RE-THINKING MARITIME RISK: LINKING PIRACY, GLOBAL SHIPPING AND PORTS –AND- WHAT CRUISE/FERRY TERMINALS CAN LEARN FROM AIRPORTS

by
Mark I. Kuperman

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

Baltimore, Maryland
December, 2014

Abstract

This thesis addresses two issues related to maritime risk. The first concerns recognizing high-volume shipping destined for U.S. ports initially journeys through foreign waters and ports where crime, piracy and terrorism are hazards. The second issue is prioritizing maritime risk mitigation in response to multi-variable threats and vulnerabilities. This subject is compounded by limited resources and a reliance on collaborative partnerships. The thesis mainly focuses on the relationship between piracy and U.S. maritime interests since piracy has a nexus offshore and in waterways where U.S.-bound ships originate or transit. The approach is three-fold. First, the initial two chapters identify piracy as a threat which shipping encounters in global hot-spots before entering U.S. waters. Chapter 1 associates connections between piracy and terrorism, mariners' safety in regions/waterways, and challenges of eradicating piracy, with a focused study on the Straits of Malacca. Chapter 2 identifies when offshore piracy may threaten the U.S., emphasizing the Gulf of Guinea. Chapter 3 transitions back to U.S. solutions in protecting ferry and cruise passengers within confined terminal spaces.

The thesis results indicate risk-related findings. Chapter 1 highlights collaborative challenges foreign nations need to overcome while trying to protect citizens and eradicate crime/piracy. Also in Chapter 1, the findings reveal piracy and terrorism in the Straits of Malacca do not appear related. Chapter 2 categorizes the types of *offshore piracy* that pose risk to the U.S. Chapter 3 undertakes a multi-variable analysis of inter-modal risk mitigations and suggests certain airport models may work in ferry and cruise terminals.

Thesis Advisors: Sarah Clark, Dr. Jacob Straus, Dr. Sarah O'Byrne

Thesis Readers: Dr. Jacob Straus, Mr. James Norton

Acknowledgments

I would like to thank my wife Christine and my children, Hunter, Liam and Makayla for their support during my time in this academic program. They have been patient and supportive. In addition, each member of the family remains a loyal servant to our nation, uprooting whenever and wherever duty calls. I am also grateful to the United States Coast Guard for funding the expenses and allowing me valuable time to attend this program. Finally, thanks to my parents. They have always encouraged learning and have been by my side through every challenge faced. Mom, if you are watching above… the pursuit of knowledge continues.

Table of Contents

List of Tables

Thesis Introduction

Threats to the maritime environment are unique in their complexity. For example, conceive a scenario in which a 700-foot gas tanker carrying anhydrous ammonia is breached by explosive charges in a congested U.S. port. In addition to burning, suffocating and blinding scores of civilians, the chemical release would overwhelm responders' capabilities and equipment. If the explosion were to occur in a major port, this would entail co-location with a highly populated city. Were the detonation timed to coincide with a passing cruise ship or ferry at peak travel time, thousands of passengers could be affected by the blast or downwind effects. Further, the vessel would be likely owned by a foreign company, typically registered under the flag of yet another country, and generally manned by an assorted crew of foreign nationals. In the last year, this ship may have experienced direct contact with crime or terrorism, potentially evading Somalian pirates or repelling armed robbers in the Straits of Malacca. In the last month, the tanker may have spent several days at anchorage in a third world country's waters while awaiting open pier space, or idled for hours in a queue of ships pending passage through Turkey's Bosporus Strait. These circumstances make the ship highly vulnerable to a shaped charge or limpet mine being attached by divers for time-delay detonation in a U.S. port. In the last week, the ship may have offloaded at three overseas port calls before arriving to the U.S. Each of these foreign ports may have corrupt dock workers or government employees that are amenable to bribes in exchange for allowing radiological or biological contaminants to be loaded onboard. Only a random Customs or Coast Guard boarding with minimal detection gear would stand between detection and destruction in this hypothetical scenario.

As this scenario indicates, shipping is complex, dangerous and transnational. Add in high volume; over 95% of all U.S. imports arrive by ship. Thousands of foreign vessels, many carrying chemicals, gas or fertilizers, arrive in U.S. ports daily. Shipping, by its nature is a risk-laden business. Anti-American sentiment among foreign crews, narco-funded ownership or lax security standards at overseas ports are all vectors for maritime sabotage or terrorism. This thesis does not solve the introductory scenario. Each step that can go wrong is complex and interwoven with other aspects. Security experts also recognize there are finite resources, limited thresholds for delaying cargo and a need to prioritize unacceptable risks. If the scenario is grim and the options for countering the consequences even grimmer, then how does this thesis add value?

The first two chapters begin overseas by examining piracy in foreign locations where U.S.-bound shipping transits. These locales include the Straits of Malacca, one of the busiest shipping lanes on earth, plagued until recent years by hit-and-run pirates, and the Gulf of Guinea, a boon for premium offshore oil. The Gulf entices major petroleum companies to drill offshore for exploration and production. The oil also attracts pirates who steal from the oil rigs, ships and barges; black-market resale is a thriving business for Gulf pirates. Although neither piracy issue is in U.S. waters, each stems back to the scenario in which harming a U.S. port has linkage to a foreign nexus. U.S. maritime risk therefore has roots overseas. The first two chapters' associate piracy with their regional origins, addressing the concerns of states where *offshore* and *choke-point* piracy threaten vessels and crew alike. The linkage between piracy and U.S. risk is a topic that has not been previously well-researched. Nor has the subject of Chapter 3 - the challenge of identifying inter-modal security practices that can work in *both* terminal hubs.

For our purposes, the term risk will be defined throughout the thesis in DHS terminology, where Risk = Threat x Vulnerability x Consequence (TVC). Each of these terms can be weighted according to varying scenarios (i.e. a military base might have low vulnerability to attack, but a high consequence, if successful). Risk in our definition assigns equal value to each TVC-term.

In short, the first two chapters examine facets of piracy that compel risk prioritization based on the overseas nature of shipping and law enforcement/resource-constraints. A first chapter study of the Straits of Malacca raises the question of whether piracy and maritime terrorism are connected and whether targeting one helps extinguish the other. If so, then counter-piracy strategies may offer value as "buy one, get one" for counter-terrorism. In the second chapter, the thesis asks whether the U.S. has risk-concerns related to offshore piracy. To accomplish this, the study uses the Gulf of Guinea, a region where piracy remains a problem. In terms of risk prioritization, piracy off Nigeria may not sound the same alarms as Somalian piracy did, although Nigerian piracy is more aggressive.

The last Chapter of the thesis assesses what is required for risk reduction protocols to crossover from an airport or rail transportation hub to a cruise or ferry terminal. While only the third chapter directly addresses solutions to the challenges posed by the opening scenario, each chapter seeks ways to help prioritize risk and counterbalance resource constraints in a maritime setting. Two Chapters look at issues related to piracy in regions where shipping originates or travels. The third Chapter appraises U.S. ferry and cruise terminals, unique locations where waterborne and shore-based threats converge and thousands of travelers gather.

Using the opening scenario, the thesis examines relationships between maritime risk and security variables that are not obvious, by seeking to define new ways of recognizing and forecasting maritime risk. Piracy for example, affects ships that arrive in the U.S. The final Chapter turns focus towards U.S. airport risk-mitigation procedures, incorporating lessons from established passenger terminal practices. The thesis explores a risk analysis linking U.S. ports to global shipping and searches new methods of applying existing airport security practices to reduce risk passenger ferry and cruise terminals, often directly adjacent to arriving foreign ships.

Chapter 1 Overview

This Chapter examines piracy issues related to perceptions of risk, including a nexus to terrorism. Since shipping has global reach; the U.S. will likely have maritime concerns with piracy if terrorism is associated. The model for the study is the Straits of Malacca. Since shipping destined for the U.S. often must first transit global hotspots, the Straits of Malacca present a strong example of a location that links to U.S. ports. Over 70% of shipping destined for the U.S. transits through this narrow chokepoint, an area that in recent years has suffered piracy.

The literature review considers who Malaccan pirates are, their motivations, and explores any potential nexus between pirates and maritime-based terrorists who also operate in the region. The case study looks at collaborative partnerships in the littoral Straits between Singapore, Indonesia and Malaysia and the types of challenges these proximate nations needed to overcome in attempting to end piracy. An implied analogy to the case study is extracting lessons that may apply to the frequent challenges encountered by federal-state-local partners who also have cultural, jurisdictional and authority issues.

My initial two-fold hypothesis suggests vessels transiting the Straits tend to be safe from piracy and terrorism. In the end, this tends to be true, although the data reveal smaller vessels are still in danger from piracy. The second part of the Chapter's hypothesis affirms that littoral counter-piracy challenges were overcome. This assertion is supported and the methods of overcoming risks from piracy are highlighted.

The case study discovers several key challenges to combatting piracy in SE Asia. Among these are the function and importance of sovereignty, the rejection of U.S. intervention, and the difficulty of verifying the magnitude of piracy when it is underreported or reported inaccurately. In addition, this region offers both hard and soft power approaches from three governments that jointly fight piracy and discourage maritime terrorism from developing.

Chapter 2 Overview

This Chapter addresses the types of situations when offshore piracy might threaten the U.S. Beginning with a hypothesis that gels around energy concerns and harm to U.S. citizens, both the literature review and case study eventually reveal other piracy variables present greater risk to the U.S. The Chapter's research leads to a revised hypothesis that ultimately reflects the importance of European Union imports from the Gulf region, and likelihood of U.S. involvement if American/allied citizens are kidnapped or murdered in this violent environment. The literature also helps typify the motivations and personality types that drawn towards piracy. This profile is cross-compared with Somali pirates, offshore criminals that share certain commonalities with Gulf pirates and differ greatly in other respects. The idea of piracy as 'opportunity' is highlighted as a driving stimulus, especially in the Gulf where limited options exist for other livelihoods.

The Chapter's case study examines a range of factors that might place U.S. interests at risk. These include decreased U.S. and European imports, impacts to multi-national corporations investing in the region, impacts to both coastal and central African states, and kidnappings or murder of ship crews and oil rig personnel. The paper's analysis section matches up the most dangerous piracy character profile (Gulf of Guinea) with internationally-related factors that might threaten or endanger the U.S. These factors are mined and interpreted from data in the case study and examined in a macro-level context. Essentially, this involves looking at piracy-related impacts to the U.S. using a strategic *risk-lens* (i.e. energy impacts, foreign import transitions, Gulf-state profits). In combination with this high-level view, the role of the singular prototypical offshore pirate is addressed. The Chapter combines a top-down perspective (threats to U.S. strategy) with a bottom-up assessment (individual pirate-profile), examining and prioritizing the type of risk conditions in which the U.S. would be likely threatened by offshore piracy.

Chapter 3 Overview

This Chapter focuses on risk-based solutions in the U.S. port environment. This process identifies solutions meticulously, first by scrutinizing transportation security concepts via the literature review. The selected terms embody risk-principles that are already employed by airport specialists and to an extent, by rail security. In the course of this initial evaluation, the following core criteria are deemed as offering highest versatility for inter-modal transportation security: *resiliency, effectiveness, efficiency*, and *risk-layering*. The rationale for selecting these terms is explained in the Chapter, as is their utility in high-volume airports or ferry terminals. In addition, I have coined the term *Human-Technology Interface* (HTI) and used it freely, as HTI implies neither a machine

nor human can accomplish quality security alone. HTI-based models underscore the value of synergizing computer-derived anomalies with on-scene decision making.

The Chapter's hypothesis infers that the airport protocols best suited for maritime passengers meet the five criteria found essential to risk mitigation. Three different types of models are then tested in a case study to determine whether they adhere to these criteria. The models include the British TASS system, Social Force Model and Behavior Detection protocols. Each model is gauged against the five criteria using strict business rules (stated in Methodology).

The case study seeks long-term maritime security solutions that are verifiable as: multi-layered, resilient, efficient, effective and able to fuse technology and human judgment (HTI). This combination suggests even just a few personnel can accomplish quality risk buy-down in even the most congested transportation hubs. The Chapter calibrates solutions using transportation security systems already employed by airports, rather than devising new models from scratch. In the end, the hypothesis suggests that the Social Force Model would be best suited for adjusting to the security demands of a ferry or cruise ship terminal.

To recap, the three thesis chapters are characterized by several underlying maritime risk-related tenets. The first involves finding ways to offset resource limitations and test the boundaries of U.S. risk tolerance for piracy, either as a nexus to terrorism (Chapter 1), or as an impediment to American strategic agenda (Chapter 2). The second risk-related tenet is the idea behind Chapter 3 - the concept of crossover utility. This final chapter suggests certain airport security models can transpose to U.S. ferry and cruise

terminals. There is an opportunity for the terminals to employ airport security concepts already tested and refined since 9/11.

In short, the thesis reveals several noteworthy findings that relate back to the opening scenario. For one, there does not currently appear to be a linkage between piracy and terrorism. This is important since U.S.-destined shipping transits through piracy hotspots. Collaboration is also essential to developing counter-piracy strategies. This was demonstrated in the Straits of Malacca as three nations combined to overcome cultural and geo-political variances. As with the beginning scenario, defining collaboration between local, state and federal partners is vital; there are lessons to be learned from three nations who used both hard and soft power approaches to achieve solutions. On a strategic level, offshore piracy violence indicates there may be a grander threat to the U.S. in terms of piracy's potential to reduce EU oil imports, as this dynamic would affect international relations. Finally, selective transportation security systems appear to offer crossover utility benefits; airports already prioritize transportation hub risk factors.

The introductory emphasis on risk management and limited resources oblige security experts to consider how proven models can work in transportation contexts that serve both air and ship passengers. As discussed in the beginning, eliminating all threat variables is impossible, but incorporating best practices is attainable. Piracy and multi-modal transportation protocols can show maritime risk and security specialists a new way to approach even the toughest scenarios.

Chapter 1

Introduction

In 2000, the International Maritime Bureau (IMB) cited 75 acts of piracy in the Straits of Malacca, a vital shipping connection between the Indian Ocean and the South China Sea. In 2008 and 2009, there were three acts of piracy in the same region.[1] In 2011, IMB cited zero attacks in these Straits.[2] How did this drastic reduction in piracy happen? Did the coordinated efforts of the littoral states (Singapore, Indonesia, and Malaysia) simply reduce piracy and limit terrorism in a region surrounded by water, or did other factors contribute?

The Straits of Malacca are a vital sea lane of communication (SLOC) for global shipping. Over 500 miles long, and yet just more than a mile wide at its narrowest point, these Straits are a slender conduit that supports passage of nearly 30% of world trade each year, and 2/3^{rds} of all liquid natural gas shipping. The Straits see between 50,000 and 60,000 vessels transit annually, making it the most transited route in the world.[3] The Malaccan Straits are also the fastest route from the Indian to the Pacific Ocean. The threat of piracy or armed robbery at sea here has vast implications. For example, the Straits are a maritime chokepoint, a narrow body of water where shipping accidents or an intentional vessel sinking can clog the flow of traffic and shut down the waterway.

Should these Straits be blocked through piracy or terrorism, the repercussions would be severe. In the event of a blockage, ships would require 500 miles further transit

[1] Catherine Z. Raymond, "Piracy and Armed Robbery in the Malacca Strait", *Naval War College Review*, Summer (2009): Vol. 62, No. 3

[2] Oceans Beyond Piracy 2013, http://oceansbeyondpiracy.org/matrix/malacca-strait-patrols Accessed 25FEB2014

[3] Graham Gerard Ong, "The Threat of Maritime Terrorism and Piracy", *Regional Outlook* (2006): 12-5.

to circumvent the region, putting worldwide shipping near full capacity. Unavoidably, this would increase shipping rates and delay global delivery of goods such as coal. This series of events would (in varying degrees) impact world economies.[4] The status of the Straits also has implications for American military force projection and naval mobility. A potential closing of the Straits could compel U.S. Navy battle groups to detour around Australia, adding two weeks transit time, 6,000 additional miles, and $7 million more for every re-route.[5] The Straits, therefore, must remain open.

Based on this background, this chapter asks two difficult questions about piracy. First, and more over-arching, *are piracy and terrorism interrelated?* Using the Straits of Malacca as a point of reference, this is a complex area of the world. Three nations are within immediate proximity of another, surrounded by water, and factious Islamic separatist groups have established roots in this region. It would be easy to cite a linkage to Al Qaeda and declare the Straits are in peril; this is often done with Arab nations where Al Qaeda-affiliates reside. Yet, as a predominantly Muslim region, the littoral states of Southeast Asia present a different socio-political dynamic than the Middle East. In fact, as other global areas have seen terrorism flare in hotspots or even grown insidiously, the Straits have seen a general decline in piracy and maritime terrorism chatter is low. So, can the Straits be judged safe? While it is difficult to tell whether governments' initiatives are working, supplementary factors are at play, or if this is just calm before the storm, the first part of our hypothesis suggests the Straits of Malacca can be declared safe from piracy and largely (by counter-piracy association), safe from

[4] J. Ashley Roach, "Enhancing Maritime Security in the Straits of Malacca and Singapore", *Journal of International Affairs*, Fall/Winter (2005): Vol. 59, No. 1.
[5] Jurg E. Kursener, "Straits of Malacca and Singapore- Unique Chokepoint", *Singapore Focus*, Naval Forces 11/2007

terrorism. The literature review encompasses expert opinions that generally support the fact Indonesia, Singapore, and Malaysia have taken distinct actions that attributed to reducing the frequency of piracy attacks in the Strait, and subsequently, by their effectiveness, threats of maritime terrorism. These actions include multi-national policy agreements, augmented surface/air patrols and even understated methods like outreach to moderate Muslim leaders. In many ways, their triumph is as much about collaborations as it is their operational effectiveness.

Next, *were the littoral SE Asian nations able to overcome underlying challenges in their collaborative effort to reduce threats of piracy and terrorism in the Strait of Malacca?* The hypothesis suggests cultural and geo-proximate challenges involved in counter-piracy were overcome by three distinct nations that are physically proximate, confronted by maritime-based threats along contiguous borders and territorial waters, and compounded by differing state authorities and cultures. The underlying challenges faced by these littoral states requires a case study that hinges on how political, economic, and cultural nuances were overcome by these nations when forming regional strategies.

Lastly, the analysis melds key findings from the literature review and the case study to appraise how differing regional perceptions of piracy and maritime terrorism have led to a variety of best practices that help keep this vital world chokepoint open. As discussed, global shipping eventually turns into American interests when these vessels reach U.S. ports. The literature review incorporates perspectives from academics and maritime professionals, both well-versed in South East (SE) Asian maritime security, to help determine whether piracy, terrorism, both or neither should currently be interpreted as U.S. concerns.

Literature Review

Are piracy and terrorism interrelated? The Straits of Malacca presents the greatest likelihood of a connection and is the focal area of study in this literature review.

By the Numbers

Was piracy ever really a problem in the Straits of Malacca? Ho contends that statistically, piracy has always been a minimal concern, when examined purely by percentages. Even in heavier years of piracy (2000-2005), attacks occurred at a frequency of 0.04% to 0.11% of all shipping that transited through the Straits.[6] These numbers appear small when compared to equivalent crime statistics in most major cities. However, the percentages exponentially surpass the population assault rates (per 100,000 persons) for both Indonesia (.0009%) and Singapore (.00015%),[7] two relatively crime-free nations. Ho's frequency of piracy attacks would seem insignificant when compared to other nations where land-based crime statistics are prevalent.

In the littoral states, however, maritime piracy actually stands out as above-average when compared with assaults. In addition, Ho notes that the vessels attacked in the Straits tend to be trawlers and fishing vessels, far smaller boats than the freight or tanker vessels often associated with piracy. There are two important interpretations that must be made of Ho's study. First, the rates of piracy, while slight, are still higher than the rates of crime on land in these littoral nations (Malaysian rate of assault was unavailable). Second, the types of vessels in question are generally small boats being

[6] Joshua H. Ho, "The Security of Sea Lanes in SE Asia", *Asian Survey*, Vol. 46, No. 4 (July/August 2006), pp. 558-574

[7] NationMaster: *Crime, Assault Rates, Countries Compared.* (2011 data) Accessed from http://www.nationmaster.com/country-info/stats/Crime/Assault-rate

attacked by other little boats; the opinion that very large crude tankers are routinely attacked is a misnomer.

What Makes a Pirate (and potentially, a Maritime Terrorist)?

The fact that large ships are generally not frequently targeted should not deter our scrutiny as to whether piracy or maritime terrorism is cause for alarm. Who these pirates are should be the foremost concern. Ho categorizes the pirates as falling into one of several categories: criminals, gang members, or "armed separatists."[8] To support this view, Ho cites Young and Valencia, who distinguish pirates by their motivation. Piracy, they contend is a financially motivated crime. Terrorists, on the other hand, act based on a religious ideology and/or need to right a perceived wrong. Young and Valencia's view however, does not preclude the possibility that the Malaccan Strait pirates can still be acquiring finances to help fund terrorism, or that the pirates may be either knowingly (or unwittingly) teaching tactics to terrorists for ideological purposes. It also does not speak to the extent of damage that a few small armed boats can accomplish when they swarm or ram vessels, such as Al Qaeda accomplished in targeting the USS Cole and M/V Limburg. Furthermore, despite air and sea patrol initiatives from the contributing nations, it is difficult to distinguish fishermen in the Strait from pirates who appear exactly like fishermen, or from terrorists who also look like fishermen. I do concur with one of Ho's major takeaways, his depiction that "piracy forms the background noise from which maritime terrorist attacks may materialize"[9] clear associates the two, and implies piracy cannot be ignored when assessing maritime piracy in this region.

[8] Ho, "The Security of Sea Lanes in SE Asia", p. 562
[9] Ibid., p. 562

Bad Luck, Followed by Worse Luck

The Malaccan Straits have suffered two significant events in the last 17 years that may have furthered high rates of piracy at the start of this century. First, as Young and Valencia point out, the Asian financial crisis of 1997 not only decimated SE Asian economies, it created political upheaval, particularly in the Indonesian government, the nation from which many of the pirates hail.[10] Since a majority of pirates were originally fishermen by trade, they simply applied their maritime expertise and knowledge of currents, shoals and topography to the more lucrative profession of piracy, especially as supply chains dwindled during the crisis.

Second, the tsunami of 2004 wreaked physical devastation a few years later on the littoral states, particularly in Aceh, Indonesia. Raymond says as many as 70% of the pirates may have originated from this region, an area hit hard by the tsunami. It is unclear whether the tsunami- related population was decimated or a sudden presence of multi-national emergency responders and military aid in SE Asia helped create an environment unfavorable to piracy. Alternatively, the littoral nations' 2004-2005 initiative to combat piracy can be credited with drastically reducing piracy in the region. I contend no one factor is sufficient to understand the decrease of piracy in the Straits of Malacca. Trilateral enforcement efforts were likely reinforced by a rebounding economy. Tsunami-related deaths of pirate leadership weakened pirate gangs. Naval and relief-worker reinforcements in the littoral states also have made piracy increasingly difficult to accomplish. Finally, there were fewer vessels available to attack.

[10] Adam J. Young and Mark J. Valencia, "Conflation of Piracy and Terrorism in Southeast Asia: Rectitude and Utility", *Contemporary Southeast Asia* (2003): Vol. 25, No. 2 (Aug)

Maritime Terrorism: Cause for Alarm?

For academics, maritime terrorism remains a debatable threat. To start, while the Indonesian Al-Qaeda affiliate Jemaah Islamiyah (J.I.) is still actively evaluating future targets, Chalk, for instance, cites that in spite of J.I.'s presence, the "risk of a decisive maritime strike in the Malacca Strait is low."[11] Chalk states that while attack scenarios on LNG and freighters are difficult to achieve, as recently as 2010, a joint Malaysian/Singapore collaboration led to the arrest of 14 J.I. terrorists planning attack in Straits. Clearly, J.I. has not been completely suppressed. The arrests followed a notable May 2009 Al Qaeda communique that declared maritime targets and chokepoints as marked for destruction. Despite these arrests, Chalk argues that in order for a maritime attack to succeed, the terrorists would require fast attack vessels and the target would most likely need to be a ferry, since accessibility to ferries and their vulnerable structural design make them a compelling target. Chalk describes this apparent contradiction by stating the only organization in the region capable of accomplishing this type of attack is J.I., a group with minimal maritime training. Further, Chalk believes J.I. is unlikely to build this skill set now, based on blows to their organizational leadership. Ong tends to agree with Chalk, citing that while Malaysian authorities interrupted a 2001 maritime attack in the Straits and Singapore prevented a similar maritime terrorist plot in 2002, the probability of a maritime attack is not supported by historical data. Ong explains there has only been a 225:1 ratio of land attacks to maritime attacks from 1981-2001.[12] Ho concurs with the low probability of maritime terrorism, stating maritime accounts for approximately 2% of all attacks over the last 30 years.

[11] Peter Chalk, "Assessing the Recent Terrorist Threat to the Malacca Strait", *CTC Sentinel* (2010): Vol. 3. Issue 4

[12] Ong, "The Threat of Maritime Terrorism and Piracy", p. 13

Murphy concurs with both Chalk and Ho, yet for different reasoning. Murphy states that a maritime attack offers low risk reward and contends that "maritime terrorism is not a serious threat."[13] According to Murphy, terrorism at sea requires knowledge of several trade crafts, namely boat handling and attack techniques. In addition, committing terrorism at sea does not compute intuitively into the minds of people who generally live on land. The media is also limited in access to maritime terrorism. The impact of an event at sea is reduced to the few who experience it firsthand, as opposed to targeting media-rich, populated cities. Lorenz concurs, citing "maritime terrorism necessitates considerable overhead, appropriate vessels, mariner skills and, specialist weapons (and) explosive capabilities."[14] Lorenz suggests that terrorist funding, especially in an era where authorities can seize and freeze bank accounts has made terrorist events too expensive and risky to entertain the idea of pursuing an attack that might not work.

Vulnerabilities to Consider

Murphy does cite a major vulnerability for maritime terrorism in SE Asia as the massive archipelago that comprises this stretch of ocean. The volume of small islands offers potential to create "black holes."[15] Murphy references the Niger Delta and Mindanao as other examples of black hole activity.[16] In another article by Chalk, he identifies a vulnerability of the cargo trade system, the concept termed within the industry

[13] Martin N. Murphy, "The Unwanted Challenge", *U.S. Naval Institute Proceedings* (2008), 134, No. 12: 48-51.
[14] Akiva J. Lorenz, "Al Qaeda's Maritime Threat", *Intelligence and Terrorism Information Center, Israel Intelligence Heritage & Commemoration Center* (IICC) 2007.
[15] Murphy, "The Unwanted Challenge", p. 48-51
[16] The term "black hole" infers locales where insurgency is far enough removed from routine government access that terrorism can breed followership, establish training camps and then challenge local government authority.

as "just enough, just in time."[17] This term implies that cargo is delivered globally in such a way that costs to wholesalers, retailers and consumers are kept to a minimum. There are few excess products in a port or distribution chain. Generally, this is a good thing. For those bent on impacting the global supply chain though, this offers opportunity. Fortunately, at least in Chalk's view, disrupting shipping is complicated and untried. He suggests that an event of this type is unlikely as disrupting the supply chain is not sensational, plus oceanic shipping takes place out of public view.

Chalk does cite one noteworthy and differing point of view on this subject - the Aegis Group's 2005 Report on Piracy and Maritime Terrorism,[18] which underscored the severity of impacting the Straits of Malacca, a major sea lane of communication (SLOC). While Lloyd's of London took heed of the report and declared the Strait the equivalent of a war-zone, the littoral states refuted the report, along with any formal connection between piracy and maritime terrorism in the Strait.

Banlaoi sees an association between maritime terrorism and piracy and suspects this dynamic will only continue emerging in the Straits. His view is that "the line between piracy and terrorism [has] blurred in Southeast Asia."[19] Pirates can seize a vessel like terrorists did in seizing commercial aircraft on 9/11, or worse, get aboard a vessel and plant either a weapon or biological dispersion device that can be detonated or released in the next major port. By mimicking pirate techniques, Banlaoi views that maritime terrorists can board and depart a vessel, unsuspectingly planting the seed to cause real

[17] Peter Chalk, "The Maritime Dimension of International Security: Terrorism, Piracy, and Challenges for the United States", *RAND-Project Air Force*. Santa Monica, CA (2008), p. 44
[18] Ibid., p. 55
[19] Rommel C. Banlaoi, "Maritime Terrorism in Southeast Asia", *Naval War College Review* (2005): 58 (4) (09): 63-80.

harm in a populated environment like Singapore or Los Angeles. He cites Abu Sayyaf, a radicalized Muslim terrorist organization's role in the sinking of Superferry 14; Abu Sayyaf reportedly detonated a device onboard. Officials had been watching Abu Sayyaf but did not suspect this group (with a sea-faring background) would execute civilians with this particular attack profile. Banlaoi cautions us not to underestimate the ingenuity of organized littoral-state groups, the parallels between piracy and terrorism, or the infrequency of maritime terrorism, which can lull a false sense of security. Banlaoi states "maritime terrorism in Southeast Asia must prudently be considered no longer a question of if, but rather of when and where."[20]

Clarifying Terms

One of the difficulties in determining whether piracy is truly a problem is interpreting the potentially misleading data sets on piracy. To explain, Bradford describes that piracy may be underreported. Since small fishing vessels are frequently targeted, these local fishermen may well be unaware of International Maritime Bureau (IMB) reporting criteria[21] or the role of the Regional Cooperation Agreement on Combating Piracy and Armed Robbery against Ships in Asia (ReCAAP), a trilateral initiative that also captures piracy data. Vessel owners may also be unwilling to make reports out of fear of reprisal from corrupt local authorities. Plus, there is a financial downside to making a report of piracy/armed robbery. A vessel owner who has already suffered fiscal loss from piracy may be reluctant to suspend their fishing or vessel operations while a formal investigation is completed, and increased insurance rate premiums would only add

[20] Ibid., p. 65
[21] John F. Bradford, "Shifting the Tides Against Piracy in SE Asian Waters", *Asian Survey*, (2008): Vol. 48, No. 3 (May/June), p. 473-491

to their financial burden. For these reasons, Bradford suggests those who suffer piracy unsuspectingly contribute to harming their governments from making sensible anti-terrorism decisions. For example, data that is lacking on piracy attacks only limits governmental justification for future air/sea resource acquisitions and prevents assigning patrols to meaningful locations where piracy and/or terrorism can be thwarted. Bradford also implies that pirates who operate unconstrained make more money and this in turn allows them to acquire better radios, advanced weapons, radar, and other equipment,[22] continuing a vicious cycle. Murphy also describes the situation in the Straits by which Indonesian pirate gangs cross over to Malaysian waters where they rob fishing vessels. Because the pirates do not kill, or generally harm the fishermen, he terms this "sustainable predation… in that the cost and physical danger it adds to the fishermen's lives are never enough to stop them putting to sea completely."[23]

Lastly, one of the greatest challenges in evaluating a maritime terrorism profile of the littoral states is defining the semantics of how piracy differs from terrorism, as well as making a distinction between piracy and armed robbery of a ship. According to International Maritime Bureau (IMB)'s international shipping counterpart, the International Maritime Organization (IMO), piracy takes place on the high seas, while armed robbery occurs within 12 miles of a nation's shoreline. Aside from the noteworthy differences in geographical location, the IMO definitions of these incidents are very

[22] Bradford, "Shifting the Tides Against Piracy in SE Asian Waters", p. 476
[23] Martin N. Murphy, "Suppression of Piracy and Maritime Terrorism*", Naval War College Review* (2007): 60 (3) (Summer): 23-45

similar - both are "illegal acts of violence, committed for private ends."[24] Kim states that "there is no agreed definition of maritime terrorism in international law."[25] This is problematic. As an additional key reference for the ocean-going ships that transit the Straits, the International Law of The Sea Conventions defines piracy but prohibits applying piracy-laws to acts of maritime terrorism. This creates a loophole for maritime terrorists. If caught at sea, it would be difficult to prosecute offenders until piracy or armed robbery statutes can be defined, much less charged against maritime terrorists. Even more puzzling is clearly identifying ownership of the ships that can be exploited for either piracy or maritime terrorism. The flag-state of the vessel is a corporate convention that allows ship-ownership to sail under the 'flag' of a country that is paid for sponsorship. Nincic explains that "a list of countries in which Al Qaeda's vessels have allegedly been flagged illustrates this point: Yemen, Somalia, Senegal, Liberia and St Vincent have all been tied to the 'Al Qaeda navy.'"[26]

The Cultural Variable

One of the unique challenges facing the littoral Malacca Strait nations is the perception as to which parties are responsible for maritime terrorism along the junctures of these Muslim nations. Aljunied points out that the terrorist group and Al Qaeda affiliate J.I. "hopes that maritime states in Southeast Asia will mismanage terrorism as being a 'Muslim problem', thus fuelling hard feelings against the state and other co-

[24] ReCAAP, Definitions and Methodology in Classifying Incidents http://www.recaap.org/DesktopModules/Bring2mind/DMX/Download.aspx?Command=Core_Download&EntryId=290&PortalId=0&TabId=78 Accessed 25FEB2014

[25] Kim, Suk Kyoon, "Maritime Security Initiatives in East Asia: Assessment and the Way Forward", *Ocean Development & International Law* (2011): 42 (3) (Jul): 227-44.

[26] Nincic, "The Challenge of Maritime Terrorism: Threat identification, WMD and Regime Response", p. 634

religionists."[27] In other words, these nations are compelled to be cautious how they publicly state issues of maritime terrorism, treading carefully when attributing blame to a group that may benefit by being blamed. In addition, any show of armed or verbal support from the U.S. would be welcomed by J.I. as "anti-Muslim" propaganda, capable of rallying anti-government sentiments. This apprehension makes it difficult for regional security specialists and littoral states to definitively assert the existence of maritime terrorism without fail-proof evidence. Aljunied illustrates this trepidation benefits up-and-coming prospects for maritime terrorism as the U.S. would hesitate to interfere in this region unless terrorism was confirmed, fearing a rally of anti-Americanism if innocent fishermen or island-based communities were inaccurately vilified.

Hypothesis

This Chapter uses a twofold Hypothesis to assess the success of counter-piracy initiatives and growth of maritime terrorism in the Straits of Malacca. The first question asked is - *Are piracy and terrorism interrelated?* (The Straits of Malacca make an illustrative model for this study). In response, the literature review suggests the first part of the hypothesis is **the Straits of Malacca can be declared safe from piracy (and by association between counter-piracy and counter-terrorism efforts), also declared generally safe from terrorism**. The next question asks - *Were the littoral SE Asian nations able to overcome underlying challenges in their collaborative effort to reduce threats of piracy and terrorism in the Strait of Malacca?* The second half of this Chapter's hypothesis suggests our case study will illustrate that **cultural and geo-proximate challenges involved in counter-piracy were overcome.**

[27]Syed Mohammed Ad'ha Aljunied, "Countering Terrorism in Maritime Southeast Asia: Soft and Hard Power Approaches", *Journal of Asian and African Studies* (2012): 47: 652

Methodology

The objective of the case study is identifying what types of challenges the littoral states encountered when reducing the threat of piracy over the last few years. This includes improving our understanding of whether piracy was ever an issue and how recent upticks in Indonesian piracy should be assessed in a statistically relevant context.

It is also necessary to assess views on piracy and maritime terrorism as a shared concern, particularly where the two subjects may intertwine. Our case study seeks to explain how a reduction in piracy may, as an offshoot, reduce growth prospects for maritime terrorism. Finally, the Chapter identifies whether there are security (or other) measures that should remain consistent in the region if piracy is expected to remain at low levels and for maritime terrorism to remain absent in the Malaccan environment, where global shipping also transits.

Case Study: Strait of Malacca

Were the littoral SE Asian nations able to overcome underlying challenges in their collaborative effort to reduce threats of piracy and terrorism in the Strait of Malacca?

Malacca, there might be a Problem

In June 2005, the Joint War Committee of Lloyd's Market Association, the leading global shipping insurer, had seen enough of piracy in the Malacca Straits. Lloyds declared these Straits "an area in jeopardy of war, strikes, terrorism and related perils."[28] For Indonesia, Malaysia and Singapore; this essentially made the Straits comparable to a

[28] Yun Yun Teo "Target Malacca Straits: Maritime Terrorism in Southeast Asia", *Studies in Conflict & Terrorism*, (2007): 30: p. 541

war zone. The call to action was clear; piracy was being viewed on an internationally economic scale as a serious issue, although the littoral states did not see piracy as an urgent problem. Something needed to be done. In order to make immediate and long-lasting impacts, the SE Asian nations would need to collaborate since the Straits encompass territorial waters of all three littoral states.

Sharing Boats and Planes

Some of the regional solutions took hold immediately. Singapore can be credited with undertaking several proactive enterprises in response to the Lloyd's declaration of the Straits as a war-zone. Without delay, this small nation linked up their three nautical agencies via a Maritime Security Task Force, placed tracking devices on private yachts and smaller vessels (as a protection measure), and adopted standards of the International Maritime Organization (IMO), specifically the International Ship Port Security (ISPS) code. In August 2005, Singapore hosted an international forum that embraced President Bush's Proliferation Security Initiative (PSI).

For Malaysia, Bradford notes this country transitioned from treating piracy and threats of maritime terrorism as a traditionally low national priority to prioritizing these missions as a focal subject.[29] Malaysia created the Malaysian Maritime Enforcement Agency (MMEA), the equivalent of a nationalized Coast Guard. The MMEA was essentially a littoral counter-terrorism initiative because it represented the presence of smaller, faster vessels reliant on law enforcement authority. This was a different tactical capability in the near shore environment than purely relying on a Navy that uses slower

[29]John F. Bradford, "Shifting the Tides against Piracy in Southeast Asian Waters" *Asian Survey*, (2008): Vol. 48, No. 3 (May/June), p. 478, 481

warships and military rules of engagement. To address the full expanse of the Malaccan Straits, the trilateral nations combined to form the Malaccan Sea Patrols. This was a noteworthy trilateral effort on behalf of Malaysia, Singapore and Indonesia to cover the entirety of this waterway, although the pact came with one major jurisdictional issue that will be discussed shortly. While the Sea Patrols had actually been established since 2004, the major upgrade to the Sea Patrols occurred a year later with the addition of "Eyes in the Sky."[30] This program incorporated flights from all three nations' aircraft to conduct surveillance and reconnaissance in the Straits.

In 2006, the Malaccan Strait Patrols (MSP) program debuted, representing a collaborative effort amongst the littorals to link air and sea patrols together more meaningfully than the precursor Malaccan Sea Patrols. MSP (code named MALSINDO) is a prime example of 3 nations working together to not only achieve sea/air coordination, but also to identify practices that were not working and then adapt to improve the process. While most academics agree MALSINDO has shown excellent results eliminating piracy, there are critics. Roach, for example disagrees, stating "unfortunately the patrols appear to have had little success."[31]

Here to Help

Khalid emphasizes that because the three nations of Malaysia, Singapore and Indonesia are termed littoral states, there is a frequent misconception these nations are all aligned in their views on the Malaccan Straits. For Singapore, the Straits are the

[30] Ibid., p. 482. Bradford states the "Eyes in the Sky" program got off to a rough start. Aircraft could not convey information rapidly enough to surface patrol craft to take prompt action against suspect piracy vessels and the aviation units' tasking was not distributed equitably between the involved nations.
[31] J. A. Roach, "Enhancing Maritime Security In The Straits of Malacca And Singapore", *Journal of International Affairs* 59 (1) (Fall 2005): p. 108

economic lifeblood of their small nation, for Malaysia they are a key trade route, and for Indonesia, the Straits primarily represent an issue of sovereignty. Khalid points out these nations are aligned however in their approach to foreign assistance; they do not envision the answer to issues of piracy or terrorism comes in the form of U.S. intervention.[32] The challenge with consulting these littoral nations is an assisting country must factor in 'sovereignty', a notion which is endemic to the political landscape of the region, particularly for Indonesia and Malaysia. Bradford notes that two excellent Japanese concepts, "Ocean Peace-Keeping" and a "Regional Coast Guard" died on the drawing table, as Japan did not factor in sovereignty of the states they intended to aid.

It should be noted that based on its size, Singapore is not as adamant regarding strict loyalty to their maritime borders as Indonesia and Malaysia; Singapore is a long-standing partner to many nations and one of the first countries to have joined the U.S. in the Global War on Terror. Singapore's role in combatting regional terrorism, including the Strait of Malacca, cannot be underscored enough. Singapore is an important U.S. ally both economically for American Multi-National Companies (MNC's) and as a logistical port for the US Navy. In a broader spectrum, Singapore is also a close partner with Australia and Japan. Tan cites the true trilateral relationship in this region may better be defined as Singapore-U.S.-Australia, based on a broad swath of economic and military

[32] Nazery Khalid, "With A Little Help from My Friends: Maritime capacity-building measures in the Straits of Malacca", *Contemporary Southeast Asia: A Journal of International & Strategic Affairs* (2009): 31 (3) (12): p. 425.

support initiatives.[33] In addition, these countries share a consolidated apprehension regarding the rising naval presence of India and China in the Indian Ocean and Straits.[34]

Regionally, Singapore is a vocal leader within the Association of Southeast Asian Nations (ASEAN). This role proved vital in the years following 9/11 when Singapore brought Indonesia and Malaysia into the ASEAN fold, especially once Indonesia saw the reality of Al Qaeda-affiliated terrorism following J.I.'s Bali bombings of 2002 and 2005. More broadly, Singapore's partnership with its neighboring states helped alleviate Indonesian and Malaysian anti-U.S. sentiments; Singapore focused on coalescing positive counter-terrorism initiatives such as the Malaccan Strait Patrols. As Tan paraphrases, "Malaysia has been very aware of the terrorist threat, and has moved proactively to work with Singapore on exploring other measures to improve maritime security."[35]

The littoral states have all benefited from receiving counter-terrorism financing through their ASEAN memberships. Of note, the ASEAN+3 member-countries of Japan and South Korea have made generous financial contributions; the Strait is vital to the economic lifeblood of these nations. As a stakeholder in the Straits of Malacca, 60% of Japan's economic trade flows through this waterway, which includes 90% of Japanese oil imports. The reliance on the Straits has made Japan a vocal consultant and financier of littoral counter-terrorism initiatives.

For the most part though, piracy and potential for burgeoning maritime terrorism has been reduced through the littoral nations' strong internal partnership efforts or

[33] Australia allows Singapore to train extensively on their soil as well.
[34] Andrew T.H. Tan, "Singapore's Cooperation with the Trilateral Security Dialogue Partners in the War Against Global Terrorism" *Defence Studies*, (2007): Vol. 7, No. 2 (June), p. 196-204
[35] Ibid, p. 199

"maritime capacity-building measures", as Khalid terms this coordination. Nincic disagrees with Bradford and Khalid's emphasis on the successful collaboration to date between the littoral nations, stating "the maritime security regime response is still little more than a collection of at best bilaterally coordinated policy responses loosely organized under the (ISPS) code."[36] In fairness, Nincic's view in 2005 predated an opportunity for these littoral states' maritime counter-terrorism measures to be field-tested and eventually, to become well established. For the most part, the maritime capacity building measures have been successful, as illustrated by the decline in piracy and several notable terrorist events (ashore) that were thwarted since collaboration began.

This is not to say that all international efforts to assist with stifling piracy and inhibiting the Straits from becoming a spawning ground for maritime terrorism have been abandoned. For example, the concept of ReCAAP (Regional Cooperation Agreement on Combating Piracy and Armed Robbery against Ships in Asia) is a groundbreaking effort. Originally conceived by Japan in 2001 and later formalized in 2006, ReCAAP receives reports, analyzes information, collates existing intelligence and operationally coordinates through a fusion center to have nations take action, including arrests. Kim states ReCAAP "is the first multilateral framework specifically designed to enhance maritime security and combat piracy and armed robbery in Asia."[37]

Self-Imposed Boundaries

Malaysia and Indonesia send representatives to ReCAAP meetings, but are not considered formal members. Unlu points out these nations request the intelligence offered

[36] Donna J. Nincic, "The Challenge of Maritime Terrorism: Threat identification, WMD and Regime Response", *Journal of Strategic Studies*, (2005): 28:4, p. 619-644

[37] Suk Kyoon Kim, "Maritime Security Initiatives in East Asia: Assessment and the Way Forward", *Ocean Development & International Law* (2011): 42 (3) (Jul), p. 230

by the ReCAAP[38] Information Sharing Center, but remain adamant that other nations' vessels cannot cross over Indonesian/Malaysian territorial boundaries. This has serious ramifications for Indonesia and Malaysia when *hot pursuit* issues arise. Hot pursuit involves gaining consent from an adjacent nation to cross into their territorial seas. This prohibition is well known by pirates who exploit the seams, knowing they can commit a crime in Malaysian waters and then flee to Indonesian waters (or vice versa) since "hot pursuit" prevents law enforcement from crossing borders and the adjacent nation cannot prosecute a crime committed outside their seas.

As another example of the type of challenge created by sovereign limitations in the Straits of Malacca, Admiral Fargo's Regional Maritime Security Initiative (RMSI) was met with strong Malaysian and Indonesian resistance in 2005, when the U.S. Navy suggested assigning forces to the region to help combat piracy. As Mr. Razak, Malaysia's former Deputy Prime Minister, stated, "Let me reiterate Malaysia's position that safeguarding the Straits is a primary responsibility of the littoral states."[39] Rosenberg and Chung point out Malaysia's public-address was not singularly pointed at the U.S. There are other nations such as China and India[40], who have vested interests in the region and possess well-developed Navies that could easily establish long-term presence in the Straits, if allowed or requested.

[38]Dr. Nihan Ünlü, "Current Legal Developments: Straits of Malacca, Protecting the Straits of Malacca and Singapore against Piracy and Terrorism" *International Journal of Marine and Coastal* Law (2006): Vol. 21, No 4, p. 540

[39]Dato' Sri Mohd Najib Tun Haji Abd Razak. "Enhancing Maritime Security Cooperation", *Military Technology* 12/2005

[40] David Rosenberg and Christopher Chung. "Maritime Security in the South China Sea: Coordinating Coastal and User State Priorities" *Ocean Development & International Law*, (2008): 39: 51–68

In a promising gesture, Australia breached the sovereign-hurdle of the trilateral nations who have opted to address piracy and maritime terrorism alone, by requesting to participate in the "Eyes in the Sky" program. In time, Australia's full-fledged contribution may allow other nations to help the littoral countries meet the operational demands of sustaining routine aerial surveillance. Raymond notes that the "Eye in the Sky" program now also allows trilateral aircraft to cross into each other's airspace[41] by including conditions that sponsor representative riders in each other's aircraft. Technically, this arrangement allows planes to cross over *lines* of sovereign airspace since adjacent nations' representatives are on board.

Soft Power and Hard Power Approaches

Aljunied illustrates that within Indonesia, there are two primary Muslim organizations, Muhammadiyyah and Nahdatul Ulama,[42] which spiritually guide 50 million people in this nation. Indonesia has collaborated with these two groups to form a united front for the Global War on Terror. The support from these associations is essential to Indonesia's goal of stopping maritime terrorism from ever developing. By espousing zero tolerance for terrorism, these two moderate Muslim organizations play a significant role as a pulpit for millions of supporters. The Indonesian style of including religious leadership in state-policy represents a *soft-power* approach deemed critical to limiting the growth of maritime terrorism in the littoral Straits.[43]

---

[41]Catherine, Raymond. "Piracy and Armed Robbery in the Malacca Strait", *Naval War College Review* (2009): 62 (3) (Summer): p. 38

[42] Syed Mohammed Ad'ha Aljunied. "Countering Terrorism in Maritime Southeast Asia: Soft and Hard Power Approaches", *Journal of Asian and African Studies*, (2012): p. 657

[43] Recall the earlier discussion on how Indonesia assists some of their outlying, poverty stricken areas, which could theoretically otherwise become *black holes*.

Singapore has taken a different approach to nipping maritime terrorism in the bud. Through their expanded use of the Internal Security Act (ISA), Singapore can detain suspected terrorists without trial.[44] In tandem with Singapore's complete support for the U.S. Global War on Terrorism, this nation has cultivated a fear amongst its population, not only of terrorism, but of even being associated with terrorism. Malaysia has adopted a similar approach. In one instance, Malaysia arrested 70 members of J.I., dealing a crippling blow to maritime terrorism using the ISA as a counter-terrorism policy sledgehammer. Malaysia also suppressed the rise of the Pan-Malaysian Islamic Party (PAS), a radical Muslim opposition party that showed propensity for violence and potential as a maritime terrorist threat. Aljunied states in one instance, Malaysia stemmed PAS' anti-U.S. declarations by "unconditionally"[45] detaining their leadership. In another example, the nation even changed the national Islamic-based educational curriculum, instructing Malaysian children that terrorist views would not be tolerated.

Narrowing the Playing Field

As stated earlier, 50,000-60,000 vessels transit the Malaccan Straits annually. Bateman, Ho and Mathai also cite a 2006 Japanese study of all vessels using the Straits as numbering 93,755 vessels (above 100 gross tons).[46] This is an enormous number of vessels to track and the study includes coastal trade and cross-Strait commerce (rather than transiting through the Strait); it is these smaller near-coastal boats that are often frequented for attack. Bateman and cohorts describe there are essentially three qualities

[44]Aljunied, "Countering Terrorism in Maritime Southeast Asia: Soft and Hard Power Approaches", *Journal of Asian and African Studies,* (2012): p. 659
[45] Ibid., p. 662-663
[46] Sam Bateman, Joshua Ho, and Mathew Mathai. "Shipping patterns in the Malacca and Singapore Straits: An Assessment of the Risks to Different Types of Vessels", *Contemporary Southeast Asia: A Journal of International & Strategic Affairs* 29 (2007): (2) (08), p. 326.

that make a vessel vulnerable to piracy and potentially theft of the vessel itself. These attributes are: height of the freeboard (distance from lowest deck to the waterline), speed of the vessel, and number of crew onboard.[47] With over 32,000 fishing vessels operating from Malaysia, and a similar number from Indonesia, as well as thousands of tug boats, this creates an immense challenge for authorities. Fortunately, the ReCAAP Information Sharing Center (ISC) and the International Maritime Bureau's Piracy Reporting Center track statistics on the types and number of vessels being targeted. For ISC, this information is updated constantly. Attacks are profiled as piracy, armed robbery, or petty theft events. Mariners can be advised and trilateral patrols can be adjusted based on this information. In fact, the ISC (and its counter-part, the Information Fusion Center) have created a handbook[48] for tug-boat operators since tugs are among the highest number of attacked vessels. Included in the handbook are details on how to report an incident of piracy or armed robbery, protect a vessel from attack and even guidelines on planning a safe passage through the Strait.

