankers too big to enter Galveston or Houston. Both the facility and anchored petroleum tankers awaiting offloading are vulnerable to kinetic attacks.
- The oil/petroleum storage facilities in Cushing, Oklahoma. This facility is a nexus of major pipelines and constitutes the majority of the U.S. oil reserve.

Case studies as a methodology are fitting in this scenario for a number of reasons. Case studies allow for a researcher to conduct comparisons across a variety of levels. I can compare each case study to the existing literature on an individual basis, as well as compare case study examples to one another. This versatility allows me to build a thought-out, thorough examination of viable economic and infrastructure nodes that provide viable targets for a kinetic terrorist attack.

All four case studies involve targets which are vulnerable to attack by small groups of lightly-armed men, similar to the groups who carried out the Mumbai attacks in 2008 and the Paris attacks in November of 2015. One case study examines two major nodes in the U.S. electrical infrastructure in the American West – the Hoover and Glen Canyon dams. The other three involve, to one degree or another, elements of the oil and petroleum infrastructure in the U.S., as well as major ports (Case Study #2 – Ports of Galveston and Houston). The case studies examine targets vulnerable to attack from air, land, and sea; a successful attack on any of these targets could result in economic, environmental, and infrastructure damage in place of the traditional high-body count from a terror attack. Additionally, the case studies examine targets that range from rural to major urban locations – this plays a role in the scale and ability of a law enforcement response to any terror attack.

The biggest disadvantage of using case studies as a methodology is the risk of favoritism – where the researcher intentionally chooses cases which validate the theory being explored. This academic "cherry-picking" weakens the researcher's argument by failing to present a well-rounded argument. To avoid this, the cases examined in this paper cover a wide range of infrastructure, from electrical grid, to oil/petroleum, to

shipping, and concern possible targets which are located in both rural and urban locations. This highlights the viability of a kinetic small-unit terrorist attack capable of producing significant economic and environmental impacts.

Case Studies

Case Study #1 – the Hoover and Glen Canyon Dams

Hoover Dam

Built from 1931-1936, Hoover Dam is a major lynchpin in water distribution, electricity generation, and tourism – approximately seven million people tour the dam each year[150]. Located on the border of Arizona and Nevada, Hoover Dam impounds the Colorado River, creating Lake Mead, the largest reservoir in the United States. Responsible for controlling water flow to numerous Western states, including Arizona, Nevada, and California, one of Hoover Dam's primary functions is generating electricity through hydropower. Still one of the nation's largest hydroelectric operations, despite its age, Hoover Dam provides power to over 1.3 million households[151].

Glen Canyon Dam

Farther upstream on the Colorado River, Glen Canyon Dam creates Lake Powell, another of the largest man-made reservoirs in the United States. Opened some thirty years after the Hoover Dam, Glen Canyon Dam also plays a vital role in irrigation and power generation for the Western United States. Hoover Dam is the largest producer of hydroelectric energy in the southwestern U.S.; Glen Canyon Dam is the second-largest. A

[150] "Hoover Dam", *History.com*
[151] *Hoover Dam Frequently Asked Questions*, United States Bureau of Reclamation website.

key component of the Colorado River Storage Project[152], the Glen Canyon Dam also provides electricity to approximately five million people across Arizona, Colorado, Nevada, New Mexico, Utah, and Wyoming[153]. Glen Canyon Dam also serves as the cold-start energy source for secondary power plants in the region, providing the electric boost necessary to bring other plants online.

High Voltage/Large Power Transformers

High Voltage (HV) transformers, also known as Large Power Transformers (LPTs), are in use at both the Hoover and Glen Canyon dams, as well as other key electrical infrastructure nodes around the United States. Extremely heavy, large, and usually custom-built for an application[154], HV transformers are usually not interchangeable, nor are there extensive spare inventories due to the custom nature and high cost of HV transformers and their parts[155]. HV transformers can cost in excess of $10 million, not counting transportation and installation costs[156]In addition, the average lead time for a transformer varied from five to twelve months for domestic producers; international manufacturers see an average lead time of six to sixteen months from order to delivery[157]. Actual delivery of HV transformers can also prove challenging, as most transformers weigh hundreds of tons[158] - one recent event required the hiring of a Russian

[152] *Glen Canyon Unit*, United States Bureau of Reclamation website.
[153] *"Frequently Asked Questions", Glen Canyon Dam Adaptive Management Program website, 4 April 2013.*
[154] Paul W. Parformak, "Physical Security of the U.S. Power Grid: High-Voltage Transformer Substations", *Congressional Research Service*, 17 June 2014, p. 10.
[155] Edvard Csanyi, "Large power transformer tailored to customers' specifications", *Electrical Engineering Portal Online*, 30 December 2013.
[156] Parformak, "Physical Security of the U.S. Power Grid: High-Voltage Transformer Substations", p. 4.
[157] *Large Power Transformers and the U.S. Electric Grid*, U.S. Department of Energy, April 2014 update, p. 9.
[158] ICF International, p. 27.

Antonov-225, the largest airplane in the world, to transport an HV transformer from Austria to Arizona[159].

At Hoover Dam, the HV transformers (indicated by arrows) are located on the wings along both sides of the base of the dam, as depicted below (Figure 2):

Source: U.S. Bureau of Reclamation website, https://www.usbr.gov/lc/hooverdam/images/ramp.jpg

[159] Rebecca Smith, "Transformers Expose Limits in Securing Power Grid", *The Wall Street Journal*, 4 March 2014.

At the Glen Canyon Dam, the HV transformers (indicated by arrows) are located along the deck at the base of the dam (Figure 3):

Source: Bureau of Reclamation website, https://www.usbr.gov/uc/img/gallery/gcd/images/6.jpg

Case Study #2 – the Ports of Houston and Corpus Christi

Port of Houston/Houston Shipping Channel

The Port of Houston and the corresponding fifty-mile-long Houston Shipping Channel makes up the second-busiest port, by volume, in the United States[160]. The numerous refining and petrochemical complexes also make the port of Houston a key node in the nation's petrochemical/refinery infrastructure, in addition to shipping

[160] *"U.S. Port Ranking By Cargo Volume", American Association of Port Authorities. 2013.*

infrastructure[161]. Numerous terminals transfer a wide range of goods for import and export; Houston is the number-1 ranked U.S. port in foreign tonnage[162], and most Volkswagen and Audi cars for sale in the U.S. pass through the Port of Houston[163]. This versatility in handling a wide range of goods, both foreign and domestic, from wheat to oil refining, makes the Port of Houston a critical component of both the U.S. shipping infrastructure, and also the U.S. domestic oil/gas infrastructure.

Port of Corpus Christi

The Port of Corpus Christi, another Texas Gulf port like the Port of Houston, is ranked as the fifth-largest port in the U.S.[164]. Similar to the Port of Houston, the Port of Corpus Christi's top three commodities traded in 2014 were petroleum-based, including crude oil, fuel oil, gasoline, and diesel[165]. Wind turbines are another key commodity that passes through the Port of Corpus Christi in high quantities – Texas' surge to the top wind-energy producer in the U.S, and one of the highest in the world, has led to an increased demand for wind turbines. Like the Port of Houston and the Houston Shipping Channel, the Port of Corpus Christi possesses a forty-five-foot-deep main channel to handle all but the largest ship traffic.

[161] Kiah Collier, "Houston has the busiest seaport in the U.S.", *Houston Chronicle*, 23 May 2013.
[162] *Statistics*, Port of Houston website.
[163] Eric Beech, "Factbox: Five facts about the Port of Houston", *Reuters Business News*, 13 December 2009.
[164] *"U.S. Port Ranking By Cargo Volume", American Association of Port Authorities*.
[165] *Liquid Bulk*, Port of Corpus Christi website.

