NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

TERRORISM IN THE MARITIME DOMAIN

by

Eng Hock Tng

March 2013

Thesis Advisor: Gary O. Langford
Second Reader: John Osmundson

Approval for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704–0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202–4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704–0188) Washington, DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** March 2013	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE TERRORISM IN THE MARITIME DOMAIN		**5. FUNDING NUMBERS**	
6. AUTHOR(S) Tng, Eng Hock			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943–5000		**8. PERFORMING ORGANIZATION REPORT NUMBER**	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A		**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number ____N/A____.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approval for public release; distribution is unlimited		**12b. DISTRIBUTION CODE**	

13. ABSTRACT (maximum 200 words)

The impact of the September 11, 2001, attack by Al Qaeda was felt worldwide with increased security measures. However, maritime security measures are not as encompassing. This thesis investigated the possibility of maritime domain terrorism threats and what could be done to prevent such attacks as modeled on the basis of system of systems. Only certain terrorist groups have the capability to launch maritime terrorist attacks. The terrorist motives are to spread their political message, responding to what they have perceived as oppression. The system of systems model suggests (and is validated) that container vessels and cruise ships are potential targets, with possible human and economic consequences. However, these maritime targets failed to match the terrorist groups' objectives. Political assets such as warships and land-based maritime infrastructure align well to terrorist motives. Enhanced security measures protecting military and maritime infrastructure may require terrorists to use uncommon forms of attack. Terrorists could use submersible vehicles to remain undetectable. Costly submersible vehicles limit the type and number of terrorist groups that can employ such capability.

14. SUBJECT TERMS Terrorism, Human System			**15. NUMBER OF PAGES** 79
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540–01–280–5500

Standard Form 298 (Rev. 2–89)
Prescribed by ANSI Std. 239–18

THIS PAGE INTENTIONALLY LEFT BLANK

Approval for public release; distribution is unlimited

TERRORISM IN THE MARITIME DOMAIN

Eng Hock Tng
Civilian, Defence Science and Technology Agency
B.Eng., National University of Singapore, June 2006

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN SYSTEMS ENGINEERING

from the

NAVAL POSTGRADUATE SCHOOL
March 2013

Author: Eng Hock Tng

Approved by: Gary O. Langford
Thesis Advisor

John Osmundson
Second Reader

Cliff Whitcomb
Chair, Department of Systems Engineering

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The impact of the September 11, 2001, attack by Al Qaeda was felt worldwide with increased security measures. However, maritime security measures are not as encompassing. This thesis investigated the possibility of maritime domain terrorism threats and what could be done to prevent such attacks as modeled on the basis of system of systems. Only certain terrorist groups have the capability to launch maritime terrorist attacks. The terrorist motives are to spread their political message, responding to what they have perceived as oppression. The system of systems model suggests (and is validated) that container vessels and cruise ships are potential targets, with possible human and economic consequences. However, these maritime targets failed to match the terrorist groups' objectives. Political assets such as warships and land-based maritime infrastructure align well to terrorist motives. Enhanced security measures protecting military and maritime infrastructure may require terrorists to use uncommon forms of attack. Terrorists could use submersible vehicles to remain undetectable. Costly submersible vehicles limit the type and number of terrorist groups that can employ such capability.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

APEC	Asia-Pacific Economic Cooperation
ASG	Abu Sayyaf Group
ATSA	Aviation and Transportation Security Act
CBP	Customs and Boarder Protection
CLIA	Cruise Line International Association
CSCAP	Council for Security Cooperation in the Asia Pacific
CSI	Container Security Initiative
CWS	Coast Watch System
EEZ	Exclusive Economic Zones
JI	Jemaah Islamiyah
LTTE	Liberation Tigers of Tamil Eelam
PLF	Palestine Liberation Front
PLO	Palestine Liberation Organisation
PSCs	Private Security Companies
SDV	Swimmer Delivery Vehicles
SLN	Sri Lanka Navy
TBA	Tri-Border Area
TEUs	Twenty-Foot Equivalent Units
TSA	Transportation Security Administration
UNCLOS	United Nations Convention on the Law of the Sea
UUV	Unmanned Underwater Vehicle

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

The way of life in the United States of America changed after Al Qaeda terrorist attacked New York City and Washington, D.C., on September 11, 2001. The impact of those attacks was felt worldwide with increased security measures. Unlike the air travelers, maritime security measures were not as encompassing. Whereas nearly all air cargo is inspected, the bulk of cargo transported by ship is either not inspected or only partially inspected. This thesis looks into the possibility as well as the nature of maritime domain terrorism threats and what could be done to prevent such attacks. Noted attention to the specific makeup and characteristics of terrorists, terrorist groups, and specific terrorist methods are dealt with in the early chapters. A system of systems model is then presented.

Terrorist groups are characterized by their hierarchical pyramid structure. There are certain terrorist groups like Al Qaeda, Liberation Tigers of Tamil Ealam (LTTE) and Jemaah Islamiyah (JI) who have the financial resources and capability to launch maritime terrorist attacks. Their motives are to generate public attention and to spread their political message. They are responding to what they perceived as oppression. "Terrorism is generally the tool of the weak; the weak do not expect to get all they desire, and accept the possibilities of compromise during the course of negotiations, as long as they get *adequate* relief from the oppression against which they are fighting," (de Bivot, 2008).

Container vessels and cruise ships are potential targets. The attack of these targets will usually cause human and economic losses. Historically, attacks on container vessels and cruise ships seem to have failed to match the terrorist groups' objectives. This mismatch is perhaps due to the intent which has been to negotiate for release of imprisoned terrorists, with the intent of having minimal impact on the number of "innocents" affected (as with the death of Leon Klinghoffer, an American passenger on the Achille Lauro Cruise Ship in October 1985 to secure release of 50 Palestinian prisoners from Israel (Walker, 2010). However, Al Qaeda planner Younis al Maruretani, plotted to destroy a cruise ship and its several thousand passengers (Robertson,

Cruickshank, and Lister, 2012). Political assets such as massive deaths on a cruise ship or warships will align to terrorist motives.

Attacking armed military vessels is difficult as the security measures surrounding them will be extensive. Countries can improve their security measures by collaborating between the nations in fostering a better system to eradicate the terrorist groups. A more capable exchange of intelligence among intelligence agencies also helps in combating the intentions and execution of plans of terrorist groups.

To overcome intensive security measures, terrorist groups might use other forms of attack. Employing the tactics used by drug cartels in delivering their cargoes, submersible vehicles move quietly undetected over great distances in open water. Submersibles are difficult to detect and have the capacity to carry many tons of cargo. A single submersible or a small group of these submersibles might be an avenue by which the terrorist groups could execute their mission with deadly results. While these vehicles are expensive for the terrorist groups, if the objectives are met with submersibles, terrorists would find willing shipbuilders. With the improvement of technology and proliferation of the requisite shipbuilding skills, such underwater systems might be more affordable in the future. Authorities should be prepared and well-equipped to deal with such evolutionary threats in the maritime domain.

System of systems thinking is typically relegated to complex systemic conditions and behaviors. Specifically, the architecting of or analysis through modeling of a system of systems is at its earliest stage of maturity. Consequently, the approach taken in this research was to build on the theory of integration (Langford, 2012) to determine if a systems theory was germane and palpable to a system of systems viewpoint of terrorism in the maritime domain.

ACKNOWLEDGMENTS

I would like to thank my thesis advisor, Professor Gary O. Langford, for his effort and patience in guiding me throughout my thesis work. His comments are enlightening and his encouragements are heartwarming. He is knowledgeable and always followed through whenever I encountered difficulties in the learning. I am grateful to him for providing me such a conducive learning environment.

I would also like to thank my thesis second reader, Professor John Osmundson, for taking the effort in reviewing and providing valuable feedback for my thesis.

Lastly, I would like to thank my fiancée, Sze Yue, for her constant love and concern throughout this period. She is the reason why I managed to push through this graduate program.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

The way of life in the United States of America changed broadly and permanently after Al Qaeda terrorists attacked New York City and Washington, D.C., on September 11, 2001. The impact of those attacks was felt worldwide resulting in increased security measures (Lawrence, 2011). International and domestic air-travelers must now move through security check points, take off their shoes, be radiographed, and restrict their carry-on items (e.g., small quantities of fluids). As with air travel, unattended bags or packages on public transports such as trains and buses are presumed suspicious. Following the enactment of the Aviation and Transportation Security Act (ATSA) on November 19, 2001, air and land travel for passengers, baggage, and freight has been managed to achieved heightened security across the United States of America's 429 commercial airports (Blalock, Kadiyali, & Simon, 2007). A survey taken by Unisys Corporation in 2010 ("Most Americans Willing to Sacrifice Some Privacy to Enhance Safe Air Travel, According to Latest Unisys Security Index," 2010) indicates 93 per cent of Americans are willing to give up some privacy for increased security when using air travel. Noting that there are differences in perceptions between peoples of different countries, a uniform system of security measures, procedures, and equipment has not been forthcoming. Consequently, those differences reduce the overall security level to a commonly held denominator. The result is various points of "weaker" security measures that may in some manner jeopardize the integrity of the global security system. Moreover, heightened vigilance is also prevalent in the cruise ship industry. Similar screening of their passengers is in force, but the bulk of ship transport of cargo is only partially inspected. Maritime terrorism is a distinct possibility. This thesis looks into the possibility of maritime domain terrorism threats and what could be done to prevent such attacks through the perspective of a system of systems paradigm based on the theory of systems integration (Langford, 2012).

A. BACKGROUND

About 71 per cent of the Earth's surface is covered by water. One out of six jobs in the United States of America is marine-related and over one-third of the United States of America's Gross National Product originates in coastal areas ("Ocean," n.d.). The bodies of water on the Earth's surface play a very important role as they provide transportation and connection between continents for large quantities of goods. This commerce affects the economies of all countries. The overall dependency on the bodies of water for trades is causal to the wellbeing of the world's population. Thus, it is paramount that these countries ensure the safety of the bodies of water.

1. Maritime Terrorism

Terrorism refers to the unlawful use, or threatened use, of force or violence against persons, societies, cultures or governments motivated by political ends in order to create a desired change. The change sought by terrorists may be political, religious, or social in nature ("What is Terrorism?," n.d.). Therefore, maritime terrorism is defined for this thesis to be the politically motivated violence against persons, societies, cultures or governments that are related to the maritime domain. The Council for Security Cooperation in the Asia Pacific (CSCAP) Working Group defines maritime terrorism as the undertaking of terrorist acts and activities, using or against vessels or fixed platforms at sea or in port, or against any one of their passengers or personnel, against coastal facilities or settlements, including tourist resorts, port areas and port towns or cities (Chalk, 2008). Both definitions are similar and focus on the act of violence against different targets within the maritime domain.

Here, we distinguish between terrorism and piracy. In Article 101 of the 1982 United Nations Convention on the Law of the Sea (UNCLOS) ("United Nations Convention on the Law of the Sea," n.d.), it defined piracy as

> any illegal acts of violence or detention, or any act of depredation, committed for private ends by the crew or the passengers of a private ship or a private aircraft, and directed: (i) on the high seas, against another ship or aircraft, or against persons or property on board such ship or aircraft;

(ii) against a ship, aircraft, persons or property in a place outside the jurisdiction of any State.

The definition for maritime terrorism and piracy appears to be similar. However, there are differences between the two. Firstly, the motivations behind the attack are different. For terrorism, it is usually due to political oriented. As for piracy, it is usually for economic reason. Another difference is the geography of the attack. For terrorism, it includes both the open seas and the coastal targets whereas piracy only focuses on the high seas or area outside the jurisdiction of any State. That being said, there are also some instances where certain coastal targets attacks are classified as piracy. This thesis discusses the objectives of terrorism in Chapter II. Chapter 0 investigates the key terrorist groups that possess maritime capabilities. Chapter IV discusses on some possible terrorist targets

A system engineering approach is use to understand the interaction between the terrorism and the authorities in Chapter VIII. The boundaries and boundary conditions identified helps to review the security measures. A system of systems model represents the various groups and looks into the possible conditions that sustain the terrorist system. The system of systems model enables the assessment of the situations in a holistic approach.

2. Possible Maritime Targets

As defined earlier, maritime targets includes vessels or fixed platforms at sea or in port, associated passengers or personnel, and coastal facilities or settlements including port with its surrounding towns, cities, and infrastructure. There are numerous potential targets that may be of interest to terrorists. Some examples include cruise ships, container vessels, ports, naval bases, off-shore oil rigs, rail and trucking depots, warehouses, and coastal resorts. The research paper discusses some of these targets in Chapter IV while Chapter VI looks into possible future targets.

