OVERVIEW

- Introduction
- Systemigram
- Detection
- Action
- Resilience
- Crisis Simulation
- Conclusion
PROBLEM STATEMENT

- Small Boats......How small is too small???
MARITIME TRANSPORTATION SYSTEM

- Small Boats......How small is too small?
- What are the Components?
- What region?
- How do we do this?
THREAT SCENARIOS

- Small Vessel used as:
  - Water Borne Improvised Explosive Device (WBIEDs)
  - Smuggling Terrorist
  - Smuggling Weapons (can be CBRNE)
  - Small boat as an attack platform
  - Obstruction
  - Gain access to large
PROBLEM STATEMENT

- What is the applicability of systems thinking to the development of a small vessel security and resilience strategy for six identified threat scenarios for the Port of NY & NJ through the incorporation and synthesis of technological and organizational elements?
SYSTEMS APPROACH TO AN ATTACK

Detection → Preventive Action → Resilience

PROACTIVE  REACTIVE
OVERALL DETECTION STRATEGIES
OVERALL DETECTION STRATEGY

- Covers the six scenarios identified in the beginning of the summer research
- Prepares the system to expect different scenarios
- Decreases the overall vulnerabilities
CITIZENS IN THE DETECTION SYSTEM

- The first line of defense in a coherent technological system are the citizens.
- They are the first responders in situations that involve the safety of the port.
- They are best able to judge whether activity in their marinas, near critical land structures, and in their home port is suspicious.
SATellite

- The satellite system faces limitations that prevent it from being extremely useful in real-time small vessel detection.
- The satellites used during this research can detect vessels larger than 10m and wakes created by small vessels.
- Based on these limitations we decide that the satellite are not convenient in the pre-attack section.
- Satellite are useful in pattern recognition.
HF RADAR

- Are very useful to detect vessel's distance and velocity.
- Gives real time data, allowing the proper agencies to take action on the situation before it occurs.
- This technology is the first real-time technological line of defense.
ACOUSTIC AND ELECTRO-OPTICS

- Using passive acoustics technology, we will detect any object that emits sound under water.
- In this recommended detection strategy data processors rely on a collection of previously recognized motor sound signatures, to better identify the size and speed of the vessel in question.
ACOUSTIC AND ELECTRO-OPTICS

- Electro-optic technologies, such as infrared imaging, play an enormous role in night surveillance and are accurate in sensing otherwise undetectable small vessels, namely kayaks.
VIDEO SURVEILLANCE

- CCTV network is used in London and New York for city surveillance
- Use of private camera feeds
- Similar network can be created for coast-wide surveillance
- Boat ramps, Marinas, Buoys, Bridge Piers, etc.
SYSTEM DETECTION

- HF radar system to provide longer range detection of vessel speed.
- Use of ship borne radar to augment detection capabilities
- Bearing and intensity is given by acoustic.
- IR technologies provide that crucial near-range detection capability.
WBIED

- The most likely targets will be cruise ships and cargo ships.
- The best detection for these situation will be the citizens and workers near coastal area.
- HF radar and acoustics will be very useful in tracking the vessel’s path.
SMUGGLING TERRORISTS/WEAPONS

▪ Smuggling groups will try to reach remote areas and avoid security patrols.
▪ Satellite images will give us the warning of any uncommon path around the coast.
▪ Constant patrols and citizen vigilance will be the better method of detection.
VESSEL AS OBSTRUCTION

- Satellite will play a tremendous role pinpointing the exact location of the obstruction.
- Give information for alternative routes for shipping lines to continue with their operations.
GAIN CONTROL OF A LARGER VESSEL

- Human intelligence is essential in preventing this situation.
- In terms of technologies HF radar and acoustics can track any vessels near the larger vessels and under water threats.
RECOMMENDATIONS ON DETECTION

- General public seminar to learn to notice suspicious activities.
- Report all suspicious activities to one specific well-know agency.
- Research in plotting data on a more visible way, like google earth. This will allow us to track the vessels more easily.
OVERALL ACTION STRATEGY
SCENARIOS

- Using a small vessel
  - As a WBIED
  - To smuggle terrorists
  - To smuggle weapons of mass destruction
  - As an obstruction
  - As an attack platform
  - To gain access to a larger vessel
SIMILARITIES BETWEEN SCENARIOS

- The way the scenarios are carried out
  - The vessels used for each scenario
  - The behavior of vessels when approaching a target
  - Behavior of vessels when smuggling persons or WMD’s
SIMILARITIES BETWEEN SCENARIOS

- After effects
  - Loss of life
  - Environmental Damage
  - Psychological Impact
  - Disruption in Ship Movement
  - Impact on Tourist Activity
  - Economic Impact
WBIED

- Most likely target would be of high value
  + High loss of life
  + High economic loss
- Action to be taken:
  + Civilians report suspicious behavior
  + Law enforcement narrow down on suspects
    ✗ Use HF Radar-Velocity
    ✗ Electro Optics- Night Visuals
    ✗ CCTV-Surveillance of suspects path
- Recommendations: Use waterborne barriers
SMUGGLE TERRORISTS/ WEAPONS