Anchored off the coast

Despite their ability to handle high quantities of ship traffic, the Ports of Houston and Corpus Christi nonetheless require ships to anchor outside of the ports to await loading or offloading. This creates a naval "parking lot" just off the coast as ships wait to enter the port facilities. In addition, accidents and unforeseen circumstances can result in a further increase in anchored ships: in 2010, a barge crash which toppled power lines spanning the Houston Ship Channel idled 75% of the Port of Houston's terminals for at least three days[166], and in November 2015 over 40 oil tankers were anchored off the coast due to a glut in global oil supply[167], more than usual.

Shipping backlogs have a knock-on effect as well – once the ports resume standard operational pace, they require additional time to process the increased number of waiting ships. This can result in dozens of ships anchored off the coast for weeks, or even months as the ports work overtime to sort through the backlog. The cost of this backlog can result in a severe economic impact, as well as supply delays, as goods being imported and exported fail to reach their destinations on time, or not at all.

Case Study #3 – the Louisiana Offshore Oil Port

The Louisiana Offshore Oil Port (LOOP) is located approximately 18 miles off the coast of Louisiana, in the Gulf of Mexico. Consisting of two platforms (the control platform and the pumping platform) which resemble offshore drilling rigs, the LOOP is responsible for loading and offloading "very large crude carriers" (VLCCs) and "ultra large crude carriers" (ULCCs), the largest petroleum-transporting ships in the world that

[166] Zain Shauk, "Barge crash blocks access to Port of Houston", *The Houston Chronicle*, 3 October 2010.
[167] The Associated Press, "Oil Tanker Traffic Jam Off Texas Is Viewed as Sign of Oversupply", *The New York Times*, 11 November 2015.

are too large for regular port facilities[168]. The LOOP also receives oil directly from two of the largest Gulf of Mexico oil fields[169]. Responsible for processing approximately 13% of imported foreign oil, the LOOP processes about 1.2 million barrels a day. Oil offloaded by the LOOP is transported by pipeline to storage and refinery sites on shore.

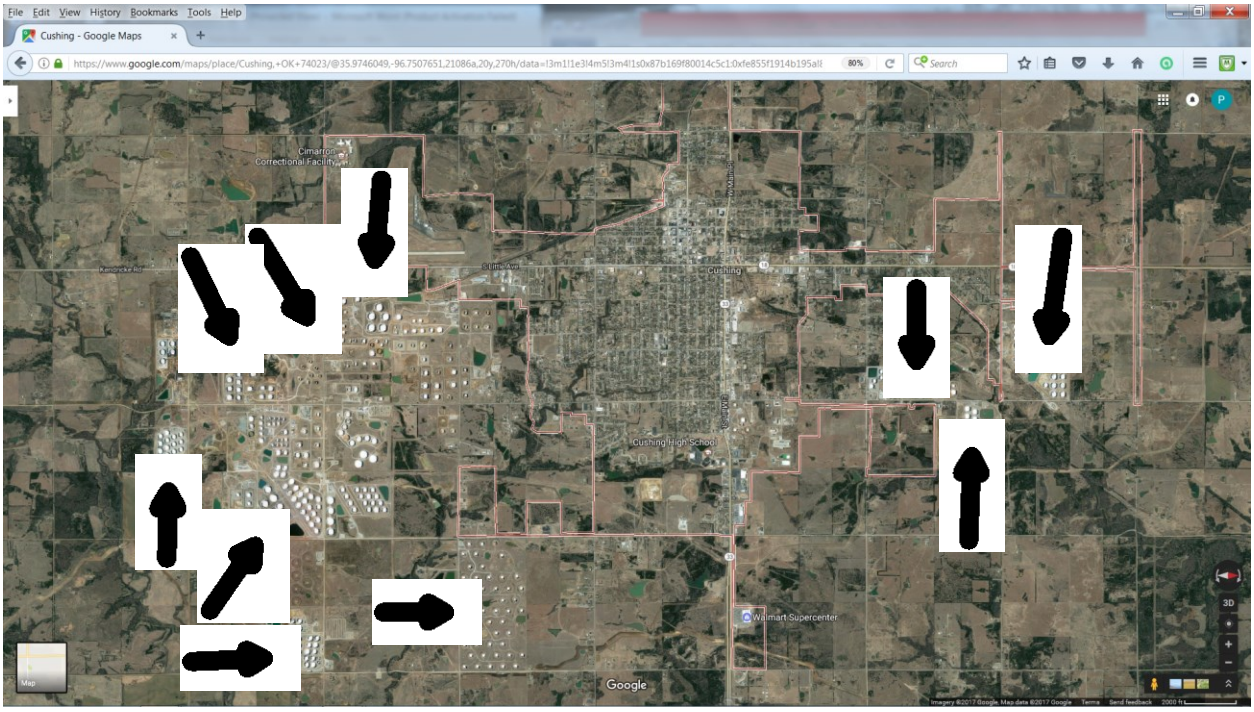
To offload, the VLCCs and ULCCs anchor at designated single-point mooring (SPM) bouys, whereupon hoses are hooked up and pumps begin offloading the anchored ship[170]. The LOOP is capable of offloading tankers at a rate of 100,000 barrels and hour; with most VLCCs and ULCCs capable of carrying approximately 2 million barrels, offloading is still a time-consuming process.

Case Study #4 – the oil storage facilities in Cushing, Oklahoma

Cushing, Oklahoma is approximately an hour north of Oklahoma City, OK, a small town with the 2010 census showing a population of less than 8,000[171]. However, far from being a small Midwestern farming town, Cushing is also known as "The Pipeline Crossroads of the World"[172]. Home to the largest oil storage facility, and one of the largest petroleum refining operations, in the United States, Cushing holds roughly 13% of the U.S.'s oil reserves[173]. As of early 2016, due to depressed oil prices, Cushing's storage facilities were at approximately 89 percent full[174], which represents billions of U.S. dollars in value. Cushing also serves as the delivery point for West Texas

[168] *Tanker Offloading*, LOOP LLC website.
[169] *Domestic Terminalling*, LOOP LLC website.
[170] *Tanker Offloading,* ibid.
[171] *Cushing, OK overview*, Census Viewer website.
[172] Morgan Brennan and Justin Solomon, "The small US town holding billions in black gold", *CNBC.com*, 7 March 2015.
[173] Adam Wilmoth, "Gushing Into Cushing: Oil fills major storage hub in small Oklahoma town", *The Oklahoman*, 2 August 2015.
[174] Arthur Berman, "Cushing, Oklahoma is the center of the oil universe", *Business Insider*, 1 March 2016.

Intermediate (WTI), a specific blend of light sweet crude found in the U.S., which is traded on the New York Stock exchange. To hold all this oil, numerous above-ground tank farms are found all around Cushing, predominantly to the north and south of the town, as seen on a satellite overlay of GoogleMaps (see image below, right side of image is North). Each tank can hold anywhere from 350,000 to 575,000 barrels of oil, and there are hundreds of tanks that make up the Cushing complex [175](Figure 4).



(Source: GoogleMaps overhead of Cushing, OK. Rotated 90 degrees clockwise. Accessed 4 January 2017)

Analysis

Turning Out the Lights – HV Transformers

HV transformers represent a unique vulnerability in the U.S. electric grid. As previously mentioned, there is little in the way of spare parts as each transformer is

[175] "Confidence in Oil Hub Security Shaken By Oklahoma Earthquakes", *NPR Morning Edition*, 30 November 2015.

unique, and replacement of transformers can take months, not to mention cost millions of dollars. Furthermore, there is consensus amongst experts that "a coordinated and simultaneous attack on multiple HV transformers could have severe implications for reliable electric service over a large geographic area, crippling its electricity network and causing widespread, extended blackouts"[176].

There is also a precedent for this sort of attack in the United States. In the early morning hours of 16 April, 2013, after infiltrating and cutting fiber optic cables linking the power station's alarm and communications to the outside, two individuals fired over 100 rounds into seventeen power transformers at a San Jose power substation, disappearing before police arrived – the entire attack taking less than twenty minutes[177]. Engineers were able to cover the loss of power through increased production at other stations, but it still took twenty-seven days before repairs were completed[178].

