News Center | News Articles Collection

2015-03

Alum and co-authors model and quantify efforts to deter WMD transfer through maritime supply chains

Center for Homeland Defense and Security
Naval Postgraduate School, Monterey, California

http://hdl.handle.net/10945/50959

Alum and co-authors model and quantify efforts to deter WMD transfer through maritime supply chains

Continuing research to help decision makers better safeguard critical infrastructure, master's alumnus Eric Taquechel, colleague Ian Hollan, and former CHDS Executive Director Ted Lewis recently published an article in support of risk management advancement in the February 2015 edition of the Journal of Homeland Security Affairs, "Measuring the Deterrence Value of Securing Maritime Supply Chains against WMD Transfer and Measuring Subsequent Risk Reduction."

The overall goal of this new research was to propose an approach to analyzing the risk of an adversary exploiting the maritime supply chain by using a container to transfer a WMD or parts thereof into the U.S. Conceptually, this work integrated detection technology effectiveness modeling with network theory, deterrence, game theory, reliability engineering, and risk analysis.

The authors proposed a way to model a supply chain composed of foreign ports, U.S. ports, and inland U.S. cities. They introduced the concept of "exploitation susceptibility" as a substitute for the classic quantitative estimate of "target vulnerability". This meant that the potential for a port to be exploited was quantified, rather than a port's vulnerability to direct attack. This was modeled as a function of WMD detection technology investments at those ports. The ratio of dollars invested in detection technology to the "optimal" investment to maximize detection probability at 95 percent influenced the actual modeled exploitation susceptibility, a nonlinear function of that ratio.

When combined with probability of encountering a WMD given one was shipped into a specific port, detection probability yielded an "organic exploitation susceptibility" reflecting probability of WMD transfer through that port. However, as discussed in previous work, the authors also incorporated the concept of inherited exploitation susceptibility, based on possible permutations of attacker "transfer pathways."

Logic gate principles were used to proxy attacker preferences for different combinations of foreign ports, US ports, and inland target cities. This put discussion of possible attacker tactics to move WMD into the US into quantitative terms. The assumption for this modeling approach was that an inland city would be the target of attack, meaning a truck or other non-maritime form of transportation would ship the WMD to its final destination.

Taquechel and co-authors also incorporated concepts from earlier work on quantifying deterrence effectiveness of defensive CIKR investments. In this case, they showed how to create equations representing risk of a WMD detonation in an inland U.S. city, given an adversary had to exploit some permutation of foreign ports and US ports to move the weapon. Those conditional risk equations were then converted to expected utility functions and used in a notional game theoretic scenario where defender courses of action included optimal investment in WMD technology, sub-optimal investment, or other options, and attacker courses of action included the various permutations of transfer pathway.

This game allowed the authors to glean proxies for attacker intent probabilities, allowing the measurement of deterrence and creating unconditional risk equations reflecting both attacker intent and transfer pathway overall exploitation susceptibility. When combined with estimated consequences from detonation, these terms produced risk equations and helped create a "WMD deterrence portfolio". This allowed the authors to measure how various investments in WMD detection technology might deter adversary exploitation of supply chains and estimate resulting WMD risk reduction.

Taquechel and colleagues applied their methodology in a case study using notional investments in WMD detection technology in U.S. ports to deter exploitation of the maritime supply chain, and presented findings and implications for CIKR risk practitioners.

One finding of the case study that applied the authors' methodology was that the best investment in WMD detection technology was against a specific transfer pathway that differed from what traditional attacker-defender modeling efforts might suggest. This was because the methodology did not necessarily rely on the equilibrium output of the deterrence game analyzed, but instead hedged against the possibility that an adversary might not consider an "optimal" transfer pathway to exploit.

As with previous work, the modeling approach leveraged capabilities from Lewis' Model Based Risk Assessment (MBRA) tool.

This methodology has potential implications for DHS programs – possibly the Global Nuclear Detection Architecture sponsored by the Domestic Nuclear Detection Office. It might inform efforts to find and use the best possible WMD detection equipment. Another practical implication of this research was that intelligence collection and analysis efforts might focus on attacker preferences for exploiting various US ports of debarkation. This could inform decisions on how to invest in WMD detection technology, accounting for foreign port exploitation preferences.

Overall this work laid a foundation for offering an alternative to a claim made in the Maritime Commerce Security Plan: that inspecting containers for WMD once they arrive in US ports is too late. The authors suggested that this is not necessarily true if the target is an inland city.

"Our goal was to take ideas from previous work and synthesize them into a new framework to help think about the WMD threat" said Taquechel. "Ted, Ian and I enjoyed this research effort and we hope it can prove valuable to the Homeland Security and Emergency Management enterprise. Even several years after leaving CHDS, I am finding ways to use that education to good effect."