Maritime Security Series:

To Arm or Not to Arm: A Rational Analysis of Deterrence Theory in Modern Piracy

Sagebrook Research

Table of Contents

Executive Summary

The debate over whether to arm vessels in an effort to prevent maritime piracy is one that has raged for several years. The increasing number of attacks, as well as the increasingly violent tactics employed by the pirates, has caused the debate to reach a fevered pitch. On one side of the debate are those that espouse the use of non-lethal, or less than lethal, tactics to dissuade the pirates while waiting on patrolling navy vessels to provide security. On the other side of the debate are those that believe that the ships are better served to arm themselves to deter pirates from attacking the ships or to prevent attacking pirates from successfully taking control of a vessel. This paper advocates for arming maritime vessels to prevent a ship from being taken by pirates. This paper will illustrate the rationale for such a choice.

Deterrence Theory

To understand whether arming ships provides any value it is important to have a working definition and basic understanding of the concept of deterrence. Deterrence has application in military and criminal areas and, as any parent can attest, has some value in dissuading children from doing things they should not. When discussing the concept as it applies to piracy none of the referenced examples are fully applicable. Deterrence theory rests on the premise that humans are, by nature, rational. Deterrence, at its most basic level can be defined as: *"the prevention of actions through the fear of retribution."*

The Rational Actor Theory posits that humans are rational and will take actions that are in their own best interests. Each decision a person makes is based upon an internal cost/benefit analysis. By altering the cost-to-benefit ratios, behavior can be changed accordingly. When put into the context of the definition provided above, deterrence from piracy rests on elevating the "…fear of retribution..." to a point where it is no longer a rational choice to attack a vessel. While the concept is simple in theory, it can be somewhat more complex in practice.

The saying, "the punishment should fit the crime." is an application of the theory of deterrence when used in crime prevention. If a person is faced with $100 fine for robbing a bank, a thief may decide that the risk of paying $100 for an act that will, on average, yield $3,000 is a risk worth accepting and they will attempt to rob a bank. If, on the other hand, a person is faced with 15 years in federal prison, the cost/benefit analysis changes and therefore behavior changes. Rationality has some potential pitfalls that will be covered briefly. To change the cost/benefit analysis it is critical to understand what it is that a particular person values. In general, we can understand a person's calculus of value, but it is not always accurate. Take the bank robbing example used previously. If a bank robber values the comfort of prison, then the threat of 15 years in prison would not change the cost/benefit analysis for that particular person. A more cogent example would be that of a person driven by ideology. When a

person is driven by ideology the value calculus becomes very difficult to understand and traditional deterrence is likely not effective. This is why crime cannot be prevented, only mitigated.

General and Specific Deterrence

Deterrence theory relies upon the rationality of actors to be effective. Criminal justice proposes two broad types of deterrence; general deterrence and specific deterrence. Both types of deterrence have application for maritime security. General deterrence is proactive and attempts to target potential crimes *before* they are committed. Examples of general deterrence may include "no trespassing" signs warning that trespassing is a crime and stating the particular law and penalty. It is likely that most readers are familiar with the posted signs in post offices that warn of the "…minimum of 15 years in federal prison for robbing a post office." For those who have travelled to Singapore, a form of general deterrence to drug trafficking is the very obvious sign that warns people entering the country that trafficking in drugs is punishable by death in Singapore. Other forms of general deterrence include video cameras and armed guards in public view. Many of the companies that advocate for less than lethal techniques propose using security guards with wooden or plastic rifles as a general deterrence to would be pirates. The hope is that the mere sight of a person holding what is believed to be a real weapon would be enough to dissuade a potential attack. In theory, there is little reason to believe that this would not work. It is when the general deterrence does not work that the strategy becomes less than effective. If general deterrence was entirely effective bank robberies would be non-existent. Instead, in the US alone, there are more than 10,000 bank robberies every year. Clearly, general deterrence has its limitations.