B. RESEARCH QUESTIONS

The research work utilizes the following questions as a guiding tool in laying out the content.

- Can a system of systems perspective be useful in determining the maturation of a terrorist group?
- Why is the maritime domain chosen by terrorists?
- Which type of terrorists are the threats?
- Where are the likely areas for terrorist attacks?
- What are the consequences of a maritime terrorist attack?
- What means are available to neutralize the effects of these threats?

II. MOTIVES OF MARITIME TERRORISM

A. MARITIME TERRORISM

Terrorist groups are typically characterized by their hierarchical pyramid structure and utilized a centralized command system. However, there are notable examples of heterarchical organizational structures (i.e., Al Qaeda, and Second Network). Historically, according to the RAND Corporation's terrorism database, maritime terrorist attacks have accounted for about two per cent of all terrorism incidents since 1969 (Lorenz, 2007). Terrorist groups have preferred not to venture into the maritime domain as seafaring skills are needed in addition to incurring greater expenses than land-based operations. Maritime attacks require different knowledge, skills, and abilities than necessary for land-based attacks, in addition to a wide range of necessary resources and equipment (such as boats and ships) to carry out a maritime related attack. Furthermore, many of these terrorists groups are not located near to coastal regions. Therefore, these "inland" groups do not have the means to perform maritime terrorist acts. The result of this required specialization is a strong preference to continue with land-based terrorist attacks. Notably, there are some terrorist groups who have certain maritime capabilities. These terrorist groups include Liberation Tigers of Tamil Eelam (LTTE), Al Qaeda, Palestine Liberation Front (PLF), Jemaah Islamiyah (JI), Abu Sayyaf Group (ASG) (Lorenz, 2007).

Regardless of the type of terrorist groups, their motives are identical. They are only interested in generating public interests and attracting the attention of the media (Lorenz, 2007). The typical means of attracting attention include bombings (explosive and fire), kidnappings, hostage taking, assassinations, arson, hijackings, skyjackings, cyber destruction, and nuclear, chemical, and biological releases. Terrorists continue to evolve their tactics and expand their means based on changes in technology. Consequently, terrorist acts continually adapt to both defense tactics and innovations that bring new tools and means. Moreover, terrorists have capitalized on technological improvements for more responsive communications, greater economic benefit, and

increased levels of operations. Surveillance capabilities have been enhanced, damage assessments after an attack are more accurate, and transportation has been improved.

The maritime domain poses different problems for terrorists than land-based operations. Technology helps to extend the reach of terrorism into the maritime domain. Since vessels may be out in open waters, they will be out of sight and easy reach of the media. As such, an attack on the ships in the open sea will not create as much publicity as those attacks on land vehicles (Chalk, 2008). Further, the details of such an attack will be less definitive and encumbered without "live video." Therefore, it is highly likely that terrorists will only target vessels that are beneficial to their political motives (Nelson, 2012). As highlighted by Lawrence de Bivort, terrorists are generally politically motivated. Terrorists respond to what they perceive as oppression and the oppression may be military, political, social, economic, civil rights denial, or even cultural (Bivort, 2008). Maritime threats may include vessels with iconic value (e.g., naval ships), vessels that when attacked might disrupt economic activity, and vessels which could be used as a weapon of mass destruction.

1. Mind of a Terrorist (Lawrence de Bivort)

Lawrence de Bivort's report on the cognitive patterns of terrorists, their organization, and strategies (Bivort, 2008), identified the six characteristics of a "typical" terrorist. Terrorists

- are rightly convinced of a profound moral cause;
- perceive themselves as reacting to oppression;
- aim to reduce oppression rather than destroy those that oppress;
- concentrate on the needs of their group rather than society at large;
- believe in the path to negotiation as the expected outcome; and
- expect negotiation to be successful if adequate relief is received.

As such, the vast majority of terrorists are rational, directed toward positive goals to improve conditions, generally define with interests in terms of their local group or community, and have a positive view toward the strategy of negotiation.

de Bivort's report was based on an extensive set of interviews with individuals designated as terrorists by either the United Nations or the United States. Terrorists are generally politically motivated (an attribute that distinguishes terrorists from pirates). The terrorist (assuming the role of an insurgent) is to use attacks on people and infrastructure to show the ineptitude of government and their inability to protect, illuminate the authoritarian nature of the government leaders, expose the dependency of government on foreign interests, highlight the non-interest in the people, and to point out the inability of the government to eliminate the terrorist group (de Bivort, 2008). The use of violence is justified in the mind of the terrorist.

In general, the terrorists' plans are rationally reasonable reflections of their objectives and operational environments. Terrorists are able to focus on their objectives and adjust their plans to improve their probability of success. Terrorists are an adaptive, learning group. Terrorists believe that even suicide missions are rational and often promote self-commitment and unwavering dedication to the cause. Their concept is more of a 'martyr' than 'suicide'. Terrorists view their objectives positively as they are trying to improve their communities and relieve their constituency from the oppressions that were the call to action. Terrorists also focus on the needs of their group instead of the larger society. The premise is that no government should subjugate or deny any group of like-minded people under national governance. The terrorist leaders feel a strong sense of responsibility for the well-being of their community and justification for their cause. Terrorists can associate themselves to their cause (as moral and just) and they believe not just in their indispensability, but in their infallibility as leaders of the cause. A strong motivator for following the terrorist leader sometimes derives from a religious affiliation. Religion is a method of reaching out to those who are neutral to their activities, but share a common kinship or affiliation with those impacted by unjustness. Terrorists place distinct differentiation between those who support the cause and those who oppose the cause.

Depending on the system of governance, terrorist will adapt their tactics to accomplish their objectives. In general, the terrorist strategies begin with verbal demands for redress and then escalate if those demands are met with ire and oppression (or are

simply ignored). de Bivort identifies ten strategies that are often used by terrorist, listed in order that reflects increasing frustration in being able to achieve their objective(s).

1. making verbal demands
2. making threats that action will take place to get attention
3. carrying out civil disruption (e.g., strikes)
4. appealing for international assistance
5. sabotage against targets selected to embarrass government
6. attacks against symbols and property of government
7. attacks on government officials, police, and military
8. inconveniencing the general population (including violence)
9. disrupting the general population (including violence)
10. terror actions to "shock and awe" the general population

The ranking of the terrorist strategies reflects the degree of violence associated with each, increasing from items designated as category "1" to category "10."

Ultimately, terrorists expect negotiations will occur with their oppressors. The negotiation might reduce the oppressions faced. However, sometimes conflicts arise within the terrorist groups on both what degree of violence is sufficient and how the negotiations should be carried out. In the course of negotiation, the terrorists are willing to compromise, on the conditions they are able to get sufficient relief from the oppressors against which they are fighting.

Interestingly, few of the terrorists are inclined to the use of violence aimed at civilians and other 'innocent' populations. A strong motivator in the decision to use violence is the influence of the community and family on the terrorists (Osmundson, Langford, & Huynh, 2007). Terrorists will only use violent tactic as a fallback plan if their grievances are ignored or are unrequited. Terrorists are aware that violence to the innocent will alienate neutral people who might otherwise be favorable to their cause.

B. PIRACY

Historically, there were more incidents of pirates attack as compared to maritime terrorist attack. It is estimated that there were a total of 2,463 actual or attempted acts of

piracy that were registered between the year 2000 and 2006 (Chalk, 2008). The actual number of piracy attacks is most likely greater than reported as ship owners might be reluctant to acknowledge an attack. The investigations that follow usually lead to delays in their operations or an increase in insurance premiums. These will affect the ship owners' profits and the security of the goods. The reputation of the owner and the shipping consort is at stake.

Unlike terrorism, the motives of pirates are for personal economic gains. Pirates show interest in anything that is valuable for trade or personal use. This plunder includes cash, cargos on the vessels, kidnapping the crew for ransoms, and taking possession of the vessels (Nelson, 2012). The seized cargos can be sold or traded in the black market. Therefore, the pirates will be looking for vulnerabilities in the vessels from which they can profit. It will be more profitable for them to board and take control of the ship instead of blowing up the vessel.

C. NEXUS BETWEEN TERRORISM AND PIRACY

It is interesting to note that there were suggestions a nexus might be forming between terrorism and piracy (Nelson, 2012). One possible reason (speculation) for such connection is that the terrorists might work with the pirates to secure funding for their land-based terrorist operations. Another possible reason is that the terrorists might be learning the seafaring trades from the pirates so that they can stage a maritime terrorist attack. In order for such relationship between piracy and terrorism to exist, both parties must benefit from it. However, there is no supportable evidence for such nexus. Moreover, as highlighted earlier, the motives behind the two groups are different. Piracy works towards financial gains whereas terrorism works towards the political motive (Chalk, 2008). Therefore, no one can be sure such a working relationship exists.

One terrorist group, the LTTE, a Sri Lankan terrorist group carried out both acts of terrorism and piracy to support their opposition to government policies in Sri Lanka. The LTTE had both surface ships (cargo and military) as well as a mini-submarine (Lichtenwald, Steinhour, & Perri, 2012).

III. MARITIME THREATS

Seamanship is essential to executing maritime domain terrorist attacks. The skills include navigation, ship-handling, operation of onboard equipment, anchors, rope handling, and the understanding of weather. The terrorist groups have to undergo trainings to equip themselves with these skills. The availability of skills to use Global Positioning Systems, satellite communications, scuba diving equipment, diver propulsion vehicles (sometimes referred to as diver tugs or sea scooters), jet skis, and submersibles are within the economic reach of many terrorists groups.

A. AL QAEDA

Al Qaeda was founded by the late Osama Bin Laden. Al Qaeda's main ideology is the use of jihad against Muslim deserter rulers, the Crusaders and Zionists, such as the United States of America and its allies. Al Qaeda believed that every Muslim should have the duty to fulfill the jihad mission (Lorenz, 2007). Al Qaeda uses the advancement of technology to reach its followers. They use webpages and blogs to spread their ideologues and to raise funds and resources for their activities. The media is an important avenue for them to wage psychological warfare with the public. In an interview with Dr. Bruce Hoffman by Bilal Y. Saab (Bilal Y., 2013), Dr Bruce Hoffman believed that despite the death of Al Qaeda's founder, the group's ideology and brand have prospered. Al Qaeda's affiliates and associates are present in more places than Al Qaeda was ten years ago.

There is evidence of maritime terrorist attacks carried out by Al Qaeda in the past. Examples include the attack on USS Cole and MV Limburg.

1. USS Cole

On October 12, 200, a United States of America Arleigh Burke class destroyer, the USS Cole, was attacked by a small craft loaded with 270 kg of C-4 explosives (Lorenz, 2007). The navy warship was docked in the port of Aden, Yemen, for refueling when the attack occurred. The attack was carried out by two suicide terrorists who

steered their small craft alongside USS Cole and ignited the explosives, blasting a 40-foot hole on the side of the warship. The terrorist attack killed 17 members of the ship's crew, wounded 39 others, and caused serious damage to the warship (Perl & ORourke, 2001). It was estimated that Al Qaeda spent $40,000 to carry out the attack (Lorenz, 2007).

The attack was planned by Abdul al-Rahim al-Nashiri, the mastermind of maritime terrorist operations for Al Qaeda (Lorenz, 2007). He based his planning on the intelligence provided by his informers who were working at the Aden harbor and posted along the Red Sea. His team leased a safe house for six months in Aden and the terrorist group increased the security of the place by installing gates and heightening the surrounding fence. All these activities were done in preparation for the attack. According to Michael Richardson, a visiting Senior Research Fellow at the Institute for Southeast Asian Studies, Singapore, al-Nashiri based his operation on four pillars (Richardson, 2004a):

- use of fast boats loaded with explosives to attack United States of America warships and other targets;
- use of medium-sized ships that could be blown up near other vessels, including passenger liners;
- use of private planes bought or stolen from flying clubs and small airports that could be loaded with explosives and used as suicide boomers against ships; and
- training underwater demolition teams to attack vessels.

