THE UTILITY OF RISK ASSESSMENT TOOLS IN MARITIME SECURITY ANALYSIS

Donna J. Nincic

Dr., ssociate Professor and Chair
Department of Global and Maritime Studies
California Maritime Academy, California State University
200 Maritime Academy Drive, Vallejo, CA USA 94590
Email: dnincic@csum.edu; phone: 707.654.1202; fax: 707.654.1110

Bruce Clark

Captain, irector of Maritime Security
Office of Sponsored Projects and Extended Learning
California Maritime Academy, California State University
200 Maritime Academy Drive, Vallejo, CA USA 94590
Email: bclark@csum.edu; phone: 707.654.1273; fax: 707.654.1158

Abstract The international maritime community has embraced the need to introduce and adopt security measures to protect vital shipping, facility and port assets from terrorist attacks. This said, the maritime security environment is dynamic and changing, and the specific nature of the threat can vary across time, from country to country, and – within an individual country – from port to port. Threat and risk assessments, and training scenarios, need to become more dynamic, and tailored to specific needs of individual ports, facilities and even vessels. To this end, we introduce a simple set of tools that may allow port and facility managers, and vessel security officers to perform their own individualized risk assessments; specifically the use of *risk matrices* to help identify their most likely risks, and develop security and training plans accordingly. Very simply, a risk matrix allows the user to identify how serious a risk is, based on the expected destructiveness (cost) of an event, and the probability of that event occurring.

Keywords Maritime security; ritime terrorism; isk assessment; isk matrix; isk analysis

0 Introduction the complexity of the global maritime domain

Terrorist risks to merchant shipping are a growing part of the overall spectrum of terrorist threats and present significant challenges to control and prevention due to the nature of the global maritime trade environment. Between 80% and 95% (depending on measure) of global trade is carried by ship[1], with more than 1.2 million seafarers[2] on 120,000 vessels in the global maritime

fleet,[3] making calls at over 2,800 ports in the world[4] The maritime environment is so extensive and so complex, that securing the maritime environment a) from attack, b) from being used in an attack, or c) in support of an attack, is a global challenge.

The international maritime community recognizes the vulnerability of the global maritime domain to terrorist attack, and since September 11, 2001, has embraced the need to introduce and adopt security measures to protect vital shipping, facility and port assets. The International Ship and Port Facility Security Code (ISPS), initiated by the International Maritime Organization in 2002 as an amendment to the Safety of Life at Sea Convention (SOLAS, 1974), describes minimum requirements for ship security, with Part A providing mandatory requirements, and Part B providing non-mandatory guidance for the implementation of Part A. The main objectives of ISPS are:

- To detect security threats and implement security measures;
- To establish roles and responsibilities concerning maritime security for governments, local administrations, ship and port industries at the national and international levels;
- To collate and disseminate security-related information;
- To provide a methodology for security assessments so as to have in place plans and procedures to react to changing security levels.[5]

The latter requirement – providing an assessment methodology to allow for changing security levels – presents a complex and challenging task: The maritime security environment is shifting and dynamic, and the specific nature of a given threat can vary across time, from country to country, and – within an individual country – from port to port. There is a need for threat and risk assessments, and training scenarios, to become more responsive to the specific needs of individual ports, facilities and even vessels. However, coming up with individualized risk and threat assessments, and appropriate training exercises, can be a daunting task, involving significant amounts of time and money (both of which are always in short supply).

To this end, the introduction of a simple set of tools, drawn from risk assessment techniques used in the social sciences and computer science, may allow port and facility managers, and vessel security officers to perform their own *individualized* security assessments; specifically the use of *risk matrices* to help identify the most likely risks to their shipping and port facilities, and develop security and training plans accordingly. Very simply, a risk matrix allows the user to identify how serious a risk is, based on the expected negative impact (destructiveness, cost) of an event, the vulnerability of a ship, port or facility to attack, and the associated probability of that event occurring.

1 Defining threat and risk

It is important to define the terms “threat” and “risk”. The two terms are often used interchangeably, but there are subtle differences between the concepts that are worth emphasizing.

1.1 Threat: A function of will and capacity

Threat refers to both the *will* and the *capacity* to inflict damage or harm:

- *Will* consists of the desire not only to *acquire* the means to inflict harm, but actually to *use* these means. If, for example an individual/group/country has acquired WMD, but has no desire to use them against its adversaries, there is no immediate threat;

- *Capacity* consists of the means to inflict harm on a desired target; specifically any necessary *knowledge* and/or *materials*. Capacity is a considerably higher obstacle than will – it is easy to desire to do harm but much harder to operationalize the desire into a credible threat.