Specific deterrence, on the other hand, is reactive and is focused upon punishing those that perpetrate crimes. It is here that the criminal justice theory is not quite as applicable for maritime security. While the use of force is not intended to punish pirates, the possibility of being injured or killed while attempting to hijack a ship is a specific deterrence for a person considering such an action. The objective is that the potential pirate believes that by attempting to perpetrate an act of piracy there is a possibility of being hurt or killed in the act. Complementing this is the fear of being captured and prosecuted, although it is suggested that today this provides little deterrence effect.

The 3 Keys to Deterrence: Certainty, Celerity, and Severity

Deterrence is based upon the three principles of certainty, celerity, and severity. Certainty applies to the likelihood of the threat (whether arrest, punishment or retribution) being carried out. Studies suggest that a certain, consistent level of certainty must be achieved to produce desired consequences. In short, if a law is all bark and no bite, the threat of a bite will have no impact on the cost benefit analysis. The greater the likelihood of punishment, the deterrent will have greater affect. Celerity applies to the promptness of the threat being carried out. If there is the threat of immediate action as opposed to the threat of action at some point in the distant future, the deterrent will have greater

effect. Consider a teenager that wants to attend the coolest party of the year but is told that if they break curfew they will not be allowed to go to a different party set six months in the future. Even if the likelihood of the punishment is 100%, the teenager will evaluate the celerity in making the value proposition. As any parent of a teenager will likely confirm, the curfew will be an afterthought and the party will come first. Finally, the severity of punishment is critical to any deterrent. As stated previously, the "punishment must fit the crime". The increase in severity has a correlation to the effectiveness of the deterrent. In short, the greater the severity of the action, the less likely the prospective criminal is to perpetrate the act. An easy way to show the correlation is through the traditional model of risk analysis.

The Concept of Risk

Experience demonstrates that risk is one of the topics that is frequently discussed and used but often not well understood or properly applied. From deciding whether to walk down a dark alley to deciding upon a particular financial investment, people deal with risk on a daily basis and analyze risk numerous times per day. While often the analysis is not intentional or may not be a conscious or intentional, it is applied when making decisions. Understanding risk and how to analyze risk allows people to make informed decisions about potential actions. This section will discuss the basic terms and concepts and how they apply to deterrence theory and maritime security.

Analyzing and Modeling Risk

Risk is commonly described as the probability or likelihood of a known loss. Risk can be quantified or qualified. For our purposes, we will use a basic model to quantify risk simply to demonstrate the value of deterrence. This paper will define Risk as a function of the following:

The likelihood of an *Event* occurring and the resulting *Impact* should the event occur.

For the purposes of this paper, the Event is the deterrent. The likelihood applies to certainty described earlier while the Impact applies to the severity of the act. Overarching each of these is the concept of celerity. In short, regardless of the probability and impact, if the threat cannot be realized immediately, there is little deterrence. A simple method of quantifying risk is to multiply the likelihood of an event occurring in a given time frame (expressed as a probability) by the expected impact should the event be realized.[1] The calculation can thus be expressed as:

(% of Event A occurring) X ($ Impact should Event A be realized) = Annualized Loss Expectancy (ALE)

The following will demonstrate the use of this model to quantify a given risk. First, assume there is a 5% probability that an event will occur in a given year and the estimated damage will be $10,000. In this scenario the Annualized Loss Expectancy (ALE) is calculated at $500 per year (5% x $10,000). This is the

[1] The general ALE model has been modified for the purposes of the paper.

basic premise, though certainly there are much more advanced actuarial data and more sophisticated models on which insurance premiums are based. In a perfect world, actuarial and other information would be available to allow people to evaluate Risk with a great degree of accuracy. While the risk model described above quantifies risk it is presented as an easy way to understand the correlation between the concepts of certainty and severity as they apply to deterrence. For our purposes the model will be changed to the following:

(% of Event A occurring) X (Impact should event A be Realized)= Calculated Deterrence Expectancy (CDE)

