Preprint Manuscript:
Patterson, Douglas A., and Raj Bridgelall (2020). Attack risk modelling for the San Diego maritime facilities. *Marine Policy*. DOI: 10.1016/j.marpol.2020.104210.

Attack Risk Modelling for the San Diego Maritime Facilities

Douglas A. Patterson
Captain
United States Navy
23609 Galeria Circle, Ramona, CA 92065
Phone: 619-455-9074; Email: douglas.patterson@navy.mil
ORCiD: 0000-0001-9414-7318

Raj Bridgelall (Corresponding Author)
Assistant Professor of Transportation and Program Director
College of Business, North Dakota State University
Department of Transportation, Logistics, and Finance
P.O. Box 863676, Plano, TX 75086
Phone: (408) 607-3214; Email: raj@bridgelall.com
ORCiD: 0000-0003-3743-6652

Declaration of Interest: None

Disclaimer: This academic paper was co-authored by Captain Douglas A. Patterson, USN, in his personal capacity. The views expressed in this article are the author's own and do not necessarily represent the views of the United States Navy, the Department of Defense or its Components, or the United States.

1. Introduction

California is the largest economy in the United States and is also home to the nation's most productive marine ports. California ports process more than 40% of the containerized cargo entering the U.S. and almost 30% of the nation's exports (CAPA, 2020). In addition to facilitating trade, cruise ships call on 4 of the 11 California ports. Each cruise ship call adds an average of $1M to the local economy (The Port of Los Angeles, 2020). California ranks second behind Florida in economic impact of the international cruise ship industry (CLIA, 2019). In 2018 cruise ship embarkments in the U.S. totaled 12.7 million passengers (CLIA, 2019).

1.1 Port Security

A compromised U.S. port would pose severe economic challenges to the region and national defense. Perpetrators continuously seek ways to exploit vulnerabilities in the physical security and cybersecurity of ports. Terrorists could transport dangerous cargo or weapons in containers, or attack ships in a harbor to kill people and destroy assets. One example of maritime terrorism is the 2000 bombing of *USS COLE* while in port Aden Yemen. Utilizing an explosive-laden small boat, two terrorists detonated the devices while alongside the U.S. Navy destroyer. The attack killed seventeen U.S. sailors. Since that attack, there were three other maritime terror attacks and 147 maritime terror incidents (START, 2020).

Marine ports are particularly vulnerable to physical attacks because of the sheer quantity of hazardous and complex cargo that they process, the inconsistency of regulatory environments around the world, and difficulties enforcing regulations at sea and ashore (Bateman, Assessing the Threat of Maritime Terrorism Issues for the Asia-Pacific Region, 2006). Hence, terrorists could exploit unforeseen vulnerabilities to cause harm that can cripple the American economy. In reaction to the

USS COLE attack, the U.S. Congress released a report of their investigation with the following recommendations (Staff, 2001):

1) implement better processes to ensure useful operationally oriented intelligence
2) conduct formal vulnerability assessments at regular intervals
3) standardize a threat level system
4) increase preparedness for water-borne terror attacks
5) establish clear lines of authority and responsibility for force protection efforts.

The degree to which U.S. ports have been following the congressional recommendations is not studied as part of this project.

1.2 The Port of San Diego

The cruise ship business in San Diego is the fastest growing in California (CLIA, 2019). San Diego bay is a strategically located harbor with maritime infrastructure that supports trade, cruising, and military operations. The Unified Port of San Diego (UPSD) is a public benefit corporation that controls 2400 acres of land, 3500 acres of water, and 34 of the 54 miles of San Diego bayfront property (Economics & Planning Systems Inc, 2019). The port has two marine cargo terminals that transship automobiles, agriculture commodities, lumber, wind energy components, and other bulk commodities (Pate, Taylor, & Kubu, 2007). The Broadway Pier and B Street cruise ship terminal serves the cruise industry.

The UPSD also supports ship movements for the U.S. Navy and rapid troop deployment in case of a national emergency. The U.S. Department of Defense manages seven bases within the port's area of operations. The U.S. Department of Defense and the U.S. Department of Transportation designated the UPSD as a "strategic" port where services must be available during a defense mobilization (Pate, Taylor, & Kubu, 2007). The port is also designated as a "controlled" port

to limit vessel access from certain countries that pose a threat (Pate, Taylor, & Kubu, 2007). In 2008, the San Diego County Office of Emergency Services completed an assessment of vulnerabilities to critical infrastructures within the county (URS, 2008). As a maritime infrastructure, the UPSD has, in some form, adopted the congressional recommendations to improve port security. However, since then the port has not conducted a formal vulnerability assessment.