To use the standard "bomb-in-a-box" "nightmare" scenario as an example: For there to be threat from a dirty bomb hidden in a shipping container, *each* of the following must occur:

- There must be someone who both desires this to occur, and is willing actually to undertake the logistics, organization and planning necessary to set such an event in motion (*will*), and

- They must have the ability actually to undertake the logistics, organization and planning necessary to set such an event in motion; they must also have the knowledge necessary to build an effective radiological device, *and* they must have access to radioactive material, and the materials needed to build an effective device (capacity).

It is important to remember that threat is a multiplicative function: If there is will, but no capacity, there is no threat. Similarly, if the capacity to do harm exists, but there is no will, then there is no threat.

1.2 Risk: threat, vulnerability and impact

Risk, on the other hand, can be seen as a partial function of threat:

$$\text{Risk} = f(\text{Threat } x \text{ Vulnerability } x \text{ Impact})$$

Where:

- *Threat* (as above) consists of both will and capacity to do harm. Again, it is important to think of this as multiplicative (will *x* capacity) because if either will or capacity is equal to zero, there is no threat;

- *Vulnerability* refers to the opportunity given (usually inadvertently) to others to do harm. It is a reflection of how well protected (or not) the target (ship, port, etc) is against an attack or harmful event – either through fortunate circumstance or through sound security policies. ("Fortunate circumstance" occurs when a category of threats does not obtain due to geography, nature of the cargo handled, etc. For example, an offshore oil platform is not vulnerable to a truck bomb; a port which does not handle LNG is unlikely to be vulnerable to an LNG attack).

Vulnerability is, therefore, related to *probability*. The more vulnerable a facility is (for whatever reason) the more probable the event, *ceteris paribus*. (It is important to note that the ship, port facility, etc. has a considerable degree of control over its own vulnerability).

- *Impact* refers to the destructiveness, cost, etc., of the event, should it occur. In addition to loss of life, destruction of infrastructure, and financial losses due to stopped or delayed business, impact can also include time lost due to employees refusing to come to work, having difficulty working once they have returned, or time diversion due to the need to respond to

the press, local and national politicians, community concerns, etc.

This is to say, someone may wish to do me great harm and have the ability to do me great harm – may, in fact, be a threat to me – but I run no risk from this threat if my vulnerability to it is zero ***or*** if the impact of the threat is zero. Similarly, I may be extremely vulnerable, and the impact of any act of harm may be significant, but if no one wishes to do me harm or has the capacity to do me harm (ie, there is no threat) my risk exposure is zero.

To use the "bomb in a box" scenario again:

- Someone may have both the desire and capability to plant a radioactive device in a shipping container and place it on a vessel scheduled to call at one of my nation's ports (Threat > 0);
- The global supply chain from the point where the container is loaded, placed on a ship, and delivered to my port (with possible numerous other transfers in between) is not one hundred percent secure – that is, possible weaknesses can be identified in the supply chain, either in one's own port, during points of transit, or in the ports of one's trading partners which makes the probability of the event occurring greater than zero (Vulnerability > 0);

While other definitions exist, these will obtain for the purpose of this analysis. "Threat" will refer to specific scenarios that can cause harm; "risk" will refer to a multiplicative function of an existing terrorist threat, a ship or port's vulnerability to that threat, and the impact of the terrorist event, should it occur.

Once again, the analysis of threat and the analysis of risk – while intrinsically intertwined – must be kept conceptually and operationally separate. For any given threat, the risks associated with that threat will differ, because vulnerabilities differ. The distinction between the two concepts is very important when conducting a risk assessment – not all identifiable threats will be risks for a given ship or port facility.

1.3 Implications

Once threats and risks have been identified, the fact that even in an identifiable risk environment (assuming a constancy of this environment), vulnerabilities and impacts can vary enormously, creating three problems:

(1) The magnitude of conducting risk analyses for all the ports. (While it is tempting to focus on only the "major" ports, this may well at best create only a "diversion" effect – and a terrorist attack on a smaller port could well have a major economic impact due to the psychological impact an attack would create).

(2) Second (and related) – there is no uniform risk analysis for all ports – not globally, not within a single country. There might be a "grouping" of "like ports" that can be determined – i.e., ports with similar enough profiles that the risks are considered similar enough for them to be determined and analyzed as a single category. This said, this cannot be known until an assessment has been done, compiled, and analyzed for a significant number of a nation's ports. Those who are in the best position to do this are the port managers and security personnel on the ground -- perhaps in conjunction with external security analysts/experts -- but not with complete reliance on them.

