Risk Reduction and Deterrence: Two Sides of the Same Coin?

By Eric Taquechel

Abstract

Government documents and academic articles focus on risk reduction and deterrence, sometimes simultaneously. With limited resources, how should CIKR stakeholders invest? If the objective is to deter, that may have certain implications for investment. If the objective is to reduce risk, that may have different implications. However, what if the objective is to account for both? What are the investment implications in that case? If CIKR stakeholders understand how deterrence metrics influence risk-reduction efforts, they may view investment in CIKR protection and resilience differently. In addition, this may have implications for risk- reduction metrics reporting, a government concern. This work therefore explores the relationship between quantitative deterrence and quantitative CIKR risk reduction under a variety of assumptions and with notional scenarios and data.

Suggested Citation

Taquechel, Eric. "Risk Reduction and Deterrence: Two Sides of the Same Coin."
Homeland Security Affairs 17, Article 3 (April 2021) www.hsaj.org/articles16993.

Introduction

Government strategies advocate reducing risk to critical infrastructure and key resources (CIKR). Academia provides various theories and methodologies to do so. Furthermore, governments and academics have advocated deterrence theories and strategies both prior to and post-9/11, with the post-9/11 advocacy emphasizing CIKR protection in addition to classical deterrence theory. Therefore, with respect to CIKR, there are two areas of study: reducing CIKR risk, and deterring attacks, each of which can trace their theoretical roots back to different sources. Often, these studies address networks of CIKR, beyond just individual infrastructures.

As we will show, lots of government documents and academic articles focus on risk reduction and deterrence, sometimes simultaneously. With limited resources, CIKR stakeholders naturally want decision frameworks to support investments. If the objective is to deter, that may have certain implications for investment, a natural practitioner concern. If the objective is to reduce risk, that may have different implications.

However, the objective might be to account for both deterrence and risk reduction. If CIKR stakeholders understand how deterrence metrics influence risk-reduction efforts, they may view investments differently. In addition, this may have significant implications for risk-reduction metrics reporting.

Taquechel and Saitgalina (2018)[1] advocate that those responsible for exploring risk-reduction metrics in antiterrorism programs should assess:

> "whether metrics can accommodate quantifiable deterrence/adaptive adversary considerations, network exploitation susceptibility, and/or network effects on consequence and resilience."[2]

Research Goals

Given the above problem statement, we want to explore whether we can, given limited resources:

1. Reduce risk to CIKR in an optimal fashion while also maximizing deterrence
2. Optimally increase network resilience while maximizing deterrence

Alternatively, there may necessarily be trade-offs between risk minimization/resilience maximization and deterrence. In other words, these two goals may be complementary or mutually exclusive, depending on the scenarios, modeling assumptions, and data. Findings from exploring these issues may have implications for risk analysts, CIKR protection stakeholders, budget developers, and policymakers.

Before we explore these issues, we provide context from government and academia on these topics. To be clear, the objective of this research is NOT to claim whether deterrence is or is not an important consideration for anti-terrorism policies, programs, or activities. It is difficult to take seriously the proposition that deterring attacks is not important and that we should ignore hypothetical effects of our actions on adversary decision making.

Instead, this research will leverage various frameworks and simulations with notional quantitative information to elucidate the relationships between deterrence and probabilistic risk under various assumptions.

Article Organization

The overall organization of this article is as follows. We:

1. review relevant literature from government and academic sources,
2. introduce the six analysis frameworks we will use to elucidate the relationships between risk reduction and deterrence,
3. lay out each framework in detail by explaining the framework's overall concept, objective the framework will solve, and results of applying the framework to solve the objective using notional data,
4. summarize findings from the six frameworks in context of the original research goals and modified goals,
5. offer recommendations for future research, and
6. offer practical implication of this research, and offer concluding remarks.

Literature Review

The literature review will cover two broad categories:

1. Government documents and initiatives, including risk terminology, government strategies, resource management considerations, and ongoing WMD detection/resilience efforts, and
2. Academic efforts, including risk-reduction modeling, deterrence theory and application to critical infrastructure protection and WMD risk management, and supply chain resilience modeling.

Risk Terminology, Government Strategies, Resource Management: Department of Homeland Security Risk Lexicon[3]

- A *deterrent* is "a measure that discourages, complicates, or delays an adversary's action or occurrence." Change, delay, or outright abandonment of an attack are all options. Threat shifting, or changes in the location or tactics of an attack (vice attack abandonment altogether) is noted.

- *Return on investment* is a "calculation of the value of risk-reduction measures in the context of the cost of development and implementation of those measures." Notably, this definition does not claim risk reduction does/does not (or should/should not) include deterrence consideration.

- *Game theory* is a branch of mathematics that can be used to model behavior in response to potential security measures.

- *Networks* are groups of components that interact with each other to perform a function. The DHS Risk lexicon does not explicitly discuss deterring attacks on networks.

- *Resilience* is the ability to adapt to changing conditions and prepare for, withstand, and rapidly recover from disruption. It may be a deterrent.

Government Strategies and Plans – Risk Reduction, Deterrence, Resilience

The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets (2003)[4] makes general reference to the importance of deterring attacks on CIKR through protective and incident response capabilities. It also mentions resilience, and advocates cost-effectiveness.

Presidential Policy Directive (PPD) 21, Critical Infrastructure Security and Resilience[5], does not mention deterrence. The National Maritime Transportation Security Plan[6] mentions deterrence once. The Maritime Commerce Security Plan[7] mentions deterrence twice. The 2015 Transportation System Sector-Specific Plan[8] does not mention deterrence.

The National Infrastructure Protection Plan (2013)[9] lays out a general framework to reduce CIKR risk, identify threats, reduce vulnerabilities, and mitigate consequences. It does not explicitly discuss deterrence beyond a general statement of purpose to deter threats in order to protect CIKR. It furthermore advocates consideration of "cascading effects" and resilience.

The Cybersecurity and Infrastructure Security Agency (CISA) strategy document[10] advocates risk analysis and resilience in support of "national critical functions" but does not explicitly discuss deterrence. It advocates interdependency analysis.

The DHS Strategic Framework for Countering Terrorism and Targeted Violence[11], while presumably authored in response to domestic terrorism and targeted violence events, alludes to critical infrastructure protection and risk analysis, but only mentions "deterrence" once.

Resource Management Documents

The President's 2020 budget for DHS[12] provides for securing U.S transportation systems in an effective and efficient way, as well as for ensuring resilience post-disaster.

The DHS 2020 budget justification for countering WMD[13] mentions the importance of funding studies in deterrence theory. The CISA budget not does explicitly discuss deterrence.

Ongoing WMD Detection and Resilience Efforts

The former Domestic Nuclear Detection Office (DNDO), now the Countering Weapons of Mass Destruction Office, does not mention deterrence on its homepage.[14]

The Federal Emergency Management Agency (FEMA) FY19 Port Security Grant Program Overview, Objectives, and Priorities[15] emphasizes priority allocation of grant dollars for, among other things, "enhancing WMD and improvised explosive device prevention, detection, response, and recovery capabilities." However, it does not mention deterrence.

Furthermore, it states funding allocation decisions are based on port area risk, with some references to port facility resilience and resumption of trade protocols. However, it does not explicitly discuss efforts to fund port infrastructure to resume operations specifically to minimize the cascading downstream effects in supply chains, or maximize supply-chain (vice individual facility or port) resilience.

Synthesis – Government Documents

These government documents, while non-exhaustive, suggest that risk reduction is important, as is resilience. Deterrence seems less emphasized, especially in budget documents.
This might suggest cost efficiency is more valuable for risk reduction and resilience, than for deterrence. It might also suggest deterrence is less important than risk reduction, in general. Such possibilities beg the question of whether government agencies should continue to focus on deterrence or not.

While such matters may warrant additional philosophical discussion, we focus on technicalities here. We now provide examples of academic efforts to analyze risk, resilience, deterrence, networks, and resource constraints. Therefore, the groundwork for the technical approach in this article assumes that we want to explore deterrence effects from a technical standpoint, regardless of interpretation of government strategies.

Academia

CIKR Risk Reduction- Networks, Generally

Taquechel (2010a)[16] shows how to quantify and optimally reduce network risk when we account for layered defenses in the global supply chain.

Mathematical Optimization to Reduce CIKR Network Risk

Al-Mannai and Lewis (2007)[17] explore different allocation strategies to defend CIKR networks: linear cost models and exponential cost models. The former assumes CIKR vulnerability reduction is a linear function of money invested to defend CIKR from attack; the latter assumes it is an exponential function. Allocation strategies change depending on these assumptions. With linear, an analyst allocates funds to only a few CIKR nodes; with exponential, an analyst more equitably distributes funds amongst more CIKR nodes. This may have implications for practitioner implementation: the model may recommend a different distribution of funding based on exponential vs linear risk buy down.

Al-Mannai and Lewis (2008)[18] show how to optimize risk reduction for a network of CIKR targeted by a potential attacker, based on a "network allocation strategy", as compared to risk reduction based on a "non-network strategy".

Deterrence, Generally

There is a wealth of literature on deterrence theory outside the context of CIKR protection; see Taquechel (2010b)[19] for some examples.

Deterrence – CIKR, Generally

Bier and Kosanoglu (2015)[20] present a target-oriented utility approach for modeling the deterrence effects of counterterrorism investments. Their objective function treats probability of deterrence as probability of successful attack upon an infrastructure:

$$Z = \min\ L[1 - P_d(P_s(x))]P_s(x) + x$$

Equation 1. Objective function, Bier and Kosanoglu (2015)

Where

L = expected loss from successful attack;
$P_s(x)$ = probability of attacker success given investment x; and
$P_d(P_s(x)$ = probability of attack deterrence given probability of attacker success.

The authors then propose a functional form of $P_d(P_s(x)$ based on deterrence research from criminology literature. They propose notional values of the parameters of this functional form, and then show optimal investment levels to minimize expected loss. They also model the relationship between $P_s(x)$ and $P_d(P_s(x)$. Generally, as the former decreases, the latter increases, although the specifics depend on the functional form of the former term (exponential or Rayleigh distribution).

The authors claim that the Israeli defensive strategies have led to deterrence of attacks on higher-consequence targets, as evidence that "there should be fewer attacks on large targets" given theoretically greater defender investments as a function of target value. Notably, even though they incorporate deterrence into their equation, their objective function is still to minimize loss that incorporates deterrence metrics, not quantify deterrence itself.