1.3 Goals and Objectives

The importance and significance of the San Diego harbor raises the question, "What is the risk of an attack on the UPSD relative to other California ports?" Hence, the **goal** of this study is to seek an answer to that question by conducting a data-driven risk assessment. The **objective** is to apply a standard risk assessment model by quantifying the variables based on economic, operational, and historical data about likely terror tactics on maritime assets. The unique **contribution** of this paper is a vulnerability assessment based on expertise from personal knowledge of the port characteristics accumulated from more than 30 years of maritime experience, including service as Executive Officer and Captain of a U.S. Navy ship that uses the port facilities regularly (US Navy, 2020).

The organization of the remainder of this paper is—Section 2 describes the risk assessment model and the data sources used to quantify the variables. Section 3 elaborates on characteristics of the data that points to the potential for threats, likely tactics of an attack, and possible consequences from compromised security. Section 4 analyzes the vulnerability of the UPSD attack surface to likely attack scenarios. Section 5 discusses the value of using simple models despite their limitations in encapsulating the unpredictable behaviors and the adaptability of terrorists. Section 6 provides concluding remarks about the significance of the work, the findings, implications for action, and comments on future work to investigate the application of more complex models.

2. Methods

The Department of Homeland Security uses the Risk Analysis and Management for Critical Asset Protection (RAMCAP™) framework to standardize risk assessments (USGAO, 2010). The United States Coast Guard currently uses an asset-level decision tool based on the framework (USGAO, 2010). The RAMCAP framework quantifies risk across all critical infrastructure as

$$R = T \times V \times C. \quad (1)$$

The variables R, T, V, and C encapsulates the levels of Risk, Threat, Vulnerability, and Consequence, respectively (Brashear & Jones, 2008). This TVC model defines *risk* as the probability of loss due to an event that causes harm. *Threat* is the likelihood of an attack. *Vulnerability* is the probability that an attacker can exploit weaknesses in the design, implementation, or operation of the system. *Consequence* is the relative level of loss incurred or harm inflicted. The quantification of each variable requires a thorough qualitative and quantitative analysis that lists all the critical assets, their relative attractiveness to terror threats, vulnerabilities that attackers can exploit, and the economic impacts due to their loss.

The linearity of the TVC model dictates that a low value for at least one of the three factors will dominate in lowering the overall risk. Conversely, all three factors must take on a similarly high value to equate to a high risk. Best practices normalize all variables so that the values are between 0 and 1 or classified into an ordinal range of low, medium, and high. Some practices simplify the model by combining T and V into a probability of attack P. This simplifies the risk assessment because evaluators need only list all the attack probabilities for each asset along with the associated consequences of its loss, including any potential fatalities. The total risk R for asset i is then the sum of products of probabilities and losses where

$$R_i = \sum_i P_i C. \quad (2)$$

It is not viable to use this simplification when an exhaustive list of assets is difficult or impractical to obtain, such as for this study. Therefore, the expanded TVC model must suffice.

A criticism of the TVC model is that it consolidates multiple attack-surface threat probabilities into a single probability score that can diminish the representation of the threat and undermine the ability of risk managers to guide the optimum allocation of resources to reduce risk (Cox, 2008). Critics of the model also suggest that it does not necessarily reflect what terrorists do when making decisions about targets (Brown & Cox, 2011). Furthermore, the model assumes that each of the three factors is independent. For example, threat probability is not influenced by the vulnerability of the target or the potential consequence. However, the model is simple, has an intuitive appeal, and has broad applicability to a first-order risk assessment in the face of high uncertainty. Subsequent research suggested that "strength of knowledge judgments" can modify the confidence of the probabilities in such models (Askeland, Flage, & Aven, 2017). The knowledge of a potential attacker's capacity, intention, knowledge, and behavior provide modulation for the probability. These findings validate the need to utilize experts in vulnerability assessments because of their knowledge, experience, and familiarity with the characteristics of the attack surface.

Figure 1 illustrates the use of data to quantify each factor in the TVC model. The relative level of *threat* is a measure of UPSD attractiveness as a terror target based on the port's proportional value of commodity flow for California ports.