(3) Third – even if a thorough risk analysis (and corresponding solutions) were performed, it would be static – as the times change, so do the threats, vulnerabilities and impacts; and, consequently the associated level of risk.

What is perhaps most useful at this stage is a *risk framework for analysis* that can be used by port managers and security specialists to self-analyze their individual threats and risks. If a uniform framework for analysis can be adopted, it could provide numerous benefits, including ease of comparability not only between ports, but also within individual ports over time.

Therefore, using the simple terms defined above, any risk analysis will consist at a minimum of two general parts:

- Identification of threat – (will x capacity x opportunity)
- Identification of risk – (threat x vulnerability x impact)

The specific details of these two components are presented in the following section.

2 A risk framework for analysis (RFA)

The basic risk model outlined above forms the foundation of a *risk framework for analysis*, when added to specific techniques for identifying and assessing threat, vulnerability and impact. Risk analysis techniques are commonly used in many businesses – computer technology comes to mind – where security is a daily concern. These techniques are used whenever an event could cause unacceptable losses – in human life, financial losses, infrastructure, business delays, etc. Proper risk and threat analysis techniques – at the level of scenario formation – are the foundation of successful plans, strategies, and training.

Risk analysis has two key components: 1) risk assessment, and 2) risk management. In 1981, Kaplan and Garrick[6] posed three fundamental questions that constitute the risk assessment process:

- What can go wrong? (What are the threats?)
- What is the likelihood? (What is the probability of the event occurring; or how vulnerable is the ship/port?)
- What are the consequences? (What are the possible impacts should the event occur?)

Risk management (beyond the scope of this study), on the other hand, addresses the following:

- What can be done and what are the options available?
- What are their associated tradeoffs in terms of cost, benefit and risk?
- What are the impacts of current management decisions on future options?[7]

2.1 The risk filtering, ranking and management (RFRM) method

To address these questions, we have partially adopted the *Risk Filtering, Ranking, and Management* method (RFRM) developed by Haimes, Kaplan, and Lambert[8]. Divided into seven phases, the RFRM introduces a process to filter, prioritize, and manage a large number of risk

scenarios:

- Phase I: Scenario Identification. A hierarchical holographic model (HHM) is developed to identify all risks applicable to a system; in our case, a port facility. Holographic refers to "holistic" and "multi-dimensional" in system-component identification (ie, in the maritime domain, being aware that threats can be subsurface and airborne, and not just attacks from land or sea-surface).

  Taken to greater complexity, the HHM can be viewed as a "master chart" with different perspectives on the system, sub-systems within the system, etc (ie, subsurface is a system component – human attacks could be viewed as a subsystem, as could technological attacks, animal attacks, etc). The utility of this approach is that it encourages those performing the threat assessment to think through all possible arenas of threat and attack.

- Phase II: Scenario Filtering, the set of risk scenarios identified in Phase I is filtered according to the needs, preferences, and interests of the system user.

- Phase III: Bi-Criteria Filtering and Ranking: The scenarios are filtered further, using qualitative assessments to arrive at a matrix of "likelihood and consequence", probability and impact, yielding a severity – or risk – *value*.

- Phase IV: Multi-Criteria Evaluation: Scenarios that remain after Phase III are examined in the context of the facility, to see if the identified scenarios can "defeat the resiliency, robustness, and redundancy of the underlying system".

- Phase V: Quantitative Ranking; Based on the results of Phase IV, a quantitative matrix scale of likelihood and consequence is developed and applied to represent both the relative and absolute importance of the remaining scenarios (and thus the importance of addressing them). The scale is based on which scenarios are more of a threat to the facility, given the security systems already in place. For example, scenarios that may be less severe (low risk value) may actually rank high on the Quantitative Ranking if the facility does not yet have the means adequately to address the threat.

- Phase VI: Risk Management is performed, involving the identification of management options for dealing with the most urgent remaining scenarios, and estimating the cost, performance benefits, and risk reduction of each.

- Phase VII: Safeguarding Against Missing Critical Items, the performance of the options selected in Phase VI is examined against the scenarios that have been filtered out during Phases II to V.

- Phase VIII: Operations Feedback, the experience and information gained in system operation is used to refine and update the scenario filtering and decision processes in Phases II –VII.

