Measuring the Deterrence Value of Securing Maritime Supply Chains against WMD Transfer and Measuring Subsequent WMD Risk Reduction

Eric Taquechel, Ian Hollan, and Ted Lewis

ABSTRACT

We propose a methodology to analyze the risk of an adversary exploiting the maritime supply chain by smuggling a WMD in a container. We call this risk "WMD transfer risk". We describe an extension of an existing modeling/simulation tool wherein we show how to quantify the deterrence effects of optimal investments in WMD detection technology at U.S. ports; and measure subsequent reduction in WMD transfer risk.

From a theoretical perspective, the implications of notional results from this model are different from implications of the results of traditional "game theoretical" models. From a practitioner perspective, our results emphasize the importance of tailoring foreign intelligence gathering efforts, hardening foreign ports against exploitation in addition to hardening U.S. ports, and comparing simulated optimal technology costs to real-world R&D and implementation costs. The audience for our proposal includes WMD detection technology engineers, law enforcement and security personnel, port operators, and agency executives.

INTRODUCTION

The security of the international maritime supply chain is vital to the economic well-being of the United States. The National Strategy for Global Supply Chain Security,[1] Maritime Commerce Security Plan,[2] and other national strategies emphasize the importance of supply chain integrity to economic prosperity. Thus, we want to protect the supply chain from overt disruptions such as direct attacks on ports.

However, supply chain security is also important for a different reason: to prevent its exploitation by way of smuggling illicit materials and people into the United States. Other strategies such as the National Strategy to Combat Transnational Organized Crime,[3] and reports such as Maritime Transport and Destabilizing Commodity Flows,[4] emphasize the attractiveness of supply chain exploitation to criminal and terrorist elements. This includes possible "transfer" of a weapon of mass destruction (WMD) into the United States, with the intent to detonate it in an inland city. While this is not the same problem as a direct supply chain disruption, the consequences of an inland WMD detonation are extremely important to address.

To address this issue, technology analysis, and modeling and simulation coupled with risk analysis, can help us determine where supply chains are susceptible to exploitation by WMD transfer. This can help us think about where to place limited resources to mitigate this susceptibility. The Maritime Commerce Security Plan advocates:

> Maritime security now involves risks that must be met with a layered approach that identifies and interdicts the threat as far as possible from the U.S. borders. A potential worst case scenario is the risk that a weapon of mass destruction is concealed in a container. Such a threat has severe consequences and must be detected as early as possible. A successful strategy will use risk management to align capabilities with threats to achieve the optimal response and protect the nation.[5]

It can be debated whether a shipping container is the most *likely* mechanism for smuggling a WMD into the U.S. Nonetheless, analyzing the risk of WMD smuggled in shipping containers is one possible approach to reducing WMD transfer risk, since shipping containers

carry much of the goods shipped internationally via maritime conveyance. Before we propose an approach to do this, we review existing and emerging WMD detection technology, risk analysis, and modeling/simulation initiatives.

Existing and Emerging Technological Solutions

The Domestic Nuclear Detection Office (DNDO), a Department of Homeland Security (DHS) component agency, has for the last several years managed the implementation of the Global Nuclear Detection Architecture (GNDA). The GNDA is a multilayered framework of radiological and nuclear weapon detection technologies and coordinating mechanisms, both within the United States and overseas.[6] Example initiatives include:

- The Department of Energy (DOE) Megaports initiative leverages technology to identify and screen high risk cargo shipments overseas, before they depart enroute U.S. ports.[7]
- Customs and Border Protection (CBP's) Radiation Portal Monitors (RPMs) leverage technology to detect the presence of radioactive material in cargo shipments, primarily in U.S. ports.[8]
- U.S. Coast Guard (USCG) officers, equipped with radiation detection equipment, board vessels to ensure security and verify compliance with various regulations.[9]

One emerging technology is the Advanced Spectroscopic Portal monitor (ASP) initiative. This initiative was intended to replace the existing RPMs, which only detect a radiological or nuclear signature. Then, secondary screening must be performed to identify the source of the signature. In contrast, the ASPs were intended to provide both a primary and a secondary screening function.[10] However, this technology has had some challenges to implementation, as detailed in a National Academies report.[11] Going forward, the lessons learned from ASP development may benefit any efforts to develop the next generation of WMD detection technology.

There are many other initiatives not listed here. Together, these initiatives help reduce WMD transfer risk. Located both overseas and in the U.S., they constitute a layered defense. But, currently most of the focus is on the evaluation and testing of existing and emerging technologies. In addition to modeling technology effectiveness, we might also model how technology influences supply chain exploitation risk. Modeling and simulating supply chain exploitation risk requires quantitative representation of the layered defenses in the supply chain, and how technology effectiveness measurably contributes to those defenses. Furthermore, Taquechel and Lewis make the case for quantifying deterrence effectiveness of risk mitigation solutions,[12] and applying that metric to determine unconditional risk.[13] There is also work on optimal solutions to network risk problems, which could support a WMD layered defense strategy within budget constraints.[14] These concepts could be applied to a holistic framework for analyzing WMD transfer risk reduction, and could contribute to efforts to develop new WMD detection technology.

Existing and Emerging Risk Analysis and Network Modeling

Existing risk models such as the Coast Guard's Combating Maritime Terrorism Strategic Risk Model analyze risk of a WMD attack on U.S. port cities and grossly estimate risk reduction effectiveness of current USCG activities.[15] However, it is unclear whether this model explicitly measures deterrence effectiveness of these activities, or allows an analyst to simulate optimal activity levels or resource allocations to minimize WMD risk. It is also unclear whether this model incorporates estimates of WMD detection technology effectiveness into its algorithms, and whether it accounts for overseas exploitation. Also, the U.S. Coast Guard's Maritime Security Risk Analysis Model (MSRAM) is a risk analysis tool that might be

enhanced to analyze WMD risk, but it does not model network effects,[16] so it is unclear whether MSRAM in its current state could support a layered defense strategy for reducing WMD risk.