- Behavior associated with these scenarios creates difficulties for detection and therefore an added difficulty for action strategies
- Action to be taken:
  + Civilians notice suspicious vessel and report to authorities
  + Authorities of area where report was made share information with surrounding areas
  + Acoustics and electro optics used to pinpoint location of vessel
- Recommendations: Can not be planned for
OBSTRUCTION

▪ Most likely targets: Shipping channels and areas of high vessel traffic
  + Psychological impact
  + Economic Impact

▪ Action to be taken:
  + Satellites
    ✗ Pinpoint location of vessel
    ✗ Updated information for alternative routes for shipping lines

▪ Recommendations:
  + Salvaging companies and tug operators to move vessels
  + Waterborne barriers
ATTACK PLATFORM

- The only time you know when a vessel is being used as an attack platform is once it has already fired a weapon from the vessel.
- Most likely targets: expensive and critical real estate around the port area.
- Actions to be taken:
  - Civilians report suspicious activity.
  - Video surveillance of area to keep track of the vessel.
- Recommendations:
  - Targets are on land so involve land based law enforcement.
  - Departments that traditionally don’t deal with maritime matters but have an action plan for an attack platform scenario.
GAINING ACCESS TO A LARGER VESSEL

- Most likely target: Any large vessel
- Action to be taken:
  + HF Radar system and acoustics should be used to find the exact location of the small vessel
- Recommendations:
  + The large vessel should have it’s own action plan
    ✗ Captain should have
    ✤ entryways into the cabins locked
    ✤ crew stand watch to look for suspicious approaching vessels
    ✤ water cannons ready to be operated
FORMS OF DETECTION

- Vigilant Civilians
- HF Radar
- Acoustics and Electro Optics
- Satellites (pattern recognition and post attack clean up)
RESPONSE

- Crime Scene – Owner (Insurance)
- Oil and Debris – Clean-up Issue
- Water – Land Operation (Jurisdiction)
- Ship Salvage – Navy
- Contract to move ship
- Business Continuity Plan
JURISDICTION

Water
- COTP
  - ICC
    - Fed.
    - State
    - Local
    - Owner

Land
- Mayor
- Governor
- Federal
  - Guard
  - FEMA
OVERALL RESILIENCE STRATEGIES
RESILIENCE

- The ability of a system to bounce back to a baseline state after being disrupted by a shock

- Examples in Maritime Systems:
  - Transportation System
  - Economic Flow
RESILIENCE STRATEGIES

- Reduce the probability of an attack to the system
- Minimize the bounce back period of time the system needs to recover from an attack
Actors

Federal
- Dept. of Homeland Security
- Dept. of Justice
- Central Intelligence Agency
- Dept. of Transportation
- Dept. of Environmental Conservation

State
- Office of Cyber Security and Critical Infrastructure
- Office of Public Security
- Emergency Management Office
- State Police Dept.

Bi-State
- Port Authority Police Dept.
- Two State Police Depts.
- Harbor Waterfront Police

City
- Office of Emergency Management
- City Police Dept.
- City Fire Dept.
- City Dept of Health and Mental Hygiene
- City Dept of Environmental Protection

Private
- American Waterways Operators
- Global Shipping Firms
- Railroad/Trucking Firms
- User Commercial Firms

Andalibi, N., Architecting Cognitive Port Processes. Unpublished Manuscript
ENVIRONMENTAL CLEAN UP

- Vessel Obstruction
- Gain Control of Large Vessel
- WBIED Attack
  - Vessel Used as Attack Platform
  - Remove Hazardous Waste and Debris from Water
  - Response Army Corps. of Engineers
  - Universal Sign Signaling the Restriction of Boats
  - Impedance or Stoppage of Flow and Commerce in Port
    - Initiation of Business Continuity Plan
      - Maintaining Public and Private Trust
      - COTP Ensures Maritime Control
  - Future Shipments Notified
    - Important Cargo Waits At Anchorage
      - Plan for New Berthing Schedule
    - Goods Rerouted to Nearby Ports
INCAPACITATED SHIP

- Vessel as an Obstruction
- Gain Control of Larger Vessel
- WBIED Attacks
- Vessel used as an Attack Platform
- Move ship to Anchorage
- Navy Lack of Resources for Salvaging
- Database of Ship Salvaging Companies
- Moving Ship to Anchorage (Cranes, Floating Dry Docks, Tugs)
- Impedance/Stoppage of Flow and Commerce in Port
INLAND TARGET ATTACK

- Vessel used as an Attack Platform.
- Inland Target Hit
- Block Off Area.
- Reroute Ships In Harbor.
- Impedance/Stoppage of Flow and Commerce in Port.