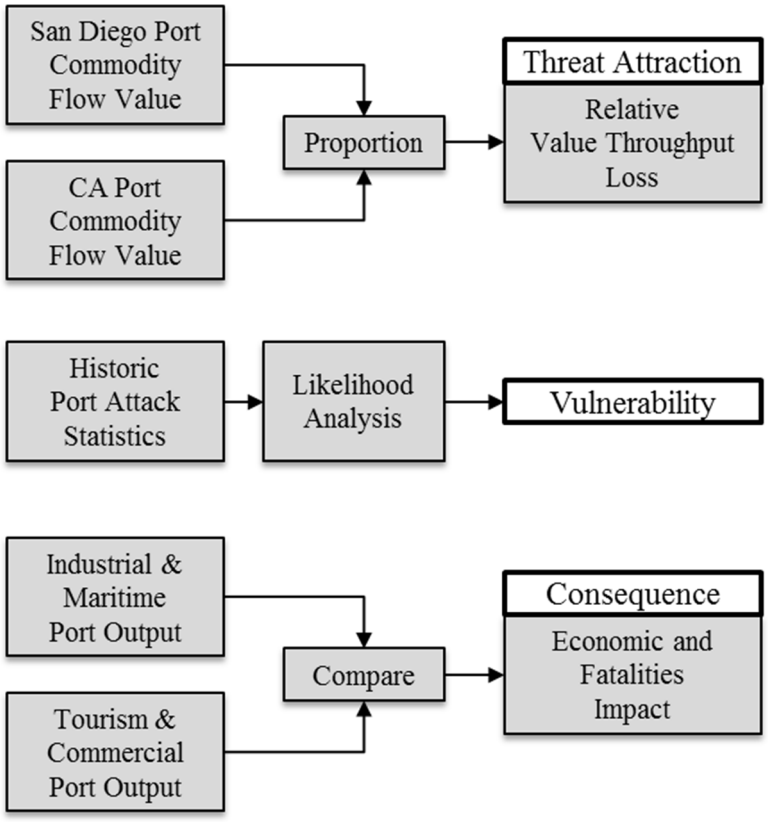

Figure 1. Data used to evaluate the TVC risk quantification model.

The notion that perpetrators assess the trade-off between risk and reward as a function of their capabilities, the effort or cost required to complete a successful attack, and the degree to which their objective is achievable, form the bases for threat attractiveness. *Vulnerability* assessment will use data from the literature and data mining of a global terrorism database to determine the expected tactic based on profiling previous maritime attacks and assessing the likelihood of an attempt using the expected tactic. Quantification of the attempt likelihood leverages expert knowledge of characteristics of the UPSD attack surface. The authors base expert knowledge on the first author's decades of experience with at-sea service and experience as the Executive Officer and Captain of a U.S. Navy ship. *Consequence* assessment will quantify the port output based on freight and cruise activities, and the regional impact in case of economic or human losses.

3. Data

The study synthesized the data for quantifying the variables of the TVC model from a variety of sources shown in Table 1.

Table 1. Data Source for the TVC Model.

Parameter	Description	Data Source
Threat	Commodity Flow (San Diego Port)	World Port Source (WPS, 2020)
Threat	Commodity Flow (California Ports)	Freight Analysis Framework (FAF, 2019)
Vulnerability	Attack date, type, method, and region	Global Terror Database (START, 2020)
Consequence	The economic impact of port activities	(Economics & Planning Systems Inc, 2019),
Consequence	Humans life at risk	(Economics & Planning Systems Inc, 2019) (CLIA, 2019), (CAPA, 2020), (The Port of Los Angeles, 2020),

A successful cargo port attack would temporarily reduce the local cargo flow capacity and disrupt the local economy. Some ports process more of one type of cargo than others. Hence, disabling a port's capacity could create a severe temporary shortage for a certain type of product, which could lead to hoarding and price increases. A significant local impact will likely lead to heightened security for all U.S. ports. Historically, such countermeasures with initially low resources create severe processing bottlenecks that could result in spoilage, delays, and shortages, which subsequently accelerates fear and stock market crashes, ultimately crippling the U.S. economy. Therefore, the attractiveness of attacking the USPD will depend on the initial local impact in capacity reduction relative to all the other California ports.

Figure 2 plots the dollar value and California share of the imports and exports handled by the UPSD. Aggregate commodity flow data were not available for the years 2008 through 2011. The value of imports increased by approximately 27% from 2012 to 2015. However, the average share is only 2.1% of all California ports. Hence, from a *threat* perspective, the UPSD will be an unlikely target if the perpetrator's goal is to significantly diminish the value and capacity of cargo movements through California's ports.

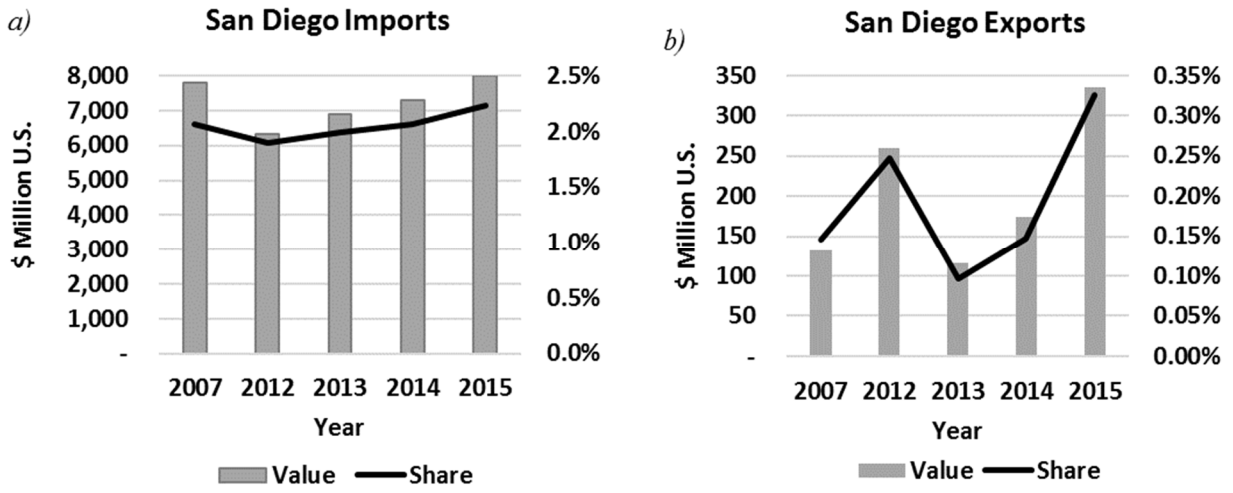

Figure 2. Value and share of San Diego port a) imports and b) exports.

The UPSD also supports 92 tourist cruise ships each year (Economics & Planning Systems Inc, 2019). The local economic impact from this cargo and tourism activity was $9.4 billion and 70,000 jobs. Tourism and related commerce accounted for 53.7% of the economic impact. Figure 3 compares the annual cruise ship calls and passenger throughput for marine terminals in the three largest California cities. Since 2017, cruise ship calls at the UPSD was comparable to the other California ports. Passenger volume through the UPSD increased by more than 75% in the four years from 2016 to 2019. This throughput increase is in stark contrast with Los Angeles and San Francisco where there were a 3% increase and a 3% decrease, respectively. UPSD has plans to accommodate record passenger volumes and port calls through 2020 (UPSD, 2020).