2.2 Risk analysis: performing a layered approach using the RFRM method

Returning to the questions posed by Kaplan and Garrick, a layered process can be performed to begin to assess the level of risk associated with a given port facility:

- *What can go wrong?* To answer this question, Phase I of the RFRM is performed – The

"holographic" components of the maritime domain are identified, and using the HHM, maritime terrorist threat scenarios are determined.

- *What is the likelihood? What are the consequences (impact)?* The RFRM, Phases II and III, are then applied; the terrorist threat scenarios are filtered and ranked, and, based on qualitative assessment, the probability and impact of each scenario is determined.

(Phases IV through VII of the RFRM are applicable to Risk Management, and are beyond the scope of this immediate study).

2.3.1 RFRM (Phase I): threat event/scenario identification

Identifying terrorist threat scenarios specific to the maritime domain is a two step process:

(1) First, all key elements of the maritime domain must be identified (the "holographic" approach);

(2) Threats for each domain component are identified, using evidence from the literature, and creative speculation about what could happen. Threat identification is, at its essence, a fundamentally creative concept – the more scenarios identified, the greater the likelihood that plans will be in place to protect against the widest range of potential threats.

2.3.2 RFRM (Phases II and III) likelihood and consequences: using a probability- impact matrix

Once a set of threats is identified (and this may run into the hundreds), the must be organized in a manner that allows for their practical assessment. A simple matrix, based on the probability of an event occurring and the impact of an event, should it occur, can be a very useful means of presenting (and comparing) a wide range of threats in a simple schematic form.

Table I is an example of a 5×5 table (risk matrices/tables can be expanded to any number of rows and columns – greater or fewer – depending on the needs of the user):

Table 1

	Probability				
Impact	1	2	3	4	5
1	(1)	(2)	(3)	(4)	(5)
2	(2)	(4)	(6)	(8)	(10)
3	(3)	(6)	(9)	(12)	(15)
4	(4)	(8)	(12)	(16)	(20)
5	(5)	(10)	(15)	(20)	(25)

The numbers 1 though 5 associated with *Probability* run from lower to higher:

(1) Lowest probability of occurring (0% to 20% probability)

(2) Low probability (21% to 40% probability of occurring)

(3) Medium probability (41% to 60% probability of occurring)

(4) High probability (61% to 80% probability of occurring)

(5) Highest probability (81% to 100% probability of occurring)

Because probability is, by definition, a number from zero (the event will not occur) to one hundred (the event will certainly occur), the probability values in a 5x5 table can be associated with their respective quintiles.

The numbers 1 though 5 associated with *Impact* also run from low to high:

(1) Lowest level of negative impact

(2) Low level of negative impact

(3) Medium level of negative impact

(4) High level of negative impact

(5) Highest level of negative impact

The number in parentheses in the middle of each cell is the ***risk value***:

$$\text{Risk Value} = \text{Probability } x \text{ Impact}$$

Items with higher risk values are considered the primary threats. Note that it is possible to have an extremely destructive event (Impact = 5) but not a high risk value if the probability of this event occurring is very low (Probability = 1). So events with high impact or high probability can be less of a risk that events with a lower impact and lower probability.

In our color coded table, the green cells represent events with the lowest risk value (RV), the blue cells have low risk values, the yellow cells have moderate risk values; the orange cells have higher risk values and the red cell has the highest risk value. The orange and red cells, therefore, represent events of the most serious concern.

3 Example: Applying the Risk Framework to an Hypothetical Port

Risk analysis requires performing phases 1-3. *Phase I* involves threat scenario identification – scenarios are identified from open sources, using previously published studies, reports and information, and interviews with experts. In a project at the California Maritime Academy, a research team under the supervision of the author identified forty-five maritime threat scenarios [9]. These scenarios are listed in Appendix A.

In *Phase II*, we filtered the scenarios, in essence performing a "reality check". We decided that the scenarios were best grouped and presented according to source, or point of origin, of the attack:

- Direct attacks on vessels;
- Surface attacks;
- Subsurface attacks;
- Airborne attacks;

- Landside attacks; and
- Water/Land interface attacks.

In *Phase III*, we prepared the scenarios for use in the Probability-Impact matrix, assigning each scenario both a probability value (1-5) and an impact value (1-5). The assignment of both the probability value and the impact value was based on an assessment of similar events that had occurred in the past, as well on educated hypotheses of what might happen in the future. Obviously, the initially assigned probabilities are *subjective* probabilities and should be updated and refined by Bayesian techniques as additional information becomes available.

Our results are as follows in Table II (the numbers in each cell refer to the number of the threat scenario in Appendix A).

Table 2

	Probability				
Impact	1	2	3	4	5
1	(1) 1, 36	(2)	(3)	(4)	(5) 19
2	(2) 14, 15	(4) 2	(6)	(8) 25, 27, 33, 26	(10)
3	(3) 24	(6) 21, 22, 16	(9) 34	(12) 12, 35	(15)
4	(4) 6, 7	(8) 17, 18, 8, 38	(12) 11, 4	(16) 30, 45	(20) 31
5	(5) 20, 37	(10) 3, 9, 10, 23, 39, 40	(15) 13, 28, 29, 41, 42, 43, 44	(20)	(25) 32, 5

For ease of use, the table is color-coded to highlight events of similar risk levels:

- Green (Risk Values 1-5): Events of lowest risk (11 events)
- Blue (Risk Values 6-10): Events of low risk (18 events)
- Yellow (Risk Values 11-15): Events of moderate risk (11 events)
- Orange (Risk Values 16-20): Events of high risk (3 events)
- Red (Risk Value 25): Events of highest risk (2 events)

3.1 The importance of individual port and security assessments

The assignment of the probability and impact values is largely subjective, with the numbers assigned better thought of as relative rankings, rather than absolute values. An event with a probability value of “four” for example, means only that the event is considered more likely to occur than an event with a probability value of “three” and less likely to occur than an event with a probability value of “five”.

Along similar lines, it is important to remember that the probability and impact values (and therefore, the risk values) will vary from port to port within and between nations. For example, an

event that is assigned a probability value of "three" and an impact value of "four" for a San Francisco port, may have a probability value of "two" and an impact value of "five" for a port in Singapore.

3.2 Interpreting the results

While all the events in the table should be taken seriously, and plans developed to guard against them, a clear hierarchy of events emerges: Those events with both the highest probability *and* the highest impact should be given priority in planning, training and testing. This does not mean that events with lower risk values should be ignored; this framework merely establishes a means of establishing priorities, and allows ports to test more realistic scenarios, rather than the generic "bomb-in-a-box" which may or may not be a risk specific to their particular facility.

Therefore, when the RFA is taken to the next level, to incorporate both Risk Management as well as Risk Assessment, the threat scenarios in the Orange and Yellow cells of the Risk Matrix should form the foundation of future training operations and scenario formation.

4 Conclusion

This article has been an effort to present a basic introduction to the use of risk matrices in risk analysis and risk management. The utility of risk matrices stems from the ease with which they can be learned and used, their flexibility, and their adaptability to dynamic and rapidly-changing security climates. Their success, however, depends on the following:

- Correct and complete identification of threat scenarios. The forty-five scenarios presented here are a partial list of threats to a hypothetical port facility. The development of an accurate threat list requires that vessel and facility security professionals have a solid understanding of the range of possible events that can occur. This is based both on historical analysis of terrorist events that have occurred, and on a creative assessment of what, hypothetically, could occur. This knowledge is a combination of experience, research, and study.

- Correct and accurate assignment of probability and impact values. Again, determining which threat scenarios are more likely to occur than others (and which are less likely to occur) depends on a solid understanding both of the historical record, and on knowledge of known terrorist capabilities. A truck bomb (a terrorist device used with some frequency) is more probably than a radiological device hidden in a shipping container – precisely because the former has happened, while the latter – while it clearly could happen – has not occurred and is beyond the capabilities of most terrorist groups operating today.

- The same requirement for accuracy holds for the assignment of impact values as well – for example, a conventional truck bomb is likely to cause a smaller impact than a successfully-detonated radiological device (although there are conditions under which this might not be true – a correct assessment of the impact value here could depend on knowing how a radiological device disperses compared to, for example, ammonium nitrate – or how destructive radiation is compared, for example, to sarin gas.

- Appropriate training in, and practice of, these techniques. This will involve not only dedicated ship, port and facility security professionals, but members of the international

maritime academic community as well. The latter, in particular, are well-placed to undertake the historical analysis of past maritime terrorist events (the range of what has happened), as well as studies of the impact (economic, structural, psychological) they had when they occurred. At the same time, it is the professionals currently working in the ports and on vessels who are perhaps best placed to understand the range of the possible hypothetical events that could occur on their ships or in their facilities.