2. MV Limburg

In October 2002, the French-registered oil tanker, MV Limburg, was crippled and set ablaze by an attack by Al Qaeda. The vessel was carrying crude oil off the coast of Yemen. The attack was carried out via an explosive laden small boat (Richardson, 2004b). The modus operandi was very similar to the attack on USS Cole. Three people were killed , including the two bombers, and the hull of the vessel damaged. This attack directly contributed to a short term collapse of international shipping business in the Gulf, leading to a 48 cents per barrel hike in the price of Brent crude oil (Chalk, 2008). In the period following the attack, Yemen's port has seen a sharp increase in insurance costs, forcing vessels to bypass Yemen and re-route to ports at Djibouti and Oman, competitors

of Yemen for shipping support. It was reported that insurance premiums increased by 300% while port activities decreased by 50%. These events and consequences resulted in an estimated loss of U.S.$3.8 million per month in port revenues for the Yemen's economy ("Yemen: The Economic Cost of Terrorism," 2002).

B. LIBERATION TIGERS OF TAMIL EELAM (LTTE)

The LTTE is a rebel group, founded in 1976, that sought to establish internal self-rule or a separate state in the Tamil-dominated areas in Sri Lanka's northern and eastern side. The United States of America designated the LTTE as a Foreign Terrorist Organization in 1997 (Kronstadt & Vaughn, 2009). The LTTE began carrying out terrorist attacks against Sri Lankan government in 1983. Both land-based and sea-based terrorist attacks were executed. The LTTE has developed a robust naval force known as the Sea Tigers (Murphy, 2009). The Sea Tigers has a force of about 4,000 seamen and has proven a formidable threat to the Sri Lanka Navy (SLN), destroying nearly one-third of its naval fleet. Targets destroyed include Sri Lanka's largest warship, the Sagarawardana, and a SLN operated passenger vessel ("Liberation Tigers of Tamil Eelam (LTTE)," 2012). The Sea Tigers were organized into different groups to carry out their sea-borne attack. For example, they have an Underwater Demolition Teams to deploy all underwater attacks. They have a Boat Building Team to build and repair the LTTE fleet. The Radar and Telecommunications Unit are responsible for monitoring the movement of the SLN and the Marine Weapons Armory Group is in charge of maintaining the Sea Tigers' weapons ("Sea Tiger Organization," 2001).

The defeat of LTTE came with the combat death of their leader Velupillai Prabhakaran in May 2009. Although the LTTE has remained inactive since 2009 it is unclear whether a new military commander has or will emerge. It is worthwhile (and recommended) to look at their past maritime organizational structure and attacks to understand motives and targets, continuity in chain of command, and operational characteristics.

1. SLN Operated Passenger Vessel

On October 23, 2000, the Sea Tigers attacked and sank a SLN operated passenger vessel in Trincomalee harbor ("Sea Tigers, stealth technology and the North Korean connection," 2001). The Sea Tigers were seen using a variant of the 107mm Katyusha rocket, fired from a lightweight tripod, in pairs. The attack was carried out at about two to three kilometers away from the naval base. The rockets were fired from speedboats that appear to have some form of stealth features. The rockets were ideal for the Sea Tigers as they provided the attackers with a portable artillery system that could strike their target at a distance. It was believed that during the attack, the Sea Tigers were also carrying 60mm mortars as part of their armaments.

C. PALESTINE LIBERATION FRONT (PLF)

The PLF originally started as PLFP-GC in 1959, by Ahmed Jibril. The party has gone through several periods of splits and mergers. Fighting occurred between the different factions of PLFP-GC due to their ideological differences. In 1977, Muhammad Zaidan, also known as Abu Abbas, broke off from PFLP-GC and formed PLF. PLF objective was to establish a Palestinian state and the destruction of Israel (Cronin, Aden, Frost, & Jones, 2004). One of the more prominent maritime terrorist acts by the PLF was the hijacking of the Italian cruise ship MS Achille Lauro.

1. MS Achille Lauro

MS Achille Lauro was a cruise ship for Rotterdamsche Lloyd based in Naples, Italy. On October 7, 1985, four members of the PLF hijacked the Italian cruise ship near Egypt. The terrorists ordered the ship to sail to the port of Tartus in Syria. In return for the 97 passengers held ransom onboard the cruise ship, the terrorists demanded the release of 50 Palestinians held captive in Israeli jails (Madden, 1988). Syria refused the docking of the cruise ship in the port of Tartus. In response, the terrorists threatened to kill passengers if their demand was not met. During the negotiation, the terrorists killed Leon Klinghoffer, a wheelchair-bound elderly American passenger. In the end, the cruise ship returned to Port Said in Egypt. After days of negotiation, the terrorists agreed to abandon the ship in return for their safe passage. It was reported that Abbas Zaidan

assisted the terrorists via shore contact. He negotiated safe passage by plane for the terrorists out of Egypt with the release of the cruise ship's passengers.

D. ABU SAYYAF GROUP (ASG)

ASG was founded by the late Ustadz Abdurajak Janjalani. The objective of setting up of ASG was to establish an independent theocratic Islamic state in the southern Philippines (Banlaoi, 2005) ASG conducted various extortion activities and kidnapping for ransom to raise funds for their activities. The group also received funding from al Qaeda, via Islamic charities operated by Al Qaeda in the Philippines (Elegant, 2004). ASG has a military arm, which has the means to gather intelligence as well as to manufacture its own mines and explosives. The group's first attack, on August 10, 1991, was a maritime operation which bombed a foreign missionary ship, the MV Doulous. Other maritime terrorist attacks included the explosion of Superferry 14. ASG members and followers have deep knowledge of the maritime domain as they came from Muslim families with strong backgrounds in seamanship. It was believed they had equipment that can be used for maritime activities. The Office of the Deputy Chief of Staff for Operations of the Armed Forces of the Philippines reported that ASG has night-vision devices, thermal imagers, satellite phones and high-speed craft (Banlaoi, 2005). ASG would seem to be well-equipped for maritime operations.

1. Superferry 14

Superferry 14 was a 10,000 ton ferry in the Philippines. An explosion on the ferry caused a fire on the vessel and resulted in more than 100 people being killed in February 2004. Investigation concluded that ASG was responsible for the attack ("Bomb caused Philippine ferry fire," 2004). The explosion was set-off from a cardboard box containing 3.6 kg of TNT, placed on a seat on the ferry (Elegant, 2004). Investigators believed that the ferry was targeted because its owners, WG&A, refused a request for one million dollars in protection money from ASG in 2003.

E. JEMAAH ISLAMIYAH (JI)

JI is an Indonesia-based terrorist group formed in the early 1990s to establish an Islamic state encompassing southern Thailand, Malaysia, Singapore, Indonesia, Brunei, and the southern Philippines. It is an Al Qaeda affiliate, receiving financial and material support from Al Qaeda (Abuza, 2009). Its members received training in Afghanistan and southern Philippines ("Jemaah Islamiya (JI)," n.d.). JI was responsible for a series of terrorist attacks targeting Western interests in Indonesia and the Philippines, including the attacks against two nightclubs in Bali (that killed 202 people) in 2002, the 2003 car bombing of JW Marriott hotel in Jakarta (that killed 12), and the 2005 suicide bombing of three places in Bali (that killed 22). Although it seems that JI executes land-based terrorist attacks, they have shown interests in attacking shipping in the Straits of Malacca. They monitored vessels visiting the naval bases in Singapore and are suspected of developing specific expertise in that area. However, it is believed that their maritime capability remains underdeveloped when compared to their land expertise (Raymond, 2006).

1. Plan to Attack United States of America Warships

JI planned to attack United States of America warships in Singapore with explosive laden small boats. They studied and surveyed Sembawang Wharf and Changi Naval Base, both of which are bases used by the visiting warships. The plan included detailed maps for a seaborne attack using a small craft against the warships as they are traveling eastwards from Sembawang Wharf, in the northern part of the island. The targeted location was in a channel and the plan identified the narrowest portion so that the target ship will have little room to make evasive maneuvers to avoid colliding with the suicide small boat. JI also monitored the route and patrol schedule of Singapore's Police Coast Guard in the area (Richardson, 2004b). Their plan was foiled in 2001 when Singapore's government managed to discover their plots.

IV. MARITIME TARGETS

As highlighted earlier, a very large percentage of Earth's surface area is covered with navigable bodies of water. The world economy depends on these bodies of water to facilitate movement of goods. These maritime domains also provide a very important form of commuting platforms for humans, besides transporting goods. For example, in the United States of America, ferries play an important role in its transportation system. In at least 38 states, more than 100 million passengers utilize the ferries every year, to transport them between work and home ("Ferries: Senators Murray, Murkowski, Cantwell, Begich and Representative Larsen Introduce Legislation to Improve U.S. Ferry Systems," 2011). Besides commuting, people also spend their vacations on bodies of water via cruise ships. To support these activities, facilities and infrastructure are built. All of these ships and infrastructures should be considered legitimate targets for terrorism. In addition, vital installations like naval bases and naval warships, which are built to provide security, could also become terrorists' targets.

A. MARINE FREIGHT INDUSTRY

According to a book published by RAND Corporation (Greenberg, Chalk, Willis, Khilko, & Ortiz, 2006), there are approximately 112,000 merchant vessels, 6,500 harbor facilities and ports, and 45,000 shipping companies. An estimated 15 million containers move within this network of marine freight industry and infrastructure, linking roughly 225 coastal nations. Certain countries' economies depended heavily on marine freight industry. In Singapore, the maritime industry employs more than 170,000 people and contributes to about seven per cent of Singapore's Gross Domestic Product ("Singapore's 2012 Maritime Performance," 2013). In 2012, container throughput reached a new record for the Port of Singapore – 31.6 million Twenty-Foot Equivalent Units (TEUs). Incoming and outgoing vessels use the Malacca and Singapore Straits. This usage includes both large vessels that carry cargo from Europe and the Middle East to East Asia as well as smaller vessels that transit locally. Approximately 30 per cent of world trade pass through the Straits each year (Bateman, Raymond, & Ho, 2006). The narrowest part of the

Malacca Strait is about eight miles wide while is it only about three miles in the Singapore Strait. Therefore, any blockage in these Straits will impede the economies of Singapore and her neighboring countries.

1. Possible Consequences

Since the marine freight industry is so important to the world's economy, a successful terrorist attack on any part of the supply chain of world goods will have undesired and severe consequences. Any terrorist attack of substance will inflict economic damage and disrupt the maritime supply chain (Greenberg et al., 2006). The terrorists could sink or disable a single ship within constricted straits or channels. The owner of the ship will have to suffer economic losses due to the repair or replacement of the vessel, and the containers' owner will incur losses due to the missing goods in the process. There may be loss of life or injuries in the attack. Besides the direct impact to the owners and crew, there are also secondary impacts to the shipping industry. Ships may have to re-route due to the disrupted shipping route, which leads to higher cost in shipping the goods. In addition, any new security measures implemented to curb future terrorists attack will increase the operating costs incurred by the maritime industry and ultimately the consumer of goods. The impacts of the attack will be worse if the attack is carried out nearer to the harbor. A near-port attack could damage the infrastructure for maritime freight, spilling over to other ships. This spillage could result in large economic losses, including possibly lengthy and costly repairs to the facilities.

Besides economic losses, people could be injured or killed in the process. The number of injuries or deaths depends on the location and type of terrorist attack. In general, container ships have fewer crew members than cruise ships and warships. Therefore, if the attack was carried out in the straits or on the open sea, the potential number will be limited to the crew size. However, if the attack was carried out in close proximity to the harbor, the number of injuries and deaths may be higher.

The publicity created by an attack will also depend on the location and type of attack. If the attack is contained within a container ship out at sea, the publicity created is most likely limited. Only the immediate families of the ship's crew and the company that

owns the ship may be affected. The countries near the location of an attack might also be put on alert and dispatch ships to mitigate further terrorist actions. The publicity may be more widespread if the attack was carried out in a harbor and its crippling effects are felt by the shipping industry.

2. Potential Areas of Vulnerabilities

Despite the importance of the freight industry, the security measures in place may be lacking. For example, in the United States of America, Customs and Border Protection (CBP) introduced the Container Security Initiative (CSI) to push the security check of containers destined to United States of America back to the containers' port of origin. CBP worked with foreign authorities to identify and screen high risk cargo , via X-ray scan and radiation scan, before the containers are loaded ("CSI in Brief," 2011). However, the initiative does not cover one hundred per cent of the containers that come into United States of America. As reported in the article (Powell, n.d.), the one hundred per cent inspection for incoming containers are not attainable as of now. Janet Napolitano, Homeland Security Secretary, quoted, "Sometimes those laws are very difficult standards to attain and we have to move in other directions in the near term to do everything we can with respect to cargo."