Quijano and colleagues (2018)[21] describe a defender-attacker-defender model where the attacker has incomplete information about defender investments to protect a CIKR network. Quijano et al. focus on consequence of loss of life at the node attacked, vice economic consequences from "cascading failures" in a network.

They analyze a Spanish rail system, treating stations as nodes, connecting tracks as links, and introduce "hotspots" or particularly attractive areas for attacker staging.

They proxy attacker decision making as the sum of binary variables (attack or do not attack) across multiple attack modes and targets. The sum of all binary variables cannot exceed one, a constraint that means only one attack will occur.

Deterrence – CIKR - Deterrence Quantification

Taquechel and Lewis (2012)[22] show how to quantify deterrence and show how that can influence CIKR risk.

Taquechel, Hollan and Lewis (2015)[23] show how to apply deterrence quantification to reducing transfer risk, or risk incurred through the international supply chain, specifically with respect to weapon of mass destruction (WMD) transfer.

Deterrence Theory - WMD

Recent thinking on WMD deterrence specifically has suggested that "regional nuclear deterrence" concepts are not adequately integrated into military officer professional military education (Bernstein, 2015).[24] Bernstein does not explain what "regional nuclear deterrence" means, but this research generally advocates for the importance of WMD deterrence theory in education.

Supply Chain Resilience and Deterrence

Taquechel (2013)[25] shows how supply-chain network risk can be minimized (optimized) when we consider reducing consequence to a network of CIKR, vice reducing vulnerability. He simulated the allocation of funding to CIKR in ports proportional to how funding would improve resilience. Reducing consequence therefore equates to increasing network resilience.

Xu and colleagues (2015)[26] model the effects of supply chain disruption, using attacker-defender modeling techniques. They estimate equilibrium allocation strategies, including supply chain backup capacity or excess inventory in their supply chains, for a military engagement with a temporal aspect. An attacker observes the military's investment to minimize supply-chain perturbations as they conduct their engagement, and responds accordingly with their own resource allocation. In game-theoretic parlance, this is a game of both complete information (both players know the "rules" of the game) and perfect information (players can observe other players' decisions).

The "backup capacity" might be similar to Taquechel's (2013)[27] concept of "redundant suppliers", whereas "excess inventory" may be similar to Taquechel's (2013) concept of "raw product" at a supply chain supplier node. However, Xu et al. use a binary variable for the capacity backup decision, suggesting a "yes" or "no" decision on investing to ensure capacity backup. In contrast, Taquechel (2013) treats redundancy investment as a given but the resulting redundancy reflects a probabilistic relationship between the actual amount invested and theoretical maximum amount needed to guarantee redundancy up to 95%.

The equilibrium solution approach proposed by Xu et al. suggests influence of defender investments on attacker decision making, and identifies circumstances in which an attacker might be deterred from investing resources to attack. They find that under certain conditions, the attacker does not seem to be deterred by defender investment in capacity backup protection, or investment in inventory, but would continue to invest more resources to attack.

Synthesis – Academia

These academic efforts paint a picture of risk-reduction modeling and deterrence-modeling efforts. These efforts lay a foundation for exploring the relationship between risk reduction and deterrence, specifically exploring whether explicitly accounting for deterrence has any quantitative impact on risk-reduction metrics. This is a gap in the existing literature.

Analysis Plan — Frameworks

With the foregoing in mind, this research will lay out six frameworks including concepts of operation and notional results, based on simulations of limited budget to reduce risk to notional CIKR networks. These simulations will alternate the structure of the risk equation, specifically "turning on" and "turning off" deterrence considerations to see how risk results change in resource-constrained environments. Detailed equations are available from the author.
These frameworks will focus on reducing vulnerability in some networks, and reducing consequence in others, to see whether results are robust to deterrence assumptions. They will use a nonlinear allocation strategy. Finally, they will include simulations where game theory influences our concept of deterrence.
Thus, there are six different frameworks:

Table 1. Frameworks

Network			
	No Deterrence	*Deterrence (Intent Ratios)*	*Deterrence (Game Theory)*
Optimize for Vulnerability	Simulation 1	Simulation 2	Simulation 3
Optimize for Consequence	Simulation 4	Simulation 5	Simulation 6

Importantly, in this research "investing to deter" and "accounting for effects of deterrence in risk reduction" are two distinct but interrelated concepts. Each framework in this research simulates the former; the latter occurs only when frameworks account for intent ratios or game theoretic equilibrium results.

Framework 1 — Optimize for Vulnerability, No Deterrence

Concept of Operations

Taquechel, Hollan and Lewis (2015)[28] list some U.S. government efforts to reduce WMD risk. Their objective is to minimize risk to the United States Maritime Transportation System (MTS) by simulating investment in U.S. port radiation detection technology. This framework mimics their approach by simulating optimal investment to minimize transfer risk, by lowering "transfer probability", defined here as probability of attack:

> inherited from foreign ports, delivered into U.S. ports by vessels exploited to move illicit people or cargo, cargo including weapons, conventional explosives, or CBRN materials.

This is different from risk of direct attack against maritime CIKR, and is similar to Adler and Fuller's (2009) definition of transfer threat as "the movement of terrorist and/or illicit material, including WMD, into the U.S. via independent transport modes from multiple countries and shipping points."[29]

This framework therefore proxies a "transfer network", modeling the global maritime commons.

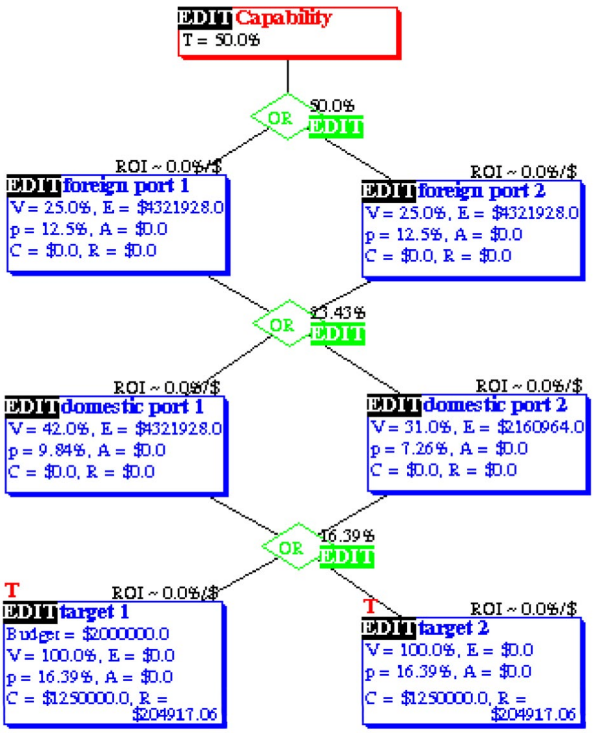

Figure 1. Notional WMD transfer network

This notional WMD transfer network has six "nodes": two foreign ports (FP), two domestic US ports (DP), and two inland targets of WMD attack. The "OR" logic gates between each layer represent one specific attacker permutation, a choice on how to move between layers of nodes.

> This framework leverages conditional WMD transfer-risk equations for a notional transfer network with two target cities. Conditional risk assumes the attacker desires a certain attack with 100% intent. The conditional risk here is the sum of consequence to both targets, multiplied by the aggregate target attack probability.
>
> These equations represent defender conditional risk, or expected loss from a WMD attack based on existing investments ("pre"), and hypothetical future deterrence investments ("post"). To specify pre-deterrence risk, the framework simulation simply sets our deterrence investment placeholders equal to zero.

Unlike pre-deterrence conditional risk, post-deterrence conditional risk is a function of:

1. existing investment to reduce network-exploitation susceptibility, but also of
2. optimized additional WMD detection investment, intended to deter.[30]

Consistent with Taquechel, Hollan and Lewis (2015)[31], this framework uses "exploitation susceptibility" or "failure susceptibility" in the present research, in lieu of "probability" in certain places. This is to emphasize the difference between probability of attack on an individual infrastructure, and probability of network node or network exploitation, a failure to contain a threat or consequence. However, for target cities, this framework uses "attack probability" which reflects upstream exploitation susceptibilities.

This framework modifies network conditional risk based on the logic-gate permutation, which represents a transfer pathway of maximum flexibility for the attacker. The permutations are OR-OR, AND-OR, OR-AND, and AND-AND.

This framework also considers an alternative rubric for assessing transfer risk: attacker individual pathways. The attacker knows their specific attack pathway, even if the defender does not. Thus, this framework models six attacker pathways, or courses of action (COA):

1. COA 1: OR-OR network, exploit either FP, exploit DP1
2. COA 2: OR-OR network, exploit either FP, exploit DP2
3. COA 3: AND-OR network, exploit both FP, exploit DP1
4. COA 4: AND-OR network, exploit both FP, exploit DP2
5. COA 5: OR-AND network, exploit either FP, exploit both DP
6. COA 6: AND-AND network, exploit both FP, exploit both DP

This framework leverages conditional risk equations reflecting these individual attacker pathway options. Importantly, it aggregates consequences over multiple targets, since regardless of exploitation pathway or permutation chosen, we do not assume a specific target will be attacked.

Objective Function/Constraints

Our objective in this framework is to minimize conditional risk in a transfer network. Using a portfolio approach, the framework represents conditional transfer risk within the context of four different pathway options:

-a specific attacker permutation;
-the sum of risk from all permutations;
-a specific attacker pathway; or
-the sum of risk from all pathways.

Specific Attacker Permutation

Our objective function for minimizing conditional risk leverages budget and probability constraints, including:

1. Total detection technology investment amongst the two network domestic port nodes cannot exceed total budget;
2. Detection technology investment at each node cannot exceed the node's postmax, or theoretical amount to minimize detection failure to 5%;
3. Domestic port detection failure susceptibilities must be between 0 and 1; and
4. Domestic port detection failure susceptibility given deterrence investment cannot exceed pre-investment failure susceptibility.

Sum across All Permutations

The framework uses the same constraints, but minimizes conditional risk across all attack permutations.

Specific Attacker Pathway

Here, the framework minimizes risk from a specific attacker pathway, subject to the same constraints as previous options. It shows risk from individual pathways, or attacker COAs.