There are three power grids in the United States – one in the western half of the country, one in the eastern half, and one in Texas[179]. All have struggled previously with even small problems, such as fallen tree branches, which result in "cascading blackouts", one of which resulted in 50 million people in the eastern U.S. and Canada losing power back in 2003[180]. Within these three grids, HV/LPTs consist of less than 3% of all transformers, but carry 60-70% of the nation's electricity[181]. While the quick re-routing of electricity through other stations mitigated the potential effects of the San Jose

[176] Parformak, p. 10.
[177] Rebecca Smith, "Assault on California Power Station Raises Alarm on Potential for Terrorism", *The Wall Street Journal*, 5 February 2014.
[178] Smith, ibid.
[179] Norimitsu Onishi and Matthew L. Wald, "Months Later, Sniper Attack at Power Hub Still a Mystery", *The New York Times*, 5 February 2014.
[180] Smith, "Assault on California Power Station Raises Alarm on Potential for Terrorism"
[181] Parformak, p. 10.

substation attack, the loss of more than one high voltage transformer could easily exceed the ability of the regional power grid to handle the increased load, results in blackouts and further damage to the grid[182]. Perhaps the biggest concern is that there is no federal body charged with protecting the nation's power grid and its components – that responsibility is largely left to individual utility owners[183]. Without federal oversight, protective measures have been uncoordinated and haphazard.

The Hoover and Glen Canyon Dams are both located in rural areas, far from major law enforcement agencies. Were a terrorist attack to occur, immediate response would be dependent on local law enforcement and security forces. When one examines how a coordinated, small-unit kinetic attack using swarm tactics, such as the 2008 attack in Mumbai or the Paris attack in November 2015 dwarfed the response capability of large-city law enforcement and dedicated counter-terrorism units, the capacity of a much smaller, more rural, and less-trained law enforcement agency does not appear promising.

The high voltage transformers at both dams are located out in the open, in full view from the canyon rims of both dams. Terrorists would not even need to gain direct access to the transformers – the San Jose attack illustrated how simple rifle fire caused significant damage. If the terrorists are able to acquire explosives, such as the suicide vests manufactured by the November 2015 Paris attackers, the possibility for catastrophic infrastructural damage widens even further.

Fire on the Water – Ports of Houston and Corpus Christi, the LOOP

[182] Ibid, p. 12-13.
[183] Peter Kelly-Detweiler, "What We Should Learn From The Attack on Pacific Gas And Electric's Transformer Station", *Forbes*, 10 February 2014.

While major U.S. port facilities are large enough that a small-unit terrorist attack would prove incapable of destroying the whole facility, the ships that pass through them are decidedly more fragile. Al-Qaeda has long targeted vital U.S. shipping interests – the suicide attack on the USS Cole, a Navy destroyer, in 2000; the attack on the *MV Limburg* by Al-Qaeda operatives in 2002 and the attempted suicide boat attack on a Japanese super-tanker in 2010 were all Al-Qaeda plots[184]. While the 2010 explosive-boat attack against the super-tanker failed to rupture the ship's hull, the explosive-boat attack against the *MV Limburg* as it transited the Gulf of Aden did result in casualties and the loss of approximately 90,000 barrels of crude oil into the Gulf[185]. In addition, the attack resulted in a short-term cessation of ship traffic through the Gulf of Aden, and Yemen lost approximately $3.8 million a month in port revenue[186]. The attack on the USS Cole nearly sank her, in addition to killing and wounding several dozen U.S. sailors. Al-Qaeda has long been a vocal proponent of suicide attacks on ships, calling on supporters to ram oil tankers with small boats laden with explosives[187].

As mentioned earlier in the paper, the ports of Houston and Corpus Christi see heavy petroleum-industry transport, with both ports experiencing heavy tanker traffic. Ships waiting to be loaded or unloaded are required to anchor in the Gulf outside of both ports, which provides large, stationary targets for individuals seeking to carry out a Cole-style attack. Ships unloading at the Louisiana Offshore Oil Port (LOOP), the VLCC and ULCC-class petroleum tankers, are moored to buoys around the port platforms for the

[184] Khaled Wassef, "UAE: Al Qaeda Responsible for Japanese Tanker Attack", *CBS News*, 6 August 2010.
[185] Charlie Savage, "Guantanamo Detainee Pleads Guilty in 2002 Attack on Tanker off Yemen", *The New York Times*, 20 February 2014. Accessed 10 February 2017.
[186] Rollie Lal, Brian A. Jackson, Peter Chalk, Farhana Ali, William Rosenau, "The MIPT Terrorism Annual 2006", *Memorial Institute for the Prevention of Terrorism*, 2006, p. 26. Accessed 10 February 2017.
[187] James Fielding, "EXCLUSIVE: Al Qaeda targets oil tankers in Gibraltar", *The Express*, 26 October 2014.

unloading process, which can take over a day. Using small, fast, pleasure-style craft loaded with explosives, several attackers could targets multiple ships, or focus all their efforts on one. Furthermore, an attack on a ship entering or exiting the Houston shipping channel that resulted in the sinking of said cargo ship or tanker would block the channel, effectively shutting down the entire Port of Houston. In a similar vein, the Houston Shipping Channel shut down previously due to toppled power lines, as explored earlier in this paper – five bridges also span the Channel. A major attack against any of these would result in a closure of the Channel, and shut down one of the more important ports to U.S. shipping.

Even without VLCCs or ULCCs anchored and unloading, the LOOP itself is vulnerable to attack by explosive-laden small boats. More than fifteen terrorist attacks have occurred against offshore oil platforms (which the LOOP closely resembles) off the coast of Nigeria in the last ten years[188]. Located only eighteen miles off the Louisiana coast, the LOOP is with easy reach of small boats, and both it and the massive tankers which unload there are vulnerable to explosive-laden small boats. Concern about the vulnerability of oil rigs to terrorist attack has been expressed domestically[189] and internationally[190], but beyond a general consensus of the looming threat little has been done to address the vulnerability of these platforms.

Beyond the immediate damage of a terrorist attack against a petroleum tanker, port, or the LOOP, the knock-on effects could prove monumentally expensive and time-consuming: the recent example of the *Costa Concordia* is a clear example of this. The

[188] Mikhail Kashubsky, *A Chronology of Attacks on and Unlawful Interferences with, Offshore Oil and Gas Installations, 1975-2010*, *Perspectives on Terrorism*, vol. 5, No. 5-6 (2011).
[189] CNN Wire Staff, "Senator warns of terrorist threat to oil rigs", *CNN*, 13 July 2010.
[190] Brendan Nicholson, "US investors fear terror attack on $300B Aussie oil rigs", *news.com.au*, 29 May 2012.

Houston Shipping channel is almost fifty feet deep and wide enough to accommodate shipping traffic – but a sunken or half-submerged ship would still completely obstruct traffic in and out of the port facilities. With busy port facilities shut down, massive economic impacts are inevitable from the interruption to import and export. Recovery operations to re-float and remove sunken ships are expensive. The clean-up costs for hundreds of thousands of barrels of oil leaked by a tanker ruptured in a terrorist attack are expensive, and the Gulf is still recovering from the Deepwater Horizon oil spill – two or three leaking supertankers could negate whatever recovery had been made thus far. A ruptured pipeline in Alabama in late 2016 resulted in shortages and price hikes downstream on the East Coast[191] - the LOOP is responsible for offloading nearly 1/5 of all foreign imported oil. The loss of the LOOP would have an immediate and significant impact on the U.S. petroleum industry, which would have further knock-on effects financially and economically.

Striking the Heartland – Cushing, Oklahoma

The oil storage facilities in and around Cushing, Oklahoma possess their own vulnerabilities. One of the single largest petroleum repositories in the United States, nearly all the oil and other petroleum products stored at Cushing are held in large, above-ground tanks (as mentioned earlier in the case study section). These holding facilities also include refining and pumping facilities, as Cushing is known as "The Pipeline Crossroads of the World"[192]. With widely dispersed facilities and a police department numbering

[191] Associated Press, "Explosion in Alabama shuts gas pipeline, shortages possible", *WTNH.com*, 1 November 2016.
[192] Brennan and Solomon, *CNBC.com*.

only sixteen officers[193], the majority of security provided to these storage facilities consists of chain-link fences and security personnel hired by the storage, pumping, and pipeline companies.

Cushing's location is not quite as remote as the Hoover or Glen Canyon Dams, but it still lies over an hour from a major metropolitan area (Oklahoma City) and significant law enforcement and counterterrorism support. A small group of terrorists, operating in a similar pattern to the Mumbai and Paris attackers, could cause significant damage before law enforcement was able to neutralize the threat. Terrorist attacks against similar storage/refinery resources have occurred in Algeria[194], Iraq[195], and Saudi Arabia[196] - the attacks in Algeria and Iraq resulted in significant loss of life and damage to the facilities. The dispersed nature of the storage, refinery, and pumping facilities at Cushing make for a security nightmare – an expansive perimeter that local law enforcement cannot effectively enforce against a determined attacker. Particularly one they cannot detect until after the first shots are fired.

Conclusion

Concentration of Targets

Despite the lack of any attacks targeting the economic and energy infrastructure of the United States, there still exists a wide range of critical junctures that are vulnerable to a kinetic terrorist attack. The LPT/HV transformers located at Hoover and Glen

[193] Per the Cushing Police Department website's list of current staff
[194] Smith-Spark, Laura and Sterling, Joe, "Bloody Algeria hostage crisis ends after 'final' assault, officials say", *CNN*, 23 January 2013.
[195] Rod Nordland and Al- Suadad Salhy, "Extremists Attack Iraq's Biggest Oil Refinery", *The New York Times*, 18 June 2014.
[196] Simon Henderson, *Al-Qaeda Attack on Abqaiq: The Vulnerability of Saudi Oil*, The Washington Institute, 28 February 2006.

Canyon dams represent a key weakness in the U.S. electrical grid – relatively easy to damage and unsecured, the loss of these transformers would create an electrical crisis in the western United States, as replacements would take months to fabricate and ship, and the power grid lacks the capacity to insert work-arounds.

The ports of Houston and Corpus Christi and the ships waiting to enter those ports remain vulnerable to explosive small-boat attacks similar to those carried out by Al-Qaeda in the past – the successful sinking of a petroleum tanker or other ship in the Houston Shipping Channel would likely shut down all or part of the entire port complex for weeks or even months. As of 2014, the Port of Houston and the Houston Shipping Channel facilities supported approximately $629.4 billion of total U.S. economic activity[197] - shutting down part of all of this facility by sinking a ship in the channel would result in massive economic losses in the U.S. and elsewhere, in addition to the environmental damage of leaking oil. The Louisiana Offshore Oil Port (LOOP) sits just eighteen miles off the coast of Louisiana, within easy reach of small craft – it and the Very Large and Ultra Large Crude Carriers that it offloads are also vulnerable to explosive small-boat attacks.

Cushing, Oklahoma, the main oil storage facility in the United States and possibly *the* key node in U.S. pipeline and pumping infrastructure, lies far from any significant law enforcement or counterterrorism help, and presents a perimeter that cannot be secured by local law enforcement. Swarm-style terrorist attacks have overwhelmed big-city law enforcement and counterterrorism units in the recent past (Mumbai in 2008 and Paris in November 2015); a police force as small as Cushing's against a comparable

[197] *The 2014 Economic Impact of Marine Cargo Activity at the Port of Houston on the State of Texas and the United States*, Martin Associates for The Port of Houston Authority, 4 September 2015, p. 4. Accessed 10 February 2017.

number of attackers to those in Mumbai or Paris would find themselves almost at a 1:1 ratio of officer-to-terrorist.

A small group of lightly armed terrorists, as witnessed in the Mumbai 2008 and Paris 2015 terror attacks, are capable of striking multiple targets simultaneously and overwhelming major law enforcement and counterterrorism agencies. The remote location of many of the critical infrastructure nodes examined in this chapter means that, should an attack occur, the necessary help would be far away in both distance and time. Both the Hoover and Glen Canyon dams are located far from urban centers and their large, experienced law enforcement agencies capable of conducting counterterrorism operations. While the ports of Houston and Corpus Christi are located in major metropolitan areas, the maritime nature of an attack might complicate responses by law enforcement. The LOOP is located nearly twenty miles off the coast of Louisiana, a nautical parallel to the remoteness of Hoover Dam. Cushing, Oklahoma is approximately one hour from Oklahoma City. Were terrorists to target any of these facilities with a swarm-style kinetic attack, the attackers could count on significant time delays before an effective counterterrorism response was mustered to confront them.

Economic Damages – Fuel Shortages to Food Shortages

Another key point to consider regarding terror attacks aimed at infrastructure and economic damage, is that it does not take a major loss of valuable commodities in order to trigger significant, if not catastrophic, knock-on effects. Eliminating the ability of the Hoover or Glen Canyon dams to produce electricity would leave millions of people without power – and thereby deprive them of refrigeration, air conditioning, water

pumping, and countless other key services. Were this loss of power to happen in the middle of summer, when much of the American Southwest is experiencing extreme heat, increased fatalities would result due to heat, food spoilage, and lack of water. Without the Glen Canyon electricity supply, because of its grid-surge function, the western power grid would not be able to bring back-up power plants online.

A disruption in the domestic petroleum supply, even if by a few percentage points, would have adverse effects on transportation, power generation, and the larger economy. Higher gas prices would increase transportation costs, which would then increase the costs of the goods being transported. While it is impossible to estimate to what degree gas prices would raise in the aftermath of an attack on key U.S. petroleum infrastructure, prices will rise, with all the attendant knock-on effects that sharp increases in gas prices bring. Historically, there are few examples of civilian populations reacting positively to rapid hikes in gas prices and other goods.

Even if the shortages were to prove relatively short-lived, the terrorists nonetheless would have accomplished a key goal, which was highlighted by Osama Bin Laden back in 2004. By striking a key economic or infrastructure node, the terrorists would force the United States to expend significant finances, effort, and attention in fixing internal infrastructure, economic, and environmental issues resulting from said attack. The financial impact, in turn, would result in reduced U.S. pressure on terrorist activities elsewhere, and provide terrorist organizations with breathing room to recoup, refit, and plan the next section of their campaign.

A Way Forward

While addressing viable counters to each case of infrastructure vulnerability to terrorism exceeds the mandate (and length restrictions) and goal of this chapter, there are two general proscriptions to offer as a means of catalyzing further specific actions.

Hardening Assets

The first counter to a terrorist attack on critical infrastructure is a hardening of current assets. Whether through physical construction, the addition of further security personnel, or a combination of the two, efforts must be made to coordinate the defense and hardening of the weaknesses in key infrastructural assets. Hardening, in turn, will provide the short-term protection necessarily to implement a greater level of resilience in the U.S. energy and environmental sectors, through dispersal.

Asset Dispersal

Looking at the case studies examined in this paper, a key theme is that of concentration. While concentration may facilitate organization and be cheaper, it is also an example of "putting all the eggs in one basket". Despite the significant cost and time required in dispersing key U.S. infrastructure and economic abilities and assets, this will ultimately result in the overall system being far more resilient to any sort of disruption. Smaller losses are easier to weather and recover from in a dispersed system. This will, however, require significant investment and cooperation between private companies and the federal and state governments, which has proven to be difficult in the past.

However, without a widespread implementation of hardening and dispersal of key assets and abilities, there remain significant weaknesses in key nodes of the U.S. infrastructure and economic sectors.

Thesis Conclusion

The overall goal of this thesis is to highlight the vulnerability of U.S. energy and economic infrastructure to a kinetic terrorist attack. Each chapter of the thesis examines a different component of a possible attack arc: using hard-to-detect narco-submarines to infiltrate terrorists and equipment into the United States covertly; the swarm tactics which could be used by smuggled terrorists to effectively carry out an attack against a target; and key transportation and utility infrastructure and economic nodes that a terrorist group could target with a swarm-style attack in order to create significant, long-lasting economic and financial damage to the United States. By exploring the feasibility of each of these assets, ideally this paper will serve as a call to action that will narrow the avenue of a future Black Swan event.