Even if the authorities managed to implement a system that screens one hundred per cent, there are other areas of vulnerabilities within the maritime freight chain. Every shipment involves multiple parties. Some of these parties includes the freight forwarders, the dock workers, the crew of the container ship, the truck drivers that deliver the container to the port, and the officers at the ports (Greenberg et al., 2006). Terrorists can plant their members within these people to facilitate their terrorist activities. In addition, with the covert nature of containers where items could be hidden inside, terrorists can utilize this concept to smuggle their goods or members. All these factors make the maritime freight industry a potential target for terrorists.

3. Likelihood of a Terrorist Target

Historically, a successful attack has resulted in limited deaths and created mainly economic losses. Minimum human consequences and limited publicity has been

generated. This lack of notoriety desired by terrorists deviates from the terrorists' intent. Were we to assume that generous and widespread headlines were one of the terrorist's primary objectives, the maritime domain might continue to have few incidents of concern. However, Al Qaeda was reported to have trained some of their people in scuba-diving attacks with no concern for decompression safety (Sakhuja, 2005). Decompression safety (the elimination of dissolved inert gases from the diver's body tissues) relates to how fast the diver ascends from depth and how many dives are made in a short period of time. Lack of concern for decompression safety is akin to learning how to fly an airplane without concern for landing.

It is known that terrorists have been using the maritime freight industry to conceal weapons or agents of attack and provide support for their operations (Greenberg et al., 2006). Therefore, in the event an attack was carried out in the maritime industry, it will lead to an increase in security measures, as seen in the air industry. Actions that result in increased security and scrutiny will hinder of terrorists' ability to make use of the containers to conceal and smuggle goods. It is unlikely that terrorists will launch an attack in the maritime freight industry, although there are potential targets available.

B. CRUISE INDUSTRY

According to a report by Cruise Line International Association, an estimated 13.5 million people took a cruise vacation in 2009 ("Profile of the U.S. Cruise Industry," n.d.). The article also mentioned that the cruise industry's total economic benefit to the United States of America's economy was estimated to be $35.1 billion in 2009. The direct spending by cruise lines and passengers on U.S. goods and services exceeded $17 billion, and the cruise industry generated nearly 314,000 American jobs. The cruise industry might be a target for terrorism. There have been cases of terrorist attacks on cruise ships in the past and there are reports of future plans in attacking cruise ships. In 2012, CNN reported that based on some internal Al Qaeda documents, Al Qaeda has the intention to take control of cruise ships and carry out attacks in Europe similar to the gun attacks by Pakistani militants that paralyzed the Indian city of Mumbai in November 2008 (Robertson, Cruickshank, & Lister, 2012).

1. Possible Consequences

Cruise ships are usually packed with large numbers of people. The ships range from a small size cruise ship, Seven Seas Navigator, which is about 566 ft. long and carries approximately 850 guests and crew ("Seven Seas Navigator," n.d.), to a large size cruise ship, Oasis of the Seas, which is about 1,186.5 ft. long and carries approximately 7,800 guests and crew ("Oasis of the Seas," n.d.). With such a large number of people confined within the cruise ship, a successful terrorist attack via explosives could lead to a massive number of injuries and casualties. In addition, a catastrophic loss of life will incur wide public attention. An accident on a cruise ship in 2013 is illustrative of the amount of publicity generated. Carnival Triumph, a cruise ship from Carnival Cruise Line, was left stranded in the Gulf of Mexico for about 5 days after a fire broke out in its engine room and damaged the power supply to the ship ("Busted toilets, hot rooms, headaches after fire strands cruise ship in Gulf," 2013). This incident generated considerable publicity as family members and friends were concerned with the well-being of the people onboard the cruise ship. The accident was widely reported by the media. Therefore, a terrorist attack on a cruise ship will most likely create a similar degree of publicity. Such publicity may boost the morale of terrorists and be seen as precipitating in attracting new members (Greenberg et al., 2006).

Economic consequences also result from terrorist attacks on cruise ships. Significant damages to a cruise ship could result in direct economic losses to the cruise lines. The physical damage could range to hundreds of millions of dollars, depending on the extent of damage and the size of the cruise ship. In addition, there will be secondary effects. Companies might suffer from human capital losses if their employees are injured or killed in the attack. Insurance cost for the cruise line might go up as cruise vacation might be perceived as more dangerous than in the past. The economic consequences might be even more extensive as people might change their travel pattern and decide to skip cruising totally, if they deemed the risks involved as unacceptable.

2. Potential Areas of Vulnerabilities

There may as yet be un-ameliorated vulnerabilities in the cruise industry that terrorists could exploit. Unlike the air travel industry, the cruise industry has always practiced stringent security checks at the port when passengers embark on the cruise ships. After the terrorist attacks of 11 September, the cruise lines reemphasized their control over access to the ship, enforced a 300 ft. buffer zone around their ships, and implemented a number of on-board security measures. Moreover, the cruise ship will anchor at different ports throughout the voyage and provides advance notice as to their intended arrival. Service employees, who have access to the cruise ships in these overseas ports, might not have undergone any form of detailed security background check (Greenberg et al., 2006). All passengers, carry-on materials, and baggage are screened and checked during the boarding process. However, as with the cargo side of shipping, terrorists could breach the cruise ships' security by bribing service employees or even pose as these working employees (Rubacky, 2013)

The docking of the cruise ships at various ports is an area where terrorists could exploit. The prolonged anchoring of the cruise ship at these ports may provide the opportunity for terrorists to carry out a collision type of attack. The terrorists could deploy an explosive laden fast craft and crash into the anchored cruise ship, causing damage to the cruise ship. If the explosive is significant, it could lead to the sinking of the cruise ship.

Lastly, the itineraries of the cruise ships are readily available. This information can be obtained from travel agency, the cruise lines, and even through the Internet. Terrorists have relied on intelligence to plan for their attacks. The terrorists can use information such as the sailing times and the docking locations of the cruise ships to assist in their planning. This is another vulnerability area where terrorists could exploit.

3. Likelihood of a Terrorist Target

The vulnerabilities within the cruise industry and the consequences from a successful terrorist attack might suggest that the cruise industry is a likely terrorist target. In order to execute such an attack, the terrorists need resources like explosives and a boat,

if they are thinking of launching a suicidal attack. Also, they might need the layout of the cruise ships so that they can pin-point the vulnerable areas to inflict the maximum damage. In the event the terrorists planned to board the cruise ship and overtake it, they would need the necessary seamanship to pilot the ship.

With the fact that the political objective of an attack on cruise ship might be minimal, there might be better targets for the terrorists. Therefore, while an attack on a cruise ship might be possible, the chances of it happening would seem to be slim.

C. POLITICAL TARGETS

Political targets in the maritime domain would seem to always be on the terrorist groups' priority list. Certain terrorist groups are formed to oppose a political force or adversary. For example, the LTTE's Sea Tigers existed because they are needed to combat the SLN. The Sea Tigers sought to establish internal self-rule or a separate state in the Tamil-dominated areas in Sri Lanka's northern and eastern side. The suicide bombing of USS Cole is another example of a political asset being targeted by terrorist groups. The ability to succeed in executing an attack on a military force might generate a lot of media attention. Furthermore, it seems that successful attacks could aid the proliferation of the terrorist groups.

1. Possible Consequences

The economic losses of an attack on a warship or naval base will be mostly limited to the damages inflicted directly on the warship or the naval base. Compensations to the families of those killed will be paid out via the country's reserves as they are killed in the line of duty. On top of the direct economic damages inflicted by the attack, there may be indirect economic losses. Businesses might lose confidence in the country's security, which leads to a negative impact on the country's economy. In an extreme case where the terrorist attack manages to killed the leader of the political party in the country, the fallout might lead to unrest within the country and unforeseen social problems. The human losses will depend on the target of interest by the terrorist group and the amount of cascading damage. That damage could range from tens of people to hundreds of people. If a terrorist attack was carried out in the open sea on a navy warship, the human

casualty would be most likely limited to the crew on the warship. Such an attack may have a maximum effect on about 100 people. However, if the attack was carried out in a naval base, the human losses are difficult to calculate.

The political impact may be large as the ability to successfully execute a terrorist attack on a military asset or an important political figure in the maritime domain speaks to the issue of state security; line of succession; and disruptive, consequential events. Furthermore, an attack on a political figure might imply the terrorist group has the capability and intelligence to circumvent considerable security measures and enforcement. An attack on an important political figure may generate a lot of publicity.

2. Potential Areas of Vulnerabilities

Military and naval bases are usually secured. The security steps after the September 11 terrorist attack were most stringent and comprehensive. However, one area of vulnerabilities was the usage of other countries' harbor when the navy warships are staging overseas. There are instances where the warships need to replenish their fuel and food supplies in a foreign country's harbor. The terrorist group can potentially work their way into the harbor by bribing employees working in that harbor if the security within the harbor is lacking. For example, in USS Cole's attack, the warship was targeted while docking in the port of Aden, Yemen, for refueling.

3. Likelihood of a Terrorist Target

The motives behind most terrorist attacks are fundamentally political. Despite the enhanced security in political assets, terrorist groups continue to try and overcome these security measures in order to achieve their objectives. Terrorists will wait for the appropriate opportunity to strike. This waiting strategy is supported by past successful maritime attacks. Although the enhanced security measures will reduce the likelihood of a terrorist attack, such measures do not necessarily remove the threats. Therefore, it is a possibility that political assets and figures in the maritime domain are potential targets of maritime terrorism.

D. CONDITIONS THAT ENABLE MARITIME TERRORISM

From the different possible terrorist targets discussed in this chapter, certain conditions have to be fulfilled in order to enable maritime terrorism. Martin N. Murphy highlighted the eight conditions which will affect maritime terrorist attacks. Many of these conditions are similar to those conditions that supported piracy. However, the motives behind these are different. The absence of any of these conditions will pose difficulties in launching any terrorism attack (Murphy, 2007).

1. Legal and Jurisdictional Weakness

Some states benefited politically in giving cover to terrorist groups as in the case of Libya, Tunisia, and Yemen in relation to the Palestine Liberation Organisation (PLO), an organization where PLF is part of (Murphy, 2007). Some states lack the means or motivation to pursue terrorists or terrorist groups residing in their territories. Additionally, law enforcement authorities of other countries have limited rights to board these vessels if the terrorist groups are in the high sea or within the exclusive economic zones (EEZs) of these states. As stated in the United Nations Convention on the Law of the Sea, the EEZ is an area where a state has special rights over the exploration and use of marine resources, including energy production from water and wind. These economic zones extend from the seaward edge of the state's land border to 200 nautical miles from its coast towards the sea ("Exclusive Economic Zone," n.d.). Terrorist groups might capitalize on this weakness in governance to establish their base camps in these states.

2. Geographical Necessity

The LTTE is an ideal example where the evolution of the terrorist group's marine capability is determined by the geography of the country. Sri Lanka, in which LTTE was based, is an island surrounded by the sea. Therefore, LTTE invested in a strong maritime force so that the SLN cannot effectively limit and control the supplies and resources to LTTE. LTTE was able to neutralize the opposition from SLN and continue to import the necessary resources to fuel their activities, including terrorist acts. Besides the LTTE, the PLF has established some maritime capabilities to mount coastal attacks in Israel, as Israel has strict control over the land borders around the country.

3. Inadequate Security

The state security activity can have an impact on the proliferation of terrorist activities in that state. In Sri Lanka, the SLN has been at war with the Sea Tigers (part of LTTE that are in charge or maritime domain activities). The Israel Defense Forces (IDF) Navy has been reasonably successful in limiting the activities of terrorist groups in Israel. In Singapore, the government security forces were able to foil JI's plan to attack the United States of America's warships that are visiting the country. The intelligence and Singapore's security force played a crucial part in preventing the attack. A state may not have the means to eradicate terrorist groups from their states if the state lacks a security force or has a weak security force. In Southeast Asia, the ASG, JI, and other terrorist groups are able to transport their goods by the sea since Indonesia and the Philippines's maritime security are generally weaker as compared to the other states in that region. However, the situation is improving, as all the states understand the importance of a strong security force in prevent future terrorist attacks (Murphy, 2007).

4. Secure Base Areas

All terrorist groups need a safe and secure base to plan, train, store their logistics, and to provide a resting point for their members. As it is not feasible to be living permanently out in the open sea, it is crucial that maritime terrorist groups have a secure base on land. For example, the PLF ran maritime operations out of a string of small workshops and bases along the Lebanese coast, with a particular concentration around Tripoli in the north. When Israel invaded Lebanon in 1982 and dispersed the PLO, Libya became the nearest maritime base area. This restricted the PLO's maritime capabilities, thus resulted in lesser maritime activities during that period (Murphy, 2007). In another example, when the tsunami in 2004 destroyed LTTE's Sea Tigers' coastal equipment (e.g., coastal radars), they immediately channeled resources to replace the items as the equipment was important for their operations. Therefore, the security of the terrorist groups' land-based logistics and facilities are as equally important as their maritime equipment.