Sum across All Pathways

Here, since the attacker has six different attack pathways, the framework accounts for risk for all possible outcomes.

Results

This framework simulates the optimal detection technology improvement allocation to the domestic port nodes in our notional transfer network, yielding an equilibrium allocation and conditional risk results per its equations.

The simulations yield the following results:

-For attacker permutations: a preponderance of investment at the weaker domestic port (here DP1) as the best investment is robust to attack permutation, including the aggregation of conditional risk across all four permutations, although the exact dollar of optimal investment amount varies, by permutation.

-For individual attacker pathways: a preponderance of investment at the weaker domestic port (here DP1) is ***only*** the best investment when the attacker is assumed to exploit both DPs, or when risk is aggregated across all six pathways. Otherwise, the best investment may be all at DP1, or maximum investment at DP2.

This framework evaluated possible conditional transfer risk in multiple ways, creating a "portfolio" of outcomes varying based on what the attacker might do. Unless a practitioner knows what specific pathway the attacker will use, it is valuable to assess a range of possibilities.

We now return to the first research goal:

1. Exploring whether we can reduce risk to CIKR in an optimal fashion while also maximizing deterrence

We modify: we want to explore whether explicitly accounting for quantifiable deterrence in our risk-reduction calculations leads to more or less relative risk reduction effectiveness.

Based on this analysis, the answer is yes, we can optimally reduce risk to transfer networks of CIKR. However, it is questionable whether the "maximization of deterrence" can be quantified in the larger context of risk reduction. Deterrence can certainly be quantified on its own, but it remains questionable how useful a metric this is. Taquechel and Lewis (2012)[32] claim that quantifiable deterrence effectiveness is also means to an end: determining the resulting change in unconditional risk.[33] At the end of the day, if we say we have reduced attacker intent by 50%, that seems incomplete. We want to know the implications for risk, or expected loss.

Given the above, we want to understand how accounting for the effects of deterrence upon risk reduction change the results of an optimization simulation. In other words, we want to know whether this portfolio of risk results is robust to deterrence considerations. We now introduce the concept of unconditional risk in the next framework.

Framework 2 — Optimize for Vulnerability, Deterrence (Intent Ratios)

Concept of Operations

The DHS Risk Lexicon claims a deterrent

> "is a measure that discourages, complicates, or delays an adversary's action by installing fear, doubt or anxiety."[34]

In their work on modeling the deterrence effects of counterterrorism investments, Bier and Kosanoglu (2015) compare their results to that of an objective function that omits deterrence probabilities. In effect, they are comparing what Taquechel and Lewis (2012)[35] call "conditional risk" with "unconditional risk." They claim that the optimal results yield better risk reduction when deterrence is considered.

With this in mind, we again simulate reducing the detection-failure susceptibility in domestic U.S. ports. However, if an adversary knows detection technology has improved, it may instill doubt in their ability to transfer a WMD or parts thereof successfully through U.S. ports, thus influencing their intent. The previous framework neglected attacker intent. Now, we introduce intent values as proxies for deterrence.

Network Risk Equation

This framework uses the same conditional risk equations from the previous framework. However, since we want to consider deterrence effects, this framework converts these equations to unconditional risk equations, leveraging attacker intent.

We define attacker intent as a function of specific attacker pathway:

$Intent^{COA}\Big|_{\$post_{DP}^{D(eq)}}$ = attacker intent to detonate[36] a WMD in a U.S. inland target city by exploiting the MTS via a specific pathway COA, given defender detection failure susceptibility reduction allocation (after simulation reaches equilibrium) across multiple domestic U.S. ports

More specifically, we define intent ratio as the ratio of attacker expected utility from attacking via one COA, to the total expected utility across all six COAs, given assumptions about defender equilibrium investment. The generic form of this is from Taquechel and Lewis (2012).[37]

$$Intent^{COA1}\Big|_{\$post_{DP}^{D(eq-COA1)}} = \frac{U_e T^{COA1}\Big|_{\$post_{DP}^{D(eq-COA1)}}}{\sum_{6}(U_e T^{COA}\Big|_{\$post_{DP}^{D(eq-COA1)}})}$$

Equation 2. Attacker intent ratio, for COA1, given defender equilibrium allocation assuming COA1

Attacker expected utility is the gain they can expect to receive from an attack. It is "probabilistic gain", as opposed to defender "probabilistic loss."

The probability of successful domestic port exploitation is the same as the failure susceptibility. Therefore, attacker expected utility *from a specific pathway* generally equates to defender conditional risk *from a specific pathway* in this approach.

Bier and Kosanoglu (2015) compared results excluding deterrence to results which assume deterrence accounts for both attack probability success and expected loss (target consequence). We calibrate the deterrence function similarly in this framework. Here, expected utility and thus attacker intent are a function of both probability and loss.

This function does not specify how the defender invests –it specifies how the attacker assumes the defender will invest. Here, the attacker assumes the defender's equilibrium investment hedges for the attacker executing COA 1. Empirically, this attribution of defender investment assumption to the attacker generally yields the best attacker intent ratios, and so seems a conservative defender assumption.

This framework incorporates intent ratios to show defender unconditional risk.
In total, there are 12 defender investment strategies. This framework applies the intent ratios for each attacker COA to calculate unconditional risk results from these investment strategies.

Objective Function/Constraints

This framework's objective function is to minimize unconditional risk in a transfer network. The constrained objective function for conditional risk thus now includes intent ratios.

This objective function equation has the same constraints as the objective function for conditional risk minimization in Framework 1, plus one additional constraint: the preference for OR-OR permutation exploitation can neither exceed one nor be negative.

Results

As with conditional risk, we evaluated unconditional transfer risk in multiple ways, creating a "portfolio" of outcomes varying on what the attacker might do. Based on simulations conducted under the auspices of this framework, we now generalize and claim that risk-reduction efforts accounting for deterrence effects and disregarding them are often equally effective, therefore adding no particular value to considering deterrence effects, explicitly.

A practitioner might know that their security investment is robust to different considerations, and a performance manager might report the same to an auditor. Unconditional risk is necessarily less than conditional risk when we multiply by an intent-ratio probability, but the proportion of risk reduced remains the same in both framework simulations.

However, in limited cases, depending on our assumptions about the attacker COA, accounting for deterrence may be MORE or LESS effective.

The unconditional risk simulations in this framework also showed the same results as did Framework 1, with respect to permutations and pathways.

Framework 3 — Optimize for Vulnerability, Deterrence — Game Theory Approach

Concept of Operations

Game theory models the outcome of interactions between players.[38] It may help characterize the interplay between risk reduction and deterrence when we evaluate transfer risk. Game-theoretic interactions may produce an equilibrium solution which suggests what each player *should* do, not necessarily what they *will* do. That said, with such insights we might be able to quantify the deterrence effects of potential COAs and incorporate those effects into risk-reduction metrics. Taquechel and Lewis (2016)[39] explored how deterrence might be quantified under "both equilibrium prospects and aggregate prospects." This framework simulates "equilibrium prospects"; the previous frameworks simulated "aggregate prospects." This supports flexible options for practitioners.

We now explore the interaction of:

1. attacker expected utility from exploiting the MTS using seven possible courses of action, and
2. defender expected utility from investing to deter attacks using seven possible courses of action, in a game theory format.

This extends the approach in Taquechel, Hollan and Lewis (2015)[40], who analyzed transfer risk without game-theoretic simulations.

This framework uses a simultaneous or normal form/strategic game, which assumes players cannot observe actions taken by other players.[41] This is a game of imperfect information. However, it also assumes complete information, meaning each player understands the expected utilities of the other.

The attacker courses of action (ACOA) are their specific transfer pathway options, and refraining from attack:

1. ACOA 1: OR-OR network, exploit either FP, exploit DP1
2. ACOA 2: OR-OR network, exploit either FP, exploit DP2
3. ACOA 3: AND-OR network, exploit both FP, exploit DP1
4. ACOA 4: AND-OR network, exploit both FP, exploit DP2
5. ACOA 5: OR-AND network, exploit either FP, exploit both DP
6. ACOA 6: AND-AND network, exploit both FP, exploit both DP
7. ACOA 7: Refrain from attack

Bier and Kosanoglu (2015) postulated that an attacker might forego attacks altogether given a sufficient defender investment in deterrence. Therefore, this framework includes the option to refrain from attack.

The defender courses of action (DCOA), given a limited budget, are:

1. DCOA 1: Invest optimally hedging for attacker COA 1 or COA 3 (the optimal investment amounts are the same for these two COAs)
2. DCOA 2: Invest optimally hedging for attacker COA 2 or COA 4 (the optimal investment amounts are the same for these two COAs)
3. DCOA 3: Invest optimally hedging for an OR-OR or AND-OR permutation, without regard to specific attacker transfer pathway
4. DCOA 4: Invest optimally hedging for an OR-AND or AND-AND permutation, without regard to specific attacker transfer pathway
5. DCOA 5: Invest optimally to minimize conditional risk aggregated across all four attacker permutations (OR-OR, AND-OR, OR-AND, AND-AND)
6. DCOA 6: Invest optimally to minimize conditional risk aggregated across all six attacker transfer pathways
7. DCOA 7: Refrain from deterrence investment

Results

Based on notional transfer network data and the expected utility calculations for both attacker and defender, the game looks like this:

	DCOA 1		DCOA 2		DCOA 3		DCOA 4		DCOA 5		DCOA 6		DCOA 7	
ACOA 1	$ 984,375.00		$ 1,119,569.94		$ 1,042,882.29		$ 1,054,361.84		$ 1,048,622.03		$ 1,049,989.09		$ 1,312,500.00	
		$ 3,015,625.00		$2,880,430.06		$ 2,957,117.71		$2,944,213.99		$2,951,377.97		$ 2,950,010.91		$2,687,500.00
ACOA 2	$ 1,093,750.00		$ 918,750.00		$ 967,848.40		$ 956,343.73		$ 961,810.95		$ 960,459.87		$ 1,093,750.00	
		$2,906,250.00		$3,081,250.00		$ 3,032,151.60		$3,044,932.81		$ 3,038,189.05		$ 3,039,540.13		$2,906,250.00
ACOA 3	$ 140,625.00		$ 159,938.56		$ 148,983.18		$ 150,623.12		$ 149,803.15		$ 149,998.44		$ 187,500.00	
		$3,859,375.00		$3,840,061.44		$ 3,851,016.82		$3,849,173.43		$ 3,850,196.85		$ 3,850,001.56		$3,812,500.00
ACOA 4	$ 156,250.00		$ 131,250.00		$ 138,264.06		$ 136,620.53		$ 137,401.56		$ 137,208.55		$ 156,250.00	
		$3,843,750.00		$3,868,750.00		$ 3,861,735.94		$3,863,561.83		$3,862,598.44		$ 3,862,791.45		$3,843,750.00
ACOA 5	$ 351,562.50		$ 335,870.98		$ 329,584.31		$ 329,251.38		$ 329,330.99		$ 329,297.11		$ 468,750.00	
		$3,648,437.50		$3,664,129.02		$ 3,670,415.69		$3,670,743.98		$3,670,669.01		$ 3,670,702.89		$ 3,531,250.00
ACOA 6	$ 87,890.63		$ 83,967.75		$ 82,396.08		$ 82,312.84		$ 82,332.75		$ 82,324.28		$ 117,187.50	
		$3,912,109.38		$3,916,032.25		$ 3,917,603.92		$3,917,685.99		$ 3,917,667.25		$ 3,917,675.72		$3,882,812.50
ACOA 7	$ -		$ -		$ -		$ -		$ -		$ -		$ -	
		$4,000,000.00		$4,000,000.00		$ 4,000,000.00		$4,000,000.00		$ 4,000,000.00		$ 4,000,000.00		$4,000,000.00

Figure 2 – Normal form game, Vulnerability

The attacker expected utility values are in the upper left of each interaction between a specific ACOA and DCOA, and the defender expected utility values are in the lower right. When the attacker refrains from attack (ACOA 7), they receive a payoff of $0, regardless of defender COAs whereas the defender retains maximum target value ($2M*2 targets = $4M).
Normal form games either will have a pure strategy Nash Equilibrium (NE) or mixed strategy equilibrium.[42] In Figure 2, there is no pure strategy.

We need to determine whether we can eliminate any strictly dominated strategies and recalculate a pure NE. Strictly dominated strategies are those that yield a smaller payoff than other strategies, regardless of what other players do.[43] This framework's simulation shows that ACOA 6 and 7 are strictly dominated, meaning a rational attacker *should* never choose either of those COAs when faced with the other COAs as options. Regardless of what the defender does, the attacker can *always* do better than ACOA 6 or 7.
We get:

	DCOA 3		DCOA 4		DCOA 5		DCOA 6	
ACOA 1	$ 1,042,882.29		$ 1,054,361.84		$ 1,048,622.03		$ 1,049,989.09	
	NE	$ 2,957,117.71		$2,944,213.99		$2,951,377.97		$ 2,950,010.91
ACOA 2	$ 967,848.40		$ 956,343.73		$ 961,810.95		$ 960,459.87	
		$ 3,032,151.60		$3,044,932.81		$3,038,189.05		$ 3,039,540.13
ACOA 5	$ 329,584.31		$ 329,251.38		$ 329,330.99		$ 329,297.11	
		$ 3,670,415.69		$3,670,743.98		$3,670,669.01		$3,670,702.89

Figure 3 – Normal form game, Vulnerability, attacker strictly dominated and defender weakly dominated strategies eliminated, "excessive" pruning

Here we achieve a pure NE result (ACO1, DCOA3). As per Taquechel and Lewis (2016), a pure NE means we can approximate an attacker's intent to choose their equilibrium COA as 100%.[44] Here, this means that the attacker ***should*** prefer to exploit DP1 and may exploit either foreign port 100% of the time, so their intent ratio is 100% for that COA. The defender ***should*** prefer to invest hedging for OR-OR exploitation or AND-OR exploitation 100% of the time.

Therefore, in this situation the defender unconditional risk is 100% * the expected attacker utility = $1,042,882. Defender expected utility was used to calculate the equilibrium solution, but for purposes of risk reduction, we continue to treat attacker expected utility as equivalent to defender expected loss, or risk.

This accounts for a deterrence in a limited fashion, not robust to either player's full suite of options. One might deem the strategy pruning excessive, as in theory, it may have eliminated an equilibrium solution. However, for expository purposes this framework's simulation prunes to drive towards a pure NE solution.

We might also explore mixed-strategy solutions, which are conceptually problematic for antiterrorism game-theoretic simulations. Rasmussen[45] and Slantchev[46] separately offer insights into interpretation of mixed strategies. This research proposes that those interpretations create challenges to accepting mixed strategies as reasonable outputs of game- theoretic interactions that inform conclusions about the relationship between risk reduction and deterrence.

Nonetheless, Bier and Kosanoglu (2015) advocated that future work on attacker deterrence explore defender appraisal of attacker choice as probabilistic. Moreover, Quijano et al. (2018) acknowledge that future work might consider continuous attacker decision variables, rather than binary.

The results of this game theoretic analysis of deterrence influence on risk are:

Table 2. Results, Normal form game, Vulnerability

Game Result	PURE NE	PURE NE	MIXED STRATEGY	MIXED STRATEGY
Assumptions	strictly/weakly eliminated, excessive COA pruning	strictly/weakly eliminated, excessive defender COA pruning only	strictly/weakly eliminated, excessive attacker pruning, ACOA 5 eliminated	strictly/weakly eliminated, excessive attacker pruning, ACOA 5 eliminated
Strategies Recommended	ACOA1, DCOA3	ACOA1, DCOA3	ACO1 56%, ACOA2 44%, ***DCOA 1***	ACO1 56%, ACOA2 44%, ***DCOA 5***
Resulting Defender Unconditional Risk	**$1,042,882**	**$1,042,882**	**$1,030,059**	**$1,010,425**

Before we compare data with that from conditional risk reduction (no deterrence) and unconditional risk reduction (deterrence using attacker intent ratios outside of game theoretic context), we clarify a fundamental issue.

The previous frameworks for exploring optimal risk reduction solutions with and without intent ratios explored what would happen ***if*** we invested a certain way, given the attacker did something specific. Those frameworks are exploratory rather that normative/prescriptive.

Furthermore, the frameworks with intent ratios treat deterrence as the influence of the ratio of attacker expected utility from one COA compared to other attacker options, ***without influence of game theoretic equilibria***. We make some assumptions about what the attacker assumes about our investments, which one might interpret as incorporating principles of attacker-defender modeling. That said, we do not explicitly explore equilibrium results.

In contrast, the game theory approach in Framework 3 explores what stakeholders ***should*** invest, given the attacker's portfolio of attack options. It is normative/prescriptive rather than exploratory. A practitioner may want to know the theoretically optimal investment solution, but may also like the flexibility of alternative investment options.

Furthermore, that framework treats deterrence as the influence of a pure or mixed strategy NE upon the attacker's assessment of their expected utility, and consequently upon our expected risk.

Given this, we find that only in one exploratory scenario of 12 can we say that consideration of deterrence effects on risk led to a larger relative risk-reduction effectiveness metric. This is not encouraging for those who might advocate maximizing deterrence in conjunction with risk reduction, although more research is needed to validate the robustness of this finding to different conditions and assumptions.

Furthermore, we find that in our predictive game-theoretic approach, it is difficult to say the consideration of deterrence has any impact on risk reduction, for a pure strategy equilibrium result. Practitioners who base their CIKR investments on game theoretic modeling might want to know this.

Framework 4 — Optimize for Consequence, No Deterrence

Concept of Operations

This framework simulates investment to reduce the consequence of cascading failure in a notional supply chain network as shown in Taquechel (2013).[47] Minimizing consequence equates to minimizing network risk, which amounts to maximizing resilience. The focus here is on the relationship between optimized network risk reduction and deterrence.

The notional supply chain network here, as in previous work, may be a petrochemical network, with refineries as supplier nodes, and links representing the means of transporting product between refineries and downstream customers, represented in the model as intermediate and customer nodes.

Network Risk Equation

This framework leverages probabilistic risk equations that describe the failure susceptibilities of all supply-chain network nodes, and consequences of failure at each node. It starts with the supplier nodes, which we assume an attacker will attack.

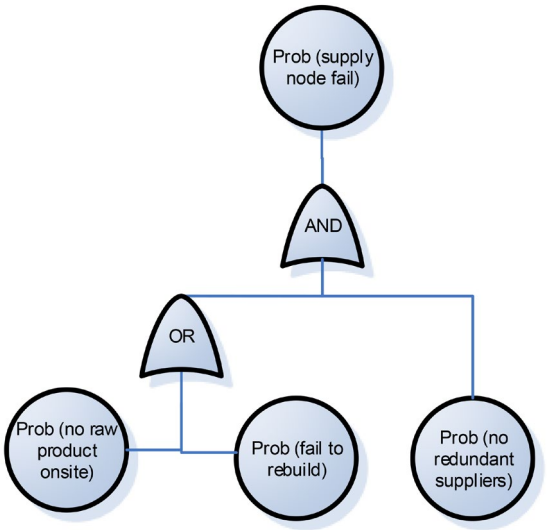

Figure 4. Fault Tree – Supplier Node Failure Susceptibility

Here, the framework assumes that in order to fail, a supplier node must either lack raw product onsite, OR lack rebuilding potential, AND must lack redundant upstream suppliers. The framework further leverages equations for overall supplier node failure susceptibility, supplier node expected consequence, network expected consequence, and conditional network risk, which combines supplier node failure susceptibility with expected consequence.

The framework's simulation leverages two hypothetical networks, network A and network B. They are identical in every respect except network A has a supplier node pre-investment rebuilding failure susceptibility of 0.25, whereas network B has a higher supplier node pre-investment rebuilding failure susceptibility of 0.5. Each network has one supplier node, two intermediate nodes, and four customer nodes.

Objective Function/Constraints

The objective is to minimize aggregate conditional risk across both notional supply-chain networks A and B. The budget and probability constraints show that:

1. Total rebuilding investment amongst the two network supplier nodes cannot exceed total budget;
2. Rebuilding investment at each node cannot exceed the node's postmax;
3. Supplier node failure susceptibilities must be between 0 and 1; and
4. Supplier node failure susceptibility given rebuilding investment cannot exceed pre-investment supplier node failure susceptibility.

Unlike the transfer scenario, we focus here on consequence mitigation after an attack. Therefore, we do not need to create a portfolio of risk results across possible attacker permutations or pathways. This framework constrains the attacker's options to attacking the supplier nodes.

Results

For a budget of $1.5M, we achieve the following results:

Table 3. Results – Optimizing for Consequence, No Deterrence

ALLOCATION NETWORK A	ALLOCATION NETWORK B	RESULTING CONDITIONAL RISK (AGGREGATE)	ALLOCATION TACTIC	% RISK REDUX
$ -	$ -	$ 91,857.91	N/A	N/A
$ -	$ 1,500,000.00	$ 72,311.40	MAX B	21.28%
$ 250,000.00	$ 1,250,000.00	$ 66,784.68	PREPONDERANCE B	27.30%
$ 580,482.02	$ 919,517.98	$ 65,069.59	MAX A	29.16%

The total postmax value for both networks is $2.24M. Since only $1.5M budget exists, this forces an optimization solution.

These results seem slightly counterintuitive, as network B had the supplier node with higher rebuilding failure susceptibility. However, we maximize investment at network A supplier node, then allocate the remainder to network B supplier node, which is more effective than putting all $1.5M at B.

Taquechel (2013)[48] defined resilience as the "potential to minimize risk, or restore performance to a pre-disruption level, if any infrastructure were attacked." Here, the percentage of risk reduced serves as a proxy for resilience. Resilience is thus a function of the allocation strategy in this research.

We now explore whether these results are robust to deterrence considerations. To do so, we introduce the concept of unconditional risk in the next framework.

Framework 5 — Optimize for Consequence, Deterrence (Intent Ratios)

Concept of Operations

The DHS Risk Lexicon claims

> "resilience…has a potential deterrence value achieved when terrorist groups perceive that the strategic impact they seek through a particular attack or type of attack will not be achieved."[49]

We are increasing the resilience of a supply-chain network by investing in rebuilding potential in this framework. Therefore, in theory, increased resilience would deter an adversary who would stand to achieve less-desirable results.

Network Risk Equation

This framework uses the same conditional risk equations from the previous framework. However, since we want to consider deterrence effects, this framework converts these equations to unconditional risk equations.

Attacker intent is a function of specific supply chain:

$Intent^{l}\Big|_{\$\,post_{s}^{reb(eq)}}$ = attacker intent to disrupt an lth supply chain by attacking the supplier node, given defender rebuilding failure susceptibility reduction allocation (after simulation reaches equilibrium) across multiple supply chain supplier nodes

More specifically, intent ratio is the ratio of attacker expected utility from attacking one supplier node (in the lth supply chain), to the total expected utility across all supply chains considered:

$$Intent^{l}\Big|_{\$post_s^{reb(eq)}} = \frac{U_e T^{l}\Big|_{\$post_s^{reb(eq)}}}{\sum_{2}(U_e T^{l}\Big|_{\$post_s^{reb(eq)}})}$$

Equation 3. Attacker intent ratio, for lth supply chain network given defender equilibrium rebuilding allocation

Attacker expected utility from attacking a specific supplier node generally equates to defender conditional risk from the cascading effects of an attack on said supplier node through the respective supply-chain network in this approach. This framework incorporates intent ratios to show defender unconditional risk.

Objective Function/Constraints

The constrained objective function for conditional risk now includes intent ratios and thus minimizes aggregate unconditional risk for supply-chain networks A and B. The budget and probability constraints are the same as in the previous framework, plus two new constraints:

1. Intent to attack an individual supply chain must be positive and cannot exceed 1; and
2. Total intent must equal one.

Results

For a budget of $1.5M, we achieve the following results:

Table 4. Results – Optimizing for Consequence, Deterrence

ALLOCATION NETWORK A	ALLOCATION NETWORK B	RESULTING UNCONDITIONAL RISK (AGGREGATE)	ALLOCATION TACTIC	% RISK REDUX
$ -	$ -	$ 46,127.69	N/A	N/A
$ -	$ 1,500,000.00	$ 37,416.63	MAX B	18.88%
$ 250,000.00	$ 1,250,000.00	$ 33,632.53	PREPONDERANCE B	27.09%
$ 580,482.02	$ 919,517.98	$ 32,537.95	MAX A	29.46%

Accounting for deterrence effects of optimal investments in risk reduction is equally effective as disregarding deterrence effects.

Framework 6 — Optimize for Consequence — Deterrence — Game Theory Approach

Concept of Operations

Game theory may help characterize the interplay between risk reduction and deterrence when we reduce supply chain risk.

We now explore the interaction of

1. attacker expected utility from attacking supply chain network supplier nodes using four possible courses of action, and
2. defender expected utility from investing to deter the attacks (and conceptually, to also deny the expected utility the attacker would realize from a cascading supply chain failure) using five possible courses of action, in a game theory format. As with the vulnerability analysis in Framework 3, we assume imperfect and complete information.

The attacker courses of action (ACOA) are:

1. ACOA1: Attack network A supplier node
2. ACOA2: Attack network B supplier node
3. ACOA3: Attack both network supplier nodes simultaneously
4. ACOA4: Refrain from attack

The defender courses of action (DCOA), given a limited budget, are:

1. DCOA1: Invest optimally hedging for either network attack
2. DCOA2: Invest sub-optimally hedging for either network attack
   (expend all funds, but distribute sub-optimally amongst supplier nodes)
3. DCOA3: Invest all funds in defending network A supplier node (up to node postmax)
4. DCOA4: Invest all funds in defending network B supplier node (up to node postmax)
5. DCOA5: Refrain from deterrence investment

Results

Based on notional supply chain network data and the expected utility calculations for both attacker and defender, the game looks like this:

	DCOA1		DCOA2		DCOA3		DCOA4		DCOA5	
ACOA1	$ 32,214.36		$ 36,224.37		$ 32,214.36		$ 42,907.71		$ 42,907.71	
		$ 13,829,052.73		$ 13,823,120.12		$ 13,829,052.73		$ 13,813,232.42		$ 13,813,232.42
ACOA2	$ 32,855.23		$ 30,560.32		$ 48,950.20		$ 29,403.69		$ 48,950.20	
		$ 13,821,953.03		$ 13,826,016.16		$ 13,793,457.03		$ 13,828,063.96		$ 13,793,457.03
ACOA3	$ 65,069.59		$ 66,784.68		$ 81,164.55		$ 72,311.40		$ 91,857.91	
	NE	$ 13,651,005.77		$ 13,649,136.27		$ 13,622,509.77		$ 13,641,296.39		$ 13,606,689.45
ACOA4	$ -		$ -		$ -		$ -		$ -	
		$ 14,000,000.00		$14,000,000.00		$ 14,000,000.00		$ 14,000,000.00		$ 14,000,000.00

Figure 5 – Normal form game, Consequence

Here we achieve a pure NE result (ACO3, DCOA1). This means that the attacker ***should*** prefer to attack ***both*** supply chains simultaneously 100% of the time, so their intent ratio is 100% for that COA. The defender ***should*** prefer to invest optimally across both supply chain networks 100% of the time.

This pure equilibrium solution is satisfying as it yields an attacker COA that might stand on its own. Furthermore, the defender tactic of optimally investing across both networks seems wisest, as that is robust to the absence of specific intelligence on which network the attacker is likely to attack. This might satisfy a practitioner in an intelligence-constrained decision space.

In this framework the defender unconditional risk is 100% * the expected attacker utility = $65,069.59. Therefore, in our predictive approach, it is difficult to say the quantification of deterrence has any impact on risk reduction, as this result is equal to the best conditional risk when we optimized without deterrence consideration, and is worse than the unconditional risk when we optimized accounting for intent ratios outside of a game theoretic context.

Findings

We initially set out to explore whether, given limited resources, we could:

1. Reduce risk to CIKR in an optimal fashion while also maximizing deterrence
2. Optimally increase network resilience while maximizing deterrence

However, we learned it might be appropriate to modify these goals, specifically exploring whether:

Explicitly accounting for quantifiable deterrence in our risk-reduction calculations (whether reducing vulnerability or reducing consequence) leads to more or less relative risk reduction effectiveness.

Transfer Risk-Reducing Vulnerability

We now explain how the results from our framework analyses above address this research goal. For reducing transfer risk by investing to improve detection technology in U.S. ports (frameworks 1-3), we showed that risk-reduction efforts accounting for deterrence effects and disregarding them are often equally effective, therefore adding no particular value to considering deterrence effects, explicitly. Practitioners therefore may rest easy knowing that their investments may effectively reduce risk from attacks whether or not that risk explicitly accounts for deterrence considerations.

However, in limited specific cases, depending on our assumptions about the attacker COA, accounting for deterrence yielded either more effective risk reduction, or less effective risk reduction. When we added a game-theoretic approach, optimal investment was not relatively more effective in reducing risk. Therefore, the general answer is, “it depends!” A practitioner might be interested in this nuance.

This is not encouraging for those who might advocate maximizing deterrence in conjunction with risk reduction. However, more research is needed to validate the robustness of these findings to different conditions and assumptions. This also calls into question the value of game-theoretic approaches for deterrence analysis, although more research is needed.

Supply Chain Risk- Reducing Consequence

For reducing supply chain network risk by investing to improve rebuilding potential and thus improving resilience (frameworks 4-6), we showed that accounting for deterrence effects of optimal investments in risk reduction is equally effective as disregarding deterrence effects. However, when we expanded the problem to include optimization amongst more supply chain networks, we found the relative efficacy of deterrence investment tactics in reducing risk is greater when we consider deterrence than when we do not. A practitioner in a larger network might appreciate evidence that their resilience investment may have additional value in terms of both deterring attacks and reducing risk, and a budget manager might appreciate the knowledge that their money is well spent, for multiple purposes and in larger networks.

Furthermore, in our predictive game-theoretic approach (limited to two networks), we found that it is difficult to say the quantification of deterrence has any impact on risk reduction. That is because this result is equal to the best conditional risk when we optimized without deterrence consideration, and is worse than the unconditional risk when we optimized accounting for intent ratios outside of a game theoretic context.

Therefore, again, the general answer is “it depends!”

Recommendations for Future Research

Given the limited data and numerous assumptions behind our findings, and the importance of more robust/generalized findings in support of decision-making, recommendations for future study include numerous opportunities to expand on the methodology behind our findings. We organize them below.