One of the biggest critiques to the overall argument presented in this paper is simply "well, an attack against U.S. infrastructure by terrorists hasn't happened yet". The author would respectfully remind critics that no one considered terrorists weaponizing hijacked airplanes before 9/11 – it was not until nearly three thousand Americans lay dead in New York City, Washington, DC and the Pennsylvania countryside that this "radical" threat received adequate credence. The sheer nature of Black Swan events means that their very concept is by definition outside the Pale and without precedent. As counter to this critique, I would highlight that each individual chapter of this paper provides multiple real-world examples of the chapter's concept – all that is lacking is for someone to link them all together in a real-world operation.

Another criticism, specific to the first chapter, is that there is no evidence that narco-submarines have been used to transport people and equipment as opposed to

narcotics. However, absence of evidence is not evidence of absence; just because something cannot be proven to be happening does not mean that it is not happening. The sheer magnitude of narco-submarine operations and capabilities, and the fact that they *can* transport cargo besides narcotics, represents a glaring hole in U.S. domestic security operations in and of itself. That the same drug trafficking organizations that operate these submarines have longstanding business relationships with Islamic terrorist organizations, and have cooperated with them in the past, should be enough to highlight the magnitude of this particular threat.

Despite the dire picture portrayed in these chapters, there are ways to address these threats. Narco-subs are a threat due to their ability to transport large amounts of cargo, their covert nature, and the fact that they represent a low-risk, high-success means of entering the United States. One way to counter this threat is to adopt a tactic implemented successfully against the Soviets during the Cold War: an underwater listening system to detect submarine traffic. The SOSUS system had resounding success against the Soviet submarine forces, and in a smaller body of water like the Gulf of Mexico, and key stretches of the Atlantic and Pacific coasts, a similar system could prove to be a valuable asset in assisting the Coast Guard and Border Patrol in interdicting more submarines, to the point of making them coast-ineffective for the cartels to operate. Slowing and restricting narco-sub traffic would make narco-subs a less-appealing means of entering the U.S., and thus less attractive to Islamic terrorist organizations looking to insert men and equipment into the U.S.

Larger and more complicated options involve hardening existing weaknesses in the infrastructure nodes explored in this thesis, and creating a more resilient system

overall. Hardening infrastructure can take a number of forms – from additional security personnel, to physical barriers such as walls, fences, and gates – and can be implemented in a relatively budget-conscious manner.

Resiliency would be the harder, more expensive course of action, but ultimately the better one. Resiliency implies to making one particular asset or facility harder to attack and destroy, but in making the entire system more resistant to the shocks of an attack or a key node being taken offline. A specific example of this would be a strategic backstock of key Large Power Transformers, like those in place at Hoover and Glen Canyon Dam. While extremely expensive and physically large and thus difficult to store, having spares would allow for a much faster replacement process, compared to waiting until a transformer breaks or is destroyed to replace it. While the majority of Large Power Transformers are owned and operated by private companies, who are resistant to spending hundreds of millions of dollars on spare transformers that might not be needed, this is a situation where government support and involvement could help offset the costs of production, transportation and storage.

Further examples of resiliency would involve the dispersal of key assets to multiple facilities. While much of the shipping and petroleum industry has been consolidated into a few key facilities – such as the Ports of Houston and Corpus Christ, the Louisiana Offshore Oil Port, and Cushing, Oklahoma – for ease of use and cost-saving measures, this consolidation also means that the loss of one facility would have an inordinately large impact on the rest of the system. Creating multiple facilities, each handling a smaller portion of the workload but capable of handling a "surge" in

requirements would mean the loss of one facility would have a far smaller impact, resulting in less disruption and financial impact.

Addressing the risks illustrated in this thesis will not be easy or cheap. However, the consequences of a successful terrorist attack against a key infrastructure node would likely be far more expensive, and have a far greater negative impact on the public. Some of the solutions will require cooperation between numerous entities, to include federal and state governments and private corporations. However, a holistic and coordinated approach towards hardening existing infrastructure and creating resiliency within the system would go a long way towards reducing the negative impacts of a successful terrorist attack. An added benefit of several of the above counterterrorism suggestions is that, by hardening and dispersing key infrastructure assets, severe weather would have a lesser impact on key infrastructure – hurricanes in the Gulf have threatened port and refining facilities before, and earthquakes in Oklahoma are increasing in frequency and severity. Thus, the government and private corporations could kill two birds with one stone, while fortifying themselves against terrorism and Mother Nature.

One final note: efforts to harden assets will prevent another potential group from disrupting the economic life of the country – domestic terrorists. Many recent lone wolf attacks were "self-radicalized" individuals who never traveled overseas, and in some cases never had direct contact with Islamic terrorists. Domestic terrorists, in many ways, pose as great a threat as those attempting to infiltrate from abroad. Domestic terrorists have no need of narco-submarines and can go straight into swarm mode. Hardening current assets, and building resiliency into key systems, would deprive *all* attackers –

foreign, domestic, and natural – the ability to land a catastrophic strike against key U.S. infrastructure and economic nodes.

Bibliography

"Let's go, we're starting" – a text message discovered on a cell phone belonging to one of the Paris attackers. Contrary to statements made in the aftermath of the attack, the attackers used no encrypted devices or other covert means of communicating. Only simple phrases, sent in the clear. Cyrus Farivar, "Paris police find phone with unencrypted SMS saying "Let's go, we're starting"," Ars Technica, posted 18 Nov. 2015. Retrieved 10 July 2016. http://arstechnica.com/tech-policy/2015/11/paris-police-find-phone-with-unencrypted-sms-saying-lets-go-were-starting/

"Drug Trafficking Interdiction Assistance Act of 2008", introduced in the U.S. Senate 28 July 2008
www.businessdictionary.com

Cushing, OK overview, Census Viewer website. Accessed 5 January 2017. http://censusviewer.com/city/OK/Cushing

Staff, Cushing Police Department website. Accessed 11 January 2017. http://cushingpd.com/staff.html

Lessons from the Mumbai Terrorist Attacks – Parts I and II, Hearing before the Committee on Homeland Security and Governmental Affairs – United States Senate, January 8 and 28, 2009, p. 9. Retrieved 10 July 2016. https://fas.org/irp/congress/2009_hr/mumbai.pdf

Tanker Offloading, LOOP LLC website. Accessed 2 January 2017. https://www.loopllc.com/Services/Tanker-Offloading

Domestic Terminalling, LOOP LLC website. Accessed 2 January 2017. https://www.loopllc.com/Services/Domestic-Terminalling

The 2014 Economic Impact of Marine Cargo Activity at the Port of Houston on the State of Texas and the United States, Martin Associates for The Port of Houston Authority, 4 September 2015, p. 4. Accessed 10 February 2017. http://porthouston.com/portweb/wp-content/uploads/2016/08/National_Economic_Impact_Report_2015.pdf

Mumbai Attack Analysis, N.Y.P.D. Intelligence Division, 4 Dec. 2008, p. 5. Retrieved 10 July 2016. https://info.publicintelligence.net/nypdmumbaireport.pdf

U.S. Joint Forces Command Millennium Challenge 2002: Experiment Report, USJFCOM, 4 Aug. 2002, p. iii. Retrieved 10 July 2016. http://www.dod.mil/pubs/foi/Reading_Room/Joint_Staff/12-F-0344-Millennium-Challenge-2002-Experiment-Report.pdf

Border Surge Report, Texas Department of Public Safety, 24 February 2015. Accessed 31 October 2016. https://www.scribd.com/document/256933420/Border-Surge-Report

PBS interview with LtGen. Paul Van Riper, USMC (ret.), commander of the Red Team during MC02. "The Immutable Nature of War", NOVA interview, PBS, posted 4 May 2004. Retrieved 10 July 2016. http://www.pbs.org/wgbh/nova/military/immutable-nature-war.html