While we cannot quantify exact probabilities, we can provide a range of probabilities and impact using the following rankings:

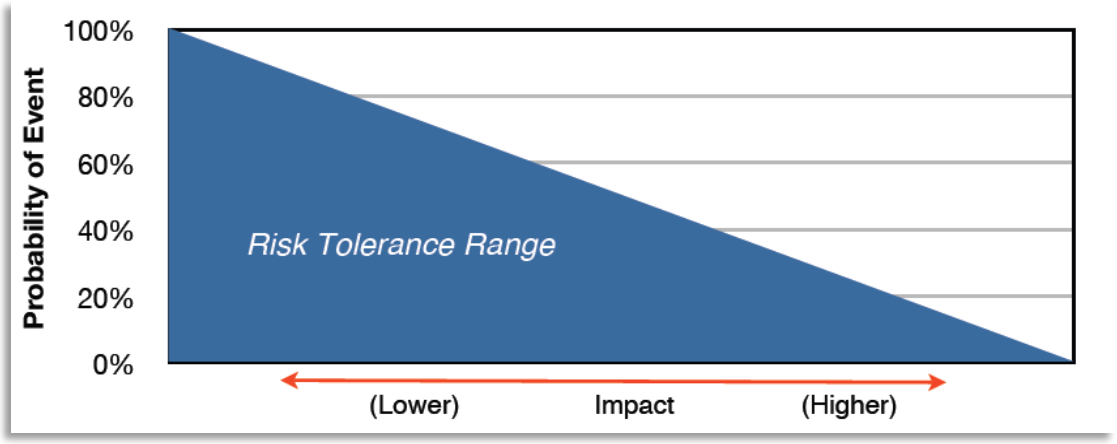
- High – 3
- Medium – 2
- Low – 1

These can be placed into a risk matrix that allows for a quick, yet accurate, analysis of the relative risk. If the impact is high (3) and the probability is high (3), the CDE is calculated as high (3 x 3) and is demonstrated by having a greater product of the two components. It should be noted that this model works for both sides of the adversarial situation. A pirate looking at a ship armed with guards would calculate that the impact would be severe, as the weapons could easily hurt of kill them. In evaluating what appears to the pirates to be a cadre of capable, disciplined guards would allow the pirates to make a mental calculation that the likelihood of being hurt or injured would be increased. This would result in a deterrence effect for the pirates. Conversely, by having armed guards, the ship would calculate that the probability of the act they are trying to prevent (ship takeover) would be decreased proportionate to the increase in deterrence effect of the guards, and the impact would be reduced, as well.

		Probability of Threat		
		High (3)	Medium (2)	Low (1)
Impact of Threat	High (3)	9	6	3
	Medium (2)	6	4	2
	Low (1)	3	2	1

Understanding Risk Tolerance

Risk tolerance describes the threshold of risk that a person is willing to tolerate given the potential 'payoff' if the act is successful. In general, if there is a high potential payoff and there is a high likelihood of an event occurring but there is little impact, the willingness to tolerate the event is high. Similarly if there is a high potential payoff and a low likelihood of an event occurring, yet a greater impact, the willingness to tolerate the impact is also high. If the likelihood increases relative to the impact or the impact increases relative to the probability the tolerance decreases. The tolerance to risk increases with the potential payoff. The old adage: "high risk, high reward" is very relevant when considering deterrence.



Protection + Deterrence = Crime Prevention

At the risk of oversimplifying the work of criminologists, crime prevention can be summarized as protection + prevention. Protection applies to the 'hardening' of targets by implementing controls that increase the level of difficulty of perpetrating a crime. A vault is a good example of a protective measure. While no vault is completely impenetrable, vaults do provide significant protective value. Armed guards provide two purposes. First, they are protective. In short, a guard's job is to prevent a criminal from completing the criminal act. Secondly, as this papers has attempted to illustrate, armed guards provide deterrence value. A potential criminal would need to evaluate the risk of being hurt of killed in the act of committing the crime. This deterrence value alone is often enough to dissuade criminals. In the instances where it is not, the guards provide protective value.