With respect to analyzing detection effectiveness in the context of supply chain network risk analysis, an attacker may exploit different supply chain network "nodes" such as foreign ports and U.S. ports to smuggle a WMD. Network science offers techniques to model the relationships between these nodes. Lewis explains network science and leverages its techniques in a modeling and simulation tool called the Model Based Risk Assessment (MBRA) model, in order to analyze network risk.[17] MBRA can perform optimization or minimization of network risk given a limited budget, and can calculate return on investment. It treats risk as a probabilistic function of simulated investments. Other network analysis efforts to examine supply chain exploitation include a University of Southern California's Center for Risk and Economic Analysis of Terrorism Events (CREATE) initiative to develop a systems-based framework to analyze WMD transfer risk.[18] Also, DNDO is expanding its Radiological and Nuclear Terrorism Risk Analysis (RNTRA) model to explicitly model pathway exploitation.[19]

These efforts are laudable. That said, there is an acknowledged need for an "integrated, holistic approach to the…security of maritime activities."[20] In this spirit, Taquechel extended Lewis' MBRA model to show a "transfer threat network" model, including foreign ports where a shipping container would originate.[21] This work also showed how attacker preferences can be used in place of traditional network science metrics. However, Taquechel's MBRA extension does not simulate how WMD detection technology effectiveness influences network risk minimization, nor does it show how to measure potential deterrence effects of WMD technology investments. We now explain how our proposed modeling approach will complement and build upon these existing and emerging efforts.

Our First Contribution: Integrating Detection Effectiveness and Network Modeling

Our defense against WMD transfer might benefit from a comprehensive approach to (1) quantitatively model the risk reduction effectiveness of existing WMD detection technology investments at different layers of the supply chain, and (2) do this in the context of overall supply chain exploitation risk. Our existing efforts might also benefit from the analysis of optimal places in the supply chain for additional investment, where we could leverage emerging technology. Thus, one way to enhance existing efforts is to develop a modeling and simulation approach that captures WMD detection technology effectiveness estimates, and that performs supply chain network analysis, risk analysis, basic optimization techniques, and return on investment analysis to produce a comprehensive WMD transfer risk evaluation framework. We propose an approach to do precisely this, by expanding Taquechel's original transfer threat model.

Our Second Contribution: Quantifying Deterrence Effects of WMD Transfer Risk Mitigation Investments

This expansion will also leverage the quantification of deterrence, as introduced in Taquechel and Lewis. Cronin and Cronin propose that deterrence occurs when an actor discourages aggression toward another actor, with the intended outcome that the former never has to respond to aggressive action by the latter.[22] Thus, we might attempt to deter an attacker from smuggling a WMD through the supply chain, rather than relying solely upon our detection equipment once a WMD has already entered the network. However, in this paper we focus instead on modeling how deterrence influences various attacker options, which we will call relative deterrence. That said, we want to quantify the relative deterrence effects of our technology investments, and

estimate how deterrence measurably reduces WMD transfer risk. The National Academies report on challenges with ASP implementation specifically identified that:

> Deterrence…is an important factor in the likelihood that a malefactor will decide to try to smuggle a weapon or weapon materials, but there is not yet a widely accepted intellectual framework…to measure or evaluate this factor.[23]

Taquechel and Lewis show how risk can change based on changes in attacker intent. We can quantify the change in that intent based on the difference between (1) attacker intent to execute a specific attack before deterrence investments, and (2) attacker intent to execute that same attack after deterrence investments. That change in intent represents deterrence, and intent is a component of the legacy DHS risk equation Risk=f(Threat, Vulnerability, Consequence), where Threat is comprised of attacker Intent and Capability.[24] The general deterrence quantification equation we will use for WMD transfer deterrence effectiveness $E_l\big|_k$ in this research is:

$$E_l\Big|_k = \frac{I_i^{pre} - I_k^{post}}{I_i^{pre}}$$

Equation 1. Deterrence effectiveness

Taquechel and Lewis originally presented this concept in the context of deterring attacks on individual infrastructures, without explicitly accounting for network effects. Thus, we now extend deterrence quantification to the problem of reducing WMD transfer risk, a network analysis problem. The Maritime Commerce Security Plan advocates deterring attacks by inspecting cargo early in the supply chain, before it arrives in U.S. ports.[25] This plan also claims inspecting cargo in a U.S. port is too late to deter an attack on that port; however, if the WMD target is an inland port, as it is in our approach, then investing in detection capabilities in U.S. ports could have deterrence value. We thus want to measure that value to use in quantitative WMD transfer risk analysis. Furthermore, RAND emphasizes the importance of deterrence in implementing technology for security improvements, as it would contribute to threat and vulnerability reduction, but they do not further address deterrence in their report.[26]

Given this context, there are various ongoing deterrence analysis initiatives in DHS, including a CREATE effort[27] and a DHS Science and Technology directorate (S&T) review of multiple methodological approaches to model intelligent adversaries and deterrence.[28] Also, DNDO's RNTRA efforts emphasize deterrence of WMD attacks.[29] These efforts are well-intentioned and useful, but it is not clear whether they explicitly measure deterrence or explicitly examine the effects of deterrence upon WMD transfer risk.

