in Proceedings of the Third International Workshop on Critical Infrastructures Security (CRITIS 08),
Posters section, October 13-15, 2008, Frascati (Rome), Italy

An Ontology-Based Approach to Blind Spot Revelation in Critical Infrastructure Protection Planning

Joshua Blackwell, William J. Tolone, Seok-Won Lee, Wei-Ning Xiang, and Lydia Marsh

Abstract One widely perceived yet poorly understood phenomenon in the practice of critical infrastructure protection is that of blind spots. These are certain aspects of the interrelationships among different critical infrastructure systems (CI systems) that could trigger catastrophe across CI systems but are concealed from planners, and discovered only in the aftermath of a crisis. In this paper, we discuss the sources of blind spots, and explore the feasibility of various techniques to help reveal blind spots.

1 Introduction

August 14th, 2003 saw the Northeastern blackout, a massive power blackout in the northeastern United States and southeastern Canada. The cascading events that resulted in failures in other infrastructure systems-telecommunication services, aviation, and transit-affected the lives of over 50 million people in both countries [5, 6]. The cause of the blackout, revealed only in hindsight, is a surprise that goes beyond anyone's imagination. It was a trivial incidence in Parma, Ohio, a suburb of Cleveland, where untrimmed overgrown trees severed one section of a high-voltage power transmission line [5, 6]. Surprises of this kind and resulting failures are manifestations of blind spots, a widely perceived yet poorly understood phenomenon in the practice of critical infrastructure protection (CIP, hereafter).

In this paper, we explore a set of questions instrumental to the revelation of blind spots. That is, what exactly is a blind spot in CIP? Where does it come from? What impacts does it have on the CIP practice? To what extent, if ever, can a blind spot be revealed or even projected before a crisis? What role(s) can information technology play in revealing blind spots? We propose the use of information technologies to facilitate explorations of the blind spots.

The University of North Carolina at Charlotte
9201 University City Blvd., Charlotte, NC. 28223-0001. USA e-mail: josblack@uncc.edu

in Proceedings of the Third International Workshop on Critical Infrastructures Security (CRITIS 08),
Posters section, October 13-15, 2008, Frascati (Rome), Italy

2 What is a Blind Spot?

One useful analogy can be drawn between a car driver and a CIP planner. A blind spot is the area the driver cannot see through the mirrors. As shown in Figure 1, there are two areas in a driver's field of vision that are not visible. If the driver was to turn and look at the side, the blind spot would be revealed to him/her, and more importantly, whatever is in the blind spot, perhaps another vehicle, will be noticed and avoided if deemed dangerous. Another type of blind spot exists in the forward vision as well. Perceptual or cognitive blind spots occur in the forward vision when drivers become used to seeing things more often than not. Their focus of attention and cognitive thought process prevent them from recognizing potential dangers in plain sight. For example, the driver may fail to brake quickly enough to avoid collision due to poor depth perception. This aspect is not depicted in the illustration but must be recognized.