Given the above considerations, recommendations for the future might involve workshops for academics and professionals to learn and practice these techniques in "table top" and "gaming" environments, as well as in-depth group or research projects for students at the world's maritime universities. The benefits in increased accuracy of risk assessments, more focused security drills and training, and financial gains (either from not trying to protect against all threats, or from failing to protect against a more likely threat in favor of a more destructive – but less likely – threat) make a better understanding of risk assessment tools well worth exploring.

Acknowledgements

The authors wish to thank Kate Barrett and Joe Mahach (Cadets, California Maritime Academy, Program in Global Studies and Maritime Affairs) for their research assistance, and the US Maritime Administration for funding a previous version of this project.

References

[1] Daly John C k. (24 October 2003). "Al-Qaeda and maritime terrorism, part I," The Terrorism Monitor, Jamestown Foundation.

[2] Richardson Michael (25 February 2004), "A time bomb for global trade: Maritime-related terrorism in an age of weapons of mass destruction," Viewpoints, Institute of South East Asian Studies.

[3] Daly John C k. (24 October 2003). "Al-Qaeda and maritime terrorism, part I," The Terrorism Monitor, Jamestown Foundation.

[4] Richardson Michael (25 February 2004), "A time bomb for global trade: Maritime-related terrorism in an age of weapons of mass destruction," Viewpoints, Institute of South East Asian Studies.

[5] (2005). "ISPS: Risk analysis, impact and contrast across the code," Intervessel, Southampton.

[6] Kaplan S, Garrick B J. (1981). On the Quantitative Definition of Risk, Risk Analysis 1(1): 11-27. Cited in Haimes, Y.Y. and Longstaff, T. (2002). The Role of Risk Analysis in the Protection of Critical Infrastructures Against Terrorism. Risk Analysis, 22(3): 439-444.

[7] Leung M, Lambert J H, Mosenthal A. (2004). A Risk-Based Approach to Setting Priorities in Protecting Bridges Against Terrorist Attack. Risk Analysis, 24(4): 963-984.

[8] Haimes Y Y, Kaplan S, Lambert J H. (2002). Risk Filtering, Ranking and Management. Risk Analysis, 22(2): 381-395. Cited in Haimes, Y.Y. and Longstaff, T. (2002). The Role of Risk Analysis in the Protection of Critical Infrastructures Against Terrorism. Risk Analysis, 22(3): 439-444.

[9] The scenarios were drawn from: The National Strategy for Maritime Security. (September 2005). The White House; Nincic, D. (2005). The Challenge of Maritime Terrorism: Threat Identification, WMD, and Regime Response. Journal of Strategic Studies, 28(4): 619-644; Nincic, D. (2005). Maritime Terrorism: Case Studies for Teaching and Analysis. International Association of Maritime Universities; and Wrightson, Margaret. (17

May 2005). Maritime Security: Enhancements Made, But Implementation and Sustainability Remain Key Challenges (GAO-05-448T). US Government Accountability Office.

Appendix A

Threat Event List: Sorted by Point of Origin

The list is separated in to several distinct categories, based on the point of origin of the attack:

- Direct attacks on vessels;
- Surface attacks;
- Subsurface attacks;
- Airborne attacks;
- Landside attacks; and
- Water/Land interface attacks.

While some attacks may fit into two or more categories, we have placed them in the one category that best suits the scenario. Also included is a rating of the probability of the event occurring (P) and its impact (I), should the event occur. Both are coded on a scale of 1 to 5, five being more probable/higher impact. The scenarios are then ranked, in their respective categories, according to their risk value (RV), or the probability of the scenario multiplied by its impact.

#	Event	P	I	RV
	Vessel (Direct Attack)			
1	*Attack ship's navigation systems, possibly cause crash in port:* This is a convoluted scenario involving tampering with the ship's radar and compass to make the ship think it is in a position according to latitude and longitude that is false. It could cause a collision, but that is not highly probable.	1	1	1
2	*Target barge with DMC for explosion:* This scenario would not be very destructive unless the barge was attached to a terminal facility.	2	2	4
3	*WMD/DMC explodes, sinks ship at entrance to port:* Not all harbors are like the San Francisco Bay, with a small mouth leading into a large bay. Thus, the destructiveness of this scenario varies from port to port.	2	5	10
4	*Missile fired from one ship to another in port.* This involves the commandeering of a vessel from which it is possible to fire missiles to another vessel.	4	3	12
5	*Truck bomb on ferry explodes.* This scenario would cause a lot of media attention, and could also cause the sinking of a ship and the loss of many lives.	5	5	15
	Surface (Attack from surface)			
6	*Hijack ship mid-voyage and use to ram an oil tanker, cause oil spill.* Hijacking is difficult. But the spill caused by ramming an oil tanker could be disastrous, taking many days to clean up and closing down a harbor.	1	4	4

#	Event	P	I	RV
7	*Concerted attack of more than one ship on another ship(s).* Due to the logistics of it, this type of attack is very unlikely. However, it could cause a larger amount of destruction than other scenarios that include vessels ramming into other vessels, because there is at least one more vessel involved. This could cause a large enough obstruction in the middle of the harbor to stop traffic.	1	4	4
8	*Hijack ship mid-voyage to use to ram another ship in port, cause traffic jam.* Again, hijacking a vessel is difficult. The destruction caused by ramming into the right type of vessel, one carrying DMC, could cause a serious explosion.	2	4	8
9	*WMD on suicide boat explodes as rammed into another ship in port.* This scenario's objective is to cause a traffic jam in port by rendering a ship dead in the water through an attack from a suicide boat. Depending on the size of the suicide boat and the amount of WMD it has, the damage could be significant.	2	5	10
10	*WMD in tug/pilot boat explodes next to ship in port.* This scenario is the same as that of a suicide boat, just the disguise of the suicide vessel is different.	2	5	10
11	*Hijack Coast Guard boats to use as suicide boats, provide cover.* The use of USCG boats allows the terrorists to get as close to the terminal as possible without being noticed, as a Coast Guard boat can go anywhere it wants unquestioned. However, original boats are hard to commandeer, but they are extremely easy and cheap to duplicate. They can cause a lot of destruction, too.	3	4	12
12	*Zodiac suicide boat.* This scenario can be easily achieved because Zodiac boats are easy to get hold of and the explosives are also easy to get hold of. It has been used by terrorists in the past, with success, so it should be assumed that it is still a tactic that will be used.	4	3	12
13	*WMD in suicide boat explodes next to ship.* This scenario is similar to that of ramming a vessel in port, the difference being that this time, the suicide boat does not ram the vessel, only sidles up alongside the vessel.	3	5	15
	Sub-surface Attacks			
14	*Dolphins trained to deliver explosives to ship in port.* This scenario involves a lot of training and resources, and so it is not very probable. Also, the target will not create a lot of destruction.	1	2	2
15	*Dolphins trained to deliver explosives to terminals.* This is similar to the scenario above. Again, this involves a large amount of training and resources. However, it could create more destruction than just targeting a vessel.	1	2	2
16	*Mines placed strategically in port.* This scenario has a very ambiguous target. It is hard to place mines in a harbor to specifically target a certain vessel. Also, there is a lot of manpower necessary.	2	3	6
17	*Divers attaching explosives to underside of ships.* This requires a large amount of resources and training, and it only has the potential to sink a vessel.	2	4	8
18	*Divers attaching explosives to terminals.* This is similar to the scenario above involving dolphins, but with more accuracy in placing explosives, more damage can be done.	2	4	8
	Airborne Attacks			
19	*WMD in aircraft crashes into ship in port.* The combination of the explosion of the aircraft's fuel along with the bomb onboard can be very destructive to the vessel and surrounding environment.	5	1	5
20	*WMD in aircraft crashes into terminal.* This scenario can be very destructive to the terminal, shutting it down so it cannot process vessels, thus affecting many vessels. Also, the explosion can be cause a lot of damage.	1	5	5

#	Event	P	I	RV
21	*Using manned/unmanned aircraft (including helicopter) to drop bomb on terminal.* This scenario is similar to the scenario above, however attacking a terminal can be more destructive than attacking a vessel.	2	3	6
22	*Using manned or unmanned aircraft (including helicopter) to drop bomb on ship*. This scenario involves using aircraft, which could be used to attack or to scope out facilities in port.	2	3	6
23	*Attack refineries, chemical factories, power plants in port by explosives-laden plane*. This could shut down the port facilities accepting the cargo that vessels bring in, causing a back up in port, and could take a long time to rebuild. It is not hard to get the materials for this scenario.	2	5	10
	Facility (attack from or on facility) (Note: Facility has been deemed to signify only facilities that directly service and interact with ships)			
24	*Terrorists blockade port.* This scenario involves a terrorist fleet, like that of the Tamil Tigers in Sri Lanka. It involves a large number of vessels that can securely blockade a port, necessitating a lot of man power and supplies to feed, refuel, etc.	1	3	3
25	*Cyber attack to disrupt vessel traffic service, possibly stop port traffic*. This scenario could be easily executed, but the damage may not be that great.	4	2	8
26	*Cyber attack to disrupt terminal operating system*. This scenario involves hacking into the terminal operating system to cause disruption.	4	2	8
27	*Terrorists disguised as casual longshoremen*. It is not hard for terrorists to become casual longshoremen, who are hired on short notice. They also might be able to smuggle in an explosive device.	4	2	8
28	*WMD delivered to terminal in container by train. T*his scenario also has the objective of destroying terminal facilities.	3	5	15
29	*WMD delivered to terminal in container by truck*. This scenario is almost exactly the same as the scenario with the train, and thus is it rated the same.	3	5	15
30	*Missile fired from one ship to port facility* (factory, refinery). This requires a vessel from which a missile can be fired, a missile, etc. But this threat seems much more destructive because it targets certain facilities that could have a larger impact on port operations. For example, if the missile hit a refinery, then it could cause the refinery to shut down for repairs and thus the tankers waiting to offload their cargo would back up as well as tankers waiting to take the refined products elsewhere.	4	4	16
31	*Cutting cables on cranes/destroying cranes*. This could be very destructive because of the fact that to repair the cables could take a very long time. It would also cause a lot of backup at the terminal, and although the ships would be running, they would not be able to unload their cargo. They would have to wait in port or find another terminal, putting pressure all through the port.	5	4	20
32	*Attack refineries, chemical factories, power plants in port by explosives-laden truck*. This is similar to the scenario with an explosive laden plane, but I see it causing more damage as a truck can carry more explosives than a small plane.	5	5	25
	Landside (attack from land) (Landside signifies attacks on parts of ports that would not directly and/or immediately affect ships)			
33	*Terrorists disguised as legitimate facilities maintenance personnel in port*. This scenario would permit terrorists unlimited access to the terminal facilities, allowing them to find out everything their superiors want to know about the different security weaknesses of the terminal. They could also smuggle in an explosive device.	4	2	8

#	Event	P	I	RV
34	*Explosives in a communication tower.* This scenario could be easily executed, and it could interrupt radio communications. Therefore, it could cause a lot of damage, even a collision.	3	3	9
35	*Blow up food truck laden with explosives near terminal entrance.* This could be a serious security risk for terminals because it could blow up the entrance to the terminal, thereby eliminating the gate that controls access to the terminal, and shutting down the terminal for the amount of time it would take to get gate rebuilt.	4	3	12
	Water/Land Interface (attack from water/land interface)			
36	*Ballast water attack, inserting disease into ballast water.* This scenario includes inserting a disease into the ballast tanks of a vessel. However, this would require access to the vessel as well as access to a large amount of the disease in order to carry out the attack. The target is ambiguous, as once ballast water is dumped out, there is no control over the disease's movements, and thus it is very imprecise.	1	1	1
37	*Concerted attack of more than one ship on terminal.* This scenario would be very unlikely because of the fact that there is more equipment needed (more than one vessel needs to be commandeered). But it could cause serious damage.	1	5	5
38	*Hijack ship mid-voyage to use to ram terminal.* The hijacking of a large vessel is difficult, but the destruction caused when the vessel rams into a terminal could be serious.	2	4	8
39	*WMD in tug/pilot boat explodes next to terminal.* This scenario is the same as if any small vessel with a WMD exploded near a terminal.	2	5	10
40	*Smuggle weapons and terrorists in cargo hold/containers to attack from within terminal.* This would not cause a lot of destructiveness because of the small amount of weapons that could pass inspection.	5	2	10
41	*WMD in container explodes on ship in port.* In this scenario, the objective of the terrorists would be to destroy the terminal facility.	5	3	15
42	*WMD in suicide boat explodes as rammed into terminal.* This scenario is similar other WMD scenarios, but the target is different. The effects of the suicide boat ramming into the terminal is a bit more destructive as it actually can affect more than just one or two vessels, since the terminal would take a while to get back up and running.	3	5	15
43	*WMD in tug/pilot boat explodes as rammed into terminal.* This is the same scenario as with any small vessel, just a different type of suicide boat.	3	5	15
44	*WMD in suicide boat explodes next to terminal.* This scenario is similar to that of a suicide vessel ramming the terminal. The damage could close down the terminal for a while for repairs, affecting other vessels indirectly.	3	5	15
45	*Terrorists disguised as port security inspection team.* This would allow the terrorists unlimited access to anywhere on the terminal and surrounding vessels. It would not be hard to buy the necessary uniforms of a port security inspection team on the black market. They might also be able to smuggle in an explosive device.	4	4	16