In an analysis of the ASP program, the Congressional Research Service (CRS) recommended that DNDO consider game-theoretical analyses to determine whether the ASP technology might offer any deterrence effects.[30] Our proposed model will quantify the WMD transfer risk reduction effects of detection technology, which could be existing technology such as the RPMs. But, our model will also quantify the prospective deterrence effects of emerging technology implementation, such as new solutions that might emerge as follow-on to the ASP initiative. We will use a modified game theoretical approach, from Taquechel and Lewis, to quantify these prospective deterrence effects in our model.[31]

Putting It All Together: Our Proposed Methodological Approach

In sum, we will enhance Lewis' MBRA model, specifically a logic tree model extension thereof, to model a supply chain as a network of nodes and links between the nodes, and we will include foreign ports, U.S. ports, and U.S. inland cities as nodes. The links will represent attacker transfer pathway options. We will also include a technique to incorporate WMD detection technology effectiveness estimates into our extension's WMD transfer risk calculations. These estimates will reflect effectiveness of equipment that detects WMD hidden within shipping containers while in port, resulting in estimated exploitation susceptibility of each network node. Exploitation susceptibility will be modeled as an explicit function of the detection equipment investments at each node. We will calculate optimal investments in emerging detection technology at U.S. ports to minimize network risk, and we will quantify the deterrence effects of those optimal investments. Finally, our model will show how deterrence investments mitigate WMD transfer risk, and will show return on investment.

This will create a holistic approach to assessing and reducing WMD transfer risk. Each of the previously discussed modeling efforts and technologies provides a critical piece of the puzzle, but we believe our approach integrates concepts from these efforts into a comprehensive systems analysis approach. Our approach may be valuable for those who need to analyze supply chain susceptibility to WMD smuggling, those who are developing solutions, and those who decide where/how to implement solutions: the U.S. intelligence community, the U.S. Coast Guard, Customs and Border Protection, DNDO, and other entities with maritime security and WMD detection responsibilities. Our approach may also be useful for agencies who evaluate the effectiveness of emerging technologies, such as DNDO. Furthermore, our approach may be useful for agency officials who report performance measures to oversight bodies.

We include the deterrence quantification effects in our WMD transfer risk analysis methodology based on the belief that incorporating deterrence effectiveness into risk calculations more accurately represents risk. The Coast Guard currently reports the general transfer risk reduction effectiveness of Coast Guard activities as measured in its Combating Maritime Terrorism Strategic Risk Model,[32] but our approach could provide additional methodological rigor.

Our Proposed Methodology: Summary of Steps

We will leverage the following methodological steps in our extension of Lewis' MBRA model:

1. We re-introduce a general transfer network model from Taquechel [2010].[33] This model will be that of a supply chain with three "layers" of nodes: foreign ports (FP), domestic U.S. ports of entry (DP), and U.S. inland cities (T, the targets of WMD attack), thus it models a "WMD transfer network." We then explain possible transfer pathways to the target nodes that an attacker could exploit by smuggling a WMD within a container. A pathway reflects the attacker's choice of exploiting specific ports in each supply chain layer. Each pathway poses a specific WMD transfer risk to U.S. inland cities.

2. We explain probabilistic risk characteristics of each port node in our model. These probabilities reflect, for example, the notional detection effectiveness of WMD detection technology in each domestic port of entry.

3. We aggregate the node risk characteristics from step 2 to develop conditional transfer risk equations for different notional network configurations. See Figure 1 which shows an OR-OR configuration. These configurations reflect the different possible permutations of logic gates in our example, showing the relationships between nodes, but presented as a framework for attacker transfer pathway options. Even though the configurations do not specify individual pathways, their equations are necessary because later we will optimize deterrence investment with respect to the configurations, not with respect to individual pathways. This will be a way of "hedging" against possible pathway exploitation.[34] In network science terms the relationships between nodes are known as "topology".[35]

4. We turn those conditional transfer risk equations into attacker expected utility function equations for our transfer pathways from step 1. A utility function represents the value to the attacker, which we equate to the risk, or expected loss, to the defender (the United States) if the supply chain is exploited and a WMD is detonated in an inland U.S. city. These functions may change if we have invested to deter; hence we create both pre-deterrence expected utility functions, and post-deterrence expected utility functions. We use these utility functions in our deterrence quantification approach.

5. We simulate a notional "pre-deterrence game" that leverages the attacker pre-deterrence expected utility functions from step 4. We show how the values of these utility functions can be used to estimate attacker pre-deterrence intent to attack, and how that intent influences **conditional** defender risk to produce defender's pre-deterrence **unconditional** WMD transfer risk.

6. We simulate a notional deterrence game that leverages the attacker post-deterrence expected utility functions from step 4. We simulate deterrence investments based on different optimal allocations of WMD detection technology. We calculate these optimal allocations using MBRA, for each possible network configuration that the attacker could exploit from step 3.

7. We leverage the results of the step 6 deterrence game simulations to compare the attacker expected utility function values after hypothetical deterrence investments. We do this in order to determine post-deterrence intent, and we compare it to pre-deterrence intent to quantify the transfer deterrence effects of such investments with respect to the different attacker transfer pathways.

8. We show how post-deterrence intent is used to calculate the defender's post-deterrence unconditional WMD transfer risk. Importantly, we average risk across multiple attacker options, or an "exploratory approach", rather than focusing on traditional game theoretical results which identify an optimal or equilibrium solution, a "predictive" approach.

9. We determine ROI of these deterrence investments.

10. Finally, we summarize this data into deterrence "portfolios" to support decision making. This methodology is expanded and applied in a notional case study to yield notional results, all available from the authors.

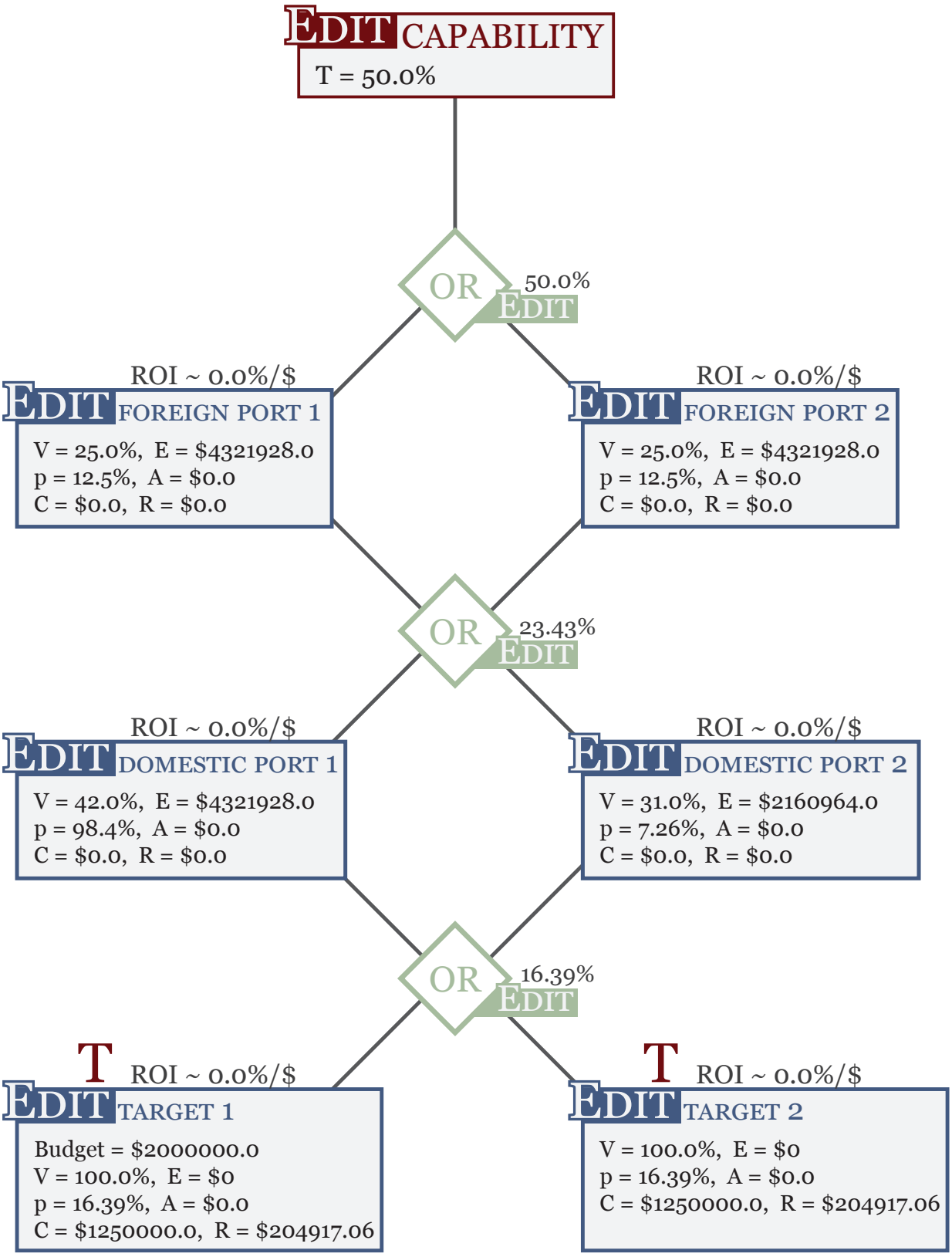

Figure 1. Notional WMD transfer network from MBRA

Summary of Practical Implications – From Case Study

This proposed methodology may offer opportunities for the spectrum of WMD risk management stakeholders: those who assess the problem, those who propose solutions to the problem, and those who make decisions on how those solutions will be implemented.

First, there are opportunities for the intelligence community. In our case study, we analyze the results of a deterrence game simulation and conclude that the possible network configurations we must analyze can be reduced by specificity of intelligence. For example, if we have no intelligence on attacker preferences for foreign port exploitation but intelligence can specify which domestic port (from among several in the simulation) an attacker is most likely to exploit based on existing detection investments and other information, then we may not want to optimize detection funding amongst domestic ports. Instead, we may want to put all available funding at the more likely domestic port and then evaluate foreign port exploitation susceptibility (e.g. whether the attacker would be more likely to exploit multiple foreign ports, or only one of several candidates). However, if intelligence is not that specific, but believes attacker will only exploit 1 of several candidate domestic ports, then we must analyze 2 configurations: OR-OR and AND-OR. And, if intelligence believes an attacker will exploit multiple domestic ports, then we must analyze AND-AND and OR-AND. Furthermore, if intelligence cannot specify whether an attacker will exploit multiple domestic ports or only one from among several candidates, then we should analyze all four configurations. The advantage of our exploratory approach with respect to attacker pathway options allows us to compare results from several possibilities, as an alternative to specific intelligence.

In our case study, if the intelligence community did have confidence that an attacker would want to exploit both **domestic** ports of entry, we found that the modeling results for optimal deterrence investment are indifferent to whether the attacker exploits a single foreign port, or multiple. With the caveat that this finding was the result of only one example, such information could help tailor intelligence collection efforts appropriately, helping the intelligence community prioritize RFIs (requests for information.)

This segues into opportunities for a second stakeholder community: international and U.S. port security analysts. In our case study, results showed that the best attacker expected utility resulted from maximum flexibility, e.g. the ability to exploit a single foreign port. This finding seems to reinforce the importance of efforts which focus on making foreign ports more unattractive to exploitation, such as the implementation of the International Ship and Port Facility Security Code (ISPS).[36] These efforts may require an attacker to exploit multiple foreign ports to have a chance of moving WMD parts through, since ISPS initiatives help lower individual foreign ports' exploitation susceptibility. Thus, attacker expected utility would be lowered, deterring exploitation. Since we are taking a network approach, overseas assessment efforts may benefit from coordination with domestic assessment efforts.

