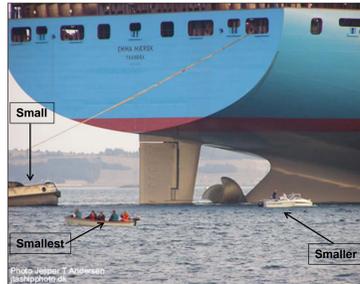


Overview

With the attack on USS Cole in 2000, small vessel security has become an anticipated part of US navy and homeland security. U.S. ports are especially vulnerable to potential exploitation by terrorists, smugglers of weapons of mass destruction (WMDs), narcotics, contraband, and criminal elements. Our research task focused on applying systems thinking to develop a small vessel security and resilience strategy for six identified threat scenarios for the Port of NY and NJ incorporating technological and organizational elements.



Methodology

To address that the small vessel security system is a highly complex and interconnected network of systems, we utilized a conceptual modeling tool known as a Systemigram. The Systemigram is used to represent an overarching image of the small vessel security system, displaying its main components and their interactions while approaching the system's objective, which is to achieve higher levels of security and resilience. In addition, we performed a live crisis simulation exercise to model what would occur if there was a threat of a WBIED on a cruise ship in the Hudson River.

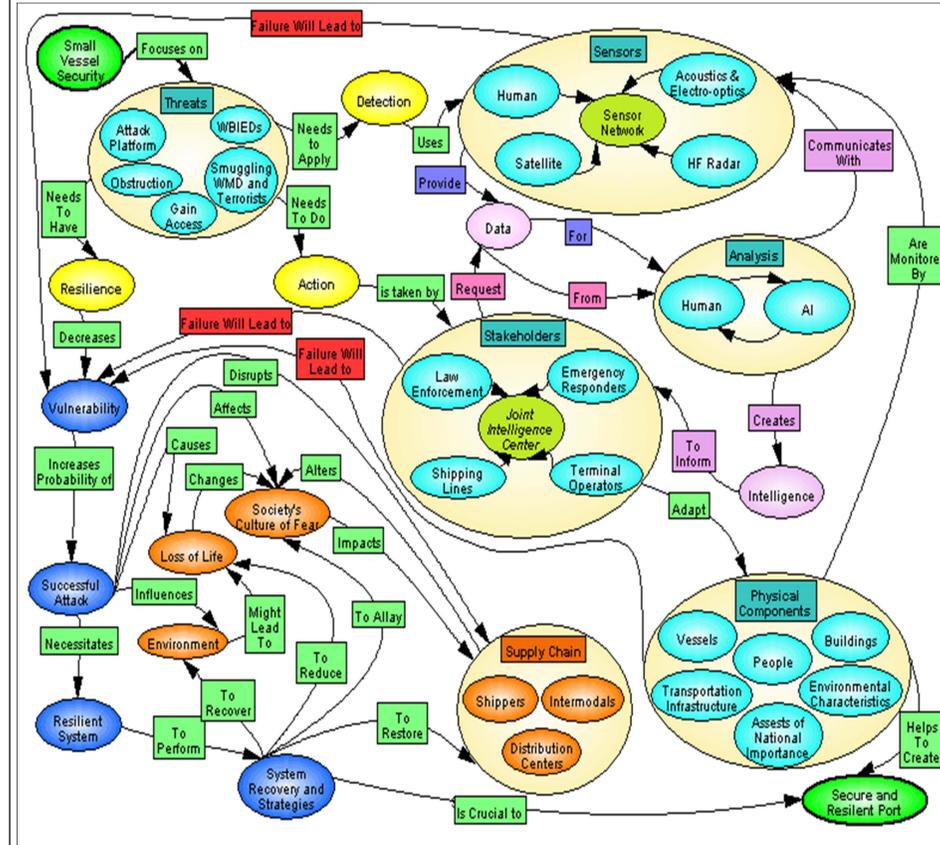


Detection Action Resilience (DAR) strategy

The primary challenge in using technological detection methods is to create an over-arching strategy that can be applied to a variety of different scenarios. Technological detection systems are however, nothing without the first line of any coherent defense system; its citizens. Civilians form the first line of defense as the zeroth responders in situations that involve the safety of the port. They figure heavily in the overall Detection strategy in concert with the four technologies explored at the 2010 SRI.