In addition to information partnerships, the trilateral nations have been receptive to accommodating stricter interpretations of ship and port security in the post-9/11 era. This includes the introduction of International Ship and Port Security (ISPS) regulations which derive from the International Maritime Organization (IMO), the UN Body for international shipping. Gunasekaran states, "The Malaysian government took seriously

[47] Ibid., p. 327. Note: the number of crew onboard can be estimated by pirates based on size of vessel and nature of work they are performing (i.e. fishing, tug/barge, transporting cargo)
[48] ReCAAP, Information Sharing Center Tug Boats and Barges (TaB) Guide http://www.recaap.org/AlertsReports/IncidentReports.aspx Accessed March 28, 2014

the requirement to implement the ISPS Code."[49] Gunasekaran's explanation is telling. Although Malaysia discounted any maritime threats within its borders, this nation wanted to proudly demonstrate they abided international IMO regulations as seriously as all other maritime nations. In addition, "Malaysia [wanted] to demonstrate its determination to defend its security from any form of infringement."[50] In other words, part of Malaysia's rationale for incorporating rigorous maritime security protocols was to impress upon the United States (a major drafter and proponent of the ISPS code) that Malaysia would address piracy and signs of maritime-terrorism on its own. As seen, this viewpoint epitomizes the security posture of the littoral states; these nations will defend safe passage through their waters as strongly as they protect their sovereignty.

Analysis

The Chapter initially asked whether piracy is still a concern in the Straits of Malacca and whether maritime terrorism is, or has been, a cause for worry. When examining statistical data over the last few years, piracy shows decline in the Strait. IMB data revealed zero piracy attacks in 2011. In looking to expert opinions on maritime terrorism, such as Chalk and Murphy, maritime terrorism appears unlikely to become an issue in the littoral states based on insufficiency of highly specialized nautical skill sets and the expenses of purchasing and maintaining boats. In terms of creating a terrorist event that justifies the risk and costly preparations, experts say there is too small a public audience at sea to witness a spectacular attack. Further, Raymond, Ong and Ho have respectively collected historical data that show land-based attacks should merit the bulk

[49] Periasamy Gunasekaran. "Malaysian Port Security: Issues and Challenges", *Australian Journal of Maritime & Ocean Affairs* (Australian Association for Maritime Affairs Incorporated), (2012): Vol. 4 Issue 2 (June), p. 60-63
[50] Ibid., p. 63

of anti-terrorism effort and resources. After all, 98% of recorded terrorism has occurred on land over the last 30 years. In the Strait of Malacca, piracy has dwindled and maritime terrorism is a rarity. While it might appear the threat is minimal, this is exactly why this subject compels further examination. A false sense of security makes a fertile opportunity for piracy or terrorism to emerge.

Getting Past the Numbers

From 2009 to 2013, something unusual happened. For Indonesia, piracy trends appeared to start reversing. Piracy increased nearly 700% over pre-2009 levels.[51] The International Chamber of Commerce, for example, reported through 2014, Indonesia experienced 68 low-level piracy attacks. At first glance, Indonesia's 700% increase seems an overwhelming number. It is not until one recognizes that pre-2009 piracy occurred with single-digit annual frequency that the 700% can be viewed in better perspective. For example, the article on current Indonesia piracy addresses global piracy statistics and is actually titled "Piracy at Sea Falls to Lowest Level in Seven Years."[52] While these numbers sound alarming, these attacks did not occur in the Strait and were primarily against vessels at anchor. Moreover, the attacks were generally conducted by amateur knife-wielding thugs. A 700% increase in piracy attacks is therefore a bit misleading when viewed as an insulated statistic. In fact, there are other misleading piracy statistics. One could conclude that Ho, Ong and Raymond's miniscule statistics on the small percentage of ships attacked in the world's busiest Strait infer piracy is

[51] Allianz Global Corporate and Specialty (2014) "Shipping losses decline, but emerging risks pose serious challenges to marine industry and insurers", http://www.agcs.allianz.com/about-us/news/shipping-review-2014/ Accessed March 21, 2014

[52] International Chamber of Commerce (17OCT2013) "Piracy at Sea Falls to Lowest Level in Seven Years", *ICC Commercial Crime Services* http://www.icc-ccs.org/news/873-piracy-at-sea-falls-to-lowest-level-in-seven-years-reports-imb Accessed April 1, 2014

irrelevant. Conversely, although maritime terrorism is a low-probability, high consequence event, a similar argument prior to this Century can be made regarding aviation-related terrorism. By peeling back a layer on piracy statistics, this brings up the first valuable point when considering piracy in the littoral states. Piracy data should not be trivialized or conversely, over-sensationalized. Instead, it is important to emphasize what may be causing fluctuations in piracy, as seen recently in Indonesia.

For Indonesia, I suggest one of two piracy trends may be taking place. Piracy may simply be getting reported more accurately. If so, an increasing trend in Indonesian piracy supports Bradford's theory on the danger of underreporting piracy. Bradford suggested that pirates may have learned in years past to exploit underreporting by limiting their threshold of violence to low-level assaults in which piracy is often unreported. The result of underreporting has been that criminals become invisible to law-makers, who believe piracy has waned, then decreasing patrols. When reporting is encouraged, a 700% increase in piracy may more accurately be indicating a 700% increase in the *reporting of piracy*. Second, the pirates may be adapting to Indonesian deterrence and detection mechanisms, and learning how to circumvent anti-piracy measures. The more promising answer is that piracy-reporting has improved. The other alternative is piracy may actually be getting worse in Indonesia. It is hard to tell which factor, or both, is at work. Based on statistics alone, a 700% increase in piracy is an arbitrary number until the underlying variables that cause piracy statistics to rise or fall are better comprehended.

A shift in how piracy-statistics are viewed may also compel a comparable shift in how piracy relates to maritime terrorism. For instance, Banlaoi infers there is a danger in

law enforcement and military forces becoming conditioned to piracy. As illustration, if U.S. fishing vessels were attacked 68 times by marauding criminals armed with machetes, there would be a startled, national response to this trend of unprecedented assault and the possibility of terrorism on U.S. soil would not be excluded. For the littoral states, piracy however has become part of the cost of business when conducting trade in a marine environment. For this reason, I would contend that spikes in (non-injurious) piracy may actually be a positive trend. Amplifying levels of piracy compel authorities to re-examine anti-piracy protocols, which in turn means more patrols, increased collaboration and less complacency in the maritime environment, thus reducing prospects for terrorism to propagate.

In addition, Banlaoi also warned of the "blurred" line between piracy and maritime terrorism. Investigating reported incidents of piracy also compels state-authorities to investigate evidence of emerging maritime terrorism. In this sense, increased piracy statistics, even by increased reporting, tend to sustain initiatives that lead to multi-year declines in piracy. Piracy, after all may be amateur thugs seeking a quick marginal profit, or increased piracy could be the flailing attempt of a weakened maritime terrorist organization (i.e. Abu Sayyaf, Jemaah Islamiyah) to finance their maritime attack plans, which as Murphy stated, is expensive.

Soft-Power: a Long-Term Necessity

In addition to the hard science of evaluating what piracy statistics are telling us, there is a social aspect to evaluating how piracy and terrorism can intertwine, if allowed. In this regard, the role of a soft-power approach cannot be overestimated. In response to the "black holes" mentioned by Murphy, Ho states that one of the practices being

employed to reduce black-holes from emerging is Indonesia's appeal to their far-removed pockets of coastal villagers who need help in overcoming desperate levels of poverty. Comparable to Afghanistan, this type of *soft-power* approach persuades loyalties through a provision of food and necessary goods. Since black-holes can be considered the maritime equivalent of Afghani caves, there is triple value in establishing a relationship between state authorities and remote villagers. If piracy is considered a crime-for-profit, then state sponsored assistance provides the commodities which piracy would otherwise purchase, such as food. Additionally, by establishing outreach to black-hole communities, the littoral nations (specifically Indonesia and Malaysia) gain access to remote areas where their humanitarian-aid presence deters maritime terrorism from sprouting in the form of training camps and land-based staging for terrorism.

Lastly, as Aljunied points out, by relying on soft-power cooperation with moderate Muslim leadership, Malaysia and Indonesia capitalized the power of their religious leadership in signalling state-sponsored messaging to the masses. For Indonesia and Malaysia, the reality is local government can be corrupt and state government may be inaccessible. By relying on clerical leaders, these states have channeled communication with their populations through the voice of respected, judicious Muslim organizations who help avert maritime terrorism from forming within, or along their borders.

Dollars and Sense

As Chalk alluded, both piracy and maritime terrorism can impact regional and global supply chains. Piracy can frustrate the flow of cargo by slowing down a ship. This in turn, can slow subsequent ships transiting through the Strait of Malacca who then need to adjust speed to maintain a safe following-distance. Although the impediment to

commerce may be fairly negligible in this case, the impact to "Just enough- Just in Time" cargo flow is largely a by-product of the pirates' criminality, rather than a consciously-sought outcome. For maritime terrorists, disrupting "Just enough- Just in time" may be a very conscious tactic. Impacting, or impeding the Strait of Malacca (if possible) has the potential to tip global cargo economies off-kilter. In this regard, the distinction between maritime terrorism and piracy may be the difference between terrorists who intentionally seek an economic impact as opposed to pirates who may unintentionally affect economies. Either way, the ripple of both piracy and terrorism touches world supply chains, shipping industry and insurers, port scheduling, vessels at anchorage, shore-side trucking, wholesale and retail markets, and ultimately consumer pricing.

As mentioned previously, the majority of piracy impacts smaller vessels transiting the Straits. These include fishing vessels and tug-boats. Bateman, et al. cites that while barge cargo is typically worthless for re-sale (gravel can sell for $9/ton as compared with $20K/ton for electronics carried on a cargo-ship), the tug or barge itself still has value. Tugs are an especially enticing target, considering the ease in which pirates can steal an entire tug, re-paint and then employ the tug elsewhere. Tugs and their barges are far slower than a cargo ship, are less maneuverable, require a handful of crewmembers (typically Indonesian), and have a very low freeboard, making them easy to board. They are in other words, nearly an ideal target. ReCAAP/ISC's *Tug Boat and Barges Guide (TAB) Against Piracy and Sea Robbery* is a well-organized handbook, designed to help protect tugs and barges. In this Chapter's context, the TAB is something more than a manual. The TAB represents information being shared not only among littoral governments, but through data provided by SE Asian (ReCAAP/ISC) and international

tracking mechanisms (IMB). Most valuably, the TAB handbook represents information-sharing between the government(s) and tug operators. The trilateral nations have employed the abilities of their collaborative Information Sharing Center (ISC) to strip out some of the most pertinent data points underscoring piracy statistics. In this case, ISC evaluated piracy-reports, and determined tugs were being targeted in certain locales. The littoral nations then devised outreach to this community of mariners, helping tug operators to help themselves. By reducing not only piracy, but thefts of entire tugs (which can be loaded with explosives and are also difficult to stop), this initiative reduces the threat of maritime terrorism. In many ways, this success story epitomizes the arguments being illustrated throughout this Chapter.

Tugs are not the only vessels that can be repainted and operated again under new ownership. Nincic points out that Al Qaeda has expressed resolve to purchase small ships; this transportation mode would magnify the ability to transport resources and expand their global reach. If Al Qaeda can afford to properly document a vessel, they can also register a ship under a number of available flag-states and routinely sail through the Straits as shipping traffic. Through this tactic, maritime terrorism in the littoral states' region could arrive in the form of *legitimate* shipping. If properly documented, Al Qaeda vessels would be allowed innocent passage through the Straits. This includes carrying any number of cargoes through the most narrow chokepoint areas within the Strait of Malacca. This problem is bigger than the littoral states can address themselves; this is an issue for the International Maritime Organization and International Maritime Bureau. Nonetheless, even suggestion of the Al Qaeda fleet bearing association with the world's most utilized waterway is a topic worthy of mention. The notion infers Al Qaeda vessels

may be allowed safe transit through the Straits under corporate-shell ownership and their *flags of convenience*. In addition, an Al Qaeda owned or operated vessel would not fit neatly under any category of crime or maritime terrorism, posing all the more threat to global shipping through a legitimized concealment of their true identity and purpose.

Sovereignty: an Integral Measure

This Chapter cannot conclude an evaluation of piracy and terrorism issues in the Straits of Malacca without re-emphasizing the importance of sovereignty in this region. Finding ways to ease littoral sovereignty concerns is a step in the right direction for any nation supporting anti-piracy or anti-terrorism initiatives. As observed, the concept of each littoral nation hosting multi-national observers on "Eye in the Sky" flights seems to have eased tensions regarding sovereign issues with airspace. In time, this success-to-date may lead these trilateral states to embrace increased compromise with sea-level enterprises, particularly if surface vessels are eventually allowed to engage "hot-pursuit" measures across territorial boundaries. As can be seen with Admiral Fargo's best intentions for the Regional Maritime Security Initiative, American efforts, especially in the U.S. "shift to the Pacific" must tread lightly. Assisting the littoral-states is likely to be best served in the form of financial assistance, rather than deploying an unwanted carrier group to the region. As Japan learned in the 2000's, even good regional security ideas should be provided to these nations upon request, or through diplomatically-arranged offers such as U.S. willingness to engage in multi-lateral training exercises.

Singapore remains an important player in the delicate balance of SE Asian sovereignty. Singapore has been dually pivotal in creating meaningful security measures alongside Malaysia and Indonesia while arbitrating U.S., Japanese and Australian

regional economic and military interests. In fact, the leadership of Singapore, Australia and Japan has been instrumental in the Straits as a form of protection for US interests. To explain, by predominantly relying on ASEAN and Japanese/Australian initiatives, U.S. Navy presence in the Straits has been restricted. The omission of a U.S. presence has actually limited anti-American sentiments from becoming rampant (and limited opportunity as well for radicalized Islamic elements to develop). The Straits are essential to both American shipping and US-bound global shipping. The fact Singapore can broker key alliances in the littoral nations and referee Japanese/Australian/U.S. agendas offers a vital service to each partner. To an extent, as Gunasekaran demonstrates, the littoral nations have alternatively found ways to patrol and protect their own waters. For example, Malaysia made international maritime security a national priority, while still abiding international maritime security standards such as the U.N.'s International Ship and Port Security (ISPS) Code. In particular, Indonesia and Malaysia's fierce independence have ensured adherence to rigorous maritime security standards (like ISPS), while Singapore has served a vital role mediating on behalf of its neighbors and interceding when first-world powers offer *assistance* that may be viewed by Indonesia and Malaysia as intrusive.

Conclusion

Piracy and maritime terrorism share a common battle space. This does not assume terrorists select identical targets, answer to similar leadership, or exploit the ocean for the same causative rationale as pirates. By the same token, nothing suggests terrorists *do not* do these things. The littoral states have experienced incidents of piracy and terrorism. The borders of Singapore, Malaysia and Indonesia all lay within proximity of another, making it impossible to say with certainty that piracy and terrorism are unrelated. In addition to sharing the waters of the Malaccan Strait, pirates and terrorists share other commonalities. They both seek finances to stay functional, require training, select vessels as targets and share common opposition to law enforcement. That said, the Chapter's first question asked- *Are vessels in the Strait of Malacca safe from piracy?* The answer depends largely on what type of boat you are using, its speed, crew, maneuverability, freeboard, and the waters in which you are sailing. Fishing boats and tugs sailing at night along coastal Indonesia present a greater vulnerability to attack than say, a large crude carrier being closely monitored by Vessel Traffic and transiting in daylight. In general, the studies conclude that larger vessels that do not stop to anchor or idle dockside have predominantly been safe over the last eight to nine years. Smaller vessels tend to under-report and typically support a family, rather than national cargo or fuel needs. In a strategic context, global shipping can accordingly be considered as generally safe from Straits of Malacca piracy. Regional fishermen and near-coastal trade (tugs, barges, and scows) however are not considered safe from piracy.

Is the Strait safe from maritime terrorism? The answer to this question is more complex. Initiatives that address piracy inevitably deter maritime terrorism, or certainly

give terrorists pause before attacking in waters being patrolled and observed by three nations. Maritime terrorism data is scarce and involves complex political agendas. For example, an essential component to keeping maritime terrorism threats low is keeping anti-Western sentiments equally low in the region. As referenced, trilateral coordination, sovereignty, Singapore's relationship with the U.S. and reliance on powerful, moderate Muslim organizations all play a role in keeping America an ally. Terrorists do not need additional reason to substantiate jihad. Acronymically, ASEAN, IMO and IMB, and ReCAAP also support collaboration, regulation and information-sharing as anti-terrorism measures. De-stabilizing J.I. leadership and eradicating black-hole opportunities have contributed to squashing terrorism from developing. As a testament to many initiatives that began in 2004-2005, the littoral nations and the Strait emerged unscathed from the 2009 Al Qaeda communique encouraging jihadists to embrace maritime terrorism. While no region should ever declare itself terrorism-proof, the Straits' safety supports the hypothesis that the Straits of Malacca can be declared safe from piracy and terrorism.

This leads to the Chapter's latter question. *Were the littoral SE Asian nations able to overcome underlying challenges in their collaborative effort to reduce threats of piracy and terrorism in the Strait of Malacca?* First, these nations have shown that multiple geo-political, cultural and sovereign challenges related to counter-piracy and counter-terrorism can be overcome. These challenges have been offset by a variety of state-led practices that collectively provide some worthy lessons learned. Singapore's hardline approach to prosecuting criminals, Indonesia's soft-power cooperation with moderate Muslim leaders, multi-state reliance on ReCAAP, ICC and IMB piracy reports, maintaining Eye in the Sky type-patrols and encouraging tug operators to adopt vigilant

standards have all been part of the answer. The larger takeaway from these trilateral nations in having overcome counter-piracy challenges is that a variety of security options helps avoid complacency and keeps piracy & terrorism off-balance.

It is important to not overestimate the recent infrequency of piracy in the Straits and maritime terrorism in the region. Statistically, 9/11 can be considered an anomaly if evaluating U.S.-based aviation terrorism as a data set. Nevertheless, airport security measures would not be curtailed simply due to the infrequency in which planes fly into buildings. The same philosophy must adhere to shipping that passes through the world's most strategically valuable economic chokepoint. Attacks on the M/V Limburg and USS Cole illustrate the level of damage that even small boats, as pirates tend to favor, can cause when ramming larger vessels. Neither frequency of attack nor delivery methods should be underestimated in a target-rich maritime zone such as the Straits of Malacca.

The most unforeseen finding in this study is the role sovereignty plays in SE Asian maritime security. The littoral nations of Indonesia and Malaysia view their territorial waters as physical extensions of nationalized pride. In terms of piracy, sovereignty remains a challenge as long as criminals are able to exploit boundary-lines. In light of this vulnerability, the littoral nations will need to consistently accommodate sovereignty by devising methods that prevent pirates and future terrorists from using territorial seams as a source of operative advantage. Piracy may be waning regionally and maritime terrorism may be globally infrequent, yet a collaborative regional effort remains essential to countering piracy and terrorism. The collaborative model for the Straits of Malacca needs to dovetail innovative solutions, make prudent use of available resources, incorporate religious-secular leadership, and fuse both soft and hard power-policies.

Chapter 2

Introduction

This Chapter asks the question - when does offshore piracy present a maritime risk to the United States? The subject of African piracy has been previously explored, but this Chapter scrutinizes aspects of offshore piracy that would compel the U.S. to transition from an observer-role to that of a regional participant. While Somalian piracy has not been eradicated, offshore crime levels are a fraction of that seen just two years ago. Contrarily, as of this writing, trends of Gulf piracy occur with a higher frequency and present the more significant threat of African piracy. Thus, this Chapter focuses on West Africa, particularly Nigeria. The variables will be confined to examining where offshore piracy has afflicted Nigeria and other nations within the Gulf of Guinea. The purpose here is to typify features of offshore piracy[53] and then determine which of these attributes present greatest concern to the U.S.

This Chapter conducts a brief comparison of Gulf and Somali pirates to emphasize similarities and distinctions in what drives East vs. West Africans towards piracy. The idea is to initially determine whether offshore piracy emerges from comparable factors and then develops over time as a similar crime pattern. If so, counter-piracy has recently proven successful in Somalia. Can the same strategy apply to the Gulf of Guinea? Setting aside geo-political aspects, counter-piracy initiatives also need to consider the nature of the people involved. Just as counter-terrorism experts would

[53] It is important to distinguish first where piracy occurs, since location plays a role. The emphasis is on offshore piracy, a crime that takes place greater than 12 miles offshore according to international maritime standards. Within 12 miles, the same crime is construed to occur within a nation's waters and is labeled armed robbery. Unlike piracy, armed robbery typically falls under jurisdiction of the state claiming sovereignty of their territorial seas. This distinction will surface throughout this paper.

approach Palestinian terrorists differently than Al Qaeda, the differences between East and West African piracy command distinctive policymaking considerations.

In brief, the Chapter progresses through a review of two piracy-related variables that will help build a base layer for a cohesive analysis. The first variable is embedded in the literature review. This is the question of who these pirates are. Before assessing any methodology on how to stop piracy, it is valuable to understand what makes them start. Pirates' origins are integral to their attraction to this way of life. By association, evaluating those motivations therefore factors into when offshore pirates pose a threat to U.S. interests.

The next variable is addressing which facets of African piracy are potential threats to the U.S. Before the Chapter can distinguish the likely effect of potential threats, it is important to understand what these offshore piracy-related threats are. Several issues may induce the U.S. to respond to offshore piracy. The first is examining the economic threat from piracy. Gulf of Guinea nations may be compelled to diminish exports and potentially see their political stability affected as a result. The next is piracy impacting multi-national corporations (MNC's), several of which are U.S.-based companies with U.S.-citizens as employees. Third, is economic effect on worldwide shipping, including vessel *flag-states* and underwriters. The next group of potential threats from offshore piracy is energy stability. This includes impact to U.S., EU and Central African nations' imports. Fifth and last, is viewing the category of threats associated with piracy-related violence. This includes hijacking-kidnappings and murdering the crew. Piracy violence would oblige important considerations such as whether the victims were Nigerian, U.S. citizens, or foreign nationals. If foreign, are those who are kidnapped or killed from U.S.

allies? Are the U.S. or West African nations able to reason with these offshore pirates, can they be recidivated, or do they need to be targeted as stateless enemies, i.e. ISIL or the Taliban?

This Chapter crafts a snapshot of *people, politics and economic* factors that will help shape a final assessment of when offshore piracy can be expected to affect U.S. security concerns. The Chapter uses two primary categories. The first assesses attributes that are people-related, examining the pirates themselves through a literature review. The second category targets larger macro-political concerns through a case study. This combination is designed to help narrow down what kinds of offshore piracy *tipping points* may threaten the U.S. In short, is it the people who present the offshore piracy threat, the impact they have, or some combination of both?

My initial hypothesis was that the U.S. would engage naval resources or maritime-related policies in the Gulf region only if Nigerian oil interests were threatened. Specifically, this hypothesis stemmed from the preliminary thought that prompted this Chapter - What if offshore piracy actually compels the U.S. to rebalance its' overall energy portfolio? What the Chapter revealed however, is that U.S.-Nigerian energy investments do not seem to be a primary causal factor as to when offshore piracy threatens the U.S. Instead, it finds that other less-apparent attributes of offshore piracy may threaten the U.S. more into considering deployments or instituting policy changes. These characteristics will have a focus.

Literature Review

To begin an exploration as to whether offshore piracy suggests maritime security concerns for the U.S., it is important to first examine the Gulf pirates themselves. Are these individuals' ragtag bandits, insurgents aimed at financing a revolution, budding terrorists, or something else entirely? This literature review will narrow down who is committing Gulf piracy.

Who Becomes a Gulf Pirate?

The ease in which Gulf piracy is carried out has brought Western Africa to a level meriting worldwide attention. Pirates have exploited coastal and offshore environments, legal loopholes, and distinctions in territorial waters. So, who are these Gulf of Guinea pirates? It would be easy to dismiss them as simply exploiting maritime targets via a regional criminal network. Yet, for many Gulf pirates, there is an ideological aspect that traces to Nigeria's checkered ascension as an oil state.

Over the last 60 years, Nigeria's partnership with international petroleum corporations has shaped Nigerian youth to become resentful of perceptions of corporate intrusion and governmental neglect. For starters, the majority of Nigerian citizens have not benefited from oil. Particularly for Nigerians local to the Delta region, Murphy describes this pervasive belief as "gaining nothing from the billions of dollars paid for oil extracted from beneath their feet."[54] The people of the Delta are generally categorized as poor, and at the mercy of stronger Nigerian ethnic clans who control employment prospects. Murphy contends that petro-rich tribes often have access to political positions where they gain favor from offshore mega-deals and use political appointments to secure

[54] Martin N. Murphy, "Petro-Piracy: Oil and Troubled Waters," *Foreign Policy Research Institute* 57, No. 3 (2013), p. 425

kickbacks associated from *bunkering*, a term that describes illegal syphoning from the national oil pipeline. Retired Ambassador Cohen suggests that as an additional factor, the 1999 restructure of Nigeria's constitution helped propel impoverished Nigerians towards oil theft. Specifically, Cohen points out more than 50% of oil revenue were reallocated between 36 Nigerian States, with the coastal states receiving double shares. At first glance this seems like a positive transition. However, in concurrence with Murphy's assessment, Cohen states this profit sharing only amplified that the "people of the Delta (were) earning no benefits in terms of roads, electricity, schools, and clinics despite the extra revenue."[55] The Ambassador takes position instead, that the misallocated shares left an increasingly disgruntled Delta population to dwell in poverty and live in a landscape decimated by oil spills and slicks.