Third, there are opportunities for technology engineers who develop/test WMD detection equipment, equipment operators, and management/budget personnel who fund operation. These stakeholders are where the rubber meets the road. After the intelligence community makes their assessment and the security analysts analyze vulnerability and risk, these stakeholders develop and implement solutions. Results of our case study deterrence analysis and subsequent risk reduction reflect optimal investments, but costs of implementing/operating detection equipment that would improve detection capability and thus deter WMD transfer may exceed those optimal costs. Thus, developers may need to find ways to increase equipment operational/maintenance cost efficiencies or alternatively, suboptimal deterrence & risk reduction may be preferred if equipment cannot be implemented for less cost. This could be an iterative process of design, testing, running MBRA simulations, and refinement. With a limited budget for detection equipment, the MBRA tool can show

where to optimally invest for best possible risk reduction. But, a workaround to maximize risk reduction in the absence of more efficient equipment is to increase the available operating budget, or from a modeling perspective, to relax the constraint on the MBRA optimization simulation.

Fourth, there are opportunities for decision makers: those who consider all of the above and decide how much to invest in detection equipment and where to put it, such as port authorities and terminal owners/operators. In our case study, we analyzed deterrence game simulation results and produced post-deterrence unconditional transfer risk scores as part of the deterrence portfolios. We then showed that this transfer risk was less when the defender invested optimally hedging for AND-OR network exploitation, or assuming minimal attacker flexibility for foreign port exploitation, than when the defender invested hedging for OR-OR exploitation. This supported the importance of overseas security improvement, but from a theoretical perspective it is worth mentioning that this result is different from what classical game theoretic or optimization approaches would suggest: to invest to defend against the attacker's best option, which would be exploiting OR-OR network configurations.

From the perspective of data informing strategy, if we continue to implement overseas security measures and "drive" the attacker toward needing to exploit multiple ports, the mathematically optimal attacker solution based on traditional modeling might no longer be the outcome for which we plan. The attacker would desire maximum flexibility (OR-OR) but that could be very difficult to attain it if individual overseas ports were highly secure. That goal of improved security and less attacker flexibility in how they exploit foreign ports would be driven by data derived from an alternative to traditional attacker-defender modeling: our proposed approach. Importantly, improving security at **domestic** ports of entry might require decision makers to make tradeoffs on costs of implementing detection technology vs. desired risk reduction, as the best engineers may not be able to design equipment that meets desired exploitation susceptibility levels within budget constraints.

There are notable findings from the quantification of deterrence as well. One finding worth mentioning, as also discussed in Taquechel and Lewis (2012), is that deterrence quantification in and of itself is an interesting metric, and when used in isolation, may have practical implications for tactical responders. But, the overall goal of our methodology is to treat changes in intent (quantification of deterrence) as means to an end: informing unconditional risk values.

Directions for Future Work

Our approach applies concepts from Taquechel (2010) and Taquechel and Lewis (2012); thus many of the same directions for future work explained in that research apply here. We discuss these and additional possibilities below, in the context of individual steps to our proposed approach.

Step 1:

We have presented a limited notional transfer network to illustrate our proposed MBRA extension and notional results. The model may need to analyze a large transfer network, based on decision-maker needs. Fortunately, our logic tree model's iterative algorithm can approximate optimal WMD detection capability investment for many nodes. The number of possible WMD transfer pathways may expand nonlinearly as additional layers of supply chain nodes which an attacker must exploit are added to the model. Such layers could include an "offshore layer" of interdiction capabilities, augmenting existing shore-based capabilities such as container facility detection equipment.

Step 2:

Initial node exploitation susceptibility and existing investment data input must be imported into the logic tree model. Thus, the usefulness of our proposed model's recommendations depends in part upon the availability and reliability of this imported input. Port operators, risk analysts, and technology engineers would need to collect this data for real supply chain networks and WMD detection equipment.

Additionally, different node risk data should be used to determine results sensitivity; we only used one set of node data in our example.

Furthermore, future work could model encounter probabilities more explicitly. DNDO claims that 99% of all containers are screened for WMD.[37] While in theory this is desirable, it may reflect an unconditional probability of encounter that does not take overseas or offshore screening efforts into consideration. The extent to which resources are being expended to maintain this high encounter probability and the resulting impacts on container traffic flow through ports might be examined. One possibility is to more explicitly focus on the probability a WMD could be smuggled within a container so as to reduce resources and time required to screen containers at U.S. ports of entry. This is especially salient as ports increase their shipping container throughput. For example, the Port of Savannah plans to increase TEU (twenty-foot equivalent unit standard measure for container capacity) throughput from 2.62 million to 6 million by 2018.[38] This presents opportunities for the intelligence community and international port security assessment community, in terms of focusing collection efforts on exploitation susceptibilities of various container vessels and overseas container terminals.

Future work may also expand the modeled number of container facilities through which an attacker could conceivably transfer a container with a hidden WMD. The model's equations would be modified. This could be done for both domestic U.S. ports of entry and foreign ports. Also, future work may expand our model to more explicitly show WMD encounter and detect probabilities in foreign ports. The challenge may be getting appropriate quantifiable data on foreign port exploitation susceptibility. Evaluating optimal investment in foreign ports to deter and reduce WMD transfer risk, or evaluating a combination of optimal investments in both foreign and domestic U.S. ports of entry, may provide quantitative support for the Maritime Commerce Security Plan's guidance to "interdict the threat as far as possible from the U.S. borders."[39]

Step 3:

We used conditional WMD transfer risk equations that reflected conditional risk of both U.S. inland targets, instead of specifying the attacker would prefer one over the other. This was a simplification for expository purposes, because the focus of this initial research was on optimizing deterrence investment in WMD technology at U.S. ports of entry. However, future work may create expected utility functions (derived from the conditional risk equations) for the deterrence game, which only reflect the consequences to **one** of the multiple U.S. inland targets. The transfer pathways would be expanded to include a specific U.S. inland target. This may change the notional results.

