



**Calhoun: The NPS Institutional Archive**  
**DSpace Repository**

---

NPS Scholarship

Publications

---

2010-12

# Mathematical Modeling Applied to Maritime Security

Center for Homeland Defense and Security

Monterey, CA; Naval Postgraduate School

---

<https://hdl.handle.net/10945/51119>

---

This publication is a work of the U.S. Government as defined in Title 17, United States Code, Section 101. Copyright protection is not available for this work in the United States.

*Downloaded from NPS Archive: Calhoun*



Calhoun is the Naval Postgraduate School's public access digital repository for research materials and institutional publications created by the NPS community. Calhoun is named for Professor of Mathematics Guy K. Calhoun, NPS's first appointed -- and published -- scholarly author.

**Dudley Knox Library / Naval Postgraduate School**  
**411 Dyer Road / 1 University Circle**  
**Monterey, California USA 93943**

<http://www.nps.edu/library>

# Mathematical Modeling Applied to Maritime Security

 [chds.us/c/item/292](http://chds.us/c/item/292)

[Download the paper: "Layered Defense: Modeling Terrorist Transfer Threat Networks and Optimizing Network Risk Reduction"](#)

Students in Ted Lewis' Critical Infrastructure Protection course are taught how mathematic modeling can provide better a foundation for making important decisions about protecting the nation's infrastructure assets.

CHDS alumnus Eric Taquechel modified that model to address maritime security. Taquechel conducts maritime terrorism security risk assessment, analysis, and management. Taquechel authored a paper that was published in the November/December 2010 edition of IEEE Network, titled "Layered Defense: Modeling Terrorist Transfer Threat Networks and Optimizing Network Risk Reduction."

1. This article explains how a modification of Lewis' Model Based Risk Assessment (MBRA) model can show where to effectively invest limited resources to optimize network risk reduction against the "terrorist transfer threat." The transfer threat means illicit people and/or weapons/components that originate overseas, travel through foreign ports and move through the global maritime commons and enter the United States via domestic ports. The article explains how to use network science, which analyzes connections/relationships between different components of a system, to think about this problem. It also leverages mathematical optimization techniques and a variation on a traditional technical approach to reliability engineering to account for the realities of the US's layered defenses against the transfer threat, and to show where to invest limited resources for maximum system risk reduction and/or return on investment. The reality of the United State's layered defense is that most "nodes" in the global maritime security network generally have some inherent security. For example, certain foreign ports generally adhere to the International Ship and Port Facility Security Code (ISPS), as do certain foreign vessels entering the US, plus many U.S. port facilities adhere to the Maritime Transportation Security Act (MTSA). These laws/codes are enforced by various authorities, reducing vulnerability to exploitation and reducing risk of transfer threat. The key to Taquechel's approach is that if one has to negotiate a first obstacle to get to a second, negotiating the second obstacle is naturally more difficult – it is an "inherited" challenge. But, how inherently or "organically" robust the first obstacle is will also influence the eventual probability of negotiating the second, as will the second's inherent or "organic" robustness. So, you combine these two "inherited" and "organic" security factors to figure out maritime defense network risk and optimal risk reduction solutions. Decision makers can also do suboptimal solutions, which may reduce system risk less but have better return on investment than optimal solutions.
2. The proposed approach could help think about how much risk to domestic critical infrastructures the United State's layered defenses reduce at different points within its defense network, and how much it costs to maintain that level of risk reduction. The tool discussed in the article, using notional data, showed that different investments in different "layers" of layered defense yield different risk reduction and return on investment results. Risk reduction from a systems perspective is important, given the nation's layered defense philosophy. Return on investment is always important, and especially so in the current budget climate, Taquechel adds.
3. Taquechel learned network theory from Lewis' 2006 book and the CHDS master's Critical Infrastructure Protection course. He was concurrently working on a project to analyze transfer threat at his job. So, Taquechel saw opportunities to apply Lewis' theories and practical tools (MBRA) to the transfer threat problem. Lewis agreed to modify MBRA to look at transfer threat analysis and also identified the special edition of IEEE magazine as a good fit for the type of article Taquechel wished to write. The article is minimally technical-intentionally so in the hopes of reaching a wide audience. One goal was to inform policy, in addition to contributing to the academic literature.

“I think this was a perfect example of how this program can contribute to the discourse on real world problems,” Taquechel said.

---

Associated file: [Layered Defense: Modeling Terrorist Transfer Threat Networks and Optimizing Network Risk Reduction](#)

[Copyright/Accessibility/Section 508](#)