Putting it all together: To arm or not arm ships?

With an understanding of risk and deterrence theory the limitations of employing less than lethal alternatives becomes glaringly apparent. Ships without an armed guard are literally at the mercy of the pirates. As there is no effective anti-piracy enforcement to prevent hijackings and the likelihood of a

pirate being caught is statistically very low, and the reward is very high they have little deterrence to prevent them from attempting to hijack a ship and great incentive to do so. There are some security vendors that have proposed placing guards on ships with fake guns in an attempt to dissuade potential pirates through general deterrence. The theory is that the sight of the weapons alone will deter a potential attacker, as the attacker will believe there is risk in attacking the ship. It is suggested that this tactic is not simply ineffective; it is dangerous to the ship and the crew. The proposed tactic works so long as the pirates believe the threat is real and so long as they calculate the potential payoff as being less than their risk tolerance will allow. Once they determine that 1) the weapons are not real or 2) decide that an attack is worth the risk, the charade of having armed guards has now turned potentially dangerous. A pirate boarding a ship with "fake" guards will likely be less than amused and will quite possibly take violent action against the crew. In short, guards armed with fake weapons present a significant liability to the crew as they cannot provide the protective value that is the second component of crime prevention.

To provide an effective deterrence and protection, armed guards are needed. Armed guards can deter potential attacks and if the deterrence does not stop the attack, can protect the ship and crew by taking decisive action against the pirates.

About The Authors

Chris Mark is a recognized payment security and risk expert. He is the former founder and CEO of the two companies and has worked for both MasterCard and Visa on their security programs. Chris has conducted payment security and risk management globally on behalf of Visa and the PCI SSC. He is the founder of the Society of Payment Security Professionals (SPSP) and led the development of the Certified Payment-Card Industry Security Manager (CPISM) and Certified Payment Card-Industry Security Auditor (CPISA) certifications. Chris is a former enlisted US Marine and US Navy Officer. He is a qualified Marine Infantryman (0311), Scout/Sniper (8541) and Reconnaissance Marine (8654) and a former Reconnaissance Instructor. Chris is a combat veteran of Operation Continue Hope and has attended numerous military training courses including: Basic Infantryman, Scout/Sniper, Urban Sniper, Basic Reconnaissance, Urban Surveillance and Reconnaissance, Airborne, Pathfinder, Navy Scuba, HRST Master, and Security Forces. Chris holds a CISSP, CIPP, CPISM/A, and numerous technical certifications. He also holds MBA and BA degrees. Chris has published numerous articles on risk, risk management, and information security and is a frequent speaker on the topics of payment card security and risk management.

Dr. Heather Mark, PhD earned her doctorate in Public Administration and Public Policy from Auburn University and since has been a sought after expert in the areas of regulatory compliance, privacy, data security, risk and governance. She has founded two successful boutique consultancy firms and has worked with a number of companies to answer complex regulatory and public policy related questions. Her experience in competitive intelligence and market analysis provides unique insight on the impact of regulatory actions on the private market. Dr. Mark is a frequent author and speaker on topics related to the intersection of private commerce and public policy.

About Sagebrook Research

Sagebrook Research specializes in providing information services to companies of all sizes in a variety of industries. Led by an experienced research and information services professional, Sagebrook Research can provide your company with the specialized services that it needs. From technical writing to competitive research and analysis, Sagebrook Research provides can assist companies in developing market strategies, positioning statements or marketing documentation. Sagebrook Research's team brings a wide diversity of experience including management, information services, and regulatory compliance consulting.

The information contained in this document represents the current view of Sagebrook Research on the issues discussed herein as of the date of publication. It should not be interpreted as a commitment on the part of Sagebrook Research and Sagebrook Research cannot guarantee the accuracy of the information presented after the date of publication. Specifications and content are subject to change

without notice. This document is for informational purposes only. SAGEBROOK RESEARCH MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.