Step 4:

We have made certain assumptions about availability of port risk information to would-be attackers, and have made assumptions about the utility theories underpinning our expected utility functions. Essentially, we have assumed perfect attacker information meaning all information is available to prospective attackers, and have assumed subjective expected utility theory meaning attackers make decisions linearly. See Taquechel and Lewis for more discussion on these theories and how utility functions could be modified in future WMD deterrence modeling to accommodate alternate theories.[40]

Step 5:

Depending on changes to conditional risk equations (e.g. discriminating between different U.S. inland city detonation consequences instead of aggregating them for all transfer pathways) and/or changes to expected utility functions, as proposed above in future research for steps 3 and 4, the information in the pre-deterrence game may change. With respect to perfect vs. imperfect information, an analyst could model the pre-deterrence game assuming either perfect information, or imperfect information, and then could examine how the deterrence effectiveness of additional WMD

technology investments changed based on pre-deterrence game information availability.

Steps 6-8:

Because we did not use a traditional game theoretical approach to our deterrence "games" in our methodology, we did not leverage defender expected utility functions. Future work might leverage more traditional game theoretical approaches to quantify deterrence. Also, we assumed a deterrence game of five defender courses of action (COAs) and six attacker COAs; future work might examine how deterrence can be quantified in a game with different numbers of attacker post-deterrence and defender deterrence options.

Furthermore, future work may simultaneously optimize investments at both foreign ports and domestic ports of entry, again emphasizing the potential role that those who help implement and evaluate ISPS could play, in addition to those who evaluate U.S. port security.

Beyond WMD and Port Exploitation:

Future research might apply this approach to problems beyond WMD transfer risk and U.S. port exploitation susceptibility analysis. For example, the transfer pathway logic could be applied to model adversarial decision making options in any sort of network, i.e. how an attacker might choose from among options to move any sort of illicit people/goods through a collection of nodes. These junctures could be just ports, a combination of ports and inland cities as described here, or solely inland targets, as a modeler or decision maker requires. It is possible an entire network could be modeled across the entire United States or internationally through land borders, modeling adversarial transfer pathway options in a much broader network than we have offered here.

It may be possible that transfer pathway logic (AND and OR gates) used here could be combined with traditional network science metrics (degree, closeness, etc.)[41] to create a more comprehensive network exploitation analysis. The AND-OR gate approach comes from fault tree analysis, used in reliability engineering. For example, suppose this analysis was expanded to include the physical links between U.S. ports and inland cities.[42] This could influence the utility and risk calculations. We propose three notional options to examine this.

One option is that absent specific intelligence, node degree might reflect a greater propensity for an attacker to choose AND vs OR, for the transfer pathway. An attacker may prefer to exploit both U.S. ports (AND) if the port "degrees" were sufficiently low (e.g. if there were only one railway leading out of each port toward the ultimate target), but might prefer to exploit only 1 (OR) if that port's degree were sufficiently high (e.g. if there were multiple railways leading from that U.S. port to exploit).

Another option is that the links might have value in and of themselves (e.g. what is the likelihood various railroad companies could be exploited after a WMD has cleared initial U.S. port of entry?), which would increase the complexity of the model's algorithm. A third option is that the links might be assumed to be of no intrinsic value, but their presence would increase each U.S. port's exploitation susceptibility proportional to degree. Lewis' MBRA tool offers ways to use both network analysis and fault tree analysis in tandem to thoroughly scrutinize a network.[43]

Also, the modeling of failure susceptibilities as a function of investment could have broad applicability beyond maritime transfer of WMD; it might be applied to other system reliability analyses where budget is a concern. Models that simulate the allocation of resources to reduce some probability of an undesirable event (or increase the probability of a desirable event) could use our methodology. Furthermore, the deterrence quantification techniques used here are general enough to be applied to various adversarial or game theoretical analyses where deterrence quantification is desirable – be they analyses of crime, terrorism, WMD terrorism, counternarcotics, immigration interdiction, etc. The basic deterrence quantification technique was influenced by literature on deterring intentional acts other than terrorism.[44]

These techniques broaden risk analysis discourse by focusing on how phenomena from "earlier in the attack chain" may influence the actual attack options. By modeling deterrence, we show how changes in attacker intent, formed during the attacker's early attack planning stages, may influence the attacker's decision making. This approach also offers an alternative to traditional defender-attacker-defender or game-theoretical modeling in WMD risk analysis, by exploring possible outcomes rather than focusing on an "optimal" outcome.

SUMMARY AND CONCLUSION

We can only hypothesize how the attacker might exploit different pathways to transfer a WMD to an inland U.S. city and detonate it. Some models make predictions, but we prefer the exploratory approach. An attacker's expected utilities from transferring a WMD within a shipping container through different supply chain pathways, and ultimately detonating in an inland U.S. city, can be calculated both before and after hypothetical transfer deterrence investments. Those expected utilities determine both pre and post-deterrence intent values for each COA, and those intent values help us quantify transfer deterrence effectiveness of the transfer deterrence investments.

We then apply those post-deterrence intent values to determine average defender post-deterrence unconditional risk. Then, we compare that average post-deterrence unconditional risk to the average pre-deterrence unconditional risk and optimal investment at each domestic port of entry, to calculate ROI of that optimal investment. Finally, we aggregate transfer deterrence effectiveness values, unconditional defender risk, and ROI of the transfer deterrence investments into concise portfolios to support decision-making.

The value of this approach is that we can calculate our risk, or expected loss from exploitation of the maritime supply chain and WMD detonation, while accounting for not only (1) the exploitation susceptibility reduction effects of hypothetical optimal investments to increase WMD detection probability, but also accounting for (2) the transfer deterrence effects those investments may have on a would-be attacker's decision-making. We account for these phenomena in context of the possible changes in network topology, or different attacker transfer pathways and network configurations. We also incorporate data representing foreign port exploitation susceptibility, as the role of foreign ports in WMD transfer risk analysis is valuable. We are measuring how we change the attractiveness of WMD transfer pathway exploitation, supporting business cases for existing and emerging WMD detection technology, and increasing the rigor of WMD transfer risk analysis and mitigation by integrating ideas from existing efforts with our own concepts into a holistic framework.

We may benefit from studying the effectiveness of emerging WMD detection technology in the context of supply chain exploitation risk to justify implementation of that technology, and from studying the costs required to develop, implement, operate and maintain that technology. Also, the deterrence effectiveness and resulting unconditional WMD transfer risk of existing solutions such as the Megaports Initiative, CBP radiation portal monitors, and other detection initiatives might be analyzed. The combined effects of both existing and new technology in a port could be modeled, as could the effects of replacing existing technology with new technology altogether.

We have given examples of deterrence effectiveness analysis and resulting risk, with other policy implications, in our case study. With such deterrence effectiveness and risk reduction metrics, the Global Nuclear Detection Architecture's layered defense approach to enhancing supply chain security against WMD transfer could be enhanced. The RNTRA methodology may benefit from concepts discussed in our approach. Also, policymakers could have rigorous justification for their investment decisions as well as additional metrics to report. Ultimately, our proposed approach could contribute to the improvement of the GNDA, and help to increase security of the maritime supply chain.

About the Authors

Eric F. Taquechel *is a U.S. Coast Guard officer with experience in shipboard operations, port operations, critical infrastructure risk analysis, contingency planning/force readiness, and operations analysis. He has authored various publications including Layered Defense: Modeling Terrorist Transfer Threat Networks and Optimizing Network Risk Reduction, in IEEE Network Magazine; How to Quantify Deterrence and Reduce Critical Infrastructure Risk, in Homeland Security Affairs Journal; and mostly recently Options and Challenges of a Resilience-Based, Network-Focused Port Security Grant Program, in the Journal of Homeland Security and Emergency Management. LCDR Taquechel earned a Master's degree in Security Studies from the Naval Postgraduate School and prior to that earned his undergraduate degree at the U.S. Coast Guard Academy. LCDR Taquechel may be contacted at nixhex3092@yahoo.com.*

Ian J. Hollan *is a chemical program analyst for the Department of Homeland Security's Infrastructure Protection Division, responsible for coordination and implementation of protection and resilience policies utilized by industry. He is also a Marine Science Technician First Class in the United States Coast Guard. He has many years of experience at various USCG small boat stations and marine safety units with extensive training in maritime law enforcement, container inspections, radiological/hazardous response, and vessel boardings. He also has extensive experience in container security, having led efforts to improve security at container facilities in Los Angeles, San Francisco, Savannah, Charleston, Baltimore, and New York City. MST1 Hollan earned a B.S. from the University of Mount Union, an M.A. from Cleveland State University, and is currently enrolled in the Executive Masters of International Service Program at American University. He has been awarded two Coast Guard Commendation Medals, and may be contacted at ian.hollan11@gmail.com.*

Ted G. Lewis *is a retired professor of computer science and former executive director of the Center for Homeland Defense and Security at the Naval Postgraduate School. He spent forty years in academic, industrial, and advisory capacities, ranging from academic appointments at the University of Missouri-Rolla, University of Louisiana, and Oregon State University, to senior vice president of Eastman Kodak Company, to CEO and president of DaimlerChrysler Research and Technology, North America. Dr. Lewis has published over thirty books and 100 research papers. He is the author of Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation (2006, second edition 2014), Network Science: Theory and Applications (2009), Bak's Sand Pile (2011), and Book of Extremes (2014). He received his PhD in computer science from Washington State University. Dr. Lewis may be contacted at tedglewis@redshift.com.*

Acknowledgements

The authors wish to thank the anonymous referees whose feedback greatly improved the paper.

Disclaimer

The original opinions and recommendations in this work are those of the authors and are not intended to reflect the positions or policies of any government agency.

Notes

1. The White House, National Strategy for Global Supply Chain Security, 2005, http://www.whitehouse.gov/sites/default/files/national_strategy_for_global_supply_chain_security.pdf.

2. The White House, Maritime Commerce Security Plan for the National Strategy for Maritime Security, 2005, http://www.dhs.gov/xlibrary/assets/HSPD_MCSPlan.pdf.

3. The White House, National Strategy to Combat Transnational Organized Crime, 2005, http://www.whitehouse.gov/sites/default/files/Strategy_to_Combat_Transnational_Organized_Crime_July_2011.pdf.

4. Hugh Griffiths and Michael Jenks, Maritime Transport and Destabilizing Commodity Flows, Stockholm International Peace Research Institute Policy Paper 32, 2011, http://books.sipri.org/files/PP/SIPRIPP32.pdf.

5. The White House, 2005, op. cit.

6. Dana Shea, The Global Nuclear Detection Architecture: Issues for Congress, Congressional Research Service report, 2009, http://www.fas.org/sgp/crs/nuke/RL34574.pdf.

7. See http://nnsa.energy.gov/aboutus/ourprograms/nonproliferation/programoffices/internationalmaterialprotectionandcooperation/-5.

8. See http://www.cbp.gov/border-security/port-entry/cargo-security/cargo-exam/rad-portal1.

9. See http://www.uscg.mil/mlea/courses/radhaz.asp.

10. Ibid.

11. National Academies of Science, *Evaluating Testing, Costs, and Benefits of Advanced Spectroscopic Portals,* (Washington, D.C., The National Academies Press, 2011). http://www.nap.edu/catalog.php?record_id=13082.
One issue cited was that modeling and simulation was not used to test the ASP performance. Our proposed approach is a modeling and simulation approach, which could help test emerging technology performance.

12. Eric Taquechel and Ted G. Lewis, "How to Quantify Deterrence and Reduce Critical Infrastructure Risk," *Homeland Security Affairs* 8, Article 12, (August 2012), http://www.hsaj.org/?article=8.1.12.

13. Unconditional risk means that the attacker's intent is less than 100%, meaning the attacker has not yet made a decision to execute a WMD transfer operation and is considering the relative attractiveness of exploiting different pathways. Unconditional risk is conditional risk multiplied by an intent probability. In contrast, conditional risk means risk given the attacker has 100% intent to exploit a pathway and has already commenced planning to execute the transfer (although their technical capability to actually do so is also expressed probabilistically).