Driven to sea

In fact, due to the environmental ruin of the Delta, the Gulf fishing industry was also devastated. Since Nigeria gained independence from Britain in 1960 (oil was discovered in 1956), and became established as a petro-state, Murphy emphasizes the extent of ruin as "millions (of) tons of oil have spilt; this equates to an Exxon Valdez disaster every year."[56] One of the impacts of this environmental scourge has been depleting a near-coastal fishing industry. This has produced unemployed fishermen who then seek outlets to supplant their deprived livelihood. Their maritime skills often make them, and their children, well-qualified for piracy.

As alluded to, the success of pirates in targeting vessels offshore is born from an aptitude for stealing oil in the Nigerian Delta from the Trans-Niger pipeline.

[55] Herman Cohen, Nigeria: A well-oiled Federation. *Journal of International Peace Operations* (2008), p. 31-2.
[56] Murphy, "Petro-Piracy: Oil and Troubled Waters", p. 425

Predominantly over the last eight years, Kashubsky's data on piracy trends indicates these criminals have simply evolved shallow water *bunkering* tactics to meet the oceanic environment.[57] The addition of transiting tankers in Nigerian territorial waters, Gulf offshore oil exploration, and using tributaries of the Delta to move stolen oil by barge for a secondary resale market all make the region increasingly lucrative for pirates.

The government has shown some culpability regarding their role in environmentally destroying the Delta region. In agreement, both Murphy and Aiyetan describe this recompense took the form of what can be described as a 2009 Nigerian amnesty program that paid 26,000 militant Delta youths to essentially cease their criminal behavior.[58] For a short time, the program seemed promising, including the Movement for the Emancipation of the Niger Delta (MEND)'s pledge to observe a conditional truce. However, the peace was short-lived. The pirates re-organized under new gang nom de plumes, including the Niger Delta Vigilantes and the Niger Delta People's Volunteer Force (NDPVF). These criminal syndicates moved their criminal actions offshore, finding tankers and in recent years, targeting offshore oil platforms.

Getting an early start

More than simply being poor Nigerians, Aiyetan suggests the Gulf pirates are largely comprised of youths, many in their teens. His first-hand insights[59] reveal this stems from a Nigerian practice in the early 2000's in which local politicians, using oil-based fortunes, often hired Delta youths as strong-arm support for their budding

[57] Mikhail Kashubsky, A Chronology of Attacks on and Unlawful Interferences with, Offshore Oil and Gas Installations, 1975–2010. *Perspectives on Terrorism* 5 (2011): 5-6.
[58] Murphy, "Petro-Piracy" p. 426, and Dayo Aiyetan, "Outgunned," *New Internationalist*, No. 465 (2013): 26
[59] Aiyetan, "Outgunned", p. 26

campaigns. Once re-elected, Aiyetan reasons these politicians abandoned the youths, leaving a generation of armed and resentful Delta youth to organize as gangs. These groundswell criminal syndicates found a common ideology and modus operandi, targeting oil workers for kidnappings and stealing Nigerian oil through illegal bunkering of shore-based pipelines[60].

Socio-culturally, there are attributes of the Nigerian youth being attracted to piracy worthy of discussion. For one, children and young men who adopt a mindset that advocates piracy are likely to embrace and foster piracy for decades until arrested, reeducated or eradicated. Second, youth pirates represent an immature, suggestible and *invincible* group of pirates, a dangerous combination. Ukiwo points out many of these youths are of the Ijaw tribe, who having become frustrated with their elders in the 1980's, formed gangs that adopted cultural beliefs in mystical abilities, such as Feibagha Ogbo (immunity to death) and Adelegba Ogbo (resistant to harm from bullets).[61]

Drumbl states that a third of the captured West African pirates are minors. Pirates can claim this status if caught, meaning their sentencing will be less severe; in some cases they are released outright. In addition, these minors often live in the Delta. In a region decimated by oil, few work prospects exist for children.[62] Drumbl illustrates the Nigerian child pirates are typically perceived to be on either ends of the spectrum, being observed as "faultless passive victims—abducted, helpless, and forced into criminal activities—or,

[60] Ibid., p. 26-27
[61] Ukoha Ukiwo, "From 'Pirates' to 'Militants': A Historical Perspective on Anti-State and Anti-oil Company Mobilization among the Ijaw of Warri, Western Niger Delta", *African Affairs*, (2007),106/425: 590, 601
[62] Mark A. Drumbl, "Child Pirates: Rehabilitation, Reintegration, and Accountability", *Case Western Reserve Journal of International Law,* 46, no. 1 (Fall 2013). 235-248

as incorrigible demons."[63] He argues that many child pirates are typically 'tricked' into becoming pirates by adolescent role models or choose piracy of their own volition, often against the wishes of parents or tribal elders. Further, Drumbl states that based on impact to crews and cargo, "child piracy, to be clear, affects Western interests."[64]

In her separate assessment on child piracy, Whitman deduces young pirates are a mechanism for wealthy pirate gang leaders to circumvent legal loopholes, such as U.N. Convention on the Rights of the Child and the Paris Principles, two judicial bodies which favor treating children as exploited child-soldiers rather than criminals.[65] Whitman extends Drumbl's argument that socio-political factors created Nigerian youth piracy. She comments that "it has become recognized in Nigeria that social mobility and the struggle for survival now necessitate the use of violence as society gradually stopped recognizing merit and force became a plausible avenue to the top of the social and economic strata."[66] In this framework, according to Whitman, child pirates can be construed as victims of child labor abuse by the International Labor Organization. Her argument suggests that international advocates for children's rights can actually provide Nigerian juvenile pirates with a convenient 'cover', should the young pirates be captured. Whitman terms this loophole as "catch and release." This ambiguity in the Nigerian legal system can be exploited as a clever ruse to avoid prison time. In the case of young pirates working as indentured crew on pirate vessels, children can be caught and then released directly back to their captors. In both cases, the Nigerian judicial system is primed for failure. "Catch and release" propagates recidivism, child exploitation and a vicious cycle.

---

[63] Ibid., 265-268
[64] Ibid., p. 269
[65] Shelly L. Whitman, "Children and Maritime Piracy," *Case Western Reserve Journal of International Law,* 46, no. 1 (Fall 2013): 219-222
[66] Ibid., p. 225, 233

Somalian Piracy Origins and Somali Child Pirates

As a comparison, Somalia's piracy does not trace to natural abundances of oil or governmental issues of bribes and kickbacks at the expense of a population, as befell Nigeria. Instead, in the absence of a functional Somalian government over the last 23 years, academics point to a variety of other explanations for this nation's piracy. Murphy claims Somalian fishermen under direction of local warlords committed piracy against other countrymen hired to protect foreign vessels fishing in Somali waters.[67] In addition, Murphy's research indicates that also in the 1990's, Puntland, one of the wealthier regions, hired a private British company to help establish a fledgling Somalian Coast Guard. When this initiative failed, the prospective Guardsmen, now well-versed in navigation, formed the original cadre of pirates. Unlike Nigeria, these pirates have primarily kidnapped and ransomed crew members for profit. The emphasis on achieving payment for the sailors, rather than the cargo, is an important distinction. Somali pirates assign more value to the crews' lives as a commodity, as opposed to the Nigerian pirates who see the crew as an obstruction to syphoning fuel for market re-sale. Like Nigeria, both pirates rely on *mother ships* to extend their offshore reach.

In contrast to Murphy's findings, Weir cites two other causal factors for the rise of Somalian piracy. The departure of the UN Peacekeeping Force and naval forces in the mid-1990's coincided with complete governmental collapse. Seeing an opportunity, pirates began taking advantage of both near-coastal trade routes as well as the historical

[67] Martin N. Murphy, "Security Responses to Piracy in Southeast Asia, West Africa and Somalia," *Emirates Lecture Series*, no. 111 (12, 2013): 4

sea-lanes to the Gulf of Aden located farther offshore.[68] Similar to Murphy, Weir cites fishing as having direct linkage to Somali piracy. However, rather than protecting foreign fishing at a protection-fee, Weir states the local fishermen resented the large trawlers who arrived in Somali waters and hauled out massive catches, following Somalia's governmental collapse. Rather than being paid by these foreigners to protect their fishing interests, Weir emphasizes the Somali clans assumed form as an informal Coast Guard, charging 'licenses' to fish and demanding extra payment from uncooperative foreigners.

As far as the types of Somali recruits, Percy and Shortland describe the dynamic of Somalian piracy as "organized - not opportunistic"[69], drawing comparisons to mafia hierarchies that establish a structure for long-term corruption rather than random crime. Organized and opportunistic are terms to be described in more detail shortly, as they are frequently mentioned in describing both Gulf and Somali pirates. Percy and Shortland also refer to Somalian pirates as having the following general qualities: innovation, patience, and a reliance on adhering to an established code-of-conduct in which pirates do not generally rob or kill one another. According to Percy and Shortland, this last attribute of Somali pirates resembles a cultural value found in advanced organized crime syndicates. Similar to Nigerian piracy, the "victims are not members of the community."[70] Also similar to Nigeria, Hansen contends that Somali piracy does not

[68] Gary Weir, Chapter 13 of Piracy and Maritime Crime: Historical and Modern Case Studies, edited by Bruce Elleman, Andrew Forbes, and David Rosenberg, *Naval War College Press*, (2010) Newport Paper 35: 5-7

[69] Sarah Percy & Anja Shortland, The Business of Piracy in Somalia, *Journal of Strategic Studies*, 36:4 (2013): 535-558

[70] Ibid., p. 560

thrive in chaos. Instead, Somalian piracy "emerges in regions where there was a semblance of stability, ideally where governing institutions were weak."[71]

In regards to Somali children being attracted to piracy, Drumbl and Whitman's theories apply largely to Nigeria and Somalia. Drumbl's research has shown that for Somali youth, roughly thirty percent of captured pirates are poor, illiterate youth. To complicate matters, Drumbl argues Somalia does not have a system for birth certificates. This has implications for processing Somalis in an international tribunal if they are caught offshore. Whitman adds that Somali youth have widely available access to light weapons and often come from families where piracy is a livelihood.[72] This is a distinction from Nigerian tribes where tribal elders often frown upon the practice. In addition, Somalia has a strong presence of Al Shabab which poses worry when considering the blurred lines between piracy and terrorism. Whitman accentuates Somalia also has vast minors from which to recruit. Over 50% of the nation's entire population is under 18 years old. In a country where children voluntarily flock to piracy, Whitman states it is "essential that we find mechanisms and solutions to interrupt the cycle of recruitment."[73]

Finally, Gjelsvik and Bjorgo conducted interviews with 16 former Somali pirates. Their research determined the youth often felt obliged to remain pirates, as the social ties from piracy were strong and leaving the pirate gangs made "being accepted back into the society difficult due to stigma and social rejection."[74] In addition, Gjelsvik and Bjorgo discovered an interesting finding amongst recidivated Somali pirates; the economic allure

[71] Stig Jarle Hansen, "The Dynamics of Somali Piracy," *Studies in Conflict & Terrorism* 35, no. 7 (Jul, 2012): 523-530

[72] Whitman, "Children and Marine Piracy", p. 220-221

[73] Ibid., p. 220-229

[74] Ingvild Gjelsvik, Ingvild Magnæs Gjelsvik and Tore Bjørgo, "Ex-Pirates in Somalia: Processes of Engagement, Disengagement, and Reintegration," *Journal of Scandinavian Studies in Criminology & Crime Prevention* 13, no. 2 (12, 2012): 94-114.

of piracy was dominant enough to overcome the taboo of piracy, a practice that is forbidden according to Islam.

Rationalizing piracy

There are two dominant theories regarding the rise of the Gulf gangs into violent organizations such as MEND or NDPVF, the groups affiliated with pipeline attacks and Gulf piracy. The first subscribes to Paul Collier's concept that pirate gangs, both Somalian and Nigerian, tend to profit "not because of the existence of historical and social grievance but because of the opportunities available for them to do well out of war."[75] Collier is suggesting poverty and suppression create an excuse or window for criminal prospects. The second idea argues the opposite; greed is not a central motive. Ukiwo believes "conflicts in Africa are generally rooted in perceptions of political and economic marginalization, social exclusion, and crises of identity and citizenship."[76] Ukiwo's opinion applies to Somali and Nigerian pirates. In addition to greed and dogma, there is another component still missing as explanation. Oil plundering in the Gulf undoubtedly has aspects of greed and social identity as motivators; but there may be another facet. Pirates in both regions might be considering their actions justifiable in the absence of other prospects for legitimate incomes. In other words, had regional oil been equitably distributed in the first place; there may have been no widespread impulse for piracy in the Gulf, nor a black market for oil. For Somalis, the government has provided nothing; gangs and Al Shabab created the opportunities. In fact, the research suggests the

[75] Paul Collier,"Doing Well Out of War: An Economic Perspective" in M. Berdal and, D. Malone (eds. *Greed and Grievance: Economic Agendas in Civil Wars* (Lynne Rienner, Boulder, CO) (2000): 91–112.
[76] Ukiwo, "From 'Pirates' to 'Militants': A Historical Perspective on Anti-State and Anti-oil Company Mobilization among the Ijaw of Warri, Western Niger Delta" (2007): 590

very term *opportunists* may aptly be the incentive that brings both Somali and Gulf youth to pursue the risk and reward of becoming a pirate.

Opportunity - A third theory

The notion of Gulf pirates as *opportunists* surfaces in several journals. Dunn argues that Nigerian pirates are typically dock workers, maritime security employees or fishermen who retain access to opportunities in the form of vessels, information (i.e. ship arrivals) or commodities (such as oil).[77] Further, Dunn postures that opportunists exploit in-port situations where ships are minimally manned or constrained in navigation, i.e. vulnerable to piracy. She considers pirates to be judged as either *opportunists* or *organized*, the latter being a term which implies structure and leadership.

Dunn also cites Gottschalk and Flanagan's definition of pirate opportunity as situations that present "ample targets worth the risk, (offer) acceptable risk of likely detection; and (include) a safe haven in close proximity for support."[78] In nearly lockstep agreement on the terms *opportunist* and *organized* regarding piracy, Tepp describes organized pirates as having the distinction of being "well-funded gangs that carry out attacks against vessels on the high seas as well as in territorial waters, (with) modern weapons, speed boats, advanced means of communications and boarding equipment."[79]

Samatar, Linberg and Mahayni make a different distinction between categorizing the opportunity for Gulf pirates. Their terminology describes pirates in two categories: "a legitimate resistance of local population to the predation of the state and oil companies; -and- criminal entrepreneurial elements which recognize that fortunes could be made from

[77] LCDR Halle Dunn, *Oil Pirates of the Niger Delta* JCSP 35, Canadian Forces College, (date unk.): 24
[78] Ibid., P. 31
[79] Tepp, Eero. The Gulf of Guinea: Military and Non-Military Ways of Combatting Piracy. *Baltic Security & Defence Review* 14 (1) (01) (2012): 187

piracy."[80] In essence, Samatar and cohorts delineate ideology and greed as the major opportunities for offshore piracy.

Finally, in a milestone study on the subject of stolen Nigerian oil, Katsouris and Sayne also cite the term *opportunist*s. They label all participants as involved with Nigerian oil theft, to include land-based criminals and pirates. The distinction they make is labeling pirates as *high-level* or *low-level* opportunists.[81] High-level comprises a status-based control of oil theft operations through *godfather*-type tribal leaders and government bureaucrats. Low-level includes the influence of local, youth gangs. In comparison with Somali warlords who hire young gangs to commit offshore piracy on their behalf, this description aptly fits both Somalian and Gulf piracy.

In all, the research on piracy affords various definitions of *opportunity*. The term *opportunist* appears prevalently in Eastern and Western African piracy. This literature review has melded various interpretations of piracy *opportunity*. While each academic profile offers a contribution in defining the term, the idea is that *opportunity* for youth to seek offshore piracy as a livelihood offers more prospects than greed or profit. There is opportunity to legitimize a cause and promote within a gang hierarchy. In addition, there is opportunity for Gulf pirates to exploit their knowledge of tanker routes/scheduling, naval patrols, shipboard weaknesses, Delta tributaries, and a secondary oil market. For Nigerian pirates, opportunity in all these forms may be a sufficient motivator for piracy. When all other prospects for a legitimate livelihood are absent, Gulf pirates have limited opportunity for alternatives, regardless of the degree of profit, risk, or legality involved.

---

[80] Abdi Ismail Samatar, Mark Lindberg, Basil Mahayni. The Dialectics of Piracy in Somalia: the Rich versus the Poor *Third World Quarterly*, Vol. 31, No. 8 (2010): 1380

[81] Christina Katsouris and Aaron Sayne, Nigeria's Criminal Crude: International Options to Combat the Export of Stolen Oil, *Chatham House* (2013): 6-7

Hypothesis

My hypothesis is that offshore piracy can compel U.S. involvement when certain American interests are threatened. Specifically, these interests include situations in which piracy threatens a balanced national energy portfolio, requires U.S. protection of shipping/oil platforms that support national energy needs, or when piracy endangers U.S. citizens deployed or employed in the region. The rationale is that innately, threats to national interests will trump individual-based threats, such as kidnapping. While threats to the national energy supply would potentially elicit lower media attraction than U.S. citizens being kidnapped by pirates, energy has more significance at the function-of-government level. In addition, the hypothesis suggests the U.S. values importing premium, foreign oil from other (non-North American) markets beyond the Middle East.

The hypothesis also suggests that the U.S. will be prompted to consider modifying protocols or deploying naval forces only when both the actual pirates (as discussed in the literature review) and the extent of their influence (discussed next in the case study) threaten the U.S. In other words, the personal qualities of the pirates and their impact make a difference. For example, aggressive, young and opportunistic pirates in the Gulf region may be more of a pressing concern than Somalian pirates who rely on prolonged negotiations and ransoming crew for profit. Using this logic, Nigerian pirates can threaten American oil interests as well as U.S. citizens working in the region. In Somalia, oil tankers are not syphoned or stolen and the crew's value relies on being kept alive as a bartering commodity. In situations such as the Gulf of Guinea, the hypothesis suggests both energy needs and U.S. citizens may be threatened by offshore piracy.

Methodology

The insights on who becomes an offshore (Gulf or Somali) pirate are useful to understanding the ground-level motivations behind offshore piracy. Pirates, as discussed in the literature review are not universal. In fact, Nigerian pirates appear to threaten both energy demands (through theft) and crew safety (through murder) more than Somalian counterparts. These qualities imply an increased level of personal danger in the Gulf of Guinea, both to those working in these waters and from those committing piracy. This hazard is compounded by the limited timeframe in which the U.S. can respond based on the *hit and run* nature of Gulf piracy. To complement these initial findings, the Chapter next uses a case study examining conditions when offshore piracy might most alarm the U.S. The conclusion merges the socio-based results derived from the literature review with strategic perspective offered by the case study to define when the U.S. is sufficiently concerned to become involved with offshore piracy.

The Chapter incorporates a case study that researches two conditions. First, does offshore piracy in the Gulf of Guinea engender a risk to U.S. security interests?[82] This will be done by integrating findings within the analysis section. These components include a socio-cultural assessment of offshore piracy, based on the literature review, and an effects-based evaluation of offshore piracy, as embodied by a case study. Second, by combining findings from a *top-down* case study and a *bottom-up* literature review, the analysis will expectedly be better balanced and hence, more objective in determining instances when offshore piracy presents a threat to the U.S.

[82] As discussed, the Gulf of Guinea presents the current 'hot-spot' for offshore African piracy. As of this writing, the Gulf offers greatest utility in examining a location for offshore piracy that has not yet been regionally eradicated or assisted by international resources or coalition task forces.

Case Study

The case study examines several potential sources of impact to the U.S. from offshore piracy. Using a focus on the Gulf of Guinea, a region that touches multiple nations' shores, piracy has mainly impacted four countries in general: Nigeria, Benin, Togo and Ghana. The emphasis of Gulf pirate attacks to date has been on Nigeria. It is important to clarify from the onset that there are two different, but related crimes occurring in Nigeria on a routine basis. The first is shore-based oil theft and the second is piracy. Although the focus here is offshore piracy, it is important to distinguish between the two. To put oil theft ashore in perspective, Thinnes states that in the first quarter of 2013 alone, Nigerian oil theft accounted for a 5% loss in total revenue or nearly 100,000 stolen barrels of oil daily.[83] Another 2013 estimate quoted even higher figures. Nigeria's President cited losses of $1 billion a month, which equate to 300-400,000 barrels a day, or 10% of Nigeria's annual oil production.[84] Offshore piracy contributes to these losses, but as evidenced by disparity in these two estimates, it is difficult to calculate how much oil is being stolen due to inconsistent reporting, corruption, and re-distribution of oil on a secondary resale market. While the focus here is on impacts from offshore piracy, Nigeria is clearly facing challenges to theft within the petro-industry, on land and at sea.

Corporate Profits

Having clarified the magnitude of oil theft ashore, but recognizing the focus here is impacts from offshore piracy, the first concern is assessing the hypothesis that U.S. policymakers would consider regional action should piracy threaten a balanced national

[83] Billy Thinnes, "Impact," *Hydrocarbon Processing* 92, no. 11 (11, 2013), 9-12

[84] John Vidal, £1 Billion a Month: the Spiraling Cost of Oil Theft in Nigeria *The Observer*, 05OCT2013 accessed October 1, 2014 from http://www.theguardian.com/global-development/2013/oct/06/oil-theft-costs-nigeria

energy portfolio. The data from U.S. Energy Information Agency (EIA) reports indicates the United States imported 9 to 11% of its' foreign oil from Nigeria in 2002-2011.[85] As of 2013 data, imports had reduced drastically to 4%, meaning Nigeria slid from the fifth highest source of U.S. petroleum imports to eighth. This slip is an economic indicator of instability in the Niger Delta and emerging offshore vulnerabilities. Yet, in mining this data, two verities come to light. For one, the U.S. simply adjusted its' foreign energy portfolio. Second, the decreased Nigerian exports have not impacted Nigerian production. In fact, Nigeria incentivizes deep-water drilling, where offshore piracy occurs. MNC's continue to invest offshore as Nigeria rewards exploratory oil wells based on a depth ratio; the deeper the water, the higher the company profit margin. In other words, the U.S. has backed away from Gulf imports while MNC's have been increasingly enticed to pursue offshore production further from shore. In contrast to decreasing U.S. reliance on Gulf oil, EIA reports Nigerian production in 2011 was 2.13 million barrels/day (bbl/d)[86]; this is an increase of .08 million/bbd over the year prior. Based on this Energy Information Administration data, the U.S. is down-sizing dependence on Nigerian oil while MNC production continues to grow.

Marketwise, the U.S. and Nigeria stand to benefit from a Gulf-reliant U.S. oil portfolio, since Nigerian oil is high quality, and low in sulfur content.[87] Analysts predict that from 2012-2019, the top seven largest oil producing nations in the Gulf will collectively generate $350 billion in oil revenue.[88] Investors, in the form of MNC's have

[85] U.S. Energy Information Administration (EIA) *Nigeria Analysis*, 30DEC2013 http://www.eia.gov/countries/cab.cfm?fips=NI (accessed October 1, 2014)
[86] U.S. Energy Information Administration (EIA) Nigeria Analysis, *Production,* 2013
[87] Damian Ondo Mañe. Emergence of the Gulf of Guinea in the Global Economy: Prospects and Challenges *International Monetary Fund Working Paper*, (2005) WP/05/235, p. 5
[88] Ibid., p. 15

recognized the potential growth in this market, particularly Shell, Exxon-Mobil, Chevron and Total, who communally have nine offshore platforms, slated for nearly 1million bbl/d production by 2016.[89]

Harm to Shipping

In contrast to this offshore growth, experts estimate the cost of piracy to oil investors and shippers' costs over $2 billion each year, based on theft alone.[90] Insurance premiums also continue to surge for oil tankers transiting the region and major oil companies building offshore oil platforms. In 2005, Lloyds of London had seen sufficient insurance claims from Somali-related piracy to re-define how they treated piracy. Instead of viewing acts of piracy as matters related to the ship's hull, Lloyds revised acts of piracy against insured ships, labeling these incidents as "war-risk" insurance.[91] Lloyds has changed the way piracy is viewed by the insurance industry. Losses of entire ships and thousands of barrels in oil cargo make this an unprecedented financial issue for global investors. While the costs of these insurance premiums are likely to be absorbed by consumers, this factor in itself is unlikely to threaten the U.S.