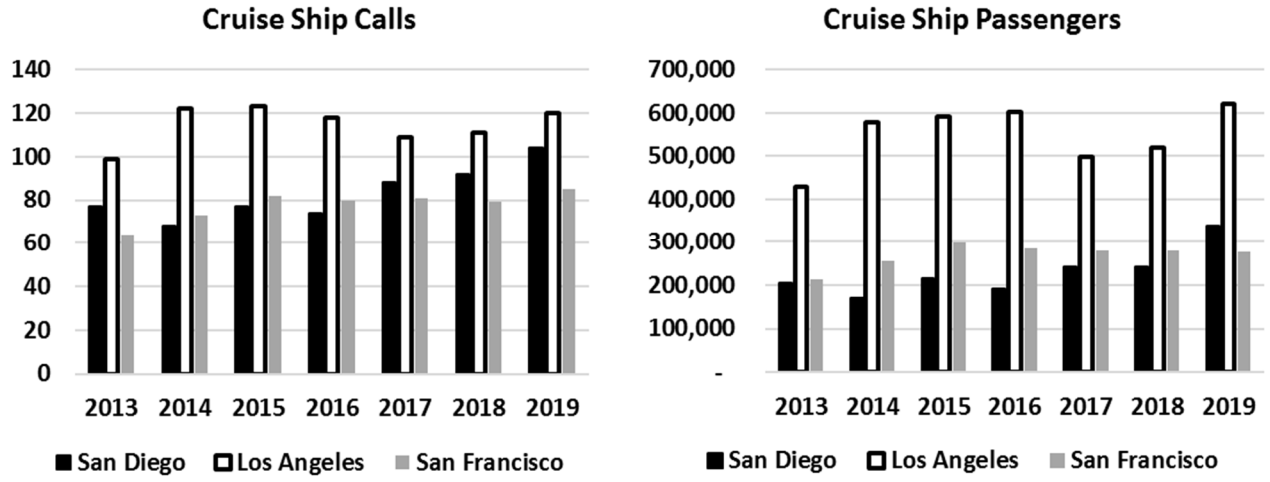

Figure 3. Top California cruise ship port a) calls and b) passenger throughput.

Analysis of nearly 1000 terror attacks on surface transportation systems found that 74% of the fatal attacks involve multiple fatalities and 28% involved ten or more fatalities (Jenkins, 2004). Research also suggests that like large commercial aircrafts, cruise ships can be symbolic and high-prestige targets for terrorists (Greenberg, 2006). Cruise ships are particularly high-profile targets because of the large number of prosperous, middle-class passengers confined within a single physical space, reliable sail schedule, and variable dock-side security standards (Walker, 2012). A U.S. Government Accountability Office (GAO) report theorized that a successful terror attack on a cruise ship in or near a U.S port would harm the U.S. economy due to the sheer size of the industry (USGAO, 2010). These statistics suggest that both the economic impact and potential fatalities would be relatively high if terrorists attacked the UPSD cruise ship terminal. Therefore, both the *threat* and *consequence* factors would be relatively high, which leaves *vulnerability* as the only factor that would determine the overall level of risk to a terror attack.

Vulnerability assessment requires knowledge of the attack types, methods, and regions to determine their likelihood as well as the characteristics of the attack surface of the UPSD. The

former comes from profiles of the nature of historical maritime attacks, and the latter comes from expert knowledge and experience of the potential target and its environment. Figure 4 summarizes the results from mining the Global Terror Database (GTD)™ to determine the proportions of weapon type, attack method, and attack region for maritime attacks from the year 2000 to 2017.

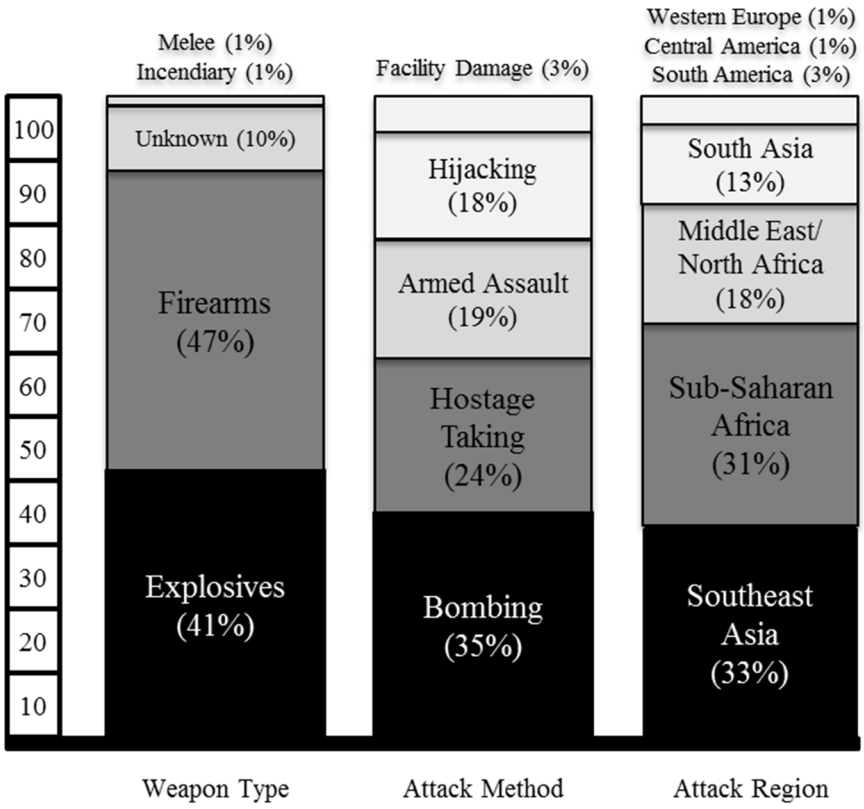

Figure 4. Historic proportions of attack type, method, and region.