5. Maritime Tradition

The terrorist groups must have seafaring skills in order to execute maritime terrorist attacks. Alternatively, the terrorists must be in a position to draw on the support and skills of a maritime community. According to Rommel C. Banlaoi, most of ASG members and followers belong to Muslim families with strong seafaring traditions. Their exposure to maritime activities equipped ASG members with the necessary skills for maritime terrorism (Banlaoi, 2005). LTTE's Sea Tigers' maritime capabilities were also connected to the local seafaring communities in Sri Lanka. LTTE leaders grew up in the town of Valvettiturai, which had a reputation as a smuggling center. The close community between the fishermen and the terrorists within the town helped LTTE tremendously in learning the necessary skills for conducting maritime terrorism (Murphy, 2007).

6. Charismatic and Effective Leadership

Without any maritime skills, the next best alternative is to tap on the expertise of a maritime community. To achieve that, the terrorist group benefits from a charismatic and effective leader. Al Qaeda did not have a seafaring history. They lacked the experience and skills to mount any maritime terrorist attacks. However, they managed to carry out the suicide bombing of USS Cole and the oil tanker, MV Limburg. The success was attributed to Al Qaeda's maritime operation mastermind, Abd al-Rahim al-Nashiri. He was able to draw on the experience of Yemeni fishermen and boat-builders for the expertise needed in launching the maritime terrorist attacks (Murphy, 2007). When al-Nashiri was captured in 2002, Al Qaeda's maritime activities seemed to be restricted.

7. State Support

State support, via the provision of arms or bases, can benefit terrorist groups. Such support should be able to bridge any gaps in the terrorist groups' capabilities. This support could allow the terrorist groups to execute larger operations. The PLO was believed to have received assistance from various states like the Soviet Union, Czechoslovakia, Yugoslavia and Arab states (Murphy, 2007). Without this external help, PLO did not seem able to execute those attacks. It was also believed that the North

Koreans provided the Katyusha rocket to LTTE's Sea Tigers ("Sea Tigers, stealth technology and the North Korean connection," 2001) which the Sea Tigers used in their maritime attacks. It has been speculated that the Sea Tigers might have obtained their modified fast craft from North Korea.

8. Potential for Reward

Terrorist groups need funding to substantiate their terrorist activities. This is especially true for maritime terrorism as they need resources for seamanship training, and equipment like small vessels and navigation systems. Similar to piracy, maritime attacks are an avenue for financial gain. Although terrorist groups will still strive for political motives in executing attacks, they might need to carry out such attacks to fund for their future operations.

The eight conditions highlighted by Martin N. Murphy are correlated and not independent. Legal and jurisdictional weakness, inadequate security, and state support in most instances are related. If a state is supportive and tolerable towards terrorist groups within their jurisdiction, the security measures put in place will not be able to support eradicate of the terrorist groups. This lack of opposition to a terrorist group may result in an implied weakness in the jurisdictional intent and actions of a state. Nevertheless, understanding these conditions is important, as they will assist countries in formulating plans to neutralize any maritime terrorism.

V. NEUTRALIZING THE ATTACKS

Despite the availability of potential maritime targets, the terrorist groups that have carried out attacks in the maritime domain did not execute their attacks with ease. In many instances there have been measures implemented to prevent and neutralize various threats.

A. IMPROVED SECURITY ENFORCEMENT

In response to the terrorist attacks of September 11, 2001, on New York City and Washington D.C, the United States of America government enacted new legislation to increase air passenger safety. A new establishment, the Transportation Security Administration (TSA) was set up and changes were made in the civil aviation security procedures (Blalock et al., 2007). Likewise, the maritime industry has continued to step up their security measures. Naval bases have increased security. Increased patrols by maritime police forces, with the support from the navy forces, are another method used to reduce and discourage the number of terrorist attacks. Combined, the heightened security measures and enforcement help create a form of deterrence for the terrorist groups. Besides the security measures provided by the authorities, private security companies (PSCs) offer a supplement security measure at sea, which can be seen in the Malacca and Singapore Straits (Bateman et al., 2006). PSCs primarily provide a deterrent role in providing security for high value, vulnerable vessels, such as oil rigs, dredgers, slow moving barges, and luxury motor yachts.

The maritime freight industry has attempted to tighten the security of the supply chain within the industry without impacting the flow of goods through the ports. CBP worked with foreign government agencies to screen high risk cargo prior to loading the containers onboard the cargo vessels. However, the measures only managed to cover a small percentage of the containers. Therefore, more efforts are needed to ensure a greater percentage of the safety of the maritime freight industry. One possible method is to introduce smart containers where electronics are installed in the containers to monitor

every instance of authorized, as well as unauthorized, opening of the containers ("Smart Containers," n.d.).

B. INTELLIGENCE

Any terrorist attack requires detailed and extensive planning to be effective. This attention to detail is especially true for maritime terrorist attacks since more logistics are involved when compared to land-based attacks. As seen in the USS Cole incident, al-Nashiri started plotting the attack as early as 1998. His planning included recruiting members to pilot the explosive-laden boat, refitting the boat to contain the explosive, leasing houses in Yemen to facilitate surveillance of the harbor, and carrying out rehearsals to ensure the plan was fool-proofed (Lorenz, 2007). Therefore, an effective method in foiling the attacks was to have a capable intelligence. Pre-emptive actions are necessary to prevent any terrorist acts. These security actions can help to provide information to eradicate the base camps of the terrorist groups. Ultimately, the security work is designed to lead to the disruption of efforts to launching any maritime terrorist attack as the terrorist groups need the support of their base camps. For example, the killing of Al Qaeda's leader, Osama Bin Laden in 2011, was made possible due to the United States of America's intelligence work in locating his hiding location. The exploitation of information involving the locating and identifying Osama Bin Laden's trusted courier in 2010 and deciphering possible locations in Pakistan where he was hiding ("How Osama bin Laden Was Located and Killed," 2011) were noteworthy.

Besides using intelligence to locate terrorist groups' whereabouts and foil their plans to execute any terrorist acts, intelligence can ultimately be used to limit the funds and resources channeled to these groups. There has been a worldwide crackdown on the sources of terrorist funding, their communications, and means of channeling money around. Border controls between countries have been tightened. Moreover, intelligence sharing between countries has effectively foil some of the terrorists' activities (Lorenz, 2007).

C. COLLABORATION

As highlighted by the United States of America Department of Homeland Security in its National Strategy for Maritime Security, the security of the maritime domain requires detailed and cooperative efforts among the nations to protect the common interest in global maritime security (Nelson, 2012). It is important for all the nations to work together in drafting the appropriate regulations in curbing maritime terrorism. Besides government agencies, these collaborative efforts should involve the industry players to ensure the measure implemented will not impact drastically the commercial and economical aspect. In the Philippines, the Coast Watch System (CWS) was initiated to improve the maritime domain awareness in the tri-border area (TBA) between the Philippines, Malaysia, and Indonesia, where terrorist activities by JI and ASG are known to exist (Rabasa & Chalk, 2012). The key objectives of the initiatives were to develop a common operating picture of the maritime domain in the Philippines; to collect, and integrate all data relevant to maritime security; and to provide real-time information for the purposes of cueing, locating, and capturing those who engage in illegal maritime activities. The CWS will consist of offshore platforms that provide surveillance and interdiction capabilities.

In order for the effort to be successful, the collaborating nations have to overcome the differences in jurisdiction in various nations and establishing a common set of regulations.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. FUTURE THREATS

With the improved security protocols for navy vessels and coastal installations, are there any other avenues which terrorist groups can utilize to execute their attacks?

There were reports of Latin-American drug cartels using submersible vehicles to move their cargoes. These simple boats are capable of operating underwater while moving tons of drugs. They have a range of up to 2,000 miles and cost a few million dollars to build (Andrew F. Krepinevich, 2011). As reported in The New York Times, United States of America's authorities have discovered at least three models of sophisticated drug-trafficking submarine capable of traveling completely underwater from South America to the coast of the United States of America (Schmidt & Shanker, 2012). These vessels were able to transport 10 tons of drugs. However, these submersible vehicles are limited by the depths in which they operate. Nevertheless, these submersible vehicles have proved to be a possible method in evading security measures while delivering their goods to their destination. Unlike these manned submersible vehicles, unmanned underwater vehicles (UUVs) can reach ocean floors. UUVs industries are proliferating as the demand for such vehicles has increased over the past several years. Commercial UUVs are readily available for a variety of commercial and scientific purposes, such as locating sunken ships and surveying the marine environment. These UUVs can be adapted to carry explosives and deliver this cargo to places where it was not possible in the past.

A. UNDERWATER ATTACKS

CBS news reported that ASG and JI, affiliates of Al Qaeda, are working together to train militants in scuba diving for maritime terrorist attacks in Southeast Asia ("Terror's New Frontier: Underwater," 2009). There were concerns that scuba diving training would enable the terrorists to elude the security measures and plant explosives in important assets like warships or naval bases. As highlighted by Akiva J. Lorenz, terrorists can use divers to plant explosives on the hull of ships or swimmer delivery vehicles (SDVs) laden with explosives as an "underwater suicide bomber" (Lorenz,

2007). For example, a ASG member shared how he and other members took up scuba diving lessons as part of a plan for a maritime-based attack. The LTTE's Sea Tigers is another group with the history of using submersible vehicles in their attacks. In October 2008, three self-propelled semi-submersible vehicles were used to attack two merchant ships off the coast of Jaffna. In February 2009, it was found that the Sea Tigers were developing four armored submersible vehicles ("Liberation Tigers of Tamil Eelam (LTTE)," 2012). All of these reports are evidence that pointed to the fact that terrorist groups are already considering executing such maritime attacks. The terrorist group can even position sea mines in narrow straits to create chokepoints, disrupting the shipping routes. With sufficient funding, terrorist groups may get hold of UUVs to execute their attacks.

The potential of terrorism going underwater brings the issue of maritime terrorism to another realm. It calls into being a set of potential new targets for terrorist groups. Oil production from offshore wells is brought to the mainland via underwater pipes. Today nearly 30% of United States of America's oil production and 15 per cent of gas production is produced from wells located on the outside reach of United States of America's continental shelf. Globally, about 30 per cent of the world's oil output comes from offshore production. Besides oil production, the world is interconnected via submerged communications cables. These cables are laid on the sea bed between land-based communication stations to transmit signals across the various oceans. These infrastructures were not built to defend against terrorist attacks as technology to reach these locations were uncommon and expensive at that time. (Andrew F. Krepinevich, 2011). However, with UUVs, reaching these locations is becoming easier.

Any disruption to the offshore oil production facility may have an impact on the oil production and extraction industry. A disruption may lead to an impact on the economy. Analogy can be drawn from the BP oil disaster, which happened in the Gulf of Mexico in 2010. On the day of the accident, an explosion occurred in the floating drilling rig, resulting in an enormous oil leak in the Gulf of Mexico. The accident spilled more than 4.1 million barrels of crude oil over 87 days into the Gulf (Johnson Jr., Calkins, & Fisk, 2012). The accident also contaminated the Gulf's ecosystem affecting the marine

species in the region. The spill impacted the Gulf Coast's economy and industries such as offshore drilling, the fishing industry, and tourism. From a Bloomberg report, at the peak of the disaster in June 2010, 40 per cent of Gulf waters were closed to commercial and recreational fishing. Businesses were affected as seafood supply was reduced, which increased food costs. Some resorts, hotels and casinos saw business plunge as tourists shunned the area.

Likewise, interruption of submarine communication cables could severely impact the communications interconnectivity between countries. In a study conducted by Detecon for the Policy Support Unit of the Asian-Pacific Economic Cooperation (APEC), an Economic Model was created to study the impact on world economy (Gerlach & Seitz, 2012). The study showed there is a probability of substantial economic losses arising from cable disruption. Most of the international business activities depend heavily on the global connectivity via the worldwide web, which depends on submarine cable systems. As quoted in the report, the direct contribution of the Internet to the Australian economy was approximately Au$50 billion in 2010.

Therefore, with the improvement in technology and the potential impacts of underwater terrorist attacks, it is possible terrorists will embark on such acts.