"Cyber Attack on Nation's Critical Infrastructure", *ABC News*, 5 November 2014. Accessed 13 January 2017. http://abcnews.go.com/WNT/video/cyber-attack-nations-critical-infrastructure-26747677

"Bin Laden: Goal is to bankrupt U.S.", *CNN.com*, 1 November 2004. Accessed 10 February 2017. http://www.cnn.com/2004/WORLD/meast/11/01/binladen.tape/

"Waving, Not Drowning". *The Economist*, 1 May 2008. Accessed 12 April 2016. http://www.economist.com/node/11294435

"Mexican Cartels Smuggle Terrorists into U.S. Through Rural Texas Border Region", *Judical Watch*, 29 July 2015. Accessed 22 October 2016. http://www.judicialwatch.org/blog/2015/07/mexican-cartels-smuggle-terrorists-into-u-s-through-rural-texas-border-region/

"Oil Tanker Traffic Jam Off Texas Is Viewed as Sign of Oversupply", *The New York Times*, 11 November 2015. Accessed 29 December 2016. https://www.nytimes.com/2015/11/12/business/oil-tanker-traffic-jam-off-texas-is-viewed-as-sign-of-oversupply.html?_r=0

"Three Hours of Terror in Paris, Moment by Moment", *The New York Times*, posted 15 Nov. 2015. Retrieved 12 July 2016. http://www.nytimes.com/interactive/2015/11/13/world/europe/paris-shooting-attacks.html

"Confidence in Oil Hub Security Shaken By Oklahoma Earthquakes", *NPR Morning Edition*, 30 November 2015. Accessed 7 January 2017. http://www.npr.org/2015/11/30/456777184/confidence-in-oil-hub-security-shaken-by-oklahoma-earthquakes

"SOSUS The "Secret Weapon" of Undersea Surveillance". *Undersea Warfare*, Vol. 7 no. 2 (US Navy). Winter 2005. Accessed 1 March 2016. http://www.navy.mil/navydata/cno/n87/usw/issue_25/sosus2.htm

"Hoover Dam", *History.com*. Accessed 12 December 2016. http://www.history.com/topics/hoover-dam

American Association of Port Authorities, "U.S. Port Ranking By Cargo Volume", 2013. Accessed 3 January 2016.

Wilson Andrews, Larry Buchanan, Haeyoun Park, Alicia Parlapiano, "Unraveling the Connections Among the Paris Attackers", *The New York Times*, 17 Nov. 2015. Retrieved 12 July 2016. http://www.nytimes.com/interactive/2015/11/15/world/europe/manhunt-for-paris-attackers.html

John Arquilla and David Ronfeldt. *Swarming & the Future of Conflict*. Santa Monica, CA. RAND, 2000, p. vii. Naina Bajekal, "The Rise of the Lone Wolf Terrorist". Time Magazine, 10.23.2014. Retrieved 06.19.2016. http://time.com/3533581/canada-ottawa-shooting-lone-wolf-terrorism/

Michael Assante, "America's Critical Infrastructure is Vulnerable to Cyber Attacks", *Forbes.com,* 11 November 2014. Accessed 12 December 2016. http://www.forbes.com/sites/realspin/2014/11/11/americas-critical-infrastructure-is-vulnerable-to-cyber-attacks/#26a3acff6b8a

Associated Press, "Explosion in Alabama shuts gas pipeline, shortages possible", *WTNH.com*, 1 November 2016. Accessed 11 January 2017. http://wtnh.com/2016/11/01/explosion-in-alabama-shuts-gas-pipeline-shortages-possible/

Rand Beers and Francis X. Taylor, "Narco-Terror: The Worldwide Connection Between Drugs and Terror", testimony before the Senate Committee on the Judiciary Subcommittee on Technology, Terrorism and Government Information, 13 March 2002. Accessed 2 March 2016. https://2001-2009.state.gov/p/inl/rls/rm/8743.htm

Cory Bennett, "Critical infrastructure cyberattacks rising, says official", *The Hill*, 13 January 2016. Accessed 13 January 2016. http://thehill.com/policy/cybersecurity/265753-critical-infrastructure-cyberattacks-rising-says-us-official

Peter Bergen and Jennifer Rowland, from the New America Foundation, in an article posted on CNN's website on 08.08.2012. Quote retrieved from the Nuclear Threat Initiative website on 06.18.2016. http://www.nti.org/gsn/article/data-points-home-grown-wmd-terror-threats-experts/

Arthur Berman, "Cushing, Oklahoma is the center of the oil universe", *Business Insider*, 1 March 2016. Accessed 7 January 2017. http://www.businessinsider.com/cushing-oklahoma-is-the-center-of-the-oil-universe-2016-3

Jeremy Bender, "Cartels are using these 'narco-submarines' to move tens of thousands of pounds of drugs at a time", *Business Insider*, 6 April 2015. Accessed 3 March 2016. http://www.businessinsider.com/cartel-narco-submarines-2015-4

Robert D. Blackwill, Peter Chalk, Kim Cragin, Angel Rabasa, et al., *The Lessons of Mumbai*, RAND Corporation, 9 Jan. 2009, p. 9. Retrieved 8 July 2016. http://www.rand.org/content/dam/rand/pubs/occasional_papers/2009/RAND_OP249.pdf

Steve Bowman. *Weapons of Mass Destruction: The Terrorist Threat*. CRS Report for Congress, published 03.07.2002. Retrieved 06.18.2016. http://fas.org/irp/crs/RL31332.pdf

Michael Braun, "Drug Trafficking and Middle Eastern Terrorist Groups: A Growing Nexus?", The Washington Institute, 25 July 2008. Accessed 4 March 2016. http://www.washingtoninstitute.org/policy-analysis/view/drug-trafficking-and-middle-eastern-terrorist-groups-a-growing-nexus

Morgan Brennan and Justin Solomon, "The small US town holding billions in black gold", *CNBC.com*, 7 March 2015. Accessed 5 January 2017. http://www.cnbc.com/2015/03/05/cushing-oklahoma-small-town-is-holding-illions-in-black-gold.html

Bureau of Reclamation, "Glen Canyon Unit". Accessed 20 December 2016. https://www.usbr.gov/uc/rm/crsp/gc/

Bureau of Reclamation "Hoover Dam Frequently Asked Questions". Accessed 20 December 2016. https://www.usbr.gov/lc/hooverdam/faqs/powerfaq.html

Gavin Cameron, "WMD Terrorism in the United States: The Threat and Possible Countermeasures". Published in The Nonproliferation Review, Spring 2000, p. 169. Retrieved 06.19.2016. https://www.nonproliferation.org/wp-content/uploads/npr/cam71.pdf

CNN Wire Staff, "Senator warns of terrorist threat to oil rigs", *CNN*, 13 July 2010. Accessed 11 January 2017. http://www.cnn.com/2010/US/07/13/offshore.rigs.security/

CNN Wire Staff, "Iranian Plot to Kill Saudi Ambassador Thwarted, U.S. Officials Say," *CNN*, Oct. 12 2011. Accessed 6 March 2016. http://www.cnn.com/2011/10/11/justice/iran-saudi-plot/

Kiah Collier, "Houston has the busiest seaport in the U.S.", *Houston Chronicle*, 23 May 2013. Accessed 3 January 2017. http://www.chron.com/discoverhouston/article/Houston-has-the-busiest-seaport-in-the-US-4486844.php

Claudia Copeland, *Terrorism and Security Issues Facing the Water Infrastructure Sector*, Congressional Research Service, 15 December 2010. https://fas.org/sgp/crs/terror/RL32189.pdf

John W. Creswell, "Research Design: Qualitative, Quantitative, and Mixed Methods Approaches", Sage Publications, Inc., Thousand Oaks, CA, 2009.