Scenario – Network vs Non-Networked CIKR

This research built on existing research into networks. Taquechel (2013)[50] advocated why infrastructure should be evaluated in context of networks, albeit under specific circumstances. Going forward, evaluation of how deterrence relates to risk reduction might also simulate allocation to a group of non-networked facilities, thereby evaluating risk or resilience across a collection of unrelated infrastructure. This has implications for public-sector managers in government coordinating councils and private industry in sector coordinating councils, when interdependencies are under scrutiny.

Network Metrics

This research evaluated failure susceptibility in supply-chain networks based on a "fault tree" mathematical technique. However, other approaches (e.g. Lewis, 2006[51]) leverage "network metrics" to support the optimization of funding for network risk minimization. Such metrics include node degree, between-ness, and cluster coefficient, among others. Future work might leverage such metrics in evaluating the relationship between deterrence and network risk reduction. The outputs may be different, with practitioner implications, even though this is a theoretical modeling consideration.

Expected Utility Functions – Equation Component Assumptions

This research omitted estimates of attacker capability as probabilistic functions. Future work might incorporate such estimates into expected-utility functions. Moreover, future work might explore the relationship between simulated investment and risk reduction based on an exponential relationship vice the logarithmic relationship used here, or even a linear relationship between investment and risk. Quijano et al. (2018)[52] model "diminishing returns" effects of deterrence countermeasures in protecting a network against attack, treating the probability of successful attack as an exponential function of defender countermeasures such as metal detectors and close circuit cameras.

Furthermore, this research leveraged expected utility functions that did not explicitly subtract investment costs from the expected retained value if a transfer network was exploited or a supply chain was attacked. Future work might incorporate those lost costs. This is a natural concern for a resource-constrained practitioner. Bier and Kosanoglu (2015)[53] explore an objective function to minimize critical-infrastructure risk that includes the costs of protection. In addition, Quijano et al. (2018)[54] model attacker and defender investment as part of expected utility, as do Xu et al.[55]

Expected Utility Functions – Probabilistic Risk Assessment vs Exceedance Probability

Taquechel (2017)[56] lists some examples of literature on risk analysis, deterrence, resilience networks and optimization and proposes additional research opportunities based on the work of Taleb and others – evaluating exceedance probability, antifragility, and other concepts. Future work might explore the relationship between risk reduction and deterrence based on expected-utility functions that leverage exceedance probability, or the probability that consequences of an attack will exceed a certain threshold, rather than the probability they will occur in the first place.

Expected Utility Functions – Utility Theory Assumptions

This research assumed Expected Utility Theory (EUT) as the basis for utility functions. There is an abundance of literature, notably Prospect Theory, showing that decision making often violates axioms of EUT. Future research might evaluate the relationship between deterrence and risk reduction by incorporating principles of Prospect Theory. Taquechel and Lewis (2016)[57] briefly explore prospect theory and deterrence outside of the explicit context of this relationship. Quijano et al. (2018) model their defender as risk averse, meaning their expected utility as a function of investment was biased by a risk aversion proxy parameter.

Optimization Assumptions – Vulnerability (Failure Susceptibility)

This research only simulated investment to improve detection technology at U.S. ports; future work might incorporate the ability to also optimize investments to improve encounter probabilities. A practitioner may be well advised to modify port operations for cargo screening based on these results.

Moreover, this research only simulated investment in U.S. ports. Future work might incorporate the ability to optimize investment in both U.S. ports and foreign ports. For example, Customs and Border Protection (CBP) invests in radiation-detection equipment and other counter-WMD technology overseas. That said, the characterization of the relationship between investment in foreign port security and resulting vulnerability reduction, or "investment efficacy," may be challenging.[58]

Optimization Assumptions – Consequence

This research only simulated investment to improve rebuilding potential in supply chain network nodes; future work may incorporate the ability to also optimize investment to improve facility ability to keep raw product onsite. Similarly, future research might simulate simultaneous investment to increase resilience in multiple layers of the supply-chain network, not just the supplier nodes.

Optimization – "Blended Approach"

Quijano et al. (2018) model optimal allocation of both protection investment and response investment, on the assumption a network is attacked and the defender needs to recover. They therefore seek optimal solutions that combine both prevention and response investments, as a single objective. For example, some of the preventive countermeasures such as security guards might also be used to respond to an attack. With this in mind, future research might explore the relationship between deterrence and risk reduction when we invest simultaneously to protect a supply-chain network from attack and reduce the impact if attacked.

Game Theoretic Approach

We simulated a game-theoretic approach for limited number of transfer networks and supply chain networks. Future work should explore game-theoretic interactions with larger sets of networks.

We also assumed complete information. Future work should explore the relationship between deterrence and risk reduction with assumptions of incomplete information. Taquechel and Lewis (2016)[59] explore games of incomplete information outside of the explicit context of this relationship.

Moreover, we did not explore sub-optimal investment in our deterrence game for transfer networks. Future work may add this defender COA.

Maximizing Deterrence

If we agree on a working definition of quantifiable deterrence for CIKR protection, and if we agree on appropriate mathematical optimization techniques, it might make sense to combine the two to explore how we could "optimize deterrence" as a stand-alone metric. Despite skepticism in the literature, a standalone deterrence metric might have value in some applications.

Practical Implications

Framework for Evaluating Relationship between Risk and Deterrence

One implication of this research pertains to a potential leadership decision. When it comes to investing to reduce network risk and account for deterrence, it seems valuable to have multiple options: a predictive solution, or an exploratory solution that hedges against a simple equilibrium outcome. This research provides data in support of both options. There may be no "right" answer.

Evaluating the Relationship

There is an abundance of research on performance metrics in government; a subset of that research looks at metrics for security and antiterrorism specifically. If we believe program evaluation is important for government antiterrorism programs, and if we believe it is important to consider whether deterrence is a useful metric to include in such program evaluation, then the relationship between deterrence and risk reduction should be understood, across a variety of scenarios, modeling assumptions, and data inputs.

Taquechel and Saitgalina (2018)[60] claim that

> the perceived effect of changes in adversary intent upon threat reduction metrics could be a valuable component of a logic-model framework to integrate risk metrics with antiterrorism program performance evaluation.

Taquechel and Saitgalina (2018)[61] propose notional simple metrics that show how to account for deterrence effects of antiterrorism activities, but implementing such metrics would not be without challenges and warrants further exploration. More specifically, if we measure how risk changes when we account for the effects of deterrence (i.e. reduce attacker intent through randomized patrolling or similar activities), but cannot show consistently that risk reduction is more effective when we account for deterrence, that may pose an additional challenge to metric validity. It does not invalidate the metric altogether, but validity simply may become situational. A practitioner who has to report performance, may want to know how robust their metrics are to various modeling assumptions.

Taquechel and Saitgalina (2018)[62] also claim that developing risk reduction metrics for antiterrorism programs might pose a chance to explore how deterrence serves as a "moderator variable", moderating the effect of investment and activities on ultimate risk-reduction outcomes. The present research suggests that sometimes accounting for deterrence moderates relative risk-reduction effectiveness; other times it does not.

Taquechel and Lewis (2012)[63] predicted agencies might eventually have to report deterrence metrics in conjunction with risk-reduction metrics. Furthermore, Taquechel and Saitgalina (2018)[64] propose a high-level framework and considerations for antiterrorism program risk metrics. Therefore, the present research responds to this prediction and one specific point of this proposal, providing more detail. To the best of our knowledge, the prediction has not yet become a reality, but if it does, this work may help position stakeholders to respond to that mandate.

Planning, Programming, Budgeting and Execution: Relevance

PPBE is a process to plan agency priorities, convert those priorities to budget proposals, defend said proposals with appropriators, and execute appropriated budget. During the planning phase, agencies with antiterrorism missions may benefit from evaluating metrics and formulating budget proposals linked to those metrics. If agency budget developers can model the relationship between terrorism risk reduction and deterrence efforts, those budgetary proposals may be well supported.

Conclusion

In conclusion, this research advances knowledge in several ways:

1. it responds to predictions and advances earlier proposals;
2. it uses fault tree logic to describe inherited failure susceptibility in a network, as an alternative to network metrics; thus posing an alternative to previous literature;
3. it applies game theoretic techniques to the previous problem of optimizing WMD transfer-risk reduction;
4. it more generally compares multiple techniques to account for quantifiable deterrence, specifically classical game theory equilibrium approaches and more recently published "intent ratio" approaches; and
5. it provides data in support of the relationship between quantitative deterrence data and quantitative risk reduction under a variety of scenarios, assumptions, and data inputs. A different way to frame this is showing whether explicitly accounting for quantifiable deterrence in our risk-reduction calculations leads to more or less relative risk reduction effectiveness.

This is a less specific framework than simply exploring whether deterrence is important in CIKR risk reduction. It thus provides more flexibility for exploration.

This approach also provides more flexibility than an approach taken within the framework of exploring whether we simultaneously maximize deterrence and risk reduction.

This approach may address another point from Taquechel and Saitgalina's notional framework for antiterrorism program logic models: the fact that "realist matrix" logic models may proxy how intervention works differently in different situations. Those situations may include the assumptions we make about how adversaries make decisions.

Regarding government strategies and other documents with their sparse reference to deterrence, perhaps "word frequency" is inconsequential and no indication of the relative importance of deterrence within the framework of all risk-management considerations. As mentioned, it is difficult to imagine a proposition that deterring attacks is not important and we should ignore hypothetical effects of our actions on adversary decision making.

That said, there are high-level documents, policy statements, and strategies, and there are operational-level program evaluation and management objectives. Managerial efforts to measure risk reduction and appropriately invest ultimately support implementation of those high-level strategies. Therefore, it makes sense to continue to explore the relationship between deterrence, investment, and risk reduction. It is not yet clear whether deterrence and risk reduction are two sides of the same coin.

About the Author

Eric F. Taquechel is a U.S. Coast Guard officer with experience in shipboard operations, port operations, critical infrastructure risk analysis, emergency planning and readiness, operations analysis, strategy/budgeting process support, and international port security management. He has authored and co-authored various publications on risk, resilience, deterrence, and performance metrics in *Homeland Security Affairs*, the *Journal of Homeland Security and Emergency Management*, and IEEE. Most recently, he and coauthor published "Risk-Based Performance Metrics for Critical Infrastructure Protection? A Framework for Research and Analysis" in *Homeland Security Affairs*. His paper "A Right-Brained Approach to Critical Infrastructure Protection Theory in support of Strategy and Education: Deterrence, Networks, and Antifragility" was a Best Paper presented at the CHDS's 2017 10th Annual Homeland Defense and Security Education Summit. Taquechel has taught courses on critical infrastructure protection and is a FEMA Master Exercise Practitioner. He holds a MPA from Old Dominion University with a graduate certificate in public procurement, a master's degree in Security Studies from the Naval Postgraduate School, and a BS from the U.S. Coast Guard Academy. He may be reached at eric.taquechel@gmail.com.

