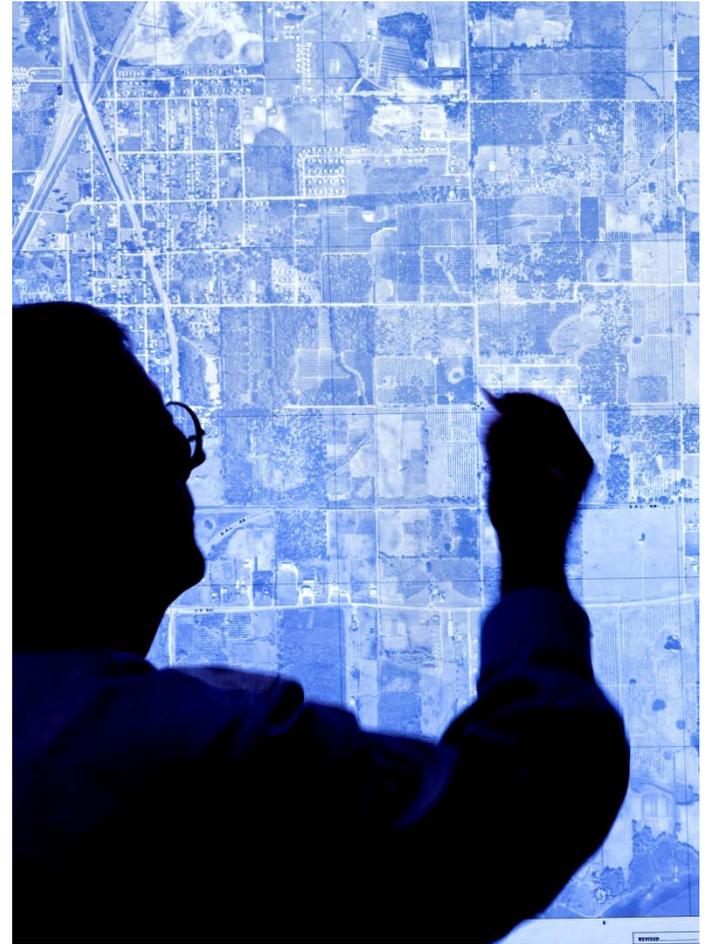


Seaborne Attack Impact at Transportation, Energy, and Communication Systems Convergence Points in Inland Waters

*Challenges & Innovations
in Risk Assessment for the
Homeland Security Enterprise –
A Panel Discussion*



Washington, DC
April 1st, 2011

Douglas E. Himberger, Ph.D.

Convergence of transportation, energy, and communication systems

provides terrorists with targets accessible by recreational watercraft. Previous similar events suggest interest in this attack vector and obtaining and operating small boats is simpler than for other vehicles.

Using **open source materials**, a potential terrorist could identify infrastructure overlaps where attacks using small quantities of explosives would create chaos and lead to substantial damage.

Studies of seaborne attacks have been conducted by the Coast Guard and others, however, **inland waters have limited security, and critical points are often at federal, local, and state jurisdictional boundaries.**

Risk assessments are needed for these areas, as are incident response and continuity of operations plans. We suggest advanced search capabilities to identify and specify elements at risk (including physical and jurisdictional geo-location techniques to catalog potential targets using prioritized methodologies), and a **focus on consequences**, including capability loss as well as environmental impact.

Inland waterway convergence points of energy, communications, and transportation infrastructure present high-risk terrorism targets.