14. Eric Taquechel, "Options and Challenges of a Resilience-Based, Network Focused Port Security Grant Program," *Journal of Homeland Security and Emergency Management* 10, no. 2 (Sept 2013).

15. M.E. Cutter, "Improving the Coast Guard Ports, Waterways and Coastal Security Outcome Measure," Master's Thesis, Naval Postgraduate School, 2009, www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA527037.

16. Government Accountability Office, "Security Risk Model Meets DHS Criteria, but More Training Could Enhance Its Use for Managing Programs and Operations," November 2011, http://www.gao.gov/products/GAO-12-14.

17. Ted Lewis, *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation* (Hoboken, N.J: Wiley Interscience, 2006). Also see Ted Lewis, *Network Science: Theory and Application* (Hoboken, N.J: Wiley Interscience, 2009).

18. Found at www.usc.edu/dept/create/assets/001/50816.pdf.

19. See http://www2.gwu.edu/~nsarchiv/nukevault/ebb388/docs/EBB029b.pdf.

20. Hugh Griffiths and Michael Jenks, 2012, op. cit.

21. Eric Taquechel, "Layered Defense: Modeling Terrorist Transfer Threat Networks and Optimizing Network Risk Reduction," *IEEE Network Magazine,* 24(6), 2010, 30-35.

22. P. Cronin and A. Cronin, *Challenging Deterrence: Strategic Stability in the Twenty-First Century*, Changing Character of War Series, (Oxford: Oxford University Press, 2007) http://ccw.modhist.ox.ac.uk/events/archives/mt06_deterrence/deterrence_report_mt2006.pdf.

23. National Academies of Science, 2011, op. cit.

24. Taquechel and Lewis, 2012, op. cit.

25. The White House, 2005, op. cit.

26. Henry Willis and David Ortiz, "Evaluating the Security of the Global Containerized Supply Chain." RAND technical report, 2004, found at http://www.rand.org/content/dam/rand/pubs/technical_reports/2004/RAND_TR214.pdf. We claim something slightly different: that vulnerability reduction (which we call exploitation susceptibility) contributes to deterrence, which changes attacker intent and thus changes threat and risk.

27. See http://teamcore.usc.edu/projects/coastguard/.

28. See http://birenheide.com/sra/2011AM/program/singlesession.php3?sessid=M4-H.

29. See http://www2.gwu.edu/~nsarchiv/nukevault/ebb388/docs/EBB029b.pdf.

30. Dana Shea, John Moteff, and Daniel Morgan, "The Advanced Spectroscopic Portal Program: Background and Issues for Congress," Congressional Research Service, 2010, found at http://www.fas.org/sgp/crs/homesec/RL34750.pdf.

31. Eric Taquechel and Ted Lewis, 2012, op. cit.

32. M.E Cutter, 2009, op. cit.

33. Eric Taquechel, 2010, op. cit.

34. The more technical reason for this is that some of the attacker transfer pathways involve exploitation of only one domestic port of entry; since we are trying to optimize investments at domestic ports of entry only, it does not make sense to optimize for a pathway where only one domestic port of entry will be exploited. Obviously all the money would go to that one port in that case, and then there is no need for an optimization simulation. Thus we optimize with respect to configurations, not pathways.

35. Topology in network science generally refers to the links between nodes, or the donor-recipient relationships in the network, with respect to the network's functionality. For example, a critical donor node such (e.g. a waterside refinery) will have outgoing links (pipelines, rail, truck) to many recipient nodes (e.g. inland petroleum storage terminals), so the functionality of the petrochemical network depends highly upon the refinery's organic exploitation susceptibility and the susceptibility of its links. The topology of many links and customers potentially make the refinery a critical node. A less critical node will have a different topology: it will have fewer outgoing links and customers. Or, if it still has the original topology of many links, they and the refinery itself will have very low organic exploitation susceptibility to make the refinery less critical. In our present research, topology is slightly different: it refers to the logic gate between each layer of nodes, reflecting attacker pathway options for a WMD transfer risk model, rather than actual supply chain component functional relationships, and the logic gates are thus proxies for links between nodes. This topology influences the nature of "cascading failure" which is the mathematical accumulation of probabilities that a weapon will be smuggled through each layer of the network.

36. See http://www.imo.org/ourwork/security/instruments/pages/ispscode.aspx for information about ISPS.

37. Written testimony of Domestic Nuclear Detection Office Acting Director Dr. Huban Gowadia for a House Committee on Homeland Security, Subcommittee on Infrastructure Protection, and Security Technologies hearing entitled "Preventing Nuclear Terrorism: Does DHS Have an Effective and Efficient Nuclear Detection Strategy". http://homeland.house.gov/sites/homeland.house.gov/files/Testimony-Gowadia.pdf. The following excerpt from this testimony could suggest that DNDO recognizes the importance of evaluating alternatives to near-100% screening at U.S. ports: "Our ongoing work with U.S. Customs and Border Protection (CBP) to facilitate container security has resulted in the scanning of over 99 percent of all incoming containerized cargo for radiological and nuclear threats entering via truck at our land borders and at our seaports, utilizing RPMs…Scanning of containerized cargo at seaports of entry will continue, in accordance with SAFE Port Act requirements. However, given the current fiscal environment, DNDO and CBP, working together, will continue to work to balance risk reduction, effectiveness of radiological and nuclear scanning, flow and volume of commerce, and life cycle costs when determining RPM deployment priorities."

38. See http://www.gaports.com/Facilities/GardenCityTerminal/FutureExpansion.aspx.
39. The White House, 2005, op. cit.
40. Taquechel and Lewis, 2012, op. cit.
41. Lewis, 2009, op. cit.
42. Again, the logic gates are proxies for links between nodes in our approach.
43. Available at https://www.chds.us/?media/resources&collection=53&type=SIMULATION.
44. Taquechel and Lewis, 2012, op. cit.