Hurting the Neighbors

Aside from the knowable costs, there are also *inferred losses*. These are instances where the extent of damage may not yet be calculable. For example, the nation of Benin, Nigeria's adjacent westerly neighbor, has already felt economic losses in revenue based on oil-related piracy. A nation that derives 80% of its revenue from oil, Benin cannot

[89] EIA, *Upcoming Oil Projects in Nigeria*, 16OCT2012, revised 30EC2013 http://www.eia.gov/countries/cab.cfm?fips=NI (accessed October 2, 2014)
[90] Scott Baldauf. Next Pirate Hot Spot: the Gulf of Guinea, *Christian Science Monitor*, February 28 2012.
[91] Llewellyn D. Howell, Pirates: Scourge of the Modern Seas, *USA Today* Magazine 134, no. 2732 (05, 2006): 18

afford impacts to their primary export. Whereas a well-established oil nation such as Nigeria may be able to weather the repercussions of a petro-industry rife with piracy and allegations of corruption, Benin will likely not survive as a regional oil producer if piracy frightens off investors. To support this deduction, in the last few years, Benin's major port city, Cotonou, has seen a 70% drop in port calls, based on Gulf of Guinea piracy.[92] Should a promising nation like Benin falter, this would be an unanticipated global consequence of Gulf piracy in terms of impact to U.S. security interests. Instead of a rising West African power, the U.S. would then need to contend with a failing state in a region where crime and terrorism have been insidious when given the chance.

Allies and emerging African nations

As U.S. imports from Nigeria have declined, the European Union (EU) has increased their share. EU now imports 40% of their oil from the region.[93] In addition, Central African nations have developing energy and financial investments in the Gulf. This dynamic reached a zenith in 2013 when the Economic Community of Central African States (ECCAS) joined the Economic Community of West African States (ECOWAS) and the Gulf of Guinea Commission (GGC) in a landmark meeting to address the effects of piracy on oil prices to their emerging nations.[94] Oil is essential to economic growth and piracy slows down production capacity, increases import rates and can create friction, if unresolved, between ECCAS and ECOWAS.

The U.S. can diminish its' own reliance on Nigerian imports based on security concerns, but there are foreign relations concerns that still make the Gulf a significant

[92] Ibid., p. 18
[93] Staff Article, Gulf of Guinea, New Danger Zone, *New African* (526) (2013): 10-14
[94] Adjoa Anyimadu, The Gulf of Guinea: Lessons Learned from the Indian Ocean, *Chatham House, Africa* (2013): 2

factor for U.S. international relations. In short, this predominantly includes consideration of EU reliance on Nigerian oil imports. The Central African states may not represent the coalition alliances the U.S. has established with the European nations, but offshore piracy nonetheless has potential to impact continental enterprises (EU, ECCAS, and ECOWAS) that rely on uninterrupted Gulf oil imports. Although not a direct threat, this dynamic can affect U.S. interests.

A difference in tactics

Anyimadu has found 2 main piracy patterns tend to occur when pirates board oil tankers offshore.[95] First, Gulf-based pirates often violently seize the cargo. This is a stark contrast from Somalian practices. Kidnapping personnel is commonplace, although Gulf kidnappings occur with lower frequency than Somalia piracy and are kept for days instead of weeks or months. Gulf pirates tend to treat victims poorly. Unlike Somalia, where the personnel are ransomed, Nigerian pirates view the crew as an obstruction to stealing the oil. Secondly, the Gulf pirates have become adept at seizing oil cargo and syphoning to another vessel. As an industry practice, this is termed ship-to-ship transfers. Navies and tankers lightering oil routinely conduct these transfers legitimately. Anyimadu has found that skilled pirates can also run through the same oil transfer evolution with minimal delay. The Gulf patterns have potential to raise U.S. concerns. Offshore piracy in this region is violent, and U.S. citizens who encounter Gulf pirates have a higher likelihood (than Somalian piracy) of being killed.

[95] Ibid., 4-17

Offshore Piracy, by the Numbers

In 2012, the Gulf of Guinea experienced 58 cases of piracy. Of these, 27 acts of piracy occurred in Nigerian waters. This number represents a threefold Nigerian increase over the previous year. Further, the International Maritime Bureau (IMB) cited 11 attacks off coastal Nigeria in the first quarter of 2013.[96] This pattern signifies a nearly fivefold increase in piracy attacks compared with 2011. The numbers of piracy attacks against shipping however is slippery. For a variety of reasons, piracy against vessels in the Gulf region may be underreported by as much as 50-80%. In the recorded data collected for all offshore attacks against oil and gas facilities, several Nigerian patterns emerge, particularly for 2004-2010.[97] Over the course of this period, Kashubsky identified 29 different piracy attacks that were directed at offshore platforms alone. These numbers are telling. As discussed, offshore drilling structures represent the future of oil exploration in the Gulf of Guinea as well the newest advances in oil production technology.

For the most part, offshore platform data however is not generally captured the same way as shipping data, which is traditionally collected by the International Maritime Organization (IMO). Piracy data is formally assembled by the International Maritime Bureau (IMB) Piracy Reporting Center.[98] Of the 29 attacks against offshore oil platforms for example, MEND, a Nigerian political group, played a role in nearly all the incidents. In addition to these 29 attacks, there was a higher incidence of murder offshore than

[96] Cristina Barrios, Fighting Piracy in the Gulf of Guinea, Offshore and Onshore, *European Institute for Security Studies*, Brief-Issue 20, May (2013): 1-4

[97] Mikhail Kashubsky, A Chronology of Attacks on and Unlawful Interferences with, Offshore Oil and Gas Installations, 1975-2010 *Perspectives on Terrorism* 5, no. 5-6 (2011).

[98] International Chamber of Commerce, 2014. International Maritime Bureau Piracy Reporting Center (IMB-PRC), Piracy & Armed Robbery News & Figures. Accessed October 3rd, 2014 from http://www.icc-ccs.org/piracy-reporting-centre/piracynewsafigures

attacks against general shipping, as well as a greater trend towards using explosives, and aims to shut-down offshore facility production.

As comparison between Somalia and the Gulf of Guinea, Somalia experienced a height of 237 piracy attacks in 2011 (a total of 15 were recorded in 2013) whereas the Gulf experienced a height of 110 pirate attacks in 2013.[99] This variance does not seem significant enough to warrant coalition efforts in the Gulf such as CTF 151, the EU's Operation Atalanta, or NATO's Operation Shield. Even more fitting a reason why coalition navies would avoid deploying to the Gulf are the kidnapping statistics. At the height of Somalia's kidnappings, this crime occurred 1,016 times in 2010, compared with 32 kidnappings in 2013[100], the worst year for the Gulf. Somalia experienced 30 times the number of kidnappings as the Gulf. For the U.S. and coalition partners, the Somalian kidnappings justify naval deployments, whereas stolen oil in the Gulf has not engendered the same type of coalition response.

Economics it seems is not the driving factor for when the U.S. is most threatened. In fact, as the study has shown, the U.S. simply reduces Nigerian crude imports in response to offshore piracy. For those who would argue that the U.S. might respond if major U.S. owned oil corporations are threatened, this does not seem the case. For example, although diminishing Gulf imports as a U.S. strategy also decreases MNC profit margins, the U.S. reduced Nigerian imports 5% in the last year; this change created a market loss for MNCs.

[99] Government Accountability Office (GAO), Maritime Security: Ongoing U.S. Counter-piracy Efforts Would Benefit From Agency Assessments, GAO-14-422: Published: Jun 19, 2014. Publicly Released: Jun 23, 2014. Accessed October 7, 2014 from http://www.gao.gov/products/, p. 11, 46-47

[100] Ibid, p. 15, 30

Location, location, location

In reviewing this data, at least four of these offshore platforms were in *deep-water* locations. IMB's 2014 assessment in fact warns mariners that "attacks (have been) reported 170 nautical miles (nm) from the coast. Pirates have hijacked vessels for several days, ransacked and looted the crew and ship properties and stolen its cargo, usually gas or oil. Crewmembers have been injured and kidnapped during the attacks. Generally, all waters in Nigeria remain risky."[101] By comparison, using shipping-based statistics, the IMO reported 554 attacks against vessels from 2003-2013.[102] 80% of these *piracy* attacks on vessels occurred in states' territorial waters (within 12nm), while 20% were in international waters. These numbers are troubling in a couple of regards. Chris Trelawney, the IMO Director for maritime security, cites that within 12(nm) of a nation's shore, piracy is technically considered armed robbery. Only when a vessel gets beyond the nation's territorial seas does an attack on a ship or offshore oil platform constitute piracy. For major oil companies, this could be an important distinction dependent on where the oil fields are located and where drilling operations are being conducted in relation to a nation's territorial seas. The issue therefore draws less international attention when the volume of offshore piracy is veiled under the guise of *armed robbery*. In addition, the U.S. cannot respond to the 80% of these incidents without permission of the coastal state in whose territorial seas they occur. Doing so would cause more grave consequences for international relations than any damage caused by piracy itself. The

[101] IMB-PRC, Piracy & Armed Robbery Prone Areas and Warnings Accessed October 3, 2014 from http://www.icc-ccs.org/piracy-reporting-centre/prone-areas-and-warnings

[102] Chris Trelawny, Piracy in West Africa: A Symptom of Wider Problems? *New African*, No. 526 (2013): 16-21

implications of coastal-water attacks differ from the rules of intervention-at-sea (>12 nm), when piracy occurs on the high seas. The pirates know this distinction.

Another international legal aspect is United Nation Security Resolutions 2018 (2011) and 2039 (2012)[103] that specifically address the Gulf of Guinea issue of offshore piracy. While these initiatives emphasize regional security, they place a vested UN interest in the Gulf, making it difficult for the U.S. to respond to piracy incidents without first attaining UN approval.

Resource Limitations

Although at-sea piracy typically involves use of naval forces, rather than traditional shore-based military and police, Gulf navy resources are limited. Nigeria boasts the largest Gulf Navy, yet this includes one corvette and one fast frigate.[104] Ghana added six new offshore patrol vessels, but the odds are in the pirates' favor; they can choose to attack knowing limited navies cannot react in time. In some cases, as reported through first-hand data collected by Kashubsky, pirates even brazenly attack the navy boats. A speedboat attack near Port Harcourt, Nigeria, resulted in pirates killing nine Nigerian sailors. In another pirate attack against the Shell *Forcados* terminal, a military gunboat was shot and sunk with 25 military personnel onboard.[105] Complicating the inability of Gulf governments to halt piracy is a lack of organized Gulf state coast guards becoming adept at the anti-piracy mission. As opposed to navies, Coast Guards rely on smaller, faster patrol boats to aid in chase situations and shallower waters. In addition,

[103] United Nations Security Council 2014, Security Council Resolutions, Accessed October 3rd 2014 from http://www.un.org/en/sc/documents/resolutions/index.shtml
[104] Staff Article, *Gulf of Guinea, New Danger Zone*, p. 12
[105] Kashubsky, A Chronology of Attacks, Accessed September 30, 2014 from http://www.terrorismanalysts.com/pt/index.php/pot/article/view/offshore-gas-and-oil-attacks/html

nations use coast guards to enforce their law enforcement authorities instead of relying exclusively on naval rules of engagement, a system of regulations designed for combat.

For the U.S., offshore piracy has the potential to compel American involvement in the absence of regional navies, but only if assistance is requested by Nigeria or ECOWAS nations. The presence of armed U.S. gunships off several African coastlines could create the likelihood of conflict and polarize anti-American sentiments should military intervention lead to killing Nigerian youth pirates. As previously mentioned, while offshore oil production attracts deep-water investors it also equates to American MNCs who may be placing their employees and energy platforms in harm's way. This situation has potential to threaten the U.S. by compelling military action against violent, young pirates should U.S. citizens be kidnapped or killed.

Harming the industries that support Gulf oil

A logistical impact from piracy is on the industries that support oil extraction in the Gulf of Guinea. For instance, offshore supply vessels (OSV's) provide a critical linkage between shore-based necessities and the rigs; these 150-300 foot vessels are often the lifeline for food, transport, cargo and technical necessities required to sustain the offshore drilling platforms. OSV's present a relatively easy target for pirates in two regards. First, these vessels cannot keep up with the speed of pirate speedboats and their freeboard (height from deck to water) makes them far easier to board at sea than an oil tanker. Second, pirates who are privy to insider information can use an OSV to deliver pirate crews to unwitting oil rig personnel on offshore platforms. Hijacked OSVs also have the range to utilize deep-water *mother ships* as a staging platform, thus eluding shore authorities by basing from sea. Lastly, OSV's are often manned by multi-national

crews, making kidnappings a complex political situation.[106] The U.S. would likely not be threatened by an OSV hijacking, but their extensive offshore range and linkage to mother-ships would be a consideration if deploying future counter-piracy task forces.

Offshore rigs and uniquely designed floating platforms called Floating Production Storage and Offloading (FPSO) units are also susceptible, stationary targets. These platforms are attached to the ocean floor, operate offshore and are poorly designed to repel attackers or provide workers with a defensible platform. These massive floating installations have been attacked on at least five reported occasions from 2004-2010.[107] FPSO *Mystras* has been subject to offshore piracy three times and FPSO *Bonga* was subject to a MEND attack in 2008. Unlike ships transiting off Somalia, FPSO's cannot easily increase speed, change course, repel invaders or find a different route. The U.S. would not feel directly threatened by piracy attack on an FPSO, although at an individual cost of $700-800 million dollars[108], destruction of these easy targets could alter global oil prices. Second, the FPSO attaches to subsea wellheads. Hijacking an FPSO and tearing an injection line to these wellheads could cause an environmental disaster.

Official U.S. Stance(s) on Gulf of Guinea Piracy

The formal U.S. position regarding offshore Gulf piracy is complicated. The White House has implied their stance, the U.S. State Department has established an economic working group, and the U.S. Africa Command (AFRICOM) has formally

[106] Barbara Starr, Catherine E. Shoichet. 2 Seized in Pirate Attack off Nigeria, *CNN* (25OCT2013) http://www.cnn.com/2013/10/24/world/africa/nigeria-vessel-attack/ (accessed October 2, 2014)
[107] Kashubsky A Chronology of Attacks, Accessed October 4, 2014 from http://www.terrorismanalysts.com/pt/index.php/pot/article/view/offshore-gas-and-oil-attacks/html
[108] FPSO World Fleet, FPSO Info. Accessed October 4, 2014 from http://www.fpso.net/page7.html

defined their position on Gulf piracy. It is fitting to include consideration of these variables in our discussion of when the U.S. may be threatened by Gulf piracy.

In 2012, the U.S. State Department established the Gulf of Guinea Working Group (GoG) in coordination with commercial shipping representatives.[109] The GoG was deemed necessary by the Overseas Security Advisory Council (OSAC), a State Dept. body that establishes public-private partnerships on a case-by-case basis. By creating the GoG, the State Dept. insinuated that Gulf piracy had become sufficiently widespread to require facilitating U.S. diplomacy on behalf of the U.S. energy sector.

Next, a comprehensive June 2014 Government Accountability Office (GAO) study reported, "the U.S. has not assessed its efforts or the need for a collective plan to address the evolving problem in the region." In addition, "according to U.S. agencies working in the region, the National Security Council (NSC) staff has not directed them to collectively assess their efforts to address piracy and maritime crime."[110] This is a significant, recent statement. The NSC is the national brokering house for issues of national security. The GAO report provides data that further supports NSC's equivocation regarding offshore piracy as a security concern. Despite the gradual increase in Gulf piracy from 2010 through 2013, U.S. counter-piracy funding has decreased from $243 million in 2010 to $69 million in 2013.[111]

In contrast to the NSC position, there are other indicators that suggest offshore piracy is still cause for U.S. concern at the senior operational level. For instance, as

---

[109] Neptune Maritime Security 2013*, U.S. State Department's OSAC Reviews Gulf of Guinea Threats* Accessed October 7, 2014 from http://www.neptunemaritimesecurity.com/u-s-state-departments-osac-reviews-gulf-of-guinea-threats/

[110] Government Accountability Office (GAO-14-422), Ongoing U.S. Counter-piracy Efforts Would Benefit From Agency Assessments, Published: Jun 19, 2014. Accessed October 7, 2014 from http://www.gao.gov/products/GAO-14-422, Executive Summary

[111] Ibid., p. 47, 51

AFRICOM's commanding officer, General Rodriguez stated in a March 2014 Hearing before the House Armed Services Committee that "maritime criminal activities in the Gulf of Guinea remain at concerning levels. Maritime insecurity in the Gulf of Guinea continues to negatively affect commerce, fisheries, the marine environment, food security, oil distribution, and regional economic development."[112] General Rodriguez's messaging illuminates how offshore piracy is a complicated U.S. foreign policy subject. There are inconsistencies in priority between the Executive Branch and the principal DOD Combatant Commander on the same topic. Next, the analysis combines discussion points from the case study and literature review, identifying the U.S. threats that appear to be of most concern.

Analysis

The subject of this analysis Section is determining when offshore piracy threatens U.S. security. Arguably, there are facets that have been discussed in terms of a pirate-personality-type that make a compelling rationale for the U.S. to not engage in countering these offshore pirates. Policymakers would be advised to heed distinctions between West and East African pirates should U.S. naval forces need to deploy to either region. The case study has already alluded to several of those reasons, summarized at the end of this section. To address this over-arching question, it is critical to begin with a re-cap of who commits piracy. Table 1 summarizes a number of piracy comparatives between Nigerians and Somalis, based on the literature review. Items that are **highlighted** (and checked) are factors more likely to threaten U.S. security.

[112] General David M. Rodriguez, (US Army), Commander, United States Africa Command (AFRICOM) before the *House Armed Service Committee Posture Hearing*, (5 MARCH 2014). Accessed October 7, 2014 from http://www.africom.mil/ p. 13

Gulf of Guinea Pirates		Somalian Pirates
Primarily youth	⟷	Primarily youth
Operate near-shore and offshore	⟷	Operate near-shore and offshore
Influence: MEND/NDPVF	⟷	Influence: Warlords/Al Shabab
✓ **Fishing livelihood impacted (oil)**		Livelihood impacted (foreign fishing)
✓ **Ideology/Profit as motives**		Profit/Ideology as motives
Political corruption-factor		✓ **Governmental absence-factor**
✓ **Reliance on Violence**		Reliance on Violence
Hijack and Syphon	⟷	Hijack and Ransom
✓ **Highly *Opportunistic* Region**		Highly *Opportunistic* Region

Table 1: *Socio-Cultural Comparison of African Piracy*

The qualities listed in the Table have been appropriated as the most principal findings offered from the literature review. So what is Table 1 telling us about the qualities of piracy in both regions that may threaten the U.S? Setting aside the *even-draws*, there are two factors that indicate Somalian pirates are a threat to the U.S. The first is the absence of a Somalian government. This suggests that while there may be no working government, this also means coalition forces can arrive unopposed to enforce counter-piracy operations, such as Command Task Force 151, NATO's Operation Ocean Shield and the EU-led Operation Atalanta.[113] For Nigeria, despite corruption, their government is still a working republic. This status includes retaining sovereign rights

[113] J.Peter Pham, Beyond the Water's Edge: Learning from the Somali Piracy Challenge *Journal of International Peace Operations* Volume 6, Number 2 — September-October, (2010): 9

over Nigerian territorial waters and resisting other warships from entering their waters. With that in mind, keeping a coalition naval presence in Somalian waters endlessly is unsustainable. Once patrolling forces depart Somalia, lawlessness will resume in the absence of an institutional government. For this reason, Somalia's absent political situation represents a greater threat to the U.S. It is worth mention that hijacking and ransoming crew may be equally dangerous to Nigeria's hijacking and syphoning operations. Killing crews in Nigeria is clearly violent, but Somali's kidnapping of U.S. crew would also demand a security response.

As Table 1 indicates, piracy in West Africa poses several threats to the United States. For one, Nigeria's Delta region is almost completely uninhabitable due to decades of oil extraction and production. There is almost no opportunity for youth to pursue any other livelihood in a region that has been rendered unfishable. This correlates with the concept of a region that is opportunistic for piracy as few other Delta occupations can vie with piracy as a source of livelihood. Somalia, by contrast, has not been decimated and fishing is still a viable option.

Next, for Gulf pirates**,** Ideology/Profit is highlighted as a greater U.S. threat. This estimation relies on the logic that unlike Somalia, the literature implies ideology is considered the primary motivator for Gulf piracy. This does not indicate greed is not a motive in the Delta. Rather, if ideology is the more prevalent motivator, then it is far more difficult to dismantle a belief system than create alternatives to alleviate greed. In the event the U.S. becomes engaged in the Gulf, changing these pirates' belief system will require a lasting and forceful commitment.

Lastly, the literature review denotes Gulf pirates display an increased willingness to use violence more willingly than Somali pirates. This violence is associated with two main aspects. For one, Gulf pirates view their trade differently than Somalian counterparts who can wait weeks or months to receive a ransom. Time is of the essence in Nigeria. Piracy must be committed quickly before navy patrols can arrive on scene. Since Gulf piracy equates to syphoning fuel, any resistance from the pirated crew slows down a ship-to-ship fuel transfer. Second, crews on MNC-sponsored vessels represent the enemy. Violence links back here to ideology. Piracy is a personal business in the Gulf, carried out by adolescents against corporate entities who have perceivably depleted their waters and fish stocks. This modus operandi should be considered threatening to anyone operating in the region; these pirates are a group that should be avoided. There is little to be gained for the U.S. by deploying to the Gulf to create an enemy of aggrieved youth who commit piracy near-shore and offshore, and rely on violence to achieve objectives.

Case Study Highlights: Effects-Based

Table 2 (page 77) illustrates the relationship between major findings from the case study. The further an issue migrates to the right of the Table, the more that issue might threaten the U.S. Table 2 is based on findings from this Chapter's Data section. Starting at the top of Table 2 and working downward through the list, the first issue that suggests moderate concern/threat to the U.S. is economic impact to Gulf nations from piracy. EIA data has shown despite decreased U.S. imports, Gulf States continue to export to EU and other markets. Estimates for gross profits 2012-2019 are in the $350 billion range. Next, can MNC economic impacts potentially threaten the U.S? Again, EU-based profits are strong and decreased U.S. business has not diminished regional production. In fact,

offshore exploration has increased. This second threat in the column is rated slightly higher based on the potential for lost tax revenue if U.S.-owned MNCs bring less oil revenue into the U.S. In terms of 'Economic impact to shipping industry', the impact from piracy is shouldered by Lloyd's and underwriters. Consumers, rather than the U.S., would be threatened by impact of piracy on shipping, as insurance premium surges would be absorbed by gas station price spikes. Next, while *Guilt by Association* seems to be a factor, as evidenced by Benin's decrease in port calls, Benin is a member of ECOWAS; profit sharing with countries like Nigeria will expectedly offset losses. The fifth threat on the list is labeled *EU energy impact*. This was rated as a fairly high risk marker. If piracy impacts EU oil imports, Europe may bolster Russian imports, making coalition sanctions less effective and swelling Russian power.

Next, decreased Central African stability is also rated as a risk factor for U.S. concern. Decreased oil flow from Western neighbors can create conflict, slow Central African growth, and allow regime shapers (Al Shabab, Boko Haram) to benefit from instability. The seventh item in the column is a *Diversified U.S. energy portfolio*, the factor this Chapter originally suggested would predominate. The data however suggests differently. U.S. imports of Gulf oil have decreased by nearly 70%; the U.S. has simply adjusted. Finally, the last three boxes on the list advocate violence can influence petro-related industries (OSV, FPSO) through use of kidnappings and murder. Yet, data from Barrios, Kashubsky and IMB studies reveals these events have already occurred with minimal U.S. response. Violence levels do suggest this can still be a risk factor for the U.S.; there may be a future event involving deaths of U.S. citizens in which American foreign-policy is unavoidable and a U.S. response becomes obligatory.