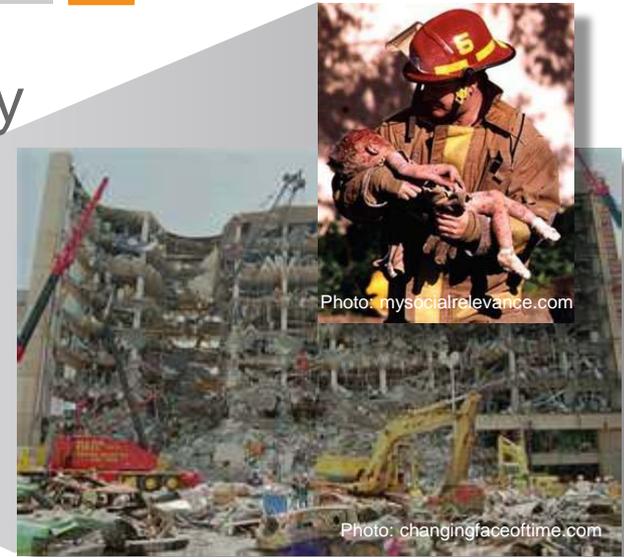
Key Questions:

- What are the **vulnerabilities of intersections** of multiple infrastructures and multiple jurisdictional boundaries to this attack vector?
- What are the **consequence elements of risk** for these infrastructure convergence points?



Background – A History of the Threat

- Could explosives made from commonly acquired materials (e.g., ammonium nitrate) cause significant damage?
 - Oklahoma City, 1995
- Could these materials be transported more easily and in greater quantities by waterways than by ground?
 - Texas City, 1947



The threat is significant

Background – A History of the Threat (continued)

- Do waterways provide unrestricted access to key targets?
 - USS Cole, 2002

**The threat
is mobile
and lethal**



Context – The Threat Going Forward

- Are the convergent point targets:
 - Real and easily identified?
 - Appealing to the threat?
- Consider Chicago, IL
 - ~3 million residents
 - Dense city center
 - Multiple resources/infrastructures

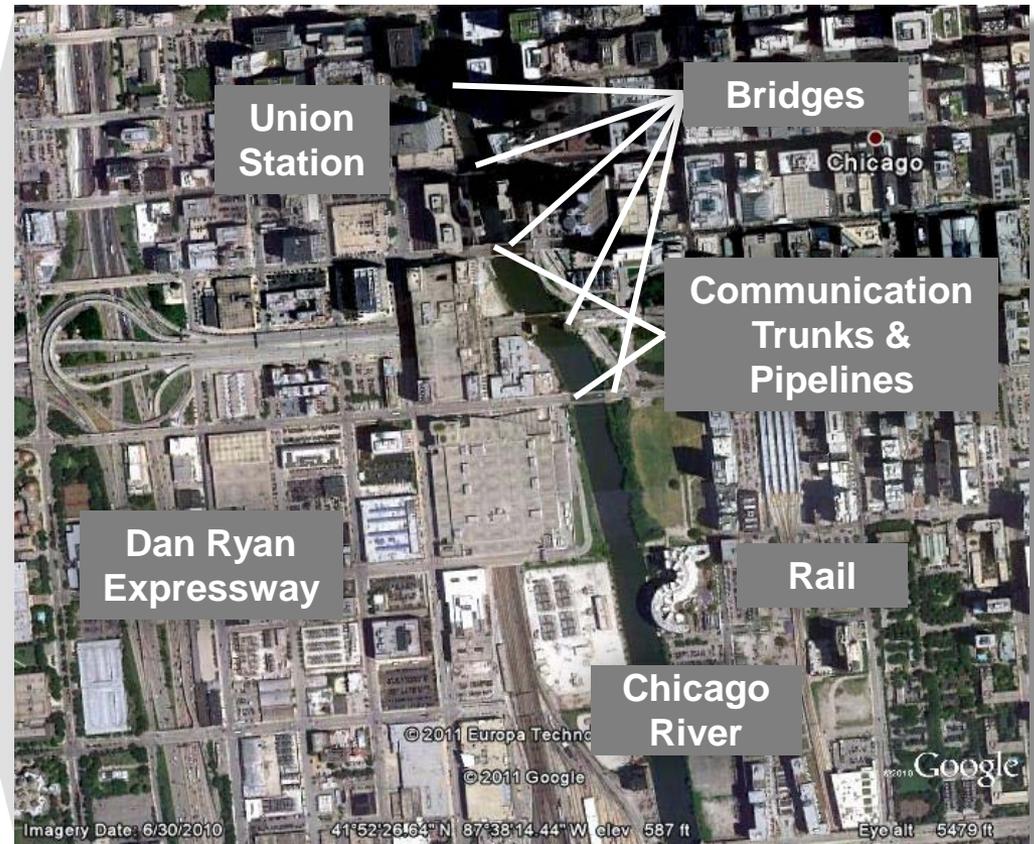
**The target
is appealing
to the threat**