THIS PAGE INTENTIONALLY LEFT BLANK

VII. ANALYZING THE MEANS OF ATTACK

An analysis was done to compare the various methods of terrorist attacks (as mentioned). There are basically four different types of potential maritime terrorist attacks, namely:

- using UUVs to plant explosives
- using semi-submersible or submersible laden with explosives
- using fast boats laden with explosives
- hijacking a vessel

This thesis used the cost of the method, the technology or skill needed to execute the method, and the estimated damage as measures by which to compare the various methods. For the technology or skill and the estimated damage, a relative scale was used to estimate the difficulties in using that system or resource to execute an attack. A designation of "one" will represent an attack that requires simple skills to execute or an attack that resulted in the least damage, whereas a designation of "four" will represent an attack that needs certain complex knowledge or skills to execute or an attack that resulted in the most damage. The target will be a vessel out in the open ocean.

A. USING UUVS TO PLANT EXPLOSIVES

Cost data for UUVs are limited. A report from the RAND Corporation stated that most of the available limited UUV cost data are small-production vehicles or larger prototype vehicles. No cost estimate could be found for relatively larger and complex vehicles (Button, Kamp, Curtin, & Dryden, 2009). In the report, it was estimated that a man-portable size UUV like the EMATT cost about $3,000 in 2007 and the payload was very small. Therefore, a good estimate for a larger size UUV might be about a few hundred thousand dollars. Another point worth noting is that currently, there are no UUVs certified to carry explosives. Therefore, terrorist groups will have to find UUVs which can carry sufficient payload and to introduce a mean to ignite the explosive. Furthermore, a UUV with very sophisticated control system is needed to execute a mission where the UUV is moving towards a targeted moving vessel. This will further

make the UUV very expensive. The complexity in operating a UUV might not be as complex as operating a submersible, a ranking of "3" will be given for the complexity of the skills needed.

B. USING SEMI-SUBMERSIBLE OR SUBMERSIBLE LADEN WITH EXPLOSIVES

Andrew F. Krepinevich reported that the submersibles used by drug cartels cost a few million dollars to build (Andrew F. Krepinevich, 2011). For the purpose of this analysis, each submersible will be estimated to cost one and a half million dollars. Each submersible can carry up to 10 tons of drugs (Schmidt & Shanker, 2012). Therefore, it is assumed the terrorist groups will load the submersibles with five tons of explosives. Among the four options, this method of transport carries the greatest mass of explosives. Thus, the relative damage for a submersible is the highest. The terrorists must have the skill and temperament (to think and work in a confined space) to operate the vehicle and it will be beyond basic maritime skills. The training might not be readily available . Therefore, a ranking of "4" will be given for the complexity of the skills needed.

C. USING FAST BOAT LADEN WITH EXPLOSIVES

The attack on USS Cole is an example of such an attack and it was used as the analogy for this analysis. From the report by Akiva J. Lorenz, 270 kg of explosives were used in the attack and it cost Al Qaeda about $40,000 (Lorenz, 2007). Therefore, the damage was ranked a "2." Also, operating a fast boat is considered easier than operating a submersible. The ranking for skills needed was assessed as a "2."

D. HIJACK THE VESSEL

As compared to the other three methods, the method that involved hijacking a vessel is the simplest in terms of the equipment needed and the skills required. Therefore, a score of "1" was assessed and used for both the technology and the complexity of equipment. The cost of executing such a mission involved the cost to train the terrorists and to pilot a fast boat. Therefore, it is estimated to cost a few thousand dollars.

E. ANALYSIS

Table 1 shows the estimated figures used for the various methods of attacks. Figure 2 and Figure 3 show how the relationships between the cost of the various methods and the technology or skills needed, and the damage inflicted respectively. The figures show that as the level of skills and technology needed increased, the cost involved increased. However, the increased cost does not always lead to an increase in damage inflicted on the target.

Table 1. Summary of the various methods of attacks and their rankings

Method	Cost (U.S.$)	Technology/Skills required (Relative)	Damage (Relative)
Hijack	$2,000	1	1
Suicide fast boat	$40,000	2	2
Semi-submersible/Submersible	$1,500,000	4	3
UUVs	$300,000	3	2.5

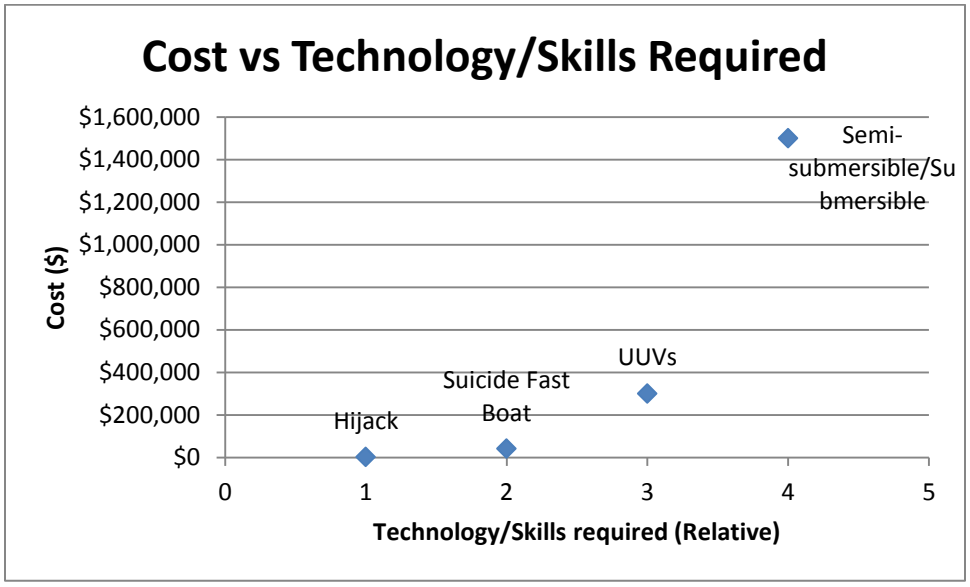

Figure 1. Graph showing the Cost vs. Technology/skills needed

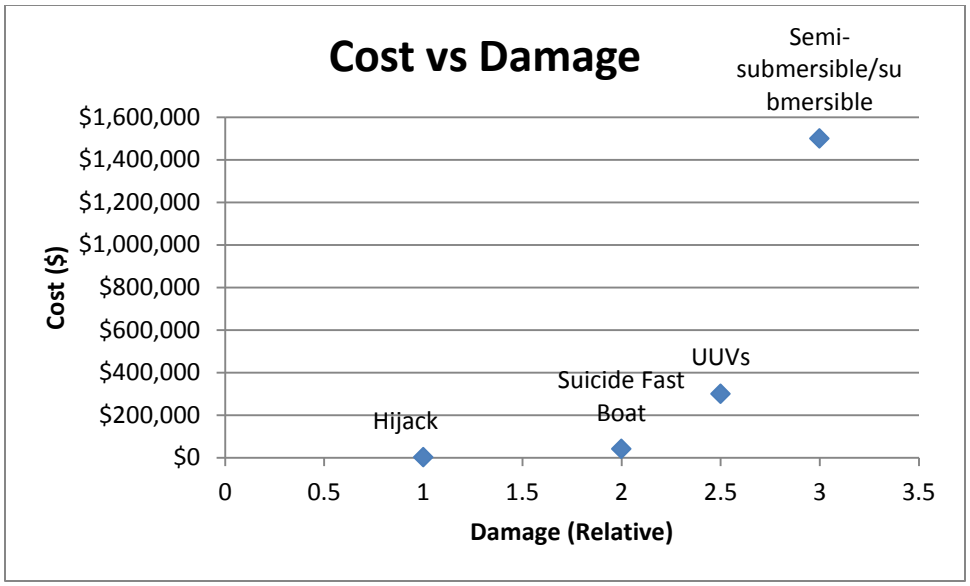

Figure 2. Graph showing the cost vs. damage caused by attack

The amount of damage inflicted by the UUVs does not justify the additional cost as the amount of explosives carried is less. Therefore, using the submersible would seem a better alternative. However, when comparing the submersible to the explosive laden fast boat, the submersible costs significantly more when compared to using an explosive laden fast boat. Therefore, the explosive laden fast boat method may be the best choice if the mission does not intend to inflict extensive damage to the intended target.

VIII. SYSTEM ENGINEERING IN MARITIME TERRORISM

The purpose of this chapter is to introduce the concept that the relations between a terrorist group and the government group as that of a system of systems (Langford, 2012). A terrorist group and its supporting infrastructure comprise a system, i.e., the "terrorist system." Moreover, the government system is comprised of the society and structures that are governed, which also includes the terrorist system that falls within the domain and purview of governance by the government system. Through this nested relation, the management system is at the same time the meta-system of control for society as well as providing for the terrorist system. The dependencies between the government system and the terrorist system are similar to that of any group within the governance of the government system, based on an appreciable set of dependencies that occur between any subgroup within the governance of a society under their purview. The notable exception that distinguishes the terrorist system from the government system is the designation by the government system that declares certain groups to result in negative externalities (Langford 2012).

A system of systems is a set or arrangement of systems that results when independent and "useful" systems (depending on perspective) are integrated into a larger system that delivers unique capabilities. This is the definition given in the DoD Defense Acquisition Guidebook (DAG) (Office of the Deputy Under Secretary of Defense for Acquisition and Technology, 2008). It is the interactions between these two systems (i.e., the government system and the terrorist system) that create the system's capabilities that are characteristically different from that found in each of these two (often time opposing) individual groups. With this concept of the government and the terrorist systems having a system of systems relation, the system's usefulness of the interaction results in a degradation of the systemic capabilities of the government system (with the terrorist group) compared to government system (without the terrorist group). The nested concept as a working model that is premised on this system of systems thinking is a trait of any society whose governance is focused on providing for the needs of its people.

This thesis investigated terrorist groups as a system comprised of stakeholders and institutions that were diametrically opposed to some, but not all of the governance of the government system. Many of the stakeholders who support the terrorists are indigenous to the government system and do so unwittingly as they provide food, monetary support (perhaps through wages), transportation, water, electricity, and communications infrastructure. As members of the society that is governed by the government system, the terrorists are "entitled" to such services and participation with its structures and objects (Langford 2012).

A system is a set of elements that are either dependent or independent, but interacting pairwise to maintain a reasonable constancy of actions across its elements (Langford, 2013). The interaction between objects or processes can be physical or enacted physically on a temporal basis (i.e., short- or long-term).

Systems are bounded entities. System boundaries represent the permanent and episodic interactions between elements, domains, and other systems. Boundaries represent the lasting and occasional interactions, as well as emergent properties and behaviors of a system or system of systems. Figure 3 shows a representation of the interactions between two systems. The interaction is highlighted by element $e_{1.3.1}$ or $e_{2.15.1}$. Elements are either objects or processes, whereas interaction transfers energy, matter, material wealth, and information (EMMI), from one element to another. Elements $e_{1.3.1}$ and $e_{2.15.1}$ are actually identical items. The different nomenclature was used because the two systems have different perspectives of that boundary element. The boundary element is the point of interaction between the terrorist system and the government system; however the two systems are manifested at that single point of interaction. Element $e_{1.3.1}$ and $e_{2.15.1}$ represents the interaction between the two systems.

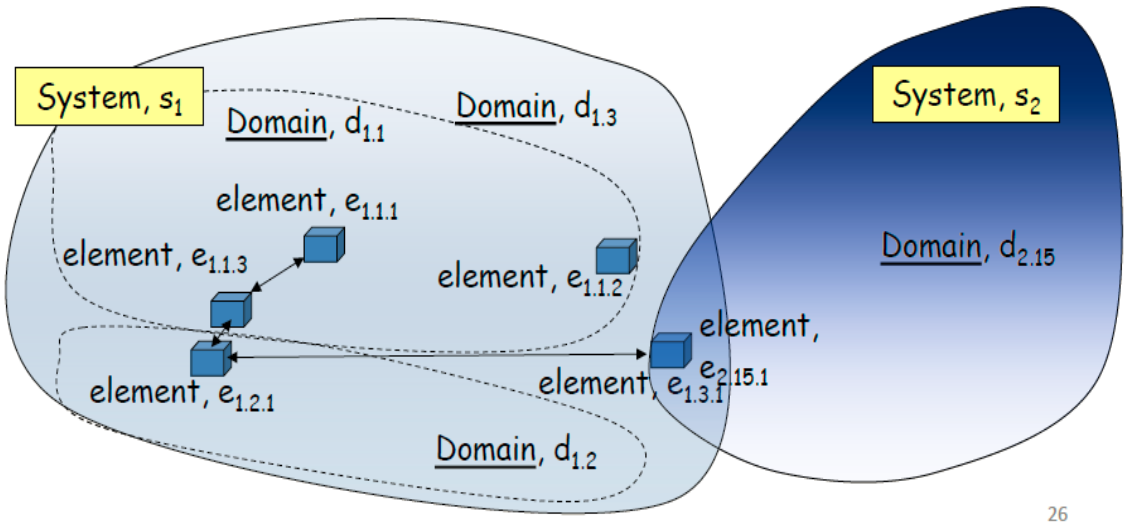

Figure 3. Interactions between Systems of Systems (From Gary Langford, 2013)

Terrorist groups can be represented by a system whereas the authorities can be viewed as another system. In that representation of the social dynamics of a group of people and their related objects and processes, the terrorist system is modeled as being independent from that of the government system. The different members of the terrorist groups and their processes within the group are represented by the different elements contained within the terrorist system. Likewise, the government system contains all elements that comprise the stakeholders that respond to the terrorist system (and the stakeholders of the terrorist system). Here we distinguish between the two groups of individuals as social and behavior even though members of the terrorist group live and work within the government system (Langford, 2012). Within the social and behavioral dynamics of systems (Fligstein & McAdam, 2012) the objects and processes of systems integration are both equivalent and appropriate to the discussion of groups within groups. In essence a society is a system of systems (Langford, 2012). The interaction between the terrorist groups and the authorities is carried out through various elements between the terrorist system and the government system.