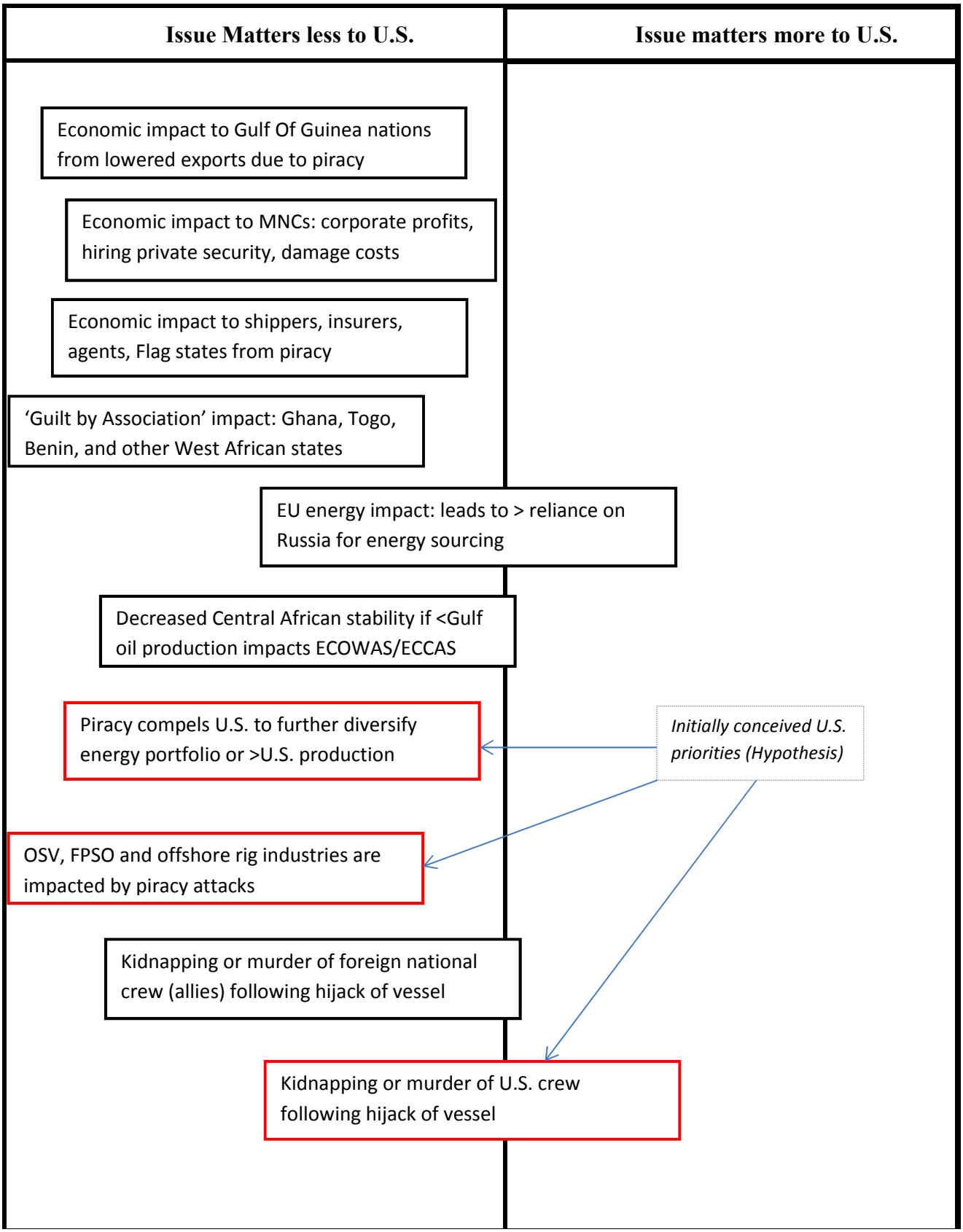

Table 2: ***Weighted Emphasis on Security Issue(s) Importance to U.S.***

Conclusion

My initial hypothesis was that on a macro-level scale, the Gulf of Guinea will compel varying degrees of U.S. involvement dependent upon which American interests are threatened. This included U.S. energy needs, protection of shipping/oil platforms supporting those energy needs, and endangerment of U.S. citizens in the region. In the end, the original hypothesis was partially supported by data and available literature. The findings diminish the significance of American reliance on Nigerian oil and the data show offshore platforms have already been attacked with limited media coverage or U.S. response. The conditions for kidnapping or murder of U.S. crew appear to have prospects for an international incident. The literature review (and Table 1 summary) reveals a dangerous Gulf pirate character-profile. Unlike Somalia, where kidnapped personnel were generally treated favorably (since ransoms depended on returning the crew), Nigerian piracy is typified by violence.

The range of academic sources has led me to consider who becomes a Gulf of Guinea pirate and whether that character profile presents a risk to U.S. security interests. The Gulf pirate is typically a socially aggrieved, young and unemployed fisherman willing to exploit oil transfer opportunities at sea through gang-affiliated support and marginal hesitation to use violence. The offshore pirate is often desperate and has little to lose. They cannot easily be stopped, either individually or as a multi-generational problem. They have killed Nigerian military, can evade international tribunals and compel naval forces to potentially hesitate in combat situations. Coalition vessels would be hampered in conducting any combat options beyond eradication. Naval patrols would also be assigned primarily near West African territorial waters.

Unlike Somalia, territorial boundaries matter to Nigeria. The U.S. would be faced with a crafty and dangerous adversary who knows how to exploit offshore and territorial seas, as well as use Delta tributaries to re-sell oil. The U.S. would likely avoid placing naval forces in the Gulf purely to protect commercial ventures from offshore pirates.

Another aspect of this Chapter's revised hypothesis is the finding that based on the fact nearly half of Europe's oil comes from West Africa, the EU may eventually be faced with a piracy situation that compels European engagement. Should NATO forces be brought to bear, the situation may likely induce the U.S. to support its EU allies. In addition, maintaining (or even increasing) EU dependence on Gulf oil is in the best interests of the U.S. As Nigerian oil reliance grows, Russian oil exports diminish. For these reasons, if Europe is threatened by piracy, the U.S. may be threatened as well.

Finally, a future item that may pose a threat to U.S. security concerns is the question of who these pirates become if regional navies or private security eventually succeed in removing offshore piracy, as largely happened off Somalia. If Gulf piracy were eliminated, the Delta would still remain devastated and unsustainable. What other occupation could these pirates do next? This is not to suggest piracy should be allowed to flourish, merely that the Nigerian youth could then access regional insurgency and extremist outlets where piracy-expertise could be well employed. As one problem is eradicated, it may become necessary for policymakers to formulate other social and political options before being faced with a new problem. Unemployed pirates may otherwise transition into shore-based crimes such as pipeline bunkering. These types of transition would represent entirely new threats to U.S. security and oblige a revised examination as to when piracy threatens U.S. interests.

Chapter 3

Introduction

This Chapter's question asks "What security-related qualities should a technology design possess for use in multi-modal transportation passenger hubs?" This is a subject that requires compelling a linkage between typically-unrelated transportation security modes. Since there is limited scholarly literature or data available on the subject of inter-modal security practices, this Chapter is not intended to canvas all possible solutions. Our contribution here is a preliminary investigation as to whether risk-mitigation (and security) models used by airports and rail *can* apply to ferry and cruise ship terminals. If so, this Chapter discusses over-arching qualities essential to a system that can protect passengers, regardless of the transportation environment.

To begin, it is important to define common characteristics shared by airport/rail passenger security and ferry/cruise terminal security. Similarly, all four transportation modes incur hubs, centralized, populated areas in which passengers congregate while awaiting their respective transportation. Next, these hubs all require a transfer of passengers to an airplane, cruise ship, ferry or train. Third, each mode involves an issue of expediency. While expediency varies by mode, each transportation system necessitates a constant, reliable flow of passengers from entry through security, to queuing areas, and finally, to conveyance. Fourth, once passengers are onboard their conveyance, the security protocols become relatively lax in comparison to the transportation hubs. Generally, there are no further security measures past the final transportation security checkpoints. An adversary, once onboard, has progressed beyond formal screening mechanisms. The security hubs, or terminals, also share important security

characteristics. They facilitate high passenger volume, are restrained by the limits of their physical space, and present scarce contingency options in the event of emergency. Lastly, each transportation mode represents a setting where explosions, fire, smoke, chemical release, or gunfire can rapidly produce devastating damage in a confined, moving battle space. For ferries, cruise ships and planes, surviving passengers would need to contend with obstacles presented by mid-air or in-water emergencies. For these reasons, it is essential security be provided at passenger terminal hubs, before boarding or embarking.

This Chapter examines four transportation modes in a format designed to compare whether airport security principles can crossover to other transportation hubs, specifically, ferry and cruise ship terminal security. This Chapter finds airport security practices have greater utility than rail for a number of reasons; a subject to be discussed. The paper then shifts to selecting three airport models that may be best suited for high volume ferry/cruise terminals. These models are selected and tested against five transportation-specific security concepts deemed essential to multi-modal success. The hypothesis is that by evaluating three airport models with five specific transportation security conditions, the resultant 15 variables will yield airport practices that can (or cannot) transplant to ferry/cruise terminal security. This approach uses a deliberative method to narrow down those principles and models well designed for transposing the demands of differing security environments. As money and time have been heavily invested into airport security since 9/11, there are superb airport models already in use that may offer lateral value. The idea of this Chapter is to not only avoid "re-inventing the wheel", but to determine whether versatile and proven airport security practices can be introduced across a variety of transportation hubs.

Literature Review

Question: "What security-related qualities should a technology possess when designed for use in multi-modal transportation passenger hubs?"

This literature review first analyzes conceptual transportation security concepts, and then includes a subsidiary airport-specific review of models that embody how airport security experts protect their airports. Using this bifurcated method, this Chapter combines analysis of concepts and practices to develop core security *criteria* that offer crossover value to cruise and/or ferry terminals. The criteria then serve as a template for testing a few technology examples in the Data Section. It should be noted there is a shallow pool of available rail security literature; airport-related security governs the existing scholarly discussion.

Resilience

Cox, et al offers several characterizations of transportation security. Foremost among these is the concept of *Resilience*. Resilience for our purposes describes whether the security system can withstand internal impact, such as an electrical outage, or external damage from an intruder. In addition, *resiliency* implies an ability to rely on contingencies and the flexibility to avoid a complete system failure. The nature of airports and train stations as fixed transportation nodes compels a resilient approach to security, including a reliance on the public to adapt, when needed, as transportation system users. Terrorists adapt as well through "threat-shifting"[114], so from a risk management view, offsetting this asymmetric volatility with resilient air, rail or maritime transportation-based security is equally essential. Cox cites Rose's definition of resilience

[114] Andrew Cox, Fynnwin Prager, and Adam Rose, Transportation security and the role of resilience: A foundation for operational metrics. *Transport Policy* (2011), 18 (2) (03): p, 308.

as either "static resiliency" in which the system must "maintain function", or "dynamic resiliency" in which the system must "recover rapidly."[115] For ferries, both static and dynamic resiliency would apply. For cruise ships, static resiliency applies. This is because cruise ships are not a primary form of public transportation. Based on a credible threat, cruise ships can delay vacationers for several hours if needed and then make up the lost time while underway, over the course of a 5-7 day cruise. Ferries do not have this luxury. Maintaining function and recovery time are both critical; as soon as one ferry departs the dock, another may be arriving.

Resilience is only one component of a risk-based approach. In Szyliowicz's examination of risk assessment methods, he points to aging infrastructure, passenger congestion, a habituation to computer-controlled systems (rail switches, air traffic, sensors), and buy-in from both private and public sector as all being key considerations.[116] In terms of private airlines, Amtrak and cruise lines, they cannot obtain classified information, putting these stakeholders at disadvantage. Private air and cruise security is expected to provide all-threat mitigation, without necessarily being privy to the threats. Szyliowicz emphasizes transportation resiliency is a viable way to offset this challenge using resource capabilities. For example, The San Francisco BART metro helped fill the void in 1989 following a major unexpected earthquake. Conversely, New Orleans revealed poor transportation resiliency following Hurricane Katrina. In our context, Szyliowicz implies that New Orleans suffered (despite advanced Hurricane awareness) whereas San Francisco persevered (without prior earthquake knowledge). In

[115] Ibid., 308.
[116] Joseph S. Szyliowicz, Safeguarding critical transportation infrastructure: The US case. *Transport Policy* (2013), 28 (07): 70.

both cases, transportation resiliency was a major factor. Bruneau and Reinhorn use the term *resiliency* slightly different in terms of transportation security; their definition encompasses four subclasses: "robustness, redundancy, resourcefulness and rapidity."[117] Bruneau and Reinhorn's terms robustness and rapidity highlight Cox's static and dynamic resiliency and echo Szyliowicz's emphasis on resourcefulness. Redundancy is a stimulating idea when looking at maritime transportation hubs. Ferries and Cruise ships both typically embrace redundancy measures within a port; other docks and terminals are typically available for contingency purposes, if needed. In short, every definition of *resiliency* afforded by these authors contributes an important facet when considering the value of this term in transportation risk assessment; *resiliency* is one of the key Criteria highlighted for discussion in the Methodology Section.

Efficiency and Effectiveness

Johnston's transportation security model initially described airport *productivity* as being a "combination of percentages of efficiency and effectiveness."[118] Security, if taken to an extreme, can become an adversary to *productivity*. In terms of an airport's ultimate goal, safe and profitable operations, this Chapter must consider both productivity and security. Johnston's 2004 model on the subject demonstrated a relationship between regulated and deregulated environments, where in a regulated environment passengers are citizens. As security becomes increasingly deregulated, passengers become customers and the government evolves into a market. The trade-off for Johnston's increased "freedom and innovation" in a deregulated environment is the expense of assuming risk (that is otherwise diminished in a regulated environment). This is an essential attribute for

[117] Ibid., 73.
[118] Van R. Johnston, Terrorism and transportation policy and administration: Balancing the model and equations for optimal security. *Review of Policy Research* (2004), 21 (3) (05): 267-69.

ferry and cruise security. It is imperative to ensure any technology *borrowed* from air/rail security is both *effective and efficient*; these terms ensure profit and security can co-exist in a transportation environment.

Johnston and Plant later revised Johnston's 2004 model in the form of a 2008 Emerging Entrepreneurial Management and Public Policy Model. In their latter view, they factored competition into their view of a de-regulated transportation environment and expanded on regulated transportation to include the idea of collaboration[119]. Competition and Collaboration are both instrumental security considerations. For Competition, one company cannot be favored over another based on overly strict or lax security. For Collaboration, public security concerns (FAA, TSA) must align with corporate priorities to ensure sustainable revenue. Efficiency and Effectiveness are critical underpinnings to a transportation risk stratagem. These terms, when properly enacted, reduce risk (effectiveness) while allowing healthy market competition and high volume ridership (efficiency). Both terms will be Criteria later in this Chapter.

Starting to come off the rails

Johnston and Plant's theory also applies to a de-regulated rail industry (as opposed to an increasingly regulated post-9/11 airline industry). The distinction between air and rail security is important; increased regulation has also equated to increases in aviation security funding, innovation and technology; conversely, the same can be said for rail security. Common to both air and rail security is a reliance on a "collaborative public-private model." A cooperative approach between public-private entities is vital to any security model. In regards to transportation security budgets, Johnstone views that

[119] Van R. Johnston, and Jeremy F. Plant, Rail security after 9/11: Toward effective collaborative regulation. *Public Works Management & Policy* 13 (1) (Jul 2008): p.13

national defense and homeland security budgets need to consolidate, stating "policy distinctions between national defense and homeland security (should) be eliminated."[120] This is an overly simplistic solution and not recommended. As indispensable as the public-private model may be, it is also critical that private partners not be required to wade through multiple layers of bureaucracy in order to achieve daily transportation security, or steady-state progress.

To offer brief insight into the complexities of rail security (and a rationale as to why rail security does **not** make a good template for ferry/cruise terminals), the following applies: Both freight and passenger trains use the same set of rails while answering to different regulations. In addition, federal rail security funding pales in comparison to aviation-related federal funding, meaning less advancements and technology for rail security. There is already a small profit margin in passenger rail; additional security measures would only slow ridership. As further financial challenge to rail security, there is also a general prohibition against private rail using federal rail funds for security. In addition, rail presents a unique vulnerability; since rails run continuously and cannot be disrupted at any point along the length of tracks, all 171 thousand miles of US tracks must be uniformly protected. Waugh aptly describes this challenge as "indefensible."[121]

Customer-Resiliency: Moving further from the tracks

Cox suggests that resilience constitutes a "supply-side" and a "customer-side."[122] Supply-side resilience includes items like repairs and debris removal; this is the responsibility of the transportation system mode. Customer resiliency requires passengers

[120] R.W. Johnstone, Not safe enough. *Issues in Science & Technology* 23 (2) (Winter2007): p. 58
[121] William L. Waugh Jr., Assessing the Risk to Rail and Transit systems. *Public Manager* 37 (4) (Winter2008): p.73.
[122] Cox, Transportation security and the role of resilience: A foundation for operational metrics.(2011), p. 309

to modify their routes, telework, and use different highways or work times. With rail, customer-side resiliency can be removed from the equation entirely, as happened with certain New York City (NYC) metro stations after 9/11. Zimmerman and Simonoff studied *ridership* on the NYC Metropolitan Transportation Authority (MTA) as an indicator of rail (metro and subway) resiliency. Representing 40% of the entire nation's transportation, NYC MTA offers a considerable sample study. In short, the findings revealed subways rebounded quicker than rail, but the unique discovery was the role played by ferries that *filled-in* NYC ridership and demonstrated transportation resiliency. Rail did not bounce back immediately, while ferry ridership increased 27% in the 3 months after 9/11 and then 42% six months later[123]. In relation to this study, Plant stated "there are no specific programs or subunits primarily concerned with railroad security."[124] It appears passengers seem to know this as well. Passengers left rail for another mass transit system entirely (poignantly, illustrating the resilience of ferries).

Considerations: Inter-modal and International Regulations

Finally, Szyliowicz, in his review of international transportation security, broadens perspective on intermodal transportation. While I disagree with his assertion that "shipping lines would require months to return to normalcy"[125] his point regarding the intermodal nature of transportation security is well-suited. In particular, identifying central nodes where airport travelers link to cruise ship terminals, or where highways lead to ferries, is worthy of future research; these locations of confluence directly fuse aviation

[123] Rae Zimmerman and Jeffrey S. Simonoff. Transportation density and opportunities for expediting recovery to promote security. *Journal of Applied Security Research* (2009), 4 (1) (01): p. 55-56
[124] Jeremy F. Plant, Terrorism and the railroads: Redefining security in the wake of 9/11. *Review of Policy Research* (2004), 21 (3) (05): p. 301.
[125] Joseph S. Szyliowicz, Safeguarding critical transportation infrastructure: The US case. *Transport Policy* (2013), 28 (07): p. 354

and maritime security agendas. For numerous reasons described in this first portion of literature review, rail security does not present nearly as promising a model for transplant to ferry/cruise terminals as aviation security. Based on the research, rail transportation security is underfunded, historically de-regulated, and by its nature, unalterably exposed to attack. Moving forward, the focus is on identifying additional qualities from aviation security-technologies that can thrive in inter-modal security.

Airport-specific Literature Review:

The most thorough scrutiny on airport security can be found in assessments conducted by subject experts who work in this field. These experts are typically represented by one of three major professions: architectural engineers, security consultants or airport security managers. This does not imply only these occupations represent a voice on the subject, but rather, these occupations tend to comprise the scholarly body of work. The body of peer-reviewed, published work in this arena tends to have two factors in common. One, aviation-security articles are well-represented in the Journal of Airport Management. While the Journal was not a default search for airport security literature, this source represented a wellspring for peer-reviewed, scholarly approaches on the topic. Second, the three major professions: engineers (hired to construct a secure environment), consultants (hired to improve security practices), and security managers (hired to oversee security practices) offered aviation commentary on security and risk-mitigation that was germane and professionally objective.

An airport engineer, Samola describes the Redesign Passenger Process (RPP), used in Amsterdam's Schiphol Airport. RPP is an approach to viewing passengers as an interactive aspect of the airport security environment, where the goals are to "increase

capacity, improve efficiency, and improve punctuality." [126] Conceptually, this engages use of fewer passenger check-in booths and allows passengers the freedom to check-in where they choose. This *randomness* facilitates indiscriminate passenger distribution patterns in airport queuing areas. Randomness is typically initiated by security experts who select impromptu security measures to be used at improvised locations or times. By allowing travelers to form the random patterns, this naturally disrupts pattern formation, making an attack on a transportation hub difficult to plan. Samola discusses that RPP allows early, on-time, and late passengers to form basic semblances of patterns, making queue areas easier to monitor atypical behaviors that may be present.

Assembly Lines and Layered Security (in a confined area)

Calder concurs with Samola's basic premise on passenger predictability, although he approaches air passengers very differently, emphasizing a structured assembly line concept. His correlative argument is that a "factory production line achieves a predictable flow… and predictable throughput."[127] Calder implies that passengers who may be receptive to new technologies, such as millimeter-wave scanners (as Samola suggests), are likely to continue to do so, unless information is brought to bear that would change their approach. Calder supports this argument by citing bell-curve data that aligns with Samola, to wit, passengers tend to arrive in batches of early, on-time and last-minute groups. Further, Calder states passenger predictability is founded on types of flights (business-oriented vs. vacation destinations), and time of day (early flights have less early-arrival passengers since people tend to sleep in). Bloch and Payne also offer a

[126] Betty Samola, Innovations in passenger and baggage processing at Schiphol Airport. *Journal of Airport Management* 2 (3) (Apr 2008): 227-229

[127] David Calder, Who says 'passengers aren't baked beans'? Making passenger security screening productive while delivering high service levels. *Journal of Airport Management* 4 (4) (Jul 2010): 335-6.

similar production-based model in which "capacity determines production rate."[128] This view aligns more with Calder than Samola, as Bloch and Payne state a reliance on successful, safe passenger travel is a norm derived from production metrics, rather than Samola's emphasis on social modeling predicting behaviors.

These passenger tendencies all tie back to the research question as to what security qualities are needed in a technology to apply in multiple transportation hubs. Each author's variation speaks to the same subtle messaging: humans need technology to manage the task of observing other humans who tend in volume to produce reliable transportation patterns. While Bloch/Payne and Calder recommend a statistical, assembly line methodology, Samola posits the airport design should be made to adapt to passenger tendencies. Bloch/Payne, Calder or Samola's perspectives can be integrated into a security model that uses existing space (i.e. cruise terminal waiting areas, passenger ferry queues) and account for passenger tendencies within confines of that space.

Regardless of how technology is implemented, there is a clear linear dynamic that should be captured as Criteria. Human security capital needs technology that interacts. The technology can be taught to observe randomness-anomalies, or assembly line disruptions, but only a human operator can truly distinguish the nuances of human behavior. Since the technology is required to handle such a large volume of passengers, the Human Security and Technology must interact to identify aberrations in Passenger Tendencies/Patterns. This concept is labeled *Human-Technology Interface (*HTI).

Human Security ⟷ Technology ⟶ Passenger Tendencies/Patterns (Anomalies)

[128] Paul Bloch and Claire Payne. Optimising passenger security-screening operations. *Journal of Airport Management* 1 (1) (Sep 2006): p. 9

Layers of Risk

Locating security checkpoints, passenger screening areas, and biometrics in the right physical airport locations is a science, contends Diedam, in his four-level Transportation Security Pyramid[129]. Diedam's Pyramid views access to the airport in terms of "openings." An "opening" can be an exterior door, an idle baggage chute or a retail-loading dock within the airport, for example. Bloch also emphasizes the physical location of doors and structures inside the airport. The proximity of screening areas to retail establishments matter, because where people buy products, it takes longer to screen for instance. Retail workers need routine access, passengers may have food/drinks in hand, etc.[130] These are valuable insights for ferry and cruise security, where terminals also have retail facilities and security must consider not only exterior access points but risk points inside the terminal where passengers tend to gather in numbers.

Similar to Diedam's approach to layered security, Lennerman examines risk-layering as well. Swedavia is a Swedish airport company where Lennerman directs security operations. His model uses a 6 layered system "based on the hypothesis that systematic work provides a high level of security regardless of whether the threat comes from, outside or inside."[131] Lennerman differs from Diedam's approach in that his Swedavia model covers boundary security in the first layer, where Diedam addresses boundaries as three of the Pyramid's first four layers. In line with these methods of layered security are the views of Ghavamifar, et al on the subject. From their civil engineering perspective, Ghavamifar and cohorts view the layers in a purely physical

[129] John Diedam. Access control: The process of securing a transportation site. *Journal of Airport Management* 3 (3) (Apr 2009): 263-73.
[130] Bloch and Payne, Optimizing passenger security-screening operations. p.11
[131] Anders Lennerman, Protecting the airport from an insider threat: A systematic approach to aviation security. *Journal of Airport Management* 6 (3) (Summer 2012): 225-30.

state, dividing the airport into an air-side, land-side and terminals.[132] Their layers raise the issue of construction personnel working at the airport, who often bring heavy equipment (potentially explosive-laden) into passenger proximity. There are many ways to layer security in an airport or ferry terminal; regardless of the procedure or technology used, the concept of *risk-layering* is essential and represents the fifth and final Criteria.

Refining Security Habits

Lastly, for aviation-specific security, although focused on passengers, the Chapter would be remiss without addressing the significance of personnel working inside the airport security layers on a daily basis. In this regard, there are 2 major elements that appear to translate well to a maritime security environment: training and testing. Lennerman's emphasis on quality compliance should be woven directly into any program that routinely assesses security protocols. Eldar does a thorough review of personnel working in the airport security community, defining roles of the employer, the passenger, and security personnel, from his article "The human factor in aviation security"[133]. Eldar's input should be considered in any selected technology or protocol: recruitment, staff retention, noisy work conditions, flux in passenger volume and seasonal change in security workforce should all be consistently viewed in a transportation security milieu. Weiss' review of the Dynamic Security Airport Simulator includes methods on how best to achieve this daunting task, testing employees with practical scenarios that identify patterns such as passenger "busyness", and "suspicious behavior."[134]

[132] Kamran Ghavamifar, Bakhshi Payam, and Touran Ali. Owner's control and risks in various airport delivery methods. *Journal of Airport Management* 5 (1) (Oct 2010): p. 44.
[133] Zamir Eldar, The human factor in aviation security. *Journal of Airport Management* 5 (1) (Oct 2010): p. 37-39.
[134] Wiliam E. Weiss, Development and use of the dynamic security model for airports. *Journal of Airport Management* 5 (3) (Apr 2011): 245-54.

In summary, there are several key findings when looking at security related qualities which a technology should possess in order to offer utility in multi-modal transportation hubs. Cox and Szyliowicz' emphasis on the value of resilience within transportation is imperative. Cox and Rose's view on static and dynamic resiliency highlights function and speedy recovery, which as indicated, differs slightly as priority when comparing ferries with cruise ship security. Cruise ships rely on passengers who vacation rather than commute. Cox also infers an imperative distinction between airports, ferry and cruise terminals. Airports and ferry terminals are akin in servicing both recreational and business travelers. Cruise terminals do not serve commuters, although they do contribute to the U.S. economy. In short, Cox, Szyliowicz and Bruneau/Reinhorn illuminate the value of resiliency, but more research is still required to distinguish the threshold speeds of recovery for cruise, ferry and airport terminals; there is a finite period of inactivity for each of these industries before they suffer financially. This body of literature has not made clear what that comparative threshold is for ferry and cruise terminals. Johnston's next point on efficiency and effectiveness can play a significant role in forecasting the macro-level resilience of a transportation system, a subject worthy of additional research.