Edvard Csanyi, "Large power transformer tailored to customers' specifications", *Electrical Engineering Portal Online*, 30 December 2013. Accessed 9 January 2017. http://electrical-engineering-portal.com/an-overview-of-large-power-transformer-lpt

Brett Davis, "Learning Curve: Iranian Asymmetrical Warfare and Millennium Challenge 2002", Center for International Maritime Security (CIMSEC), posted 14 Aug. 2014. Retrieved 9 July 2016. http://cimsec.org/learning-curve-iranian-asymmetrical-warfare-millennium-challenge-2002-2/11640

Department of Energy, *Large Power Transformers and the U.S. Electric Grid*, April 2014 update. Accessed 9 January 2017. https://energy.gov/sites/prod/files/2014/04/f15/LPTStudyUpdate-040914.pdf

Department of Homeland Security, *Energy-Specific Sector Plan 2015*, 2015. Accessed 3 December 2016. https://www.dhs.gov/sites/default/files/publications/nipp-ssp-energy-2015-508.pdf

Department of Homeland Security, *Dams-Specific Sector Plan 2015*, 2015. Accessed 3 December 2016. https://www.dhs.gov/sites/default/files/publications/nipp-ssp-dams-2015-508.pdf

Deputy Chief of Staff for Intelligence, *Critical Infrastructure Threats and Terrorism: Handbook No. 1.02*, 2006. Accessed 12 December 2016. https://fas.org/irp/threat/terrorism/sup2.pdf

Joseph Direnzo, "What the Semi-submersibles Mean: Transnational Gangs, Drugs, and Terrorism", *Defense Media Network*, 12 August 2010. Accessed 9 March 2016. http://www.defensemedianetwork.com/stories/what-the-semisubmersibles-mean/

Sean J. A. Edwards. *Swarming and the Future of Warfare*. Santa Monica, CA. RAND, p. xvii. Retrieved 06.18.2016. http://www.rand.org/content/dam/rand/pubs/rgs_dissertations/2005/RAND_RGSD189.pdf

Adam Clark Estes, "The Feds Can't Catch the Cartels' Cocaine-Filled Submarines", *The Atlantic*, 9 September 2012. Accessed 7 March 2016. https://www.theatlantic.com/international/archive/2012/09/feds-cant-catch-cartels-cocaine-filled-submarines/323833/

Ben Frankel, “Cyber attacks on critical infrastructure reach U.S.”, *Homeland Security News Wire*, 21 November 2011. Accessed 20 December 2016. http://www.homelandsecuritynewswire.com/cyber-attacks-critical-infrastructure-reach-us-bf

Jared Ferris, “Terrorist Attack Shows Vulnerability in Critical Infrastructure”, *The Daily Signal*, 19 February 2014. Accessed 29 December 2016. http://dailysignal.com/2014/02/19/terrorist-attack-shows-vulnerability-critical-infrastructure/

James Fielding, “EXCLUSIVE: Al Qaeda targets oil tankers in Gibraltar”, *The Express*, 26 October 2014. Accessed 11 January 2017. http://www.express.co.uk/news/uk/527524/EXCLUSIVE-Al-Qaeda-targets-oil-tankers-Gibraltar

Carlotta Gall and Thomas de Waal, *Calamity In The Caucasus*, NYU Press, New York City, Kindle edition

Daveed Gartenstein-Ross, “What Does the Recent Spate of Lone Wolf Terrorist Attacks Mean?” for *War on the Rocks*, 27 October 2014. Retrieved 1 August 2016. http://warontherocks.com/2014/10/what-does-the-recent-spate-of-lone-wolf-terrorist-attacks-mean/

Glen Canyon Dam Adaptive Management Program website, "Frequently Asked Questions", 4 April 2013. Accessed 10 January 2017. http://web.archive.org/web/20161126142819/http://www.gcdamp.gov/faq.html

Mark S. Hamm and Ramon Spaaij, *Lone Wolf Terrorism in America: Using Knowledge of Radicalization Pathways to Forge Prevention Strategies*. Indiana State University, February 2015, p. 6.

Simon Henderson, *Al-Qaeda Attack on Abqaiq: The Vulnerability of Saudi Oil*, The Washington Institute, 28 February 2006. Accessed 11 January 2017. http://www.washingtoninstitute.org/policy-analysis/view/al-qaeda-attack-on-abqaiq-the-vulnerability-of-saudi-oil

Andrew Higgins and Adam Nossiter, “’Scene of Carnage’ Inside Sold-Out Paris Concert Hall”, The New York Times, 13 Nov. 2015. Retrieved 12 July 2016. http://www.nytimes.com/2015/11/14/world/europe/paris-attacks.html

ICF International, *Electric Grid Security and Resilience: Establishing a Baseline for Adversarial Threats*, 2016

Mikhail Kashubsky, *A Chronology of Attacks on and Unlawful Interferences with, Offshore Oil and Gas Installations, 1975-2010*, *Perspectives on Terrorism*, vol. 5,

No. 5-6 (2011). Accessed 11 January 2017. http://www.terrorismanalysts.com/pt/index.php/pot/article/view/offshore-gas-and-oil-attacks/html

Peter Kelly-Detweiler, "What We Should Learn From The Attack on Pacific Gas And Electric's Transformer Station", *Forbes*, 10 February 2014. Accessed 10 January 2017. http://www.forbes.com/sites/peterdetwiler/2014/02/10/what-we-should-learn-from-the-attack-on-pacific-gas-and-electrics-transformer-station/#503fc6942fb0

David Kilcullen, *Out of the Mountains: The Coming Age of the Urban Guerrilla*, Oxford University Press, London, 2013. Kindle edition

Tony Kovaleski, Liz Wagner, and Mark Villarreal, "Critical Infrastructure Vulnerable to Cyber Attack, Experts Warn", *NBC Bay Area*, 1 February 2015. http://www.nbcbayarea.com/news/local/Critical-Infrastructure-Vulnerable-to-Cyber-Attacks-Experts-Warn-290370921.html

David Kushner, "Drug-Sub Culture", *The New York Times Magazine*, April 23, 2009. Accessed 7 March 2016. http://www.nytimes.com/2009/04/26/magazine/26drugs-t.html

Christopher Lagan, "Drug Subs 2.0", *Coast Guard Compass*, 13 July 2010. Accessed 8 March 2016. http://coastguard.dodlive.mil/2010/07/drug-subs-2-0/

Rollie Lal, Brian A. Jackson, Peter Chalk, Farhana Ali, William Rosenau, "The MIPT Terrorism Annual 2006", *Memorial Institute for the Prevention of Terrorism*, 2006, p. 26. Accessed 10 February 2017. https://web.archive.org/web/20060824072843/http://www.tkb.org/documents/Downloads/2006-MIPT-Terrorism-Annual.pdf

Terrance G. Lichtenwald, Mara H. Steinhour, and Frank S. Perri. "A Maritime Threat Assessment of Sea Based Criminal Organizations and Terrorist Operations." *Homeland Security Affairs* 8, Article 13, August 2012. Accessed 9 March 2016. https://www.hsaj.org/articles/227

Michael T. McCaul, "A Line in the Sand: Countering Crime, Violence and Terror at the Southwest Border", Congressional Report before Congress, November 2012. Accessed 8 March 2016. https://homeland.house.gov/files/11-15-12-Line-in-the-Sand.pdf

Testimony by Steven C. McCraw, ADOIC-FBI before the Senate Judiciary Committee on 20 May 2003. Accessed 7 March 2016. https://archives.fbi.gov/archives/news/testimony/international-drug-trafficking-and-terrorism

Rolf Mowatt-Larssen. "Al Qaeda Weapons of Mass Destruction Threat: Hype or Reality?". Belfer Center, Harvard. Published January 2010, retrieved 06.18.2016.

http://belfercenter.ksg.harvard.edu/publication/19852/al_qaeda_weapons_of_mass_destruction_threat.html

Rachel Oswold, "Despite WMD Fears, Terrorist Still Focused on Conventional Attacks". Nuclear Threat Initiative website, 04.17.2013. Retrieved 06.18.2016. http://www.nti.org/gsn/article/despite-wmd-fears-terrorists-still-focused-conventional-attacks/