One possible element of interaction between the terrorist system and the government system is a terrorist attack in the maritime domain. Here, the terrorists and the maritime domain are objects and the terrorist attacks are the processes. Each element

within the systems has boundaries, which can be categorized into functional, physical and behavioral representations (Langford, 2012). While boundaries set the limits, boundary conditions are the factors that affect the ways in which the objects interact across the boundaries between the two systems. In the case of a maritime terrorist attack using explosives, the water surface (such as the oceans or the straits) will be the physical environment in which the adversarial objects travel and where the blast wave from the explosives meets the surface material of the target is the physical boundary between the terrorist system and the government system. The functional boundary of the terrorist system is determined by the boundary condition that exists at the moment of the blast wave impinging on the target surface. If the blast is insufficient to breach, disrupt, damage, or have a measurable effect on the target, then the functions are determined to be 'to resist overpressure' and 'to resist deflagration wave' (as determined by the government system. If the blast is sufficient to breach, disrupt, damage, or have a measurable deleterious effect on the target, then the function is determined to be 'to disrupt, damage, or have a measurable deleterious effect' on the target. The atmospheric humidity will be one of the boundary conditions that contribute to the propagation and damage effects of the result of the ignition of explosives (Langford, 2012). Table 2 lists some examples of the boundaries and boundary conditions in a maritime terrorist attack using a boat laden with explosives. The behavioral boundary is far-reaching under either condition of the functions determined by the interaction of the blast with the target. These behaviors span all stakeholders in both the terrorists system as well as the stakeholders in the government system.

Table 2. Examples of boundaries and boundary conditions

Boundaries			**Boundary Conditions**
Physical	**Functional**	**Behavior**	
Water surface	Explosives' lethal range	Terrorists' risk appetite	Atmospheric pressure
Boat's weight limit	Target's reaction (e.g., 'to move')	Policies governing maritime activities	Atmospheric temperature

The interaction between the elements will lead to emergence and externalities. Emergence is the effect that produces a change in intrinsic properties, traits, or attributes that results by combining objects through the interaction of objects (Langford, 2012). Externalities take into account the effects that affect elements not involved in the interactions. In the example of a successful maritime terrorist attack using a boat laden with explosives, the emergence will be the damage inflicted on the target vessel. The status of the boat will be another emergent property. These are permanent emergent properties as the changes are irreversible. Catastrophic damage is the result of non-reciprocal emergence. The attack may lead to additional security measures in the maritime domain. These security measures may in turn lead to additional overhead costs to companies and their stakeholders (including customers) that have interactions with or in the maritime domain. These security measures are a form of externality.

Government agencies can review their security measures by analyzing the maritime terrorism via the system engineering approach applying a system of systems model. The system of systems model will enable the assessment of the situation in a holistic approach. Of particular interest is to identify specific areas where measures are lacking and improvements can be made at reasonable costs. However, trade off studies

must be carried out if the new measures create negative externalities. The benefit of system of systems thinking and modeling is to discover the negative externalities along with the substantial areas of improvement that increase the robustness of operations and lessen the effects of disruptive effects and their consequences (Langford, 2012).

System of systems models that assume a top-down, goal oriented approach (Held & Sukkarieh, 2007) (Khosravi, Nahavandi, & Creighton, 2009) must deal with the generalities and ambiguities of poorly defined terminology and the averages of intentions, rather than the specifics of physics at the most basic levels. These authors have pushed the thinking forward in system of systems models to their logical limits of effectiveness. To extend the effectiveness for a model of system of systems, either the definitional approach must be based on validated definitions ***or*** the model must include the basic phenomenological interactions and their implicit mechanisms that are foundational to a system or a system of systems.

Building on the core nature of systems as well as system of systems, the interactional model of objects and processes is well founded in mathematics and in the mereology of systems thinking (Langford 2013). The terrorist system is dynamically stable through its interactions with its stakeholders and its environment; presents non-reciprocal emergence when interacting with its own stakeholders as well as with its environment; is comprised of objects and processes that are uniquely identifiable; and has *stagility* (stability and agility) under certain conditions. The terrorist system is metastable as long as it

- continues to find sufficient resources to keep its members engaged in terrorist activities,
- replenishes its resources of equipment and goods,
- continually attracts new members at a sufficient rate to offset turnover, and
- restores its material wealth used to sustain operations (Langford, 2012).

Any one of these listed items are critical to the longer-term viability of the terrorist system. Considering the formative stages of a terrorist system as an ad-hoc, loosely coupled organization, the terrorist system is most vulnerable during start-up. As

the organization matures and moves from self-funded operations to external sources of funding (e.g., sponsorship, piracy or other illegal activities) more focus can be afforded terrorist activities. Therefore, the result of a sufficiently funded terrorist effort gains momentum to become a moderately self-sustaining Protasystem to a full-fledged system, such as with gangs embedded in societies for now more than 100 years (e.g., New York, San Francisco). Protasystem is a system that exhibits some changes in properties, traits, and attributes due to interactions between objects and elements (Langford, 2012).

Once the terrorist system receives external funding for its operations, its existence depends on the government system during its Protasystem stage. However, the Protasystem stage can be transitional to a full system, if the government is replaced by the terrorist system, at which point funding becomes self-sustaining through terrorist governance of lands and people (e.g., South American countries in the 20th century).

THIS PAGE INTENTIONALLY LEFT BLANK

IX. CONCLUSION AND RECOMMENTATIONS

This thesis investigated terrorist groups and government groups, as a system of systems, through the methods and means of the myriad of interactions between terrorists with infrastructure, government, value structures, and people, i.e., the vestiges of the government system. Answering the first research question, "Can a system of systems perspective be useful in determining the maturation of a terrorist group?" Yes. A system of systems perspective is useful in determining the maturation of a terrorist group by viewing the life cycle stages of a system, (i.e., Protasystem to System). The conditions for sustainment of both stages were discussed. The second research question, "Why is the maritime domain chosen by terrorists?" is answered by the terrorist's intention to highlight a particular goal as a focal point for discussion. The third research question, "Which type of terrorists are threats?" is determined by the life cycle of the terrorist organization and the "mind of the terrorist" (de Bivot, 2008), within the context of the maritime domain. The fourth research question, "Where are the likely areas for terrorist attacks?" is determined by the most attention that can be seen as differentiating the attack from that seen in the normal course of media reporting. A scaling approach was applied to various types of maritime attacks and the cost of acquiring the means by which these attacks could be carried out. The fifth research question, "What are the consequences of a maritime terrorist attack?" is determined by the heightened sensitivities and negotiations (if any) that follow such an attack. The consequences of the interactions between the terrorist group and the government group seem to be bent toward finding a resolution (de Bivot, 2008). The sixth question, "What means are available to neutralize the effects of these threats?" was centered on finding a different way to deal with terrorists. The recommendation is to negotiate without impunity (which is typical of the treatment given to criminals who take hostages in exchange for favors) should be considered as a method of resolving terrorist conflicts.

A system of systems view of government systems and the embedded terrorist system suggests a very different way of dealing with terrorists than the traditional methods of "no negotiation." Given that the methods of attacking maritime targets seem

weakly correlated with the cost, but highly correlated with the skills required to carry out such an attack, the source of money for terrorist activities should be a major focus of the government system. Destroying or degrading the ability of the terrorists to earn, steal, or acquire financial assistance for accomplishing their goals and their methods should be coupled with a concerted effort to change the perception of the acts of terrorism perpetuated on the government system. The U.S. relies on policy statements (backed by enforcement) and the new media to broadcast the "horror" of a terrorist attack. But singular acts of horror are often no less violent than seen in video games, films, and events carried out and reported in the news media. Some one person or some groups of people carry out acts that harm society and its people. There seems to be a blurring of the public's view of the acts of terror and other heinous crimes, with the difference between them being the verbiage that provides context and accompanies the media pundits that follow-up in the aftermath (private communication with Professor Langford, 2013).

Further, the system of systems perspective of maritime terrorism suggests that the terrorist system can co-exist with the government system as long as the terrorist system continues to find sufficient resources to keep its members engaged in terrorist activities, replenishes its resources of equipment and goods, continually attracts new members at a sufficient rate to offset turnover, and restores its material wealth used to sustain operations. The degree of stability and agility (i.e., stagility) (Langford, 2012) is determined by funding sources, amounts, and conditions. Should the terrorist system survive through the inevitable challenges posed by the government system, a long-term conflict is difficult and expensive to avoid.

Maritime terrorism is definitely possible, as seen from past incidents. Assets such as the maritime freight industry and cruise vessels are potential targets, though less likely so. Furthermore, since the resources of terrorists are limited, they might prefer to channel their funds to attack targets that could fulfill their political motives. Therefore, political assets within the maritime domain are more attractive targets. Nations acknowledged the potential threats and in response have implemented and improved their security measures in dealing with these threats. A strong and capable intelligence agency will aid in

combating these terrorist groups. Collaborations between nations will enhance the effectiveness of the security measures implemented.

With technology evolving, underwater terrorism attacks seem possible. However, executing such underwater attacks is not as easy as it seems. The conditions of the sea are unpredictable. As reported by Akiva J. Lorenz, Oded Yoffe, CEO of an Israeli maritime security firm, said that the rate of success of such an event is unlikely due to the difficult situations underwater, such as the currents and low visibility. To succeed in executing such an operation, years of experience is needed (Lorenz, 2007). Together with the security measures which the authorities have enacted, it will be difficult for terrorist groups to venture into the underwater regime and have success. Moreover, the effects from the disruption from these underwater infrastructures might impede the progress of the terrorist groups. It was well-known that Al Qaeda uses the worldwide web to propagate their missions and ideology. For example, with the underwater submarine cable destroyed, it might do more harm than good to the terrorists.

The use of submersible vehicles to deliver explosives might sound plausible. Such submersible vehicles reduce the probability of detection by the securities while inflicting significant damages. As seen in USS Cole incident, a boat laden with 270 kg of explosives can create a 40-foot hole on the side of the warship and with each submersible vehicle able to carry a few tons of explosives, the damage inflicted will definitely be greater. If UUVs are deployed in the future, terrorist groups may be able to reach targets that they have not had access to with lesser technology. The cost of the submersible vehicles is estimated to be a few million dollars. UUVs will most probably cost significantly more. Furthermore, from the simple analysis, the use of submersible only lengthens the ignition distance by about two and a half times longer, as compared to the fast boat method. However, to achieve the longer distance, 18 times more explosives are needed. Therefore, it would be a trade-off between the two methods of attacks. The amount of damage inflicted might not justify the usage of UUVs or submersibles as they are too costly at this juncture. From a system of systems perspective, any means of strategy employed by the terrorists that improves the ability to tilt the boundary conditions in favor of the terrorist is where their most productive investments should be

made. From a system of systems perspective, any means of eliminating the grievances or the budding terrorist group should be considered a good investment.

Governments should not stop their effort in fighting against terrorism. As seen from the potential underwater capability of the pirates and terrorists, terrorist groups are constantly thinking of new ways to overcome the security measures implemented. If the authorities do not keep up with the evolving terrorist threats, it is only a matter of time before the terrorist groups manage to execute an unconventional attack in the maritime domain.