Acknowledgements

The authors wish to thank the referees who helped improve the quality of this work.

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.

Bibliography

Adler, Richard and Jeff Fuller. "Decision Support for Countering Terrorist Threats against Transportation Networks." *Journal of Strategic Studies* 2 (2009): 43-64.

Al-Mannai, Waleed I. and Ted G. Lewis. "A General Defender-Attacker Risk Model for Networks." *Journal of Risk Finance* 9 (2008): 244-261.

Al-Mannai, Waleed I. and Ted G. Lewis. "Minimizing Network Risk with Application to Critical Infrastructure Protection." *Journal of Information Warfare* 6 (2007): 52-68.

Bernstein, Paul I. "Deterrence in Professional Military Education." *Air and Space Power Journal* July-August 2015. Accessed August 24, 2019. https://apps.dtic.mil/dtic/tr/fulltext/u2/a622477.pdf.

Bier, Vicki M. and Fuat Kosanoglu. "Target-Oriented Utility Theory for Modeling the Deterrent Effects of Counterterrorism." *Reliability Engineering and System Safety* 136 (2015): 35-46.

Countering Weapons of Mass Destruction Office. Accessed March 30, 2021. https://www.dhs.gov/countering-weapons-mass-destruction-office.

Cybersecurity & Infrastructure Security Agency. Accessed March 30, 2021. https://www.dhs.gov/CISA.

Department of Homeland Security. DHS Congressional Budget Justification FY2020. 2019. Accessed March 30, 2021. https://www.dhs.gov/publication/congressional-budget-justification-fy-2020.

Department of Homeland Security. DHS Risk Lexicon. 2010. Accessed March 30, 2021. https://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf.

Department of Homeland Security. National Infrastructure Protection Plan. 2013. Accessed March 30, 2021. https://www.cisa.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf.

Department of Homeland Security. Strategic Framework for Countering Terrorism and Targeted Violence. 2019. Accessed March 30, 2021. https://www.dhs.gov/sites/default/files/publications/19_0920_plcy_strategic-framework-countering-terrorism-targeted-violence.pdf.

Department of Homeland Security and Department of Transportation. Transportation Systems Sector-Specific Plan. 2015. Accessed March 30, 2021. https://www.cisa.gov/sites/default/files/publications/nipp-ssp-transportation-systems-2015-508.pdf.

Federal Emergency Management Agency. FEMA FY19 Port Security Grant Program Overview, Objectives and Priorities. 2019. Accessed October 10, 2019. https://www.fema.gov/media-library-data/1555009856483-1ac8e262baeddc0570b81bf14b1d1f13/FY_2019_PSGP_NOFO_FINAL_508.pdf .

Lewis, Ted G. *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation*. Hoboken, N.J: Wiley Interscience, 2006.

Maritime Commerce Security Plan for the National Strategy for Maritime Security. 2005. Accessed March 30, 2021. https://www.dhs.gov/sites/default/files/publications/HSPD_MCSPlan_0.pdf .

Maritime Transportation System Security Recommendations for the National Strategy for Maritime Security. 2005. Accessed March 30, 2021. https://www.dhs.gov/sites/default/files/publications/HSPD_MTSSPlan_0.pdf .

Osborne, Martin J., and Ariel Rubenstein. *A Course in Game Theory*. Cambridge: MIT Press, 1994.

Presidential Policy Directive 21. Directive on Critical Infrastructure Security and Resilience. 2013. Accessed March 30, 2021. https://www.hsdl.org/?view&did=731087 .

Quijano, Eduardo G., David R. Insua, and Javier Cano. "Critical Networked Infrastructure Protection from Adversaries." *Reliability Engineering and System Safety* 179 (2018): 27-36.

Rasmussen, Eric. "Mixed and Continuous Strategies." 2015. Accessed March 30, 2021. www.rasmusen.org/GI/chapters/chap03_mixed.pdf.

Shor, Mikhael. "Dominated Strategy." Dictionary of Game Theory Terms, Game Theory.net. Accessed March 30, 2021. http://www.gametheory.net/dictionary/DominatedStrategy.html.

Shor, Mikhael. "Simultaneous Game," Dictionary of Game Theory Terms. Game Theory.net. Accessed March 30, 2021. http://www.gametheory.net/dictionary/SimultaneousGame.html .

Slantchev, Branislav L. "Game Theory: Dominance, Nash Equilibrium, Symmetry." Accessed March 30, 2021. http://slantchev.ucsd.edu/courses/gt/04-strategic-form.pdf .

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

Taquechel, Eric F. "Options and Challenges of a Resilience-Based, Network-Focused Port Security Grant Program." *Journal of Homeland Security and Emergency Management* 10 (2013): 521-554.

Taquechel, Eric F. "Validation of Rational Deterrence Theory: Analysis of U.S. Government and Adversary Risk Propensity and Relative Emphasis on Gain or Loss." Thesis, Naval Postgraduate School, 2010. Accessed September 1, 2019. https://apps.dtic.mil/dtic/tr/fulltext/u2/a519012.pdf .

Taquechel, Eric F., Ian Hollan, and Ted G. Lewis. "Measuring the Deterrence Value of Securing Maritime Supply Chains against WMD Transfer and Measuring Subsequent WMD Risk Reduction." *Homeland Security Affairs* 11, Article 1 (February 2015). Accessed March 30, 2021. https://www.hsaj.org/articles/1304 .

Taquechel, Eric F. and Marina Saitgalina. "Risk-Based Performance Metrics for Critical Infrastructure Protection? A Framework for Research and Analysis." *Homeland Security Affairs* 14, Article 8 (December 2018). Accessed March 30, 2021. https://www.hsaj.org/articles/14699 .

Taquechel, Eric F. and Ted G. Lewis. "How to Quantify Deterrence and Reduce Critical Infrastructure Risk." *Homeland Security Affairs* 8, Article 12 (August 2012). Accessed March 30, 2021. https://www.hsaj.org/articles/226 .

Taquechel, Eric F. and Ted G. Lewis. "More Options for Quantifying Deterrence and Reducing Critical Infrastructure Risk: Cognitive Biases." *Homeland Security Affairs* 12, Article 3 (September 2016). Accessed March 30, 2021. https://www.hsaj.org/articles/12007 .

Taquechel, Eric F. and Ted G. Lewis. "A Right-Brained Approach to Critical Infrastructure Protection Theory in support of Strategy and Education: Deterrence, Networks, Resilience, and "Antifragility." *Homeland Security Affairs* 13, Article 8 (October 2017). Accessed March 30, 2021. https://www.hsaj.org/articles/14087.

The White House. Fiscal Year 2020 Budget of the U.S. Government. 2019. Accessed September 1, 2019. https://www.whitehouse.gov/wp-content/uploads/2019/03/budget-fy2020.pdf .

The White House. The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets. 2003. Accessed March 30, 2021. https://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf .

Uhl, Craig, and William Fiore. "Privacy Impact Assessment for the Radiation Detection Systems." 2016. Accessed March 30, 2021. https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp-rds-july2016.pdf .

Xu, Jie, Jun Zhuang, and Zigeng Liu. "Modeling and Mitigating The Effect of Supply Chain Disruption in a Defender-Attacker Game." *Annals of Operations Research* 236 (2015): 255-270.

Notes

1. Eric F. Taquechel and Marina Saitgalina, "Risk-Based Performance Metrics for Critical Infrastructure Protection? A Framework for Research and Analysis," *Homeland Security Affairs* 14, Article 8 (December 2018) https://www.hsaj.org/articles/14699 .
2. Ibid.
3. U. S. Department of Homeland Security, *DHS Risk Lexicon*, 2010, https://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf .
4. The White House, *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, 2003, https://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf .
5. Presidential Policy Directive 21, *Directive on Critical Infrastructure Security and Resilience*, 2013, https://www.hsdl.org/?view&did=731087 .
6. *Maritime Transportation System Security Recommendations for the National Strategy for Maritime Security*, 2005, https://www.dhs.gov/sites/default/files/publications/HSPD_MTSSPlan_0.pdf .
7. *Maritime Commerce Security Plan for the National Strategy for Maritime Security*, 2005, https://www.dhs.gov/sites/default/files/publications/HSPD_MCSPlan_0.pdf .
8. Department of Homeland Security and Department of Transportation, *Transportation Systems Sector-Specific Plan*, 2015, https://www.cisa.gov/sites/default/files/publications/nipp-ssp-transportation-systems-2015-508.pdf .
9. Department of Homeland Security, *National Infrastructure Protection Plan*, 2013, https://www.cisa.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf .
10. Cybersecurity & Infrastructure Security Agency, https://www.dhs.gov/CISA .
11. Department of Homeland Security, *Strategic Framework for Countering Terrorism and Targeted Violence*, 2019, https://www.dhs.gov/sites/default/files/publications/19_0920_plcy_strategic-framework-countering-terrorism-targeted-violence.pdf .
12. The White House, *Fiscal Year 2020 Budget of the U.S. Government*, 2019, https://www.whitehouse.gov/wp-content/uploads/2019/03/budget-fy2020.pdf .
13. Department of Homeland Security, *DHS Congressional Budget Justification FY2020*, 2019, https://www.dhs.gov/publication/congressional-budget-justification-fy-2020 .
14. Countering Weapons of Mass Destruction Office, https://www.dhs.gov/countering-weapons-mass-destruction-office .
15. Federal Emergency Management Agency, *FEMA FY19 Port Security Grant Program Overview, Objectives and Priorities*, 2019, https://www.fema.gov/media-library-data/1555009856483-1ac8e262baeddc0570b81bf14b1d1f13/FY_2019_PSGP_NOFO_FINAL_508.pdf .
16. Eric F. Taquechel, "Layered Defense: Modeling Terrorist Transfer Threat Networks and Optimizing Network Risk Reduction," *IEEE Magazine 24(*2010): 30-35.
17. W. I. Al-Mannai and Ted G. Lewis, "Minimizing Network Risk with Application to Critical Infrastructure Protection," *Journal of Information Warfare 6*(2007), 52-68.
18. W.I. Al-Mannai and Ted G. Lewis, "A General Defender-Attacker Risk Model for Networks," *Journal of Risk Finance 9*(2008), 244-261.
19. Eric F. Taquechel, "Validation of Rational Deterrence Theory: Analysis of U.S. Government and Adversary Risk Propensity and Relative Emphasis on Gain or Loss," Thesis, Naval Postgraduate School, 2010, https://apps.dtic.mil/dtic/tr/fulltext/u2/a519012.pdf .
20. Vicki M. Bier and Fuat Kosanoglu, "Target-Oriented Utility Theory for Modeling the Deterrent Effects of Counterterrorism," *Reliability Engineering and System Safety 136*(2015), 35-46.
21. Eduardo G. Quijano, David R. Insua, and Javier Cano, "Critical Networked Infrastructure Protection from Adversaries," *Reliability Engineering and System Safety 179*(2018), 27-36.
22. Eric F. Taquechel and Ted G. Lewis, "How to Quantify Deterrence and Reduce Critical Infrastructure Risk," *Homeland Security Affairs* 8, Article 12, (August 2012) https://www.hsaj.org/articles/226 .
23. Eric F. Taquechel, Ian Hollan, and Ted G. Lewis, "Measuring the Deterrence Value of Securing Maritime Supply Chains against WMD Transfer and Measuring Subsequent WMD Risk Reduction," *Homeland Security Affairs* 11, Article 1 (February 2015) https://www.hsaj.org/articles/1304 .
24. Paul I. Bernstein, "Deterrence in Professional Military Education," *Air and Space Power Journal* July-August 2015, https://apps.dtic.mil/dtic/tr/fulltext/u2/a622477.pdf .
25. Eric F. Taquechel, "Options and Challenges of a Resilience-Based, Network-Focused Port Security Grant Program," *Journal of Homeland Security and Emergency Management 10*(2013), 521-554.
26. Jie Xu, Jun Zhuang, and Zigeng Liu, "Modeling and Mitigation The Effect of Supply Chain Disruption in A Defender-Attacker Game," *Annals of Operations Research 236(*2015), 255-270.
27. Eric F. Taquechel, "Options and Challenges of a Resilience-Based, Network-Focused Port Security Grant Program," *Journal of Homeland Security and Emergency Management 10*(2013), 521-554.