- Emergency Management and Law Enforcement Collaboration
- Miscommunication and Coordination Amongst Actors and Overlapping Jurisdictions
- Evacuation and Urgent Medical Care

- Knowledge Sharing Programs and Network Interface
- Professional Education Program
- Drills, and Simulations
TERRORIST ACTIVITY

- Smuggling Terrorists/Weapons
- Identification of Terrorists Activity and Location
- Profiling and Information Sharing
- Maritime Security Intelligence Collaboration
- Integration of Universal Knowledge
- Terrorist Tracking Database for Federal agencies and Private Stakeholders
- Track Terrorists Stoppage at Entrance to Port
- Presents a threat to Citizens or Traffic in Port
- Impedance or Stoppage of Flow and Commerce in the Port
MONDAY JULY 26 CRISIS SIMULATION
GOALS

- Create a dynamic detection scenario
- Bring together the four SRI groups and demonstrate their capabilities to group representatives and faculty
- Identify the gaps still remaining
- Identify what the next Summer Research Institute should focus on
DESCRIPTION

- Two vessels R/V Savitsky and 21-foot rubber fast boat
- R/V Savitsky had a north to south route
- Fast boat proceeded south to north
- Target was the Carnival Glory cruise ship, represented by the Stevens buoy
- Four groups present at 1200 MSL
- Babbio
- Both vessels present at their waiting places at 1200

Map of Monday July 26 Crisis Simulation

1200-1215: Pre-attack systems presentation

1215-1230: Real-time detection period
Concurrent systems presentations

1230: WBIED hits Carnival Glory

1230-1240: Post-attack systems presentations
PRE-ATTACK 1200-1215

- 1200- Detection groups were presented with introductory videos
  - Civilian dock workers
  - NJSP-USCG
  - COTP
  - COTS

ATTACK 1215-1230

- Intelligence analyst ➔ Provided crucial information for the assembled groups
  + Mistaken information

- R/V Savitsky and rubber fast boat began to move towards the target

- Acoustics and HF Radar began to search for suspicious vessels
SYSTEMS PRESENTATIONS DURING ATTACK

- Satellite Role in pre-attack period and response period
- COTP - MARSEC Level 1 → 2
- COTP - Mayor-Interagency tensions
- COTS - Evasive actions taken by Carnival Glory
WBIED HITS CRUISE SHIP
POST-ATTACK (1230-1240)

- Breaking Newscast
  + Fear
  + Economic Damages
- COTP- MARSEC 3
- Terminal Operator Perspective
OEM RESILIENCE STRATEGIES

- Coordinate with NJ OEM to do the followings:
  + Emergency responders access to the site
  + Extinguishing the fire aboard the ship
- Injured passengers care and transport
- Transportation system management:
  + Shutting off the ferries / subways
  + Rerouting the ships and cruises coming into the harbor or keeping them waiting
- Notify the ships that will be coming into the harbor of the security issue
- Public information broadcast to let people know the area is not safe
LESSONS LEARNED

- Detection groups were able to detect vessels right away (particularly R/V Savitsky)
- Limitations were overcome through cooperation
LESSONS LEARNED (CONT.)

- Hard to determine what is nefarious activity
- Crucial need for inter-group communication
- Need for better integration of detection systems
  + Include ship radar systems in an overall detection network
  + Private CCTV can be used to keep the harbor under watch
- Conclusion ➔ Without direct law enforcement involvement detection is moot
CONCLUSION

- Six scenarios (DHS/self-identified)
- Tools/Methodology
  + Systemigram
  + Flow Diagrams
- DARs
  + Overall
  + Scenario specific
- Simulation
OVERALL DETECTION

- Civilians
  - Most familiar with port environment
  - Includes terminal, transportation and vessel operators
  - Need to work on public/private partnerships
  - Marine security education programs
    - Safe boating
    - Noticing suspicious activity
OVERALL DETECTION

- **Satellites**
  - Vessel as an obstruction

- **HF Radar**
  - Tracking WBIEDs, vessels used as an attack platform, and vessels gaining access to larger ship
  - Surface current/vessel velocity

- **Acoustics/Electro-Optics**
  - Tracking vessels that are smuggling weapons/terrorists, especially those occurring at night or underwater
OVERALL ACTION

- MTS consists of:
  - Technology operators
  - Balance between human and AI
    - Basis of cognition
  - Jurisdictional issues
  - Clean up issues
OVERALL RESILIENCE

- Immediate response effort flow diagrams
  + Educating first responders to attacks
  + Minimize loss of life
  + Minimize economic damage using business continuity plans
  + Clean up efforts
SIMULATION

- Detection was successful
- Cooperation is key
  + Between detection groups
  + Law enforcement
- Recommendations
  + Create a ‘safe area’ using multi-layered defense system comprised of detection technologies and preferential law enforcement
FUTURE RESEARCH

- Though this was just a preliminary study, these findings provide the basis for future research in the field of maritime domain awareness.
QUANTIFYING THE THREAT

Examples of Probabilities:

\[ P(x=a) = \frac{B-A}{B} \]

\[ P(A \mid B) = \frac{P(A \cap B)}{P(B)} \]