A. RECOMMENDATIONS:

Further research is recommended to investigate how negotiations with terrorists without impunity might be beneficial as a method of resolving terrorist conflicts. A system of systems approach can be used as part of the investigation.

LIST OF REFERENCES

Abuza, Z. (2009). Jemaah Islamiyah Adopts the Hezbollah Model. *The Middle East Quarterly*, *16*(1), 15–26.

Andrew F. Krepinevich. (2011). The Terrorist Threat Beneath the Waves. Retrieved March 15, 2013, from http://online.wsj.com/article /SB10001424052970203687504577005811739173268.html

Banlaoi, R. C. (2005). Maritime Terrorism in Southeast Asia: The Abu Sayyaf Threat. *Naval War College Review*,, *58*(4).

Bateman, S., Raymond, C., & Ho, J. (2006). Safety and Security in the Malacca and Singapore Straits: An Agenda for Action. *Neb. L. Rev.* Retrieved from http://heinonlinebackup.com/hol-cgi-bin/get_pdf.cgi?handle =hein.journals/nebklr85&section=19

Bilal Y., S. (2013). Interview with Bruce Hoffman on today's global terrorism threat. Retrieved March 12, 2013, from http://www.middleeast-armscontrol.com/2013/02/19/interview-with-bruce-hoffman-on-todays-global-terrorism-threat/

Bivort, L. de. (2008). Terrorist Motivation, Cognition and Organization. Evolutionary Services Institute.

Blalock, G., Kadiyali, V., & Simon, D. H. (2007). The Impact of Post 9/11 Airport Security Measures on the Demand for Air Travel. *The Journal of Law and Economics*, *50*(4), 731–755. doi:10.1086/519816

Bomb caused Philippine ferry fire. (2004). BBC news. Retrieved from http://news.bbc.co.uk/2/hi/asia-pacific/3732356.stm

Busted toilets, hot rooms, headaches after fire strands cruise ship in Gulf. (2013). *CNN*. Retrieved March 13, 2013, from http://www.cnn.com/2013/02/11/travel/cruise-ship-fire

Button, R. W., Kamp, J., Curtin, T. B., & Dryden, J. (2009). *A Survey of Missions for Unmanned Undersea Vehicles*. Retrieved from http://www.rand.org/content/dam /rand/pubs/monographs/2009/RAND_MG808.pdf

CSI in Brief. (2011). *CBP*. Retrieved March 10, 2013, from http://www.cbp.gov/xp/cgov/trade/cargo_security/csi/csi_in_brief.xml

Chalk, P. (2008). *The Maritime Dimension of International Security: Terrorism, Piracy, and Challenges for the United States* (Vol. 697). RAND Corporation.

Cronin, A. K., Aden, H., Frost, A., & Jones, B. See U.S. Library of Congress. Congressional Research Service.

Elegant, S. (2004). The Return of Abu Sayyaf. *Time Magazine*. Retrieved from http://www.time.com/time/magazine/article/0,9171,686107,00.html

Exclusive Economic Zone. (n.d.). *United Nations*. Retrieved March 16, 2013, from http://www.un.org/Depts/los/convention_agreements/texts/unclos/part5.htm

Ferries: Senators Murray, Murkowski, Cantwell, Begich and Representative Larsen Introduce Legislation to Improve U.S. Ferry Systems. (2011). *United States Senator Patty Murray Working for Washington State*. Retrieved March 10, 2013, from http://www.murray.senate.gov/public/index.cfm/2011/5/ferries-senators-murray-murkowski-cantwell-begich-and-representative-larsen-introduce-legislation-to-improve-u-s-ferry-systems

Fligstein, N., & McAdam, D. (2012). *A Theory of Fields*. Oxford University Press.

Gerlach, C., & Seitz, R. (2012). Economic Impact of Submarine Cable Disruptions. APEC Policy Support Unit.

Greenberg, M. D., Chalk, P., Willis, H. H., Khilko, I., & Ortiz, D. S. (2006). *Maritime Terrorism : Risk and Liability*. RAND Corporation.

Held, J., & Sukkarieh, S. (2007). A Dynamic Bayesian Network Approach To Modelling UAV Teams. In *Proceeding of the 4th International Symposium on Mechatronics and its Applications (ISM07)* (pp. 1–6). Sharjah.

How Osama bin Laden Was Located and Killed. (2011). *The New York Times*. Retrieved from http://www.nytimes.com/interactive/2011/05/02/world/asia/abbottabad-map-of-where-osama-bin-laden-was-killed.html

Jemaah Islamiya (JI). (n.d.). *National Counterterrorism Center*. Retrieved March 14, 2013, from http://www.nctc.gov/site/groups/ji.html

Johnson Jr., A., Calkins, L., & Fisk, M. C. (2012). BP Spill Victims Face Economic Fallout Two Years Later, 1–7. Retrieved from http://www.bloomberg.com/news/2012–02–23/bp-oil-spill-haunts-gulf-business-owners-almost-two-years-after-disaster.html

Khosravi, A., Nahavandi, S., & Creighton, D. C. (2009). Interpreting and modeling baggage handling system as a System of Systems. In *Industrial Technology, 2009. ICIT 2009. IEEE International Conference* (pp. 1–6).

Kronstadt, K. A., & Vaughn, B. (2009). Sri Lanka: Background and U.S. Relations. Retrieved from http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA486249

Langford, G. O. (2012). *ENGINEERING SYSTEMS INTEGRATION Theory, Metrics, and Methods*. Boca Raton, FL: CRC Press.

Langford, G. O. (2013). Life cycle Management Praxis (competencies and practice). Finger Lakes Chapter of INCOSE. Retrieved from http://www.incose.org/flc/EVENTS/

Lawrence, C. J. (2011). September 11th: 7 Ways 9/11 Has Changed Your Life. Retrieved February 20, 2013, from http://abcnews.go.com/U.S./september-11th-ways-911-changed-life/story?id=14324226

Liberation Tigers of Tamil Eelam (LTTE). (2012). *Jane's Terrorism and Insurgency Centre*, 1–39.

Lichtenwald, T. G., Steinhour, M. H., & Perri, F. S. (2012). A Maritime Threat Assessment of Sea Based Criminal Organizations and Terrorist Operations. *Homel and Security Affairs*, *VIII*(13).

Lorenz, A. J. (2007). Al Qaeda's Maritime Threat. *International Institute for Counter-Terrorism 17*, 1–22.

Madden, T. E. (1988). An Analysis of the United States' Response to the Achille Lauro Hijacking. *Boston College Third World Law Journal*, *8*(1).

Most Americans Willing to Sacrifice Some Privacy to Enhance Safe Air Travel, According to Latest Unisys Security Index. (2010). *Unisys*. Retrieved March 15, 2013, from http://www.unisys.com/unisys/news/detail.jsp?id=1120000970001910179

Murphy, M. N. (2007). Contemporary Piracy and Maritime Terrorism. *Adelphi Papers*, *388*.

Murphy, M. N. (2009). *Small Boats, Weak States, Dirty Money: Piracy and Maritime Terrorism in the Modern World*. New York: Columbia Univ. Press.

Nelson, E. S. (2012). Maritime Terrorism and Piracy: Existing and Potential Threats. *Global Security Studies*, *3*(1), 15–28. Retrieved from http://globalsecuritystudies.com/Nelson Piracy Final.pdf

Oasis of the Seas. (n.d.). *Royal Caribbean International*. Retrieved March 13, 2013, from http://www.royalcaribbean.com/findacruise/ships/class/ship/home.do?shipClassCode=OA&shipCode=OA&br=R

Ocean. (n.d.). *Administration National Oceanic and Atmospheric*. Retrieved March 01, 2013, from http://www.noaa.gov/ocean.html

Office of the Deputy Under Secretary of Defense for Acquisition and Technology, S. and S. E. (2008). *Systems Engineering Guide for Systems of Systems*. Washington, DC.

Osmundson, J., Langford, G. O., & Huynh, T. (2007). System Model of Terrorists. In *Fifth Maritime Security Workshop*.

Perl, R., & ORourke, R. (2001). Terrorist Attack on USS Cole: Background and Issues for Congress. Retrieved March 15, 2013, from http://www.history.navy.mil/library/online/usscole_crsreport.htm

Powell, S. (n.d.). Homeland security chief defends failure to inspect 100 percent of cargo arriving in U.S. *2012*. Retrieved March 10, 2013, from http://blog.chron.com/txpotomac/2012/07/homeland-security-chief-defends-failure-to-inspect-100-percent-of-cargo-arriving-in-u-s/

Profile of the U.S. Cruise Industry. (n.d.). *Association Cruise Line International*. Retrieved March 13, 2013, from http://www.cruising.org/pressroom-research/cruise-industry-source-book/profile-us-cruise-industry

Rabasa, A., & Chalk, P. (2012). *Non-Traditional Threats and Maritime Domain Awareness in the Tri-Border Area of Southeast Asia: The Coast Watch System of the Philippines.* RAND Corporation.

Raymond, C. Z. (2006). The Threat of Maritime Terrorism in the Malacca Straits. *Terrorism monitor*, 2002–2004. Retrieved from http://www.mindef.gov.sg/scholarship/Threat - Reading.pdf

Richardson, M. (2004a). *A time bomb for global trade: Maritime-related terrorism in an age of weapons of mass destruction*. Singapore: Institute of Southeast Asian Studies.

Richardson, M. (2004b). Maritime-related Terrorism: Al-Qaeda, Hezbollah, What Next from the International Jihadist Network. Institute of Southeast Asian Studies.

Robertson, N., Cruickshank, P., & Lister, T. (2012). Documents reveal al Qaeda's plans for seizing cruise ships, carnage in Europe. Retrieved March 13, 2013, from http://www.cnn.com/2012/04/30/world/al-qaeda-documents-future

Rubacky, T. (2013). How Safe are We at Sea? Retrieved March 22, 2013, from http://www.cruisemates.com/articles/consumer/security.cfm#axzz2OJIVrdwU.

Sakhuja, V. (2005). Terrorist's Underwater Strategy. Retrieved March 22, 2013, from http://www.ipcs.org/article/terrorism/terrorists-underwater-strategy-1679.html

Schmidt, M. S., & Shanker, T. (2012). To Smuggle More Drugs, Traffickers Go Under the Sea. Retrieved March 17, 2013, from http://www.nytimes.com/2012/09/10/world/americas/drug-smugglers-pose-underwater-challenge-in-caribbean.html?pagewanted=all&_r=0

Sea Tiger Organization. (2001). *Jane's Intelligence Review*, 1–2.

Sea Tigers, stealth technology and the North Korean connection. (2001). *Jane's Intelligence Review*, 1–5.

Seven Seas Navigator. (n.d.). *Regent Seven Seas Cruises*. Retrieved March 13, 2013, from http://www.rssc.com/ships/seven_seas_navigator/

Singapore's 2012 Maritime Performance. (2013). *Maritime and Port Authority of Singapore*. Retrieved March 12, 2013, from http://www.mpa.gov.sg/sites/global_navigation/news_center/mpa_news/mpa_news_detail.page?filename=nr130110.xml

Smart Containers. (n.d.). *Globalsecurity*. Retrieved March 18, 2013, from http://www.globalsecurity.org/security/systems/smart_containers.htm

Terror's New Frontier: Underwater. (2009). *CBS News*. Retrieved from http://www.cbsnews.com/stories/2005/03/18/terror/main681524.shtml

U.S. Library of Congress. Congressional Research Service. (2004). *Foreign Terrorist Organizations*. CRS Report RL32223, by Cronin, A. K., Aden, H., Frost, A., & Jones, B. Washington, DC, Office of Congressional Information and Publishing.

United Nations Convention on the Law of the Sea. (n.d.). United Nations.

Walker, J. (2010). The Death of Leon Klinghoffer on the Achille Lauro Cruise Ship - 25 Years Later. Retrieved March 22, 2013, from http://www.cruiselawnews.com/2010/10/articles/terrorism-1/the-death-of-leon-klinghoffer-on-the-achille-lauro-cruise-ship-25-years-later

What is Terrorism? (n.d.). *Maine Information and Analysis Center*. Retrieved March 09, 2013, from http://www.maine.gov/miac/miac_citizen_terrorism.shtml

Yemen: The Economic Cost of Terrorism. (2002). *Office of Counterterrorism*. Retrieved March 15, 2013, from http://2001–2009.state.gov/s/ct/rls/fs/2002/15028.htm

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Gary O. Langford
   Naval Postgraduate School
   Monterey, California

4. John Osmundson
   Naval Postgraduate School
   Monterey, California