Brendan Nicholson, "US investors fear terror attack on $300B Aussie oil rigs", *news.com.au*, 29 May 2012. Accessed 11 January 2017. http://www.news.com.au/finance/us-investors-fear-terror-attack-on-300b-aussie-oil-rigs/news-story/652efdcb041bb594a868674744b921a9

Rod Nordland and Suadad Al-Salhy, "Extremists Attack Iraq's Biggest Oil Refinery", *The New York Times*, 18 June 2014. Accessed 11 January 2017. https://www.nytimes.com/2014/06/19/world/middleeast/iraqi-oil-refinery-ablaze-as-army-and-militants-clash.html

Norimitsu Onishi and Matthew L. Wald, "Months Later, Sniper Attack at Power Hub Still a Mystery", *The New York Times*, 5 February 2014. Accessed 9 January 2017. https://www.nytimes.com/2014/02/06/us/months-later-sniper-attack-at-power-hub-still-a-mystery.html?_r=0

Paul W. Parformak, "Physical Security of the U.S. Power Grid: High-Voltage Transformer Substations", *Congressional Research Service*, 17 June 2014. Accessed 3 January 2017. https://fas.org/sgp/crs/homesec/R43604.pdf

Jim Popkin, "Authorities in Awe of Drug Runners' Jungle-Built, Kevlar-Coated Supersubs", *Wired Magazine*, March 29, 2011. Accessed 9 March 2016. https://www.wired.com/2011/03/ff_drugsub/

Jim Popkin, "The High Seas", *Slate.com*, 8 Oct. 2013. Accessed 9 March 2016. http://www.slate.com/articles/news_and_politics/foreigners/2013/10/mauner_mahecha_s_drug_submarines_inside_a_high_tech_south_american_narco.single.html

Port of Corpus Christi website, *Liquid Bulk*. Accessed 4 January 2016. http://portofcc.com/capabilities/cargo/liquid-bulk/

Port of Houston website, *Statistics*. Accessed 3 January 2017. http://porthouston.com/portweb/about-us/statistics/

Edited by Byron Ramirez and Robert J. Bunker, "Narco-Submarines: Specially Fabricated Vessels Used For Drug Smuggling Purposes", report written for the Foreign Military Studies Office, 2014. Accessed 9 March 2016.

http://smallwarsjournal.com/blog/narco-submarines-specially-fabricated-vessels-used-for-drug-smuggling-purposes

Byron Ramirez and Robert J. Bunker, "Narco-Submarines: Drug Cartels' Innovative Technology", *Center for International Maritime Security*, 2 August 2014. Accessed 9 March 2016. http://cimsec.org/narco-submarines-drug-cartels-innovative-technology/12314

Byron Ramirez, "Narco-Submarines: Applying Advanced Technologies to Drug Smuggling", Small Wars Journal. Posted 8 March 2014. Accessed 9 March 2016. http://smallwarsjournal.com/jrnl/art/narco-submarines-applying-advanced-technologies-to-drug-smuggling

Eric Randolph & Simon Valmary, "More than 120 people killed in Paris 'terror' attacks". Yahoo! News. *Agence France-Presse,* 13 Nov. 2015. Retrieved 11 July 2016. https://www.yahoo.com/news/least-120-dead-paris-attacks-investigation-source-pta-013205822.html?ref=gs

Steve Reilly, "Records: Energy Department struck by cyber attacks", *USA Today*, 9 September 2015. http://www.usatoday.com/story/news/2015/09/09/cyber-attacks-doe-energy/71929786/

Bruce Riedel, "Modeled on Mumbai? Why the 2008 India attack is the best way to understand Paris", The Brookings Institute, posted 14 Nov. 2015. Retrieved 10 July 2016. http://www.brookings.edu/blogs/markaz/posts/2015/11/14-paris-attacks-mumbai-isis-terrorism-riedel

Claudette Roulo, "Budget Shortfalls Reversing SOUTHCOM Gains, Commander Says", *American Forces Press Service*, March 13, 2014. Accessed 10 March 2016. http://www.globalsecurity.org/military/library/news/2014/03/mil-140313-afps05.htm

Charlie Savage, "Guantanamo Detainee Pleads Guilty in 2002 Attack on Tanker off Yemen", *The New York Times*, 20 February 2014. Accessed 10 February 2017. https://www.nytimes.com/2014/02/21/us/guantanamo-detainee-ahmed-muhammed-haza-al-darbi.html?_r=1

Security Studies Program, *Report: Lone Wolf Terrorism*. National Security Critical Issue Task Force; Georgetown University. 06.27.2015, p. 9. Retrieved 06.19.2016. http://georgetownsecuritystudiesreview.org/wp-content/uploads/2015/08/NCITF-Final-Paper.pdf

William D. Shannon. *Swarm Tactics and the Doctrinal Void: Lessons From the Chechen Wars*. Naval Postgraduate School, 2008, p. 4-9. Retrieved 06.18.2016. http://calhoun.nps.edu/bitstream/handle/10945/4005/08Jun_Shannon.pdf?sequence=3&isAllowed=y

Zain Shauk, “Barge crash blocks access to Port of Houston”, *The Houston Chronicle*, 3 October 2010. Accessed 5 January 2017. http://www.chron.com/business/article/Barge-crash-blocks-access-to-Port-of-Houston-1585545.php

Rebecca Smith, “Transformers Expose Limits in Securing Power Grid”, *The Wall Street Journal*, 4 March 2014. Accessed 20 December 2016. http://www.wsj.com/articles/SB10001424052702304071004579409631825984744

Rebecca Smith, “Assault on California Power Station Raises Alarm on Potential for Terrorism”, *The Wall Street Journal*, 5 February 2014. Accessed 10 January 2017. http://www.wsj.com/articles/SB10001424052702304851104579359141941621778

Sebastian Smith, *Allah’s Mountains: The Battle For Chechnya*, Nov. 2005, Taurus Park Publishing; Akron, OH. Kindle Edition

Laura Smith-Spark and Joe Sterling, “Bloody Algeria hostage crisis ends after ‘final’ assault, officials say”, *CNN*, 23 January 2013. Accessed 11 January 2017. http://edition.cnn.com/2013/01/19/world/africa/algeria-hostage-crisis/index.html

Ian Traynor, "EU ministers order tighter border checks in response to Paris attacks". *The Guardian*, 20 Nov. 2015. Retrieved 12 July 2016. https://www.theguardian.com/world/2015/nov/20/eu-ministers-order-tighter-border-checks-in-response-to-paris-attacks

Khaled Wassef, “UAE: Al Qaeda Responsible for Japanese Tanker Attack”, *CBS News*, 6 August 2010. Accessed 11 January 2017. http://www.cbsnews.com/news/uae-al-qaeda-responsible-for-japanese-tanker-attack/

Cerwyn Williams, “The Threat from Swarm Attacks: Case Studies from the North Caucasus”, published in the *CTC Sentinel*, May 2012, Vol. 5, Issue 5, p. 25. Retrieved 06.19.2016. https://www.ctc.usma.edu/v2/wp-content/uploads/2012/05/CTCSentinel-Vol5Iss56.pdf

Adam Wilmoth, “Gushing Into Cushing: Oil fills major storage hub in small Oklahoma town”, *The Oklahoman*, 2 August 2015. Accessed 6 January 2017. http://newsok.com/article/5437653

Micah Zenko, “Millenium Challenge: The Real Story of a Corrupted Military Exercise and its Legacy”, submitted to *War on the Rocks*, posted 5 Nov. 2015. Retrieved 10 July 2016. http://warontherocks.com/2015/11/millennium-challenge-the-real-story-of-a-corrupted-military-exercise-and-its-legacy/

Micah Zenko, *Red Team: How to Succeed by Thinking Like the Enemy*, Basic Books, New York City, Kindle edition

Curriculum Vitae

Patrick Collman graduated from the University of Colorado in 2009, where he double-majored in History and Secondary Education. He served as an infantryman in the United States Marine Corps from January 2010 to July 2014, and currently works as a contractor for the State Department's Bureau of Counterterrorism.