Context – The Threat Going Forward (continued)

- Are the convergent points themselves:
 - Easily reached?
 - In close proximity to one another and do they contain key infrastructures?
- Consider the Chicago River
 - Multiple key infrastructures

**The target
is irresistible
to the threat**



Context – The Threat Going Forward (continued)

- Are there critical convergent points:

- That contain multiple key infrastructures at a single point?

- Consider the Van Buren Street bridge

- Transportation (road, water)
- Energy (oil pipeline)
- Communications (fiber optic)

**The targets
are likely threat
vectors**



Context – The Threat Going Forward (continued)

- Are the targets at the intersection of jurisdictions?
- Consider the complexities of Chicago

The problem is more complex than imagined



[Note: Jurisdictions are notional]

The Way Ahead – Assessing Risk ... and Consequence

- **Assessing risk** involves:

- **Identification** of potential targets
- **Categorization** of targets using:

- **Threat** – “the relative exposure to an attack” (T)
- **Vulnerability** – “the likelihood of an attack occurring” (V)
- **Consequence** – “the expected impact of an attack” (C)

$$\text{Risk} = (T) \times (V) \times (C)$$

- We will focus on the consequence element of risk:

- Draw on concepts and models from **various disciplines** (engineering, social sciences, law, etc.)
- Quantify **specific impact factors** (denial of service, environmental, societal, economic)
- Factor in **behavioral and jurisdictional elements**

*Sources: Fiscal Year 2010 Homeland Security Grant Program Guidance and Application Kit, DHS (2009)
The Department of Homeland Security's Risk Assessment Methodology: Evolution, Issues, and Options for Congress, Masse et al (2007)*

- Potential Solution & Research Methodology -
Overall Approach

- Researchers will use **advanced information search capabilities and state-of-the-art GIS techniques** for geo-location to identify and specify relevant elements (energy, transportation, and communication infrastructure) at risk on inland waterways. Both **physical and jurisdictional mapping** should be integrated into the mapping of target areas.
- Researchers will describe **consequences of possible attacks**, including loss or degradation of communications and transportation capabilities, as well as potential environmental impact.

To derive the greatest value from this study, **methodological inputs from various disciplines must be included**. Measures of risk often attempt to quantify variables which are qualitative in nature. A truly effective risk or consequence measurement methodology will **include measurements that are common to engineering, social sciences, law, and other related fields**.

The Way Ahead – Key Questions

(part 2)

- **Who are the targeted decision makers for the modeling and analysis?**
 - **Those tasked with the preparedness and response** with respect to this threat (e.g., DHS (Coast Guard, NPPD), EPA, state and local emergency planners).
- **Who are the customers and users (or ideal customers and users) who can implement the modeling and analysis in DHS or in the extended Homeland Security enterprise to support decision makers?**
 - **Key Federal end-users** including DHS & Enterprise customers (NPPD/Office of Bombing Prevention, Coast Guard/Directorate of Assessment, Integration & Risk Mgmt, NPPD/RMA) and even components such as Customs and Border Protection (CBP), and the Federal Emergency Management Agency (FEMA).
 - **State and local government**, including port authorities and waterway patrols, along with law enforcement, fire, and other first responders, including environmental response and cleanup personnel.
 - **Entities that have missions to co-locate and provide interoperability** to these various stakeholders – such as Emergency Operations Centers (EOCs), etc.
 - **Owners of the infrastructure** at risk (energy, telecom, etc.).