The overall Action strategy focuses on exploiting artificial intelligence to create a dossier of "normal" environmental situations to identify and address abnormal situations as they may arise. In addition, public/private partnerships form the key to timely and cogent response activities. Because of the sensitivity of the local region to disruptions in trade, our overall resilience strategy for the Port Authority of New York and New Jersey (PANYNJ) focused on addressing business continuity issues for private and public organizations.

Systemigram



Crisis simulation

To test the systems concepts and strategies developed over the course of eight weeks of research Systems team organized and carried out a crisis simulation exercise. The crisis simulation enabled the four groups to display their command of the technological systems and for the Systems team, the complex interconnections that are set in motion once a crisis occurs.

The simulation modeled what would occur if there was a threat of a WBIED on a cruise ship in the Hudson River. Two detection teams (HF Radar and Acoustics) participated in the live-action portion of the simulation. Systems and Satellites teams created multimedia presentations beforehand, primarily in the form of videos detailing stakeholder's role during this scenario.

Two small vessels were sent to a pre-determined point west of SIT and HF Radar and Acoustics teams were challenged, in real-time, to identify the speed, bearing and size of the vessels. A number of crucial issues were brought to light as the performance of the two technological detection teams was monitored by the Systems team.



MV Limburg after a small vessel attack
 Source: <http://www.royalnavy.mod.uk/>

Lessons learned

- Both groups were able to detect abnormal movements by the two dummy vessels.
- Due to the timing of the simulation (12 noon) few other vessels were on the water. During rush hour in NY harbor, ferries and other small vessels would complicate detection of small vessels.
- The speed of a small vessel makes it very difficult for interceptors to reach them before an incident occurs. It is crucial to have an integrated communication network, incorporating detection teams and public and private actors who may be targeted.
- Finally, detection groups can only at best provide information that suspicious activity is occurring. The impetus is on cognitively designed systems to funnel that information and conclude that dangerous activity may be imminent. Law enforcement must at this point take control of the situation.

References

Boardman, John, and Sauser, Brian. *Systems Thinking Coping with 21st Century Problems*. (CRC Press 2008)
 DHS, *DHS' Strategy and Plans to Counter Small Vessel Threats Need Improvement*, OIG-09-100 (Washington D.C., 2009)
 DHS, *Small Vessel Security Strategy* (Washington, D.C. April 2008)
 GAO, *Maritime Security: Vessel Tracking Systems Provide Key Information, but the Need for Duplicate Data Should Be Reviewed*, GAO-09-337 (Washington, D.C., March 17, 2009)
 GAO, *Maritime Security: Varied Actions Taken to Enhance Cruise Ship Security, but Some Concerns Remain*, GAO-10-400 (Washington, D.C. April 2010)

Acknowledgment

This project was funded through the Center for Secure and Resilient maritime commerce (CSR) by a grant from the Department of Homeland Security, Science and Technology Directorate, Office of University Programs. We'd like to extend our thanks to Dr. Ali Mostashari, Dr. Brian Sauser, Dr. Thomas Wakeman and, especially, Beth Austin DeFares for her indefatigable efforts. Finally, we extend our thanks to the Stevens Institute of Technology for the opportunity to bring together disparate minds to collaborate on maritime and port security.

For further information

For more about this research please contact Leonid Lantsman (llantsman@jjay.cuny.edu) at John Jay College of Criminal Justice or Hardik Gajjar (hardikmgajjar@gmail.com) at Stevens Institute of Technology.