28. Eric F. Taquechel, Ian Hollan, and Ted G. Lewis, "Measuring the Deterrence Value of Securing Maritime Supply Chains against WMD Transfer and Measuring Subsequent WMD Risk Reduction," *Homeland Security Affairs* 11, Article 1 (February 2015) https://www.hsaj.org/articles/1304 .
29. Richard Adler and Jeff Fuller, "Decision Support for Countering Terrorist Threats against Transportation Networks," *Journal of Strategic Studies 2*(2009), 43-64.
30. See Ted G. Lewis, *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation* (Hoboken, N.J: Wiley Interscience, 2006) for an explanation of how the Model-Based Risk Assessment (MBRA) tool simulates optimal allocations. Such a model would leverage an iterative algorithm to achieve an objective function. One objective function for this research is to minimize WMD transfer risk given a limited WMD detection technology budget. This iterative algorithm would leverage the concept of emergence. This means that our model would move user-specified proportions of available budget between domestic port nodes at random, with the goal of minimizing WMD transfer risk. The model would then continue this random allocation until moving money from any domestic port node to any other domestic port node would reduce WMD transfer risk no further. Thus, the minimization of network risk emerges, resulting in an equilibrium of optimally-allocated WMD detection investment. Once an equilibrium emerges from the simulation, we can determine the resulting minimized WMD transfer risk. The advantage of this algorithm for a large network is that formal mathematical optimization is not necessary to approximate optimal allocations to each node. Formal optimization becomes unwieldy for larger supply chain networks with logic gate proxies for links.
31. Eric F. Taquechel, Ian Hollan, and Ted G. Lewis, "Measuring the Deterrence Value of Securing Maritime Supply Chains against WMD Transfer and Measuring Subsequent WMD Risk Reduction," *Homeland Security Affairs Journal* 11, Article 1 (February 2015) https://www.hsaj.org/articles/1304 .
32. Eric F. Taquechel and Ted G. Lewis, "How to Quantify Deterrence and Reduce Critical Infrastructure Risk," *Homeland Security Affairs* 8, Article 12, (August 2012) https://www.hsaj.org/articles/226 .
33. Ibid.
34. U. S. Department of Homeland Security, *DHS Risk Lexicon*, 2010, https://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf .
35. Eric F. Taquechel and Ted G. Lewis, "How to Quantify Deterrence and Reduce Critical Infrastructure Risk," *Homeland Security Affairs* 8, Article 12, (August 2012) https://www.hsaj.org/articles/226 .
36. We treat intent as a function of expected utility from detonation, not just MTS exploitation. Therefore, intent ratios include both probability of exploitation and consequence of exploitation.
37. Eric F. Taquechel and Ted G. Lewis, "How to Quantify Deterrence and Reduce Critical Infrastructure Risk," *Homeland Security Affairs* 8, Article 12, (August 2012) https://www.hsaj.org/articles/226 .
38. Martin J. Osborne and Ariel Rubenstein, *A Course in Game Theory* (Cambridge: MIT Press, 1994).
39. Eric F. Taquechel and Ted G. Lewis, "More Options for Quantifying Deterrence and Reducing Critical Infrastructure Risk: Cognitive Biases," *Homeland Security Affairs* 12, Article 3, (September 2016) https://www.hsaj.org/articles/12007 .
40. Eric F. Taquechel, Ian Hollan, and Ted G. Lewis, "Measuring the Deterrence Value of Securing Maritime Supply Chains against WMD Transfer and Measuring Subsequent WMD Risk Reduction," *Homeland Security Affairs Journal* 11, Article 1 (February 2015) https://www.hsaj.org/articles/1304 .
41. Mikhael Shor, "Simultaneous Game," Dictionary of Game Theory Terms. Game Theory.net. http://www.gametheory.net/dictionary/SimultaneousGame.html .
42. Ibid.
43. Mikhael Shor, "Dominated Strategy," Dictionary of Game Theory Terms, Game Theory.net. http://www.gametheory.net/dictionary/DominatedStrategy.html .
44. Eric F. Taquechel and Ted G. Lewis, "More Options for Quantifying Deterrence and Reducing Critical Infrastructure Risk: Cognitive Biases," *Homeland Security Affairs* 12, Article 3 (September 2016) https://www.hsaj.org/articles/12007 .
45. Eric Rasmussen, "Mixed and Continuous Strategies," 2015, www.rasmusen.org/GI/chapters/chap03_mixed.pdf.
46. Branislav L. Slantchev, "Game Theory: Dominance, Nash Equilibrium, Symmetry," http://slantchev.ucsd.edu/courses/gt/04-strategic-form.pdf .
47. Eric F. Taquechel, "Options and Challenges of a Resilience-Based, Network-Focused Port Security Grant Program," *Journal of Homeland Security and Emergency Management 10*(2013), 521-554.
48. Ibid.
49. U. S. Department of Homeland Security, *DHS Risk Lexicon*, 2010, https://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf .
50. Eric F. Taquechel, "Options and Challenges of a Resilience-Based, Network-Focused Port Security Grant Program," *Journal of Homeland Security and Emergency Management 10*(2013), 521-554.
51. Ted G. Lewis, *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation* (Hoboken, N.J: Wiley Interscience, 2006).

52. Eduardo G. Quijano, David R. Insua, and Javier Cano, "Critical Networked Infrastructure Protection from Adversaries," *Reliability Engineering and System Safety 179*(2018), 27-36.
53. Vicki M. Bier and Fuat Kosanoglu, "Target-Oriented Utility Theory for Modeling the Deterrent Effects of Counterterrorism," *Reliability Engineering and System Safety 136*(2015), 35-46.
54. Eduardo G. Quijano, David R. Insua, and Javier Cano, "Critical Networked Infrastructure Protection from Adversaries," *Reliability Engineering and System Safety 179*(2018), 27-36.
55. Jie Xu, Jun Zhuang, and Zigeng Liu, "Modeling and Mitigation the Effect of Supply Chain Disruption in a Defender-Attacker Game," *Annals of Operations Research 236(*2015), 255-270.
56. Eric F. Taquechel and Ted G. Lewis, "A Right-Brained Approach to Critical Infrastructure Protection Theory in Support of Strategy and Education: Deterrence, Networks, Resilience, and "Antifragility," *Homeland Security Affairs* 13, Article 8 (October 2017) https://www.hsaj.org/articles/14087.
57. Eric F. Taquechel and Ted G. Lewis, "More Options for Quantifying Deterrence and Reducing Critical Infrastructure Risk: Cognitive Biases," *Homeland Security Affairs* 12, Article 3 (September 2016) https://www.hsaj.org/articles/12007 .
58. Craig Uhl and William Fiore, "Privacy Impact Assessment for the Radiation Detection Systems," 2016, https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp-rds-july2016.pdf .
59. Eric F. Taquechel and Ted G. Lewis, "More Options for Quantifying Deterrence and Reducing Critical Infrastructure Risk: Cognitive Biases," *Homeland Security Affairs* 12, Article 3 (September 2016) https://www.hsaj.org/articles/12007 .
60. Eric F. Taquechel and Marina Saitgalina, "Risk-Based Performance Metrics for Critical Infrastructure Protection? A Framework for Research and Analysis," *Homeland Security Affairs* 14, Article 8 (December 2018) https://www.hsaj.org/articles/14699 .
61. Ibid.
62. Ibid.
63. Eric F. Taquechel and Ted G. Lewis, "How to Quantify Deterrence and Reduce Critical Infrastructure Risk," *Homeland Security Affairs* 8, Article 12, (August 2012) https://www.hsaj.org/articles/226 .
64. Eric F. Taquechel and Marina Saitgalina, "Risk-Based Performance Metrics for Critical Infrastructure Protection? A Framework for Research and Analysis," *Homeland Security Affairs* 14, Article 8 (December 2018) https://www.hsaj.org/articles/14699 .

Copyright