The terms effectiveness/efficiency address the private-public terminal relationship and apply to ferry and cruise terminals. Every terminal must balance the demands of regulated security while ensuring commercial *productivity*. The focus on ensuring effectiveness and efficiency remains a focal theme in any form of applicable technology. It may be possible (although not recommended) to utilize a less-resilient, or less-layered

system in a ferry or cruise environment, as those qualities can be buttressed by other supportive technologies if needed. However, any technology that transfers from airports to ports must be both highly efficient and highly effective. There is no room for compromise on effectiveness and efficiency.

Calder, Bloch/Payne, and Samola all highlight technologies that integrate human traffic tendencies, and the predictable movements of passengers. Their findings are disparate and each of their models is unlike another. However, one commonality revealed by their work is central to this Chapter; technology alone is not enough. Humans will always be required to make the final distinction in pattern anomalies at transportation hubs. As Calder implies, an assembly-line still requires someone to monitor the conveyor belt. This analogy is crucial to the study; a technology that can transplant from an airport to a cruise terminal should be comparable to an assembly line worker using the same conveyor belt in Tulsa or Detroit. The literature suggests that a technology suited for multi-modal environs may work well on its own 95% of the time. In fact, the more the technology incorporates multiple layers as Diedam suggests the more efficient it becomes and less vulnerable to a single point of failure. However, the technology must still *require* an operator to investigate those 5% of anomalies that necessitate judgment and management, as Lennerman contends. This is the strongest deduced finding garnered from my review of these multiple airport security stratagems.

Lastly, Eldar and Lennerman illustrate that while technology is vital, equally necessary are skilled personnel who are frequently trained, tested, and improved with use of any selected technology. The more security can rely on technology to help observe passenger behaviors on a large-scale, fast-moving basis, the better the human operator

will become at identifying irregularities. This concept, along with: resiliency, effectiveness, efficiency, and risk-layering form the root of the next endeavor. The idea is to now relate these multi-modal transportation concepts to actual technologies; the Methodology will create several business rules that help test these concepts on real-world airport security protocols.

Hypothesis

The literature suggests that five over-arching security principles used in airport security can apply to ferry and cruise ship terminal security. The literature also suggests that in terms of tangible airport and rail security principles (where tangible means real, operational security practices), tangible airport security protocols offer higher crossover utility for ferry and cruise ship security. Tangible rail security practices will not be pursued. It is the Chapter's hypothesis that by evaluating three designated airport security protocols against a standard of five Criteria (identified next in Methodology) serviceable qualities from aviation security that also bode well for employment in reducing security risks to ferry/cruise terminal will be demonstrated.

Methodology

The methodology for this data research derives from the hypothesis that *airport security protocols that incorporate particular criteria* (intervening variables, see criteria below) can positively influence the relationship between *ferry/cruise terminal environments* (independent variable) and the *quality of security* (dependent variable) in those environments. In order to test this hypothesis, three intervening variables are assessed: Total Airport Security System (TASS), Social Force Model (SFM), and Behavior Detection practices. These variables have been selected because they all require

an interface between humans and technology; the extent of this interaction will be examined in Criteria #2 (below). In addition, each of these models has been touted by experts as either some of the finest (TASS, SFM) or most controversial (Behavior Detection) practices being employed in airport risk-management today.

These intervening variables need to abide 2 sets of criteria that suggest an ability of these risk-reduction protocols to enhance security-quality in ferry and cruise terminal security environments. Criteria-selection is based on characteristics gleaned from the literature review and my 17 years working in maritime security. Meeting both criteria is a necessary condition.

1. Core Principles: Based on core academic principles highlighted by the Literature Review, does the airport security model embrace four essential principles? These principles are:

   Resiliency: can the protocol adapt, or withstand short-term internal/external duress?

   Effectiveness: does the protocol enhance the quality of security?

   Efficiency: can the protocol sustain peak passenger volume while remaining effective?

   Risk-layering: does the protocol include layers to shield system failure or physical intrusion?

2. Human-Technology Interface: Does the airport security model ingrain use of technology and human-derived skill sets (judgment, common sense, inference) that require human involvement in the process/system? This criterion implies that a shared strength of *human qualities –and- technology* is crucial to higher quality

of security. This criterion will be termed *human-technology-interface* **(HTI)**. The Chapter will frequently reference **HTI**.

There are many other criteria that likely merit future study (i.e. does the system require highly specialized training or can many security personnel be easily trained? Does the process work best if used randomly or incorporated as a standard procedure?) For the scope of this study, the focus is on the principles identified as having highest utility in both airport and cruise/ferry security, and evaluating whether the protocols emphasize symbiotic human/technology interface.

If one or more sets of the stated criteria are not present, then consider that model to be incomplete and not recommended for use in maritime transportation terminals.

The following Methodology assumptions apply:

- Intervening variables (airport security protocols) refer to transportation hubs only (airport, cruise, and ferry terminals).Transport modes do not apply (planes, ferries, ships).
- Intervening variables pertain to passengers only. This Chapter is not currently evaluating protocols for transporting cargo, luggage, vehicles, or hazardous material.
- Discussion on millimeter wave, backscatter, thermal sensor imagery, and other technologies in which humans operate the system is purposefully omitted. Instead, focusing on protocols where a human works ***with*** the technology.
- No specific security industry products are being endorsed. Products mentioned by trade-name simply embody an aspect of the criteria that illustrates a point.
- Partnership between public/private stakeholders is assumed necessary in all protocols.

Data

Seeing the Big Picture

It is appropriate to begin an examination of airport security models that may be suited for ferry or cruise terminals by contrasting the difference in passenger volume through a ferry terminal and a cruise terminal. Since the cruise ship environment generally vets individual passengers more closely (i.e. passenger manifests, x-ray screening on luggage) than ferries, and cruise ships depart less frequently than ferries, cruise ship security can generally conduct a more detailed scrutiny of passengers than a ferry terminal. For perspective, the Seattle terminal in the Washington State Ferry System supports 72 arrivals and departures daily through one terminal alone, using ferries whose maximum capacity can exceed 2,000 passengers.[135] In the same city of Seattle for example, the Port of Seattle will see three cruise ship departures, three days a week, at 2 cruise terminals (during height of cruise season).[136] These ships similarly carry 2000+ passengers apiece but see half a dozen weekend departures from a cruise terminal, as opposed to 500 ferry arrivals and departures a week. The frequency of vessels leaving the dock is the demarcation between total cruise and ferry passenger throughput. Based on the bulk of passengers moving through the system, a ferry terminal in effect, more closely resembles an airport on a day to day basis; a cruise terminal may resemble an airport's pace of volume on very limited occasion and only during a few summer months.

One commonality between ferry and cruise security is that operators in both environments, like airports, are required to look for uncharacteristic patterns in mass-

[135] Washington State Department of Transportation, 2013 Ferry Schedule Information (by route), http://www.wsdot.com/ferries/schedule/ extracted 07NOV2013

[136] Port of Seattle, Seattle's Downtown Cruise Terminals (2013) http://www.portseattle.org/cruise/Pages/default.aspx extracted 07NOV2013

passenger movements. The security personnel must rely on technology that is advanced enough to warn of danger, while being simple enough for the operator to keep up with a steady flow of passengers.

Over the last several years, London has shared a dubious distinction in having both their airport and metro systems targeted for attack. Perhaps for these reasons, the British are among the pack leaders in developing procedures that mesh the strengths of technology and human judgment in helping to prevent another terrorist event. At Heathrow airport, the Total Airport Security System (TASS) is in prototype development as one of the front-runners of the HTI concept.[137] Funded through the European Union, TASS allows a single user, in a command and control center, to use multiple sensors and video feeds. TASS can recognize facial patterns by linking to international terrorist databases, running vehicle plate checks, monitoring gate controls, responding to hazardous material indicators, and deploying remote bomb control robots. The computer infers an attack scenario by correlating any number of seemingly disparate factors that might go unobserved by a single command/control element. As one criterion is human-technology interface (HTI), the TASS system meets that criterion. The role assumed by airport security personnel operating these systems translates well to a ferry terminal.

As far as alignment with the stated core principles, TASS's computer is able to assimilate the license plate of a vehicle illegally parked outside 'Arrivals' as well as a passenger who is suspiciously loitering just inside the adjacent terminal door. This ability represents the principle of *risk-layering*. The computer associates an exterior layer of risk

[137] Lee Hibbert, "Alert to the Real Dangers," *Professional Engineering* 25, no. 11 (11, 2012), 24-26

(vehicle) with a second layer of risk (a person of interest who is inside the building, but still physically outside the Terminal/queuing areas). TASS then prompts a human operator to evaluate the scenario for action, further investigate, or to dismiss as a false alarm. While this scenario is indicative of the *risk layering principle*, and is more *effective* than either a machine or human could be on their own, two other principles must be considered. For one, additional data is needed on the *resiliency* of a system such as TASS. For instance: how do the CCTV-feeds operate in low light, does TASS (or a system like it) tend to false alarm, what are the likely fallibilities when an untrained or inexperienced operator uses the system, can a perpetrator bypass TASS, are there gaps in perimeter coverage, and how does the system operate under environmental duress (wind, rain, heat sensitivity, etc.)? In this case, answering *resiliency*-based questions is the crucial determinant as to whether this type of system can be highly *efficient*, or not.

In a similar vein, London's other major aviation hub, Gatwick International Airport, has also employed another variation of HTI, via their airport's experimental use of the Social Force Model.[138] Like TASS, this model fuses technology with a reliance on human interface. The Social Force Model works by applying algorithms to congested terminal areas, mathematically predicting where passengers tend to walk within the airport. This guesswork is necessary; as passengers leave one camera's field of view there is a gap in space and time before they enter another camera's view. The significance of this technology for airports and ferry/cruise terminals is that operators are allowed to not only track where passengers move within an airport, but where they tend *not* to go. If a

[138]Riccardo Mazzon, and Andrea Cavallaro. Multi-Camera Tracking using a Multi-Goal Social Force Model. *Neurocomputing* 100 (2013), (01/16): 41-50

person-of-interest disappears from view, this may prompt security to investigate, but can narrow down where the passenger most likely went next. The Social Force Model uses three general observations to track passenger flow. Mazzon and Cavallaro's model look at people moving in large "macroscopic" groups, as "microscopic" individuals moving in a crowd, and as groups of "mesoscopic" passengers, where "movements" of a targeted group of people are "like a moving blob."[139] The advantage of the mesoscopic approach is airport security can then track the movement of *blue forces* (i.e. specialized SWAT teams, bomb squads, etc.) in addition to identifying where potential terrorists may be acting in pairs or clusters. Using the Social Force Model, an HTI component is integral in two regards. The operator must remain consistently engaged with the camera and software to track movement of passengers. Second, the communication between ferry/cruise command center elements and foot-patrol security is also paramount in pinpointing a location.

For ferries, this model offers real utility; the entire flow of walk-on passengers tends to queue for embarkation and debarkation in a few centralized locations. The passengers then transit through a corridor to/from the ferry and either disperse to open seating areas on the vessel, or to exit routes, once at the dock. This limits the number of locations where cameras are required, but those points of camera-interface are decisive. If a passenger stops for example between the queuing area and the walk-on corridor, they create congestion in a *fatal funnel*, theoretically blocking hundreds of passengers in a place where they may be stopping to detonate a device. In addition to the *HTI* (human-technology interface) value of uninterrupted camera views, this model offers *resiliency*

[139] Ibid., p. 42

based on the fact the cameras are already working. Social Force Model is merely reinforcing gaps in the cameras, so any improvement in this regard is more *resilient*, and more *effective* through use of an additional *risk-layer*. The benefit of Social Force Model is this model is not a system unto itself; it is an augment to the ferry, cruise or airport surveillance systems. It can only increase the *efficiency* of CCTV systems by shoring up the ability to maintain uninterrupted camera views. In attempting to track one person, or several individuals, this concept enhances human ability to make the most of available technologies and to incorporate core principles; this concept is advocated for use in ferry and cruise terminals.

The human technology aspect must include more than training, testing and using hardware, such as TASS and the Social Force Model. Background checks and no-fly (or no-sail) lists are a valuable incorporation of technology and human capital, but the results of these checks can be misleading and overwhelming. For example, the FBI's Terrorist Screening Center hosts a list for aviation purposes of 8500 passengers who cannot fly into, within, or out of the U.S. In contrast, a separate database is also referenced in the aviation industry, called the Terrorist Watch List, containing 400,000 passenger names.[140] In reality, the number of passengers meriting additional screening is likely somewhere between these figures. For passenger no-fly lists, how does an airport screener know who requires further screening? For cruise ships, there is a passenger manifest, but for ferries who often take cash payments from travelers, there is no list. In this regard, ferry security

[140] Joshua Sinai, "New Trends in Airport & Aviation Security," *Journal of Counterterrorism & Homeland Security International* 18, no. 3 (Fall 2012): 30-37

personnel must rely on human judgment. Aside from canines that work ferry docks, security in this arena is largely reliant on *gut-instinct*.

Behavior Patterns

In looking at a proposed emphasis on HTI, ferry security would benefit from adopting a program that teaches security personnel to identify behavior patterns that are outside the norm. Behavioral pattern methodology embraces *risk-layering, effectiveness,* and *resiliency*. The one concern with this approach is *efficiency*. If security personnel are trained improperly to recognize behavior patterns, they can potentially impact the supply chain (unnecessary, additional screening), or the transit system writ large (i.e., by racial profiling). Next, this Chapter captures data that helps isolate whether behavior patterns can be *efficient* in ferry and cruise security.

As one would expect, the Israelis have been implementing behavior recognition protocols in aviation security for years. Dating back 35 years, the original behavior pattern studies began with the work of Ekman and Friesen in their research on the Facial Action Coding System (FACS)[141], where they analyzed participants' expressions and facial muscles after being asked a variety of questions. Their findings were adopted in U.S. transportation when DHS began a formalized SPOT program (Screening Passengers by Observation Technique) in 2003. DHS-TSA employed Behavior Detection Officers (BDO) to assess passenger behavioral mannerisms and the program has been viewed with mixed success.[142] Part of the positive reception behind the Israelis use of FACS has been related to the size of their airports, as compared with U.S. air terminals. Ben Gurion

[141] Justin Florence and Robert Friedman, Profiles in Terror: A Legal Framework for the Behavioral Profiling Paradigm *George Mason Law Review*, Vol. 17:2 (2010), 423-480.
[142] Ibid., p. 425

International Airport for example, hosts 10 million annual passengers, while Atlanta International boasts nearly ten times that number over the course of the same year.[143] This implies that Israeli screeners routinely process 1/10th as many passengers through the gates as screeners at a high volume U.S. airport. This attribute allows Israeli screeners to be increasingly selective with whom they select for behavioral detection as well as the time they can spend practicing this technique. This comparison makes a useful analogy for cruise terminal screening. Cruise terminals typically see 2000-6000 daily passengers, per terminal, on busy days in a summer cruise schedule. Atlanta International averages 250,000 passengers a day. This means the cruise industry by pure passenger volume could adopt a similar behavior detection program. It is important to note that since cruise travel is more of a tourist industry than a true transportation mode, this level of scrutiny would likely aggravate passengers. Although behavior detection may be an *effective* measure in cruise security, cruise ship travelers elected their voyage, using discretionary funds. Unlike a plane or ferry, cruise passengers do not require the cruise ship as a transportation service. For this reason, random behavior checks are not advocated as *efficient* for the cruise industry.

The utility of behavior detection techniques in the world of ferry security is slightly different. The presence of high passenger volume, confined spaces that hold hundreds of awaiting ferry riders, and a general absence of metal or explosives detection protocols for foot passengers necessitates a very acute level of human awareness in the ferry terminal environment. Before recommending behavior detection techniques as an

[143] Hartsfield-Jackson, Atlanta International Airport website, Fact Sheet http://www.atlanta-airport.com/Airport/ATL/ATL_FactSheet.aspx (accessed 30OCT, 2013)

efficient model for ferry security, the study should further research variations of behavior detection being utilized in airport security.

Behavior detection techniques have come under considerable scrutiny for use in airports. The JASON study, an independent report contracted by the Pentagon in 2008, and a multi-year Government Accountability Office 2010 report both cite the lack of any credible scientific data on Ekman's research with FACS.[144] Contrarily, DHS-TSA points to their success with FACS in 2006-2009, having conducted 232,000 secondary screenings, leading to over 1700 arrests.[145] Amidst the debate, DHS has nonetheless taken the next step in behavior detection with continued research on Future Attribute Screening Technology (FAST). An evolution of behavior detection, FAST tests the "malintent theory" by having passengers walk through a machine that serves as the equivalent of a human lie detector. Trained screeners look for increased heartbeat, sweating, erratic movement, and other physiological characteristics to determine anomalies using technology and human judgment. Initial scientific results suggest FAST may offer 70% accuracy,[146] making the system significantly better at pure behavioral detection than human screeners have shown to date. Advances in behavior detection are advocated as strong support of *risk-layering* and *effectiveness*. *Resiliency* of a behavior-detection system would depend on public receptivity; travelers in airports or ferries are often in a rush and stressed; the same physiological factors that indicate *malintent* may actually be stress indicators. If the FAST model can be shown to distinguish the difference between stress and malicious intent, and can enjoy some initial success in the

[144] Sharon Weinberger, "Airport Security: Intent to Deceive?" *Nature* 465, no. 7297 (05/27, 2010): 412-415
[145] Ibid., p. 414
[146] Ibid., p. 415

airport environment, then the same could be expected in a ferry environment. Passing the test of public receptivity and the *efficiency* demands of an airport suggest a FAST-type model would pass scrutiny in ferry security as well.

In a continued review of possible behavior detection procedure *efficiency*, there is value in adjusting perspective on transportation security in general. For illustration, there are two schools of thought that involve adjustments to airport screening without introducing new technologies. These philosophical approaches to security do not necessarily refute HTI; they compel a re-examination of the interface between humans and existing technologies. For example, Parks' research on "close-sensing"[147] states that a screening checkpoint is a process that combines machines (millimeter wave x-rays) as the first layer needed to sense anomalies and then human agents follow with actual touching. If HTI is applied correctly, the human uses the available tools to identify only the parts of a passenger's body that must be touched. Should this approach be categorically trained in both airports and cruise terminals, the security checkpoint experience would expectedly become increasingly *efficient* and *effective*. The idea of machine-first, human contact-second also utilizes *risk-layering*. In this case, *resiliency* increases relative to *efficiency*. When done right, passengers move through the transportation hub seamlessly, and process *resiliency* grows along with public confidence.

[147] Lisa Parks, "Points of Departure: The Culture of US Airport Screening," *Journal of Visual Culture*, 6, no. 2 (08, 2007): 183-200

In a similar approach, McLay, et al cites use of "security classes" as the future of airport screening.[148] The *classes* conform to the relative level of security risk posed by the passengers, depending on previous arrests, frequent-flyers, biometrics, etc. If implemented correctly, these "security classes" could be randomly re-ordered daily, or even by the hour, so passengers did not feel profiled or *marked* at security. This model would also allow newer screeners to work the lines of passengers posing lower risk, or to be mentored by more experienced security personnel who work the more challenging lines. The idea here is that new technologies are only as good as the people using them. Different technologies and HTI can apply differently dependent on how passengers are categorized for screening. In Parks and McLay's models, *efficiency, effectiveness* and *risk-layering* are inexpensive solutions that migrate easily between airport and cruise terminal security modes. It is critical that when evaluating the potential success of employing inter-modal models that we rely on introducing and training any *risk-layered* model in a method that advocates *effectiveness* for the terminal, *efficiency* for the passenger and system *resiliency*.

Table 3 compares the three models (TASS, Social Force Model and Behavior Detection) against the five selected variables. The Analysis Section will discuss each model's adherence or unsuitability to these variables and will explain why the Social Force Model was determined to be the best choice in meeting all five criteria defined by our Methodology.

[148] Laura A. McLay, Adrian J. Lee and Sheldon H. Jacobson, "Risk-Based Policies for Airport Security Checkpoint Screening," *Transportation Science,* 44, no. 3 (08, 2010): 333-349

	TASS	Social Force Model	Behavior Detection
Resiliency	***TBD***	✓	***TBD***
Effectiveness	✓	✓	***TBD***
Efficiency	***TBD***	✓	***TBD***
Risk-Layering	✓	✓	✓
Human Technology Interface	✓	✓	✓

Table 3: Cross-comparison of Models using Methodology *Criteria*

Analysis

Following a review of the literature, the original question was narrowed down regarding whether airport and rail security could apply to protecting passengers in the cruise ship and ferry terminal environments. Rail security was not pursued for several reasons. For one, the trove of literature on airport security outweighed any collegial dialogue available on rail security. It is unclear whether the subject of rail security has not been explored to the same extent as airport security, or whether rail protection details are shielded within industry trade craft from public exposure. A third option, as Waugh stated, is that rail security may simply be "indefensible". Unless every inch of rail is guarded, the task of maintaining a continuous set of exposed tracks is unmanageable, leaving the entire rail transportation system unprotected. In determining that rail security was not a model from which ferry or cruise security should borrow security concepts, the first deduction was to focus the methodology on airport security practices.

Seven *core principles* were gleaned from the literature review: resiliency, effectiveness, efficiency, risk-layering, intermodal regulations, refining security habits (training and testing), and use of assembly lines. The Chapter supported six of these core principles and elected to focus on the first four. Regulations are beyond the scope of this paper. In regards to security habits, training and testing should be incorporated regardless of the model (as should a public-private alliance). The principle that was not advocated is Assembly Lines; this can be a hazardous approach. The more a security system treats passengers alike in the vetting/boarding process, the more predictable a system becomes to the users. Predictability is equally detrimental to risk reduction; workers can become complacent to an assembly-line mentality.

A key, stand-alone concept inferred from the literature was the importance of a *human-technology interface* (HTI). I felt HTI was valuable enough to merit being identified as a necessary condition for the intervening variables being examined.

In looking at the Total Airport Security System (TASS), this type of approach at first seems nearly ideal. TASS employs a risk-layered approach by integrating security cues from around the airport for a human to investigate; meaning this model also aligns well with an emphasis on human-technology interface (HTI). As far as effectiveness, a model capable of compounding security situational awareness has multi-fold value in terms of effectiveness. Our reluctance to provide strong endorsement for using TASS in a ferry or cruise ship environment comes down to the relationship between resilience and efficiency. For instance, if TASS were to lose electrical power to a cruise terminal quadrant, or the exterior CCTV-feeds were disabled by wind shear, would workers know how to deliver contingency security on their own until the system came back up? TASS,

or similarly designed products, may be highly efficient when all systems are operating normally, but its' efficiency can be compromised in situations where the model is not highly resilient.

The concern here is that security would become so dependent on this all-solution technology that resilience could become suspect in the absence of a *total security* system. Until that resilience can be proven through use in the airport security industry over time, endorsement is on hold for use of this human-technology model. Wet, salty, and windy cruise ship and ferry environments will likely see technology fail from time to time and it is imperative the system be resilient when a technology is unavailable.

The Social Force Model is highly advocated for use in inter-modal transportation as a means to enhance uninterrupted visual acuity on passenger movement. My endorsement relies on the Social Force Model's ability to amplify the effectiveness and efficiency of a system, in this case, CCTV. From a ferry terminal perspective, any model that capitalizes on the current technology is a bonus. Ferry systems are typically a component of the public/state transportation system, so it is far more economical to enhance an existing security model than to replace the system entirely. A system like Social Force Model supplements the existing system; it does not replace the system. In light of current state budgetary restraints, a concept such as Social Force Model makes sense, as the technology can grow with upgrades, such as those to CCTV systems. The other advantage of the Social Force Model over a TASS-type process is the operator is not completely reliant on Social Force; if the link to the CCTV technology fails, the CCTV, for example, is presumably still working. As far as risk-layering, maritime security specialists should consider building redundancy into the technologies being used

by security professionals; redundancy adds a layer of security to passengers as well as for professionals who are increasingly reliant on technology.

In addition to redundancy, there must be a consistent element of randomness in airport, ferry and cruise terminal security. Randomness is not a concept prevalent in either the literature or data. Like airports, ferry and cruise security have departure and arrival times that must remain steadfast if passengers are going to use these services. The challenge for security personnel is meeting the demands of a clock-driven schedule, while adjusting use of the models. This could involve randomly switching qualified TASS operators, either by shift or assigned work areas. Allowing different sets of eyes to view a static terminal environment brings fresh perspective and encourages new ways of looking at security. This type of approach creates unpredictability for adversaries who may have learned the surveillance *routine*, and it also helps break security personnel from a mind-numbing cycle. Randomness in a ferry or cruise environment should also include random testing of security personnel and protocol. In addition to required drills onboard the vessels, random drills at terminals ashore help keep security personnel alert and prepared for both routine and worst-case scenarios.