The GTD, maintained by the National Consortium for the Study of Terrorism and Responses to Terrorism (START) at the University of Maryland, is the most comprehensive unclassified database of terrorist attacks in the world (START, 2020). The data from more than 160 recorded attacks reveal that firearms or explosives dominate as weapons. Both types of weapons require access to get within close range of the target while allowing for a quick escape. All the attacks were outside of North America. The proportions are the best estimators of the probability of those attack profiles.

4. Results

Risk managers use scenarios to model risks and plan countermeasure exercises. A 2007 Congressional Research Service report recommends addressing scenarios of most significant concern (Parfomak, 2007). Bateman (2006) identified six credible maritime terror-attack scenarios (Bateman, 2006):

1. Ship sunk to block a strait
2. Ship with hazardous or dangerous cargo used as a floating bomb
3. Underwater swimmer attack on ship or port facility
4. Bomb attack on a cruise liner
5. Chokepoint blocked by sea mines
6. A suicide attack by small craft

Table 2 summarizes characteristics of the UPSD attack surface and their assessed vulnerability to the six attack scenarios. San Diego does not have petroleum, natural gas, crude oil, or petrochemical processing facilities. The only presence of these commodities are petroleum fuels for cargo, cruise ship and warship use. There are minimal hazardous cargo movements around the port. Therefore, attacks involving the use of hazardous or dangerous cargo ships as floating bombs are unlikely.

Since attacks require extensive advanced planning and coordination, perpetrators must have a staging facility that is sufficiently close to the target to reduce escape time, and private enough to avoid detection. Perpetrators must also have access to conduct a thorough observation of the facilities to understand activities and traffic patterns. Hence, perpetrators must covertly blend in with natural harbor traffic. Based on expert knowledge, candidate areas for staging facilities for vessel launches at UPSD are all close to heavily secured U.S. Navy facilities. Furthermore, the UPSD uses a private security firm to transfer risk mitigation activities (Allied Universal, 2020), and uses the

International Ship and Port Facility Security Code that registers all ship suppliers (ISSA, 2016). Therefore, suspicious surveillance activities at the UPSD are likely to be detected.

Table 2. Scenario Likelihood for UPSD

Scenario	UPSD Characteristic	Vulnerability
Ship Sunk	The presence of waterborne assets from US Navy, US Coast Guard, and Harbor Police in channels deter this scenario—substantially lowering vulnerability.	Low
Hazardous Cargo Bomb	Minimal and controlled hazardous cargo movements	Low
Bomb Aboard Ship	Port security, passenger, and luggage screening	Low
Sea Mines at Chokepoint	No ideal chokepoints in the harbor	Low
Suicide Craft	Multiple agency surveillance of small craft traffic	Low
Underwater Attack	Multiple agency surveillance of small craft traffic U.S. Navy facilities are heavily secured Possible attack staging facilities can be easily detected	Low

5. Discussion

Data mining of the GTD revealed only four instances of pure maritime terror. The first was the 2000 Al Qaeda linked explosive-laden small-boat attack on the *USS COLE* while in port Aden Yemen for refueling. The second was the 2002 Al Qaeda linked explosive-laden small-boat attack on the French-flagged oil tanker *LIMBURG* as it arrived in Aden Yemen. The third was the 2004 suicide bomber attacks from within empty cargo containers in the port of Ashdod Israel. The fourth was the 2004 Abu Sayaf bombing of *Superferry 14* (Pate, Taylor, & Kubu, 2007). A profile of those cases reflects the difficulty in using their tactic because few terror groups have the mariner capability to execute this type of attack. It is tempting to conclude that terrorism is not a significant threat to military and merchant maritime operations because of this low frequency of successful maritime attacks (Ban, 2010). However, law enforcement and management efforts to coordinate and execute the International Maritime Organization and International Ship and the Port Facility Security Code requirements have been significant deterrents (Marine Insight, 2019).

Terrorists represent diverse groups with varying numbers and social, political, and economic motivations. Terrorists adapt to countermeasures and adjust to shifting political realities, but they are

susceptible to capability shortfalls. Vulnerability gaps are where terrorists utilize their capabilities and resources to realize their malicious intent. When the resources required to protect vulnerabilities from all anticipated scenarios exceeds rational economic expenditure, terror groups are, in a sense, successful (Akhtar, Bjornskau, & Veisten, 2010).