The Way Ahead – Key Questions

(part 2 continued)

- **What are the state of current practice and the limitations of current practice?**
 - By using **publicly available online tools** to locate possible attack vectors, we emulate the quality of research that could be done by potential terrorists. In assessing consequences of risk, we draw upon **inputs from various fields** to get a holistic picture of the damages that can occur from an attack on infrastructure convergence points.
 - **Resources are not currently in place to assess the outcomes** of a seaborne IED attack on the convergence of multiple infrastructures. This is due to budgetary and other constraints, including proximity of skills and specialized resources.
- **What is new in your modeling and analysis approach, and how does it help address limitations of current practice?**
 - **A comprehensive analysis should be achieved through a multidisciplinary approach**, drawing on the expertise of fields such as engineering, social sciences, law, emergency management, and other related fields.

The Way Ahead – Key Questions

(part 2 continued)

- **Why should DHS, extended Homeland Security technical practitioner community, and/or decision makers care about your modeling, analysis, findings, etc.?**
 - Our approach considers both **jurisdictional and operational overlaps**, while addressing the seaborne attack vector. The findings from such an assessment would provide a **prioritized matrix of consequences of inland waterway targets**, allowing customers to make informed choices about which targets are in need of additional protection and security.
 - Our approach will **shed light on the risks faced by multiple jurisdictions and agencies from a threat** that has yet to be realized in the United States. Currently, the **results of such an attack could be enormously damaging**, particularly given recent focus on mitigating other attack vectors (vehicle-borne IEDs, etc.).

The Way Ahead – Key Questions

(part 2 continued)

- Are there any technical or organizational challenges that still must be overcome for risk analysts in DHS or extended Homeland Security enterprise to implement and use your research?
 - **Shared right-of-way/jurisdiction** creates unique gaps that must be thoroughly catalogued and mapped to assess risk and threat.
 - Those with scarce resources must have a means to consider **allocation of preventive and reactive measures** in a target-rich, yet resource-constrained environment.
 - The sheer **number of possible targets** to be assessed is an operational challenge.
 - Some **information on potential targets may not be publicly available** because it is classified, sensitive but unclassified, or proprietary.
 - The most significant challenge is to develop a **comprehensive consequence model that examines complex infrastructure convergences using a multidisciplinary approach.**

Summary and Next Steps

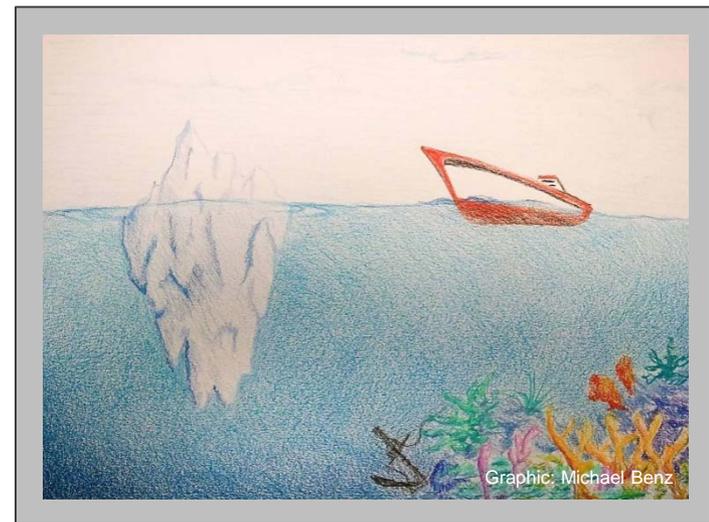
- Determine which experts from the previously mentioned fields, regionally and nationally, would be good candidates to **construct the risk assessment procedures.**
- Develop a **comprehensive consequence model that examines complex infrastructure convergences using a multidisciplinary approach.**
- **Catalog potential targets and develop mitigation techniques for those most at risk.**

The knowns ...

The known unknowns ...

And the unknown unknowns ...

We must explore them all!



[Derived from quote of Former U.S. Secretary of Defense Donald Rumsfeld]

Douglas Himberger, Ph.D.

Senior Vice President & Director

Security, Energy, and the Environment

himberger-douglas@norc.org

301.634.9433

Thank You!



NORC
at the UNIVERSITY of CHICAGO

 insight for informed decisions™