A commonality between airport and ferry terminals is the high frequency, high volume nature of passenger movement. In both modes, passengers tend to assemble in congested queuing areas while waiting to board their transport modes (airplanes, ferries) for relatively short duration travel purposes. Processes involving behavior detection, for example may have utility in a congested and fast-paced ferry terminal. For ferries, where huge volumes of passengers often check-in minutes before ferry departures, this could involve use of skilled, roving behavioral detection security personnel. These roving

personnel could be used in combination with a new way of looking at ferry-arrival checkpoints. By example, a separate line could be assigned for frequent-ferry or early-arrival passengers. These could include travelers who have completed background checks and who predominantly commute daily, allowing them expedited passage through security. For thousands using the Staten Island Ferry and Washington State Ferry systems, this approach would embrace both *efficiency and effectiveness*. The caution would be allowing a system to become so user-friendly in the interests of profit that effectiveness was compromised. This is where ferry security agents could prove useful. Trained in a dual role, these agents could *randomly* validate frequent-ferry passengers' credentials to ensure a trustworthy system. The use of frequent- ferry passengers would naturally shorten the other check-in lines. On these remaining check-in lines, the behavior detection agents could rove, querying passengers who were exhibiting drunkenness, signs of drug use, or other suspicious physiological cues. It would be essential for these agents to be well-trained, mobile, and in continual interaction with command/control personnel watching the terminal from a remote location. Also crucial, behavior detection agents need to rapidly assess the intentions of the person-of-interest so as to avoid engendering panic in a congested area, and to facilitate the majority of passengers boarding the ferry in time. As there are no passenger lists for ferries, some form of behavior recognition training and protocols should be considered an imperative.

Just as with airports, this type of approach would require ferry passengers to tolerate a higher level of perceived intrusion. The approach would also need to consider passenger volume as rapid behavioral assessments would be vital in a fast moving transportation system. Locating these roving behavior detection agents near the terminal

entrance would help deter adversaries by their presence and perimeter patrols would minimize damage should the behavioral questioning go awry. Much like the Ben Gurion International Airport example, ferry security volume as compared to airports may allow trained screeners in a smaller transportation market to query anomalies without slowing down the overall transportation system. This approach would likely not work in the cruise industry, a travel industry as opposed to a mass transportation mode.

Conclusion

This study is intended to prompt discussion on how to develop a more holistic way of looking at reducing risk in a transportation-system. Traditionally, airports, ferries and the cruise industry have approached security of their transportation hubs with solutions that have emerged from within their respective fields. I contend that as transportation hubs around the globe continue to be threatened asymmetrically, it is important to think in an equivalent manner regarding how to address intangible issues before they reach the U.S and to identify measures needed to counter these threats. This Chapter proposes using the full transportation spectrum in order to devise those solutions. From a public transportation perspective, ferry security should evaluate airport protocols. In the privatized world of transportation (and travel), cruise ship terminals can benefit by looking to airport security as well. In terms of collaboration, public and private stakeholders must work together. In more than a decade since 9-11, airports have provided us with numerous prototypes. Both ferry and cruise terminals stand to benefit from adopting, and adapting risk-mitigation principles to their own worlds of work.

The models assessed are but a few of the options available when considering a cross-pollination of intermodal security practices. More important than the examples

provided in this Chapter are the core risk-management principles deemed necessary for solid U.S. transportation security and specifically, airport security. A well-rounded, risk-oriented foundation is based on incorporating not one, but several core principles, including efficiency, resiliency, effectiveness, and risk-layering. In summary, airport security models that emphasize the stated core principles, incorporate partnerships, indoctrinate randomness, and interweave humans with technology will transpose well as future ferry and cruise terminal security models.

Thesis Conclusion

The focus of this thesis has been on addressing risk-related issues peripherally related to the introductory scenario in which a U.S. port security incident would likely be associated with foreign shipping and originate overseas. This relationship makes a connection between piracy and U.S. maritime risk. For example, a ship being hijacked in the Straits of Malacca or robbed off Nigeria may actually be terrorists appearing to be pirates, especially if piracy is so commonplace it goes unheeded. The Straits are a location where piracy has always been a problem and the Gulf of Guinea is a region where piracy is at present, highly unopposed. In these situations, an anhydrous ammonia tanker stopped by pirates for several hours leaves enough time to cause damage. Divers can attach an explosive device or pirates can board with 14 pirates and leave with 12, a tactic that would intentionally strand stowaways onboard to accomplish their nefarious purposes before (or upon) reaching the U.S. Neither of these piracy-related situations is far-fetched. While many of our risk-reduction measures are designed to protect ports, it may be the ships arriving that actually serve as the Trojan horse, meaning it is too late to start protecting ports once a ship has already arrived.

These are the types of outliers that must be considered when viewing whether piracy has ties to terrorism in Indonesia. As mentioned, 70% of U.S. shipping transits the Straits of Malacca. This equates to thousands of large ships, destined for U.S. ports, all passing through a narrow chokepoint. Regional piracy has direct linkages to American security interests. If terrorists have actually eluded authorities, all is not lost. The terrorists can still be defeated. As Chapter 1 suggests, counter-piracy initiatives can also serve as effective counter-terrorism.

In terms of offshore piracy, the thesis also examines what types of risk-variables might threaten the U.S. As mentioned in Chapter 2, if pirates inadvertently alter how the EU imports Nigerian oil for example, then this aspect of offshore piracy may threaten the U.S., especially if Iran or Russia becomes alternate oil-providers to the EU. While the global implications of piracy impacting EU imports do not mesh with our original scenario, they still align with strategic U.S. risk-mitigation objectives. An envisioned situation in which the EU decreases Gulf oil imports is not implausible. The U.S. after all, has already reduced its own Nigerian imports. The U.S. however, has access to self-sustaining energy alternatives that Europe does not.

This thesis has attempted through the first two Chapters to demonstrate linkages between piracy and the originally stated scenario. Rather than being an exercise in fear-mongering; the thesis broadened the opening-scenario beyond U.S. seaports in order to trace the foreign piracy threats back to their source. The thesis also originally placed emphasis on the tenets of balancing resource limitations and prioritizing risk variables related to U.S. maritime security. Chapter 1, for instance, explored a nexus between piracy and terrorism. Chapter 2 analyzed how offshore piracy affects when the U.S. should view offshore piracy as a threat. Chapter 3 emphasized solutions and oriented the paper to the idea of *crossover utility*. If maritime security can adopt transportation best-practices that *actually* make airports safer, then emerging cruise ship markets or existing ferry terminals should modify and incorporate these approaches as well.

The study has also revealed an interesting aspect to maritime risk. Not every coastal nation wants the U.S. to help, yet nearly every nation hosts ports or vessels that link back to the U.S. In the Straits of Malacca, deploying a U.S. naval presence to

counter piracy would have likely elevated risk more than reducing it. In the Gulf of Guinea, Nigeria elected to protect its waters and objected to U.S. (or NATO) intervention. While U.S. efforts may have worked off Somalia, there was no Somalian government to object. The role of sovereignty is a variable that should be highlighted when calculating U.S. maritime risk. Fostering anti-American sentiments may be more caustic than any threat posed by piracy. Another aspect of maritime risk is that America is restrained in the ability to stop maritime threats beyond its own territorial seas and must, alternatively, find creative approaches to handling overseas threats.

On a personal note, my experience working with DHS' port security grants program (PSGP) has left two indelible impressions regarding an adaptive approach to maritime security. First, there is a deluge of good ideas taking place across the maritime transportation security domain. Second, there is limited funding to support all of these initiatives, nor would it be prudent to do so. Some of the grant proposals mirrored one another, others offered reduced value based on the unlikeliness of their contingencies and a few were simply cost unsustainable. I am convinced that protocols, such as those shown to be successful in air transportation hubs can be adapted to maritime security, and proposals that mitigate the vulnerability of ships requiring passage through dangerous foreign waters offer value when thinking through risk-reduction practices.

This thesis did not aim to *right-size* a singular approach to maritime transportation security. Instead, it traced the ground wires of U.S. domestic security concerns to piracy-related variables that originate in far-off places where U.S.-destined ships travel and anchor. In the course of the examination on piracy, the value of collaborative partnerships, strategic impacts, and overcoming challenges have come to light. Finally,

the thesis identified crucial technology attributes offering lateral value to ferry and/or cruise ship terminal security. Solutions that have already been field-tested in air or rail transportation security and come at a reduced expense offer proven techniques for risk-mitigation. Embracing transportation security measures that have crossover-utility permits the U.S. to remain agile and adaptive, two qualities that help offset the vulnerabilities of a continuous stream of foreign ships transiting in U.S. ports, or within immediate vicinity of ferry or cruise terminals - where thousands of passengers are waiting to embark.

Bibliography

Aiyetan, Dayo. 2013. Outgunned. *New Internationalist* (465) (09): 26-7.

Aljunied, Syed Mohammed Ad'ha. Countering Terrorism in Maritime Southeast Asia: Soft and Hard Power Approaches. 2012. *Journal of Asian and African Studies,* 2012, 47: 652-665

Allianz Global Corporate and Specialty. 2014. Shipping Losses Decline, but Emerging Risks Pose Serious Challenges to Marine Industry and Insurers. Accessed March 21, 2014 from http://www.agcs.allianz.com/about-us/news/shipping-review-2014/

Anyimadu, Adjoa. 2013. The Gulf of Guinea: Lessons Learned from the Indian Ocean *Chatham House, Africa* (02): 1-17

Baldauf, Scott. 2012. Next Pirate Hot Spot: The Gulf of Guinea. *Christian Science Monitor*, (02/28): N.PAG.

Banlaoi, Rommel C. 2005.Maritime Terrorism in Southeast Asia. *Naval War College Review*, 58 (4) (09): 63-80.

Barrios, Cristina. 2013. Fighting Piracy in the Gulf of Guinea, Offshore and Onshore, *European Institute for Security Studies*, Brief- Issue 20, (May): 1-4

Bateman, Sam, Joshua Ho, and Mathew Mathai. 2007. Shipping Patterns in the Malacca and Singapore Straits: An Assessment of the Risks to Different Types of Vessels. *Contemporary Southeast Asia: A Journal of International & Strategic Affairs*, 29 (2) (08): 309-32.

Bloch, Paul, and Claire Payne. 2006. Optimizing Passenger Security-Screening Operations. *Journal of Airport Management* 1 (1) (Sep): 9-16.

Bradford, John F. 2008. Shifting the Tides against Piracy in Southeast Asian Waters. *Asian Survey*, Vol. 48, No. 3 (May/June), pp. 473-491

Calder, David. 2010. Who Says 'Passengers aren't Baked Beans'? Making Passenger Security Screening Productive while Delivering High Service Levels. *Journal of Airport Management* (4) (Jul): 335-9

Chalk, Peter. 2010. Assessing the Recent Terrorist Threat to the Malacca Strait. *CTC Sentinel*, April, Vol. 3. Issue 4

Chalk, Peter. 2008. The Maritime Dimension of International Security: Terrorism, Piracy, and Challenges for the United States. *RAND-Project Air Force*, Santa Monica, CA

Cohen, Herman. 2008. Nigeria: A Well-Oiled Federation. *Journal of International Peace Operations* 4 (2) (Sep): 31-32.

Collier, Paul. 2000. Doing Well out of War: An Economic Perspective, in M. Berdal and D. Malone (eds. *Greed and Grievance: Economic Agendas in Civil Wars* (Lynne Rienner, Boulder, CO): 91–112.

Cox, Andrew, Fynnwin Prager, and Adam Rose. 2011. Transportation Security and the Role of Resilience: A foundation for Operational Metrics. *Transport Policy* 18 (2) (03): 307-17.

Diedam, John. 2009. Access control: The Process of Securing a Transportation Site. *Journal of Airport Management* (3) (Apr): 263-73.

Drumbl, Mark A. 2013. Child Pirates: Rehabilitation, Reintegration, and Accountability. *Case Western Reserve Journal of International Law* 46, No. 1: 235-278

Dunn, Halle (LCDR) date unk. Oil Pirates of the Niger Delta. *JCSP 35, Canadian Forces College*: 1-116

Eldar, Zamir. 2010. The Human Factor in Aviation Security. *Journal of Airport Management* 5 (1) (Oct): 34-9.

Florence, Justin and Friedman, Robert. 2010. Profiles in Terror: A Legal Framework for the Behavioral Profiling Paradigm. *George Mason Law Review*, Vol. 17:2, 423-480.

FPSO World Fleet, FPSO Info Accessed October 4, 2014 from. http://www.fpso.net/page7.html

Ghavamifar, Kamran, Payam Bakhshi, and Ali Touran. 2010. Owner's Control and Risks in Various Airport Delivery Methods. *Journal of Airport Management* 5 (1) (Oct): 40-50.

Gjelsvik, Ingvild Magnæs, and Tore Bjørgo. 2012. Ex-Pirates in Somalia: Processes of Engagement, Disengagement, and Reintegration. *Journal of Scandinavian Studies in Criminology & Crime Prevention* 13 (2) (12): 94-114.

Government Accountability Office (GAO), Maritime Security: Ongoing U.S. Counter-piracy Efforts Would Benefit From Agency Assessments, GAO-14-422: Published: Jun 19, 2014. Publicly Released: Jun 23, 2014. Accessed October 7, 2014 from http://www.gao.gov/products/ (GAO-14-422, Executive Summary)

Gulf of Guinea (staff article): New Danger Zone? 2013. *New African* (526) (03): 10-14.

Gunasekaran, Periasamy. 2012. Malaysian Port Security: Issues and Challenges. *Australian Journal of Maritime & Ocean Affairs* (Australian Association for Maritime Affairs Incorporated), June, Vol. 4 Issue 2, pp. 56-68

Hansen, Stig Jarle. 2012. The Dynamics of Somali Piracy. *Studies in Conflict & Terrorism* 35 (7) (Jul): 523-30.

Howell, Llewellyn D. 2006. Pirates: Scourge of the Modern Seas. *USA Today Magazine* 134 (2732) (05): 18-22.

Hartsfield-Jackson, Atlanta International Airport website. 2013 Fact Sheet. Accessed October 30th from http://www.atlanta-airport.com/Airport/ATL/ATL_FactSheet.aspx

Hibbert, Lee. 2012. Alert to the Real Dangers. *Professional Engineering* 25 (11) (11): 24-6.

Ho, Joshua. 2011. Maritime Security and Piracy: Will it Remain Safe? *Issues in Human Security in Asia* (01): pp. 166-8.

International Chamber of Commerce. 2014. International Maritime Bureau Piracy Reporting Center (IMB-PRC), Piracy & Armed Robbery News & Figures. Accessed October 3rd, 2014 from http://www.icc-ccs.org/piracy-reporting-centre/piracynewsafigures

International Chamber of Commerce.17OCT2013. Piracy at Sea Falls to Lowest Level in Seven Years. ICC Commercial Crime Services, Accessed April 1, 2014 from http://www.icc-ccs.org/news/873-piracy-at-sea-falls-to-lowest-level-in-seven-years-reports-imb

International Maritime Organization. 2014. Piracy and Armed Robbery against Ships Accessed September 30, 2014 from http://www.imo.org/OurWork/Security/PiracyArmedRobbery/Pages/Default.aspx

Johnston, Van R. 2004. Terrorism and Transportation Policy and Administration: Balancing the model and equations for optimal security. *Review of Policy Research* 21 (3) (05): 263-74.

Johnston, Van R., and Jeremy F. Plant. 2008. Rail Security after 9/11. Toward effective collaborative regulation. *Public Works Management & Policy* 13 (1) (July): 12-21.

Johnstone, R. W. 2007. Not Safe Enough. *Issues in Science & Technology* 23 (2) (Winter2007): 51-60.

Kashubsky, Mikhail. 2011. A Chronology of Attacks on and Unlawful Interferences with, Offshore Oil and Gas Installations, 1975–2010. *Perspectives on Terrorism* 5 (5-6) Accessed September 30, 2014 from http://www.terrorismanalysts.com/pt/index.php/pot/article/view/offshore-gas-and-oil-attacks/html

Katsouris, Christina and Sayne, Aaron. 2013. Nigeria's Criminal Crude: International Options to Combat the Export of Stolen Oil. *Chatham House*: 1-85

Khalid, Nazery. 2009. With a Little Help from my Friends: Maritime Capacity-Building Measures in the Straits of Malacca. *Contemporary Southeast Asia: A Journal of International & Strategic Affairs*, 31 (3) (12): 424-46.

Kim, Suk Kyoon. 2011. Maritime Security Initiatives in East Asia: Assessment and the Way Forward. *Ocean Development & International Law,* 42 (3) (Jul): 227-44.

Kürsener, Jürg E. 2007. Straits of Malacca and Singapore – Unique Choke Points. *Naval Forces,* 28 (2) (04): 23-33.

Lennerman, Anders. 2012. Protecting the Airport from an Insider Threat: A Systematic Approach to Aviation Security. *Journal of Airport Management* 6 (3) (Summer2012): 225-30.

Lorenz, Akiva J. 2007. Al Qaeda's Maritime Threat. *Intelligence and Terrorism Information Center* at the Israel Intelligence Heritage & Commemoration Center *(IICC)*

Mañe, Damian Ondo. 2005. Emergence of the Gulf of Guinea in the Global Economy: Prospects and Challenges. *International Monetary Fund Working Paper*, WP/05/235

Mazzon, Riccardo, and Andrea Cavallaro. 2013. Multi-Camera Tracking using a Multi-Goal Social Force Model. *Neurocomputing* 100 (01/16): 41-50.

McLay, Laura A., Adrian J. Lee, and Sheldon H. Jacobson. 2010. Risk-Based Policies for Airport Security Checkpoint Screening. *Transportation Science* 44 (3) (08): 333-49.

Murphy, Martin N. 2013. Petro-Piracy: Oil and Troubled Waters. *Foreign Policy Research Institute* 57, No. 3: 424-37.

———.2013. Security Responses to Piracy in Southeast Asia, West Africa and Somalia. *Emirates Lecture Series* (111) (12): 1-60

———.2008. The Unwanted Challenge. *U.S. Naval Institute Proceedings,* 134 (12) (12): 48-51.

———.2007. Suppression of Piracy and Maritime Terrorism. *Naval War College Review,* 2007, 60 (3) (Summer): 23-45.

Neptune Maritime Security. 2013. U.S. State Department's OSAC Reviews Gulf of Guinea Threats Accessed October 7, 2014 from http://www.neptunemaritimesecurity.com/u-s-state-departments-osac-reviews-gulf-of-guinea-threats/

Nincic, Donna J. 2005. The Challenge of Maritime Terrorism: Threat Identification, WMD and Regime Response. *Journal of Strategic Studies*, 28:4, 619-644

Oceans beyond Piracy. 2013. Accessed February 25, 2014 from http://oceansbeyondpiracy.org/matrix/malacca-strait-patrols

Ong, Graham Gerard. 2006. The Threat of Maritime Terrorism and Piracy. *Regional Outlook*: 12-5.

Parks, Lisa. 2007. Points of departure: The Culture of US Airport Screening. *Journal of Visual Culture,* 6 (2) (08): 183-200.

Percy, Sarah, and Anja Shortland. 2013. The Business of Piracy in Somalia. *Journal of Strategic Studies*, 36:4, 541-578

Pham, J.Peter. 2010. Beyond the Water's Edge: Learning from the Somali Piracy Challenge *Journal of International Peace Operations* Volume 6, Number 2 — September-October

Plant, Jeremy F. 2004. Terrorism and the Railroads: Redefining Security in the Wake of 9/11. *Review of Policy Research* 21 (3) (05): 293-305.

Port of Seattle, Seattle's Downtown Cruise Terminals. 2013. Accessed November 7th, 2013 from http://www.portseattle.org/cruise/Pages/default.aspx

Rodríguez, David M. (General, US Army), 5MAR2014. Commander, United States Africa Command (AFRICOM) before the *House Armed Service Committee Posture Hearing*, Accessed October 7, 2014 from http://www.africom.mil/ (p. 13)

Samatar, Abdi Ismail, Lindberg, Mark, and Mahayni, Basil. 2010. The Dialectics of Piracy in Somalia: The Rich versus the Poor. *Third World Quarterly* 31 (8) (12): 1377-94

Samola, Betty. 2008. Innovations in Passenger and Baggage Processing at Schiphol Airport. *Journal of Airport Management* 2 (3) (Apr): 227-34.

Shoichet, Catherine E., Starr, Barbara. 25OCT2013. 2 Seized in Pirate Attack off Nigeria. *CNN,* Accessed October 2, 2014 from http://www.cnn.com/2013/10/24/world/africa/nigeria-vessel-attack/

Sinai, Joshua. 2012. New Trends in Airport & Aviation Security. *Journal of Counterterrorism & Homeland Security International* 18 (3) (Fall): 30-7.

Szyliowicz, Joseph S. 2013. Safeguarding Critical Transportation Infrastructure: The US Case. *Transport Policy* 28 (07): 69-74.

——. 2004. International Transportation Security. *Review of Policy Research* 21 (3) (05): 351-68.

Tepp, Eero. 2012. The Gulf of Guinea: Military and Non-Military Ways of Combatting Piracy. *Baltic Security & Defense Review* 14 (1) (01): 181-214.

Thinnes, Billy. 2013. Impact. *Hydrocarbon Processing* 92, No. 11: 9-12.

Trelawny, Chris. 2013. Piracy in West Africa: A Symptom of Wider Problems? *New African* (526) (03): 16-21.

Raymond, Catherine Zara. 2009. Piracy and Armed Robbery in the Malacca Strait. *Naval War College Review*, 62 (3) (Summer): 31-42.

ReCAAP. Definitions and Methodology in Classifying Incidents. Accessed 25FEB2014 from http://www.recaap.org/DesktopModules/Bring2mind/DMX/Download.aspx?Command=Core_Download&EntryId=290&PortalId=0&TabId=78

Roach, J. A. 2005. Enhancing Maritime Security in the Straits of Malacca and Singapore. *Journal of International Affairs,* 59 (1) (Fall): 97-116.

Rosenberg, David, and Christopher Chung. 2008. Maritime Security in the South China Sea: Coordinating Coastal and User State Priorities." *Ocean Development & International Law*, 39 (1) (Jan): 51-68.

Sri Mohd Najib Tun,Abd Razak. 2005. Enhancing Maritime Security Cooperation. *Monch Publishing Group*, Vol. 29.

Tan, Andrew T.H. 2007. Singapore's Cooperation with the Trilateral Security Dialogue Partners in the War Against Global Terrorism. *Defense Studies*, Vol. 7, No. 2 (June), pp. 193–207

Ukiwo,Ukoha. 2007. "From 'Pirates' to 'Militants': A Historical Perspective on Anti-State and Anti-Oil Company Mobilization among the Ijaw of Warri, Western Niger Delta", *African Affairs*, Oxford University Press on behalf of Royal African Society. 106/425: 587–610

United Nations Security Council. 2014. Security Council Resolutions, Accessed October 3rd 2014 from http://www.un.org/en/sc/documents/resolutions/index.shtml

Ünlü, Nihan. 2006. Current Legal Developments: Straits of Malacca, Protecting the Straits of Malacca and Singapore against Piracy and Terrorism." *International Journal of Marine and Coastal Law,* Vol. 21, No 4 539-549

U.S. Energy Information Administration (EIA), 16OCT2012. Nigeria Analysis/Production, revised 30DEC 2013. Accessed October 1, 2014 from http://www.eia.gov/countries/cab.cfm?fips=NI

———.Upcoming Oil Projects in Nigeria. 30DEC2013 Accessed October 2, 2014 from http://www.eia.gov/countries/cab.cfm?fips=NI

Vidal, John. 2013. £1 Billion a Month: the Spiraling Cost of Oil Theft in Nigeria *The Observer,* 05OCT2013. Accessed October 1, 2014 from http://www.theguardian.com/global-development/2013/oct/06/oil-theft-costs-nigeria

Washington State Department of Transportation, 2013 Ferry Schedule Information (by route), Accessed November 7th, 2013 from http://www.wsdot.com/ferries/schedule/

Waugh Jr., William L. 2008. Assessing the Risk to Rail and Transit Systems. *Public Manager* 37 (4) (Winter): 71-6.

———.2004. Securing Mass Transit: A Challenge for Homeland Security. *Review of Policy Research* 21 (3) (05): 307-16.

Weinberger, Sharon. 2010. Airport security: Intent to Deceive? *Nature* 465 (7297) (05/27): 412-5.

Weir, Gary. 2010. Chapter 13 of Piracy and Maritime Crime: Historical and Modern Case Studies, edited by Bruce Elleman, Andrew Forbes, and David Rosenberg *Naval War College Press*, Newport Paper 35: 5-7

Weiss, William E. 2011. Development and Use of the Dynamic Security Model for Airports. *Journal of Airport Management* 5 (3) (Apr): 245-54.

Whitman, Shelly L. 2013. Children and Marine Piracy. *Case Western Reserve Journal of International Law* 46 (1): 217-34.

Young, Adam J. and Valencia, Mark J. 2003. Conflation of Piracy and Terrorism in Southeast Asia: Rectitude and Utility. *Contemporary Southeast Asia,* Vol. 25, No. 2 (Aug)

Zimmerman, Rae, and Jeffrey S. Simonoff. 2009. Transportation Density and Opportunities for Expediting Recovery to Promote Security. *Journal of Applied Security Research* 4 (1) (01): 48-59.

Curriculum Vitae

Commander Mark Kuperman (U.S.C.G.) was born in Los Angeles, CA. in 1971. He was commissioned through Officer Candidate School in 1999. He holds a Bachelor of Arts degree in English from Binghamton University and a Master of Science in Health Science (Emergency Management and Disaster Preparedness) from Trident University, where he graduated with *summa cum laude* honors. He graduated Johns Hopkins University's Advanced Academic Programs (AAP) in December 2014 with a Master of Arts in Global Security Studies, and a concentration in Strategic Studies.