Although simple equation-based risk assessments are less expensive and easy to apply, they might miss scenarios that represent a high risk. On the other hand, more complex models are often more expensive to apply, and they may require expertise that organizations cannot afford. More expensive models may overvalue risks and cause an organization to expend resources on countermeasures that may be unwarranted. Allocating security resources to one target or location can increase the probability of success at another (Akhtar, Bjornskau, & Veisten, 2010). Therefore, there is value in conducting a first order analysis by using simple, standardized models with broad applicability and assessments based on expert knowledge of the characteristics of a potential target.

6. Conclusions

The state of California is the largest economy among states in the nation. California's marine ports are the gateways to 40% of trade that drives the economic engine of the country. Historic terror attacks previously sensitized the world about potential vulnerabilities in critical infrastructure and the transportation system that moves people and goods. However, a lapse in attacks could result in complacency. This study selected the Unified Port of San Diego (UPSD) to analyze the risk of a terror attack partly because it is the fastest-growing cruise ship port in California, and partly because of the author's expertise and familiarity with the port. There has been no publication indicating that a risk assessment of the UPSD had been done after 2008.

The methodology used to assess the risk of an attack was the standard TVC model of the RAMCAP™ framework used by the Department of Homeland Security. The framework equates risk

to the product of three variables: threat, vulnerability, and consequences. Risk is highest only when the value of all three variables is high. A low value for at least one of the variables will equate to low risk. The analysis used economic impact and port operational data to assess the relative levels of *threat* and *consequence*. When compared with other California ports, both the threat and consequence factors were relatively low for the port's cargo processing facilities. However, both factors were relatively high for cruise ship operations. Subsequently, the risk would be directly proportional to the vulnerability factor in cruise ship operations.

The vulnerability assessment considered the high likelihood tactics and weapons used in maritime attacks, based on a literature review and data mining of the Global Terror Database (GTD)™ maintained by the National Consortium for the Study of Terrorism and Responses to Terrorism (START) at the University of Maryland (START, 2020). The authors base the vulnerability assessment on the expertise of the first author as Captain of a U.S. Naval ship and his decades of experience with the characteristics and operations of the UPSD. The assessment resulted in a relatively low vulnerability for the likely attack scenarios. Hence, although the relative threat and consequences of an attack on the cruise ship operations would be high, the TVC product includes a relatively low value for vulnerability, which equates to relatively lower risk than other scenarios. However, perpetrators continuously adapt their strategies and tactics by seeking out new vulnerabilities that may be currently unknown or unanticipated.

Malicious actors can plan hundreds of attacks and be productive with only one success. Defenders can prevent hundreds of attacks and yet fail from one successful attack. The analysis suggests that any misjudgments in vulnerability can result in missing an indication of high risk, but in no way suggest that there is an imminent or probable threat of attack on the UPSD. That is, the analysis suggests that it is wise to assume that the vulnerability could change and to avoid

complacency by conducting more regular assessments. The development or update of policies to encourage a security culture will avoid complacency.

There are a variety of approaches to risk assessment. Alternative methods include game theory, event trees, and complex adaptive systems. This research focused on using the TVC model so that in future research, the authors can repeat the exercise with other types of models to compare results.

7. Acknowledgements

The authors wish to thank all reviewers of this manuscript that vetted the manuscript for pre-publication security clearance because the author is a Captain in the U.S. Navy. Reviewers include personnel from the U.S. Department of Defence, Office of Prepublication and Security Review, the Port of San Diego, the U.S. Coast Guard, local law enforcement and stakeholders, and the Security Training Assessment and Assistance Team of the Naval Criminal Investigative Service. This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

References

Akhtar, J., Bjornskau, T., & Veisten, K. (2010). Assessing Security Measures Reducing Terrorist Risk: Inverse Ex-Post Cost-Benefit and Cost-Effectiveness Anaylsis of Norwegian Airports and Seaports. Oslo: Springer Science Business Media LLC. doi:10.1007/s12198-010-0046-z

Allied Universal. (2020, April 14). *Port Security Services - Allied Universal*. Retrieved Nov 2, 2019, from www.aus.com/industry-expertise/government-institutions/ports

Askeland, T., Flage, R., & Aven, T. (2017). Moving beyond Probabilities - Strength of knowledge characterizations applied to security. *Reliability Engineering & Systems Safety, 159*, 196-205. doi:10.1016/j.ress.2016.10.035

Ban, K.-J. (2010). The Clash of David and Goliath at Sea: The USS COLE Bombing as Sea Insurgency and Lessons for the ROK Navy. *Asian Politics & Policy, 2*(3), 463-485. doi:10.1111/j.1943-0787.2010.01203.x

