

Journal of Homeland Security and Emergency Management

Volume 8, Issue 1

2011

Article 4

Interdiction Models and Homeland Security Risks

Paul J. Maliszewski, *Arizona State University at the Tempe
Campus*

Recommended Citation:

Maliszewski, Paul J. (2011) "Interdiction Models and Homeland Security Risks," *Journal of Homeland Security and Emergency Management*: Vol. 8: Iss. 1, Article 4.

DOI: 10.2202/1547-7355.1785

Available at: <http://www.bepress.com/jhsem/vol8/iss1/4>

©2011 Berkeley Electronic Press. All rights reserved.

Interdiction Models and Homeland Security Risks

Paul J. Maliszewski

Abstract

Homeland security risks remain eminent. As the risks associated with terrorist attacks and other disasters endure, questions addressing the problems associated with homeland security risks will continue to attract attention in the foreseeable future. Among the manageable problems concerning disaster preparedness and mitigation include the protection of critical infrastructures. Notwithstanding the growth in research and development of techniques and strategies for effectively managing critical infrastructure problems, issues have been left unaccounted for including the provision of open intelligence to adversaries. This letter provides a critical view of research on infrastructure vulnerability and analysis. Specifically, it warns of the potentially counter-productive nature of publishing interdiction models—methods for identifying the most vital assets within infrastructure systems—in which adversaries have the potential to adopt and apply interdiction models to maximize their own objectives of destruction. This letter calls for an incorporation of overlooked costs into the analysis of the effectiveness of techniques designed to identify and allocate fortification resources to assets within critical infrastructure systems.

Homeland security risks remain prominent. As the risks associated with terrorist attacks and other disasters persist, questions about the problems associated with homeland security risks will continue to attract attention in the foreseeable future. Among the manageable problems concerning disaster preparedness and mitigation is the protection of critical infrastructures. Despite the growth in research into and development of techniques and strategies to effectively protect critical infrastructure, problems remain—notably, the availability of open intelligence to adversaries. Taking a critical view of the research on infrastructure vulnerability and analysis, this article warns of the potentially counterproductive nature of publishing interdiction models—methods for identifying the most vital assets within infrastructure systems—as publication facilitates the adoption of these models by adversaries, who could then use them to accomplish their own objectives of destruction. This article also calls for the incorporation of overlooked costs into any analysis of the effectiveness of techniques designed to identify and allocate fortification resources to assets within critical infrastructure systems.

Although major threats to the continuity of critical infrastructure systems include both natural disasters and human-induced attacks, much of research into the protection of critical infrastructure has been directed toward the presumed scope of the latter. Indeed, the field of critical infrastructure protection has witnessed an explosion of research in the wake of 21st-century terrorist attacks. Critical infrastructure protection initiatives were borne out of homeland defense programs throughout Western countries as a result of losses sustained in those attacks and the actual vulnerability of or perceived threats against important assets that remain. Subsequently, a considerable amount of research has been published that identifies and often illustrates the crucial components of real infrastructure systems.

For example, a substantial amount of work in the field of critical infrastructure protection has sought to identify which infrastructures are deemed critical for society to function properly (see White House, 2003; Church et al., 2004; Amin, 2005; Sternberg and Lee, 2006; Garb et al., 2007; Greenberg et al., 2007) and which components within infrastructure systems are the most vulnerable (see Grubestic and Murray, 2006; Taylor et al., 2006; Murray et al., 2007; Nagurney and Qiang, 2008; Matisziw and Murray, 2009). Researchers have also developed strategies for the protection of critical infrastructures or critical assets within infrastructure systems (see Salmerón et al., 2004; Brown et al., 2006; Qiao et al., 2007; Church and Scaparra, 2007; Scaparra and Church, 2008; Maliszewski and Horner, 2010). Most of this research involves allocating resources to critical assets. The decision of where to allocate fortification resources requires that the properties and locations of critical assets be empirically identified—information that, when publicized, is habitually accompanied by

figures and tables replete with replete with an intelligent analysis of the data presented.

Terrorist plans are rational. Although terrorists' behaviors are seemingly irrational per se, adversaries plan their attacks to maximize the amount of damage and destruction they inflict for political ends. Thus, despite ample efforts to identify critical infrastructure vulnerabilities and develop techniques to protect critical assets, security risks are indeed inherent in the public knowledge available to terrorists about what is critical, what is vulnerable, and where critical and vulnerable assets are located.

Clearly, improvement in the security of existing infrastructure systems requires the answers to the following questions:

1. What is a critical asset within an infrastructure system?
2. How do we identify critical assets within infrastructure systems?
3. How can we protect critical infrastructures or important assets within them?
4. What is the best way to allocate constrained fortification resources for protecting these assets or infrastructures?

These questions are central to research on the topic of critical infrastructure protection. However, answering these questions may result in the development of methods for identifying critical assets that ironically may lead to the undoing of these same assets, should terrorists be able to acquire and adopt these methods and thus identify our critical assets for their own malicious purposes.

A key component in assessing the effectiveness of critical infrastructure protection techniques includes cost-benefit analyses of the implementations of protection strategies. Many of the benefits and costs of protecting infrastructure systems—such as reduced damage and thwarted attacks on the one hand, and the finances involved in deploying security resources on the other hand—are straightforward and measurable. However, there may be hidden costs associated with academic research involving the identification of critical infrastructures and their crucial components, a task that is necessary for the allocation of fortification resources. When the domain of identifying vulnerabilities within infrastructure systems is published and the information becomes accessible to adversaries, the potential costs of identifying critical assets for their protection increases as the direct threats to them increase. In other words, it is not the identification of critical assets or vulnerabilities per se that poses a threat; rather, it is the subsequent publication of the findings, which may inadvertently provide terrorists with intelligence about them. This problem is exacerbated by the globalization of telecommunications networks in which the rapid growth of the Internet renders knowledge transparent to anyone with access to the World Wide Web. And when vulnerable assets are identified and the information is subsequently published

while the actual fortification of such assets are neglected, such assets will be that much more vulnerable.