Bateman, S. (2006). Assessing the Threat of Maritime Terrorism Issues for the Asia-Pacific Region. *Security Challenges, 2*(3), 77-91. Retrieved from www.jstor.org/stable/26459043

Bateman, S. (2006). Assessing the Threat of Maritime Terrorism Issues for the Asia-Pacific Region. *Security Challenges, 2*(3), 77-91. Retrieved from https://www.jstor.org/stable/26459043

Brashear, J. P., & Jones, J. W. (2008). Risk analysis and management for critical asset protection (RAMCAP plus). In *Wiley handbook of science and technology for homeland security* (pp. 1-15). doi:10.1002/9780470087923.hhs003

Brown, G. G., & Cox, A. (2011). How Probalistic Risk Assessment Can Mislead Terrorism Risk Analysts. *Risk Analysis, 31*(2), 196-204.

CAPA. (2020, April 12). *California Ports – Gateways to America*. (California Association of Port Authorities (CAPA)) Retrieved April 12, 2020, from CAPA California Ports: https://californiaports.org/economic-benefits/

CLIA. (2019). *Contribution of the International Cruise Industry to the U.S. Economy in 2018.* Washington, D.C.: Cruise Lines International Association (CLIA).

Cox, L. A. (2008). Some Limitations of "Risk = Threat x Vulnerability x Consequence" for Risk Analysis of Terrorist Attacks. *Risk Analysis*, pp. 1749-1761. doi:10.1111/j.1539-6924.2008.01142.x

Economics & Planning Systems Inc. (2019). *Economic Impacts of the San Diego Unified Port District in 2017.* Oakland: Economics & Planning Systems Inc.

FAF. (2019, December 17). *Freight Analysis Framework Version 4*. (C. f. Analysis, Producer, & Oak Ridge National Laboratory) Retrieved April 15, 2020, from Freight Analysis Framework Data Tabulation Tool (FAF4): https://faf.ornl.gov/faf4/Extraction3.aspx

Greenberg, M. e. (2006). *Maritime Terrorism: Risk and Liability* . Santa Monica: RAND Corporation.

ISSA. (2016, August). *International Ship and Port Facilities Security Code.* Retrieved Sept 23, 2019, from www.shipsupply.org

Jenkins, B. M. (2004). Terrorism and the Security of Public Surface Transportation. Washington DC: RAND Corporation.

Marine Insight. (2019). *The Importance of Port Security*. Retrieved Sept 30, 2019, from https://www.marineinsight.com/maritime-law/the-importance-of-port-security/

Parfomak, P. F. (2007). *CRS Report for Congress.* Washington DC: Congressional Research Service.

Pate, A., Taylor, B., & Kubu, B. (2007). *Protecting America's Ports: Promising Practices.* Washington, D.C.: Police Executive Research Forum.

Staff, U. H. (2001). *The Investigation into the Attack on the USS COLE.* Washington, D.C.: U.S. Government.

START. (2020, April 13). (N. C. (START), Producer, & University of Maryland) Retrieved April 13, 2020, from Global Terrorism Database (GTD): https://www.start.umd.edu/data-tools/global-terrorism-database-gtd

The Port of Los Angeles. (2020, April 12). *Cruise Statistics*. Retrieved from The Port of Los Angeles: https://www.portoflosangeles.org/business/statistics/cruise-statistics

UPSD. (2020, April 14). *Port of San Diego*. Retrieved April 14, 2020, from https://www.portofsandiego.org/cruise-terminals

URS. (2008). *San Diego Operational Area Critical Infrastructure Protection Plan.* San Diego: URS.

US Navy. (2020, April 22). *Training Support Center San Diego*. Retrieved from Captain Douglas A. Patterson, Commanding Officer: https://www.public.navy.mil/netc/centers/tscsd/Leadership.aspx?PID=1

USGAO. (2010). *Maritime Security: Varied Actions Taken to Enhance Cruise Ship Security, but Some Concerns Remain.* Washington, D.C.: USGAO.

Walker, W. (2012). Cruise Ships: The Next Terrorism Target? *Travel Law Quarterly*, 124-135.

WPS. (2020, April 14). *Port of San Diego Foreign Trade*. Retrieved April 14, 2020, from World Port Source (WPS): http://www.worldportsource.com/trade/USA_CA_Port_of_San_Diego_228.php