Clearly, there are potential costs and benefits of publicly identifying critical assets and crucial components within infrastructure systems. If protecting an asset exceeds the cost of losing it, it is not beneficial to protect it. Therefore, understanding both the costs and benefits of protecting and losing critical assets is important in assessing the effectiveness of critical infrastructure protection directives. Benefits result from hardening and securing critical assets and crucial components. However, the publication of vulnerable assets potentially increases their vulnerability—a problem that critical infrastructure protection studies have generally ignored. Furthermore, if publicized protection strategies are not actually implemented, the potential costs increase even more.

Overall, this viewpoint has identified a potential hidden cost of critical infrastructure protection research. As was addressed here, published methods identifying critical assets or vulnerable components (which are likely or potential targets) and the subsequent illustration of their locations and properties may add to the costs of protecting critical infrastructures. In any case, this problem is left for further analysis.

References

- Amin, Massoud. 2005. "Energy Infrastructure Defense Systems." *Proceedings of the IEEE* 93 (5): 861–875.
- Brown, Gerald, Matthew Carlyle, Javier Salmerón, and Kevin Wood. 2006. "Defending Critical Infrastructure." *Interfaces* 36 (6): 530–544. Accessed January 16, 2011. faculty.nps.edu/mcarlyle/docs/defending_critical_infrastructure.pdf.
- Church, Richard L., Maria P. Scaparra, and Richard S. Middleton. 2004. "Identifying Critical Infrastructure: The Median and Covering Facility Interdiction Problems." *Annals of the Association of American Geographers* 94 (3): 491–502.
- Church, Richard L., and Maria P. Scaparra. 2007. "Protecting Critical Assets: The r-Interdiction Median Problem with Fortification." *Geographical Analysis* 39 (2): 129–146.
- Garb, Jane L., Robert G. Cromley, and Richard B. Wait. 2007. "Estimating Populations at Risk for Disaster Preparedness and Response." *Journal of Homeland Security and Emergency Management* 4 (1). Accessed January 16, 2011. www.bepress.com/jhsem/vol4/iss1/3/.

- Greenberg, Michael, Nancy Mantell, Michale Lahr, Frank Felder, and Rae Zimmerman. 2007. "Short and Intermediate Economic Impacts of a Terrorist-Initiated Loss of Electric Power: Case Study of New Jersey." *Energy Policy* 35 (1): 722–733.
- Grubestic, Tony H., and Alan T. Murray. 2006. "Vital Nodes, Interconnected Infrastructures, and the Geographies of Network Survivability." *Annals of the Association of American Geographers* 96 (1): 64–83. Accessed January 16, 2011. www.cnr.berkeley.edu/~bingxu/UU/spatial/Readings/GrubesticAnnals2006.pdf.
- Maliszewski, Paul J., and Mark W. Horner. 2010. "A Spatial Modeling Framework for Siting Critical Supply Infrastructures." *The Professional Geographer* 62 (3): 426–441. Accessed January 16, 2011. www.public.asu.edu/~pmalisze/MaliszewskiHorner_2010.pdf.
- Matisziw, Timothy C., and Alan T. Murray. 2009. "Modeling s–t Path Availability to Support Disaster Vulnerability Assessment of Network Infrastructure." *Computers & Operations Research* 36 (1): 16–26. Accessed January 16, 2011. pubget.com/paper/pgtmp_10065111.
- Murray, Alan T., Timothy C. Matisziw, and Tony H. Grubestic. 2007. "Critical Network Infrastructure Analysis: Interdiction and System Flow." *Journal of Geographical Systems* 9 (2): 103–117.
- Nagurney, Anna, and Qiang Qiang. 2008. "A Network Efficiency Measure with Application to Critical Infrastructure Networks." *Journal of Global Optimization* 40: 261–275. Accessed January 16, 2011. supernet.som.umass.edu/articles/JOGO Braess JOGOstyle_rev.pdf.
- Qiao, Jianhong, David Jeong, Mark Lawley, Jean-Philippe P. Richard, Dulcy M. Abraham, and Yuehwern Yih. 2007. "Allocating Security Resources to a Water Supply." *IIE Transactions* 39 (1): 95–109.
- Salmerón, Javier, Kevin Wood, and Ross Baldick. 2004. "Analysis of Electric Grid Security under Terrorist Threat." *Institute of Electrical and Electronic Engineers Transactions on Power Systems* 19 (2): 905–912.
- Scaparra, Maria P., and Richard L. Church. 2008. "A Bilevel Mixed-Integer Program for Critical Infrastructure Protection Planning." *Computers & Operations Research* 35 (6): 1905–1923.
- Sternberg, Ernest, and George C. Lee. 2006. "Meeting the Challenge of Facility Protection for Homeland Security." *Journal of Homeland Security and Emergency Management* 3 (1). Accessed January 16, 2011. www.bepress.com/jhsem/vol3/iss1/11/.

- Taylor, Michael A. P., Somenahalli V. C. Sekhar, and Glen M. D’Este. 2006. “Application of Accessibility Based Methods for Vulnerability Analysis of Strategic Road Networks.” *Networks & Spatial Economics* 6 (3–4): 267–291.
- White House. 2003. *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*. Accessed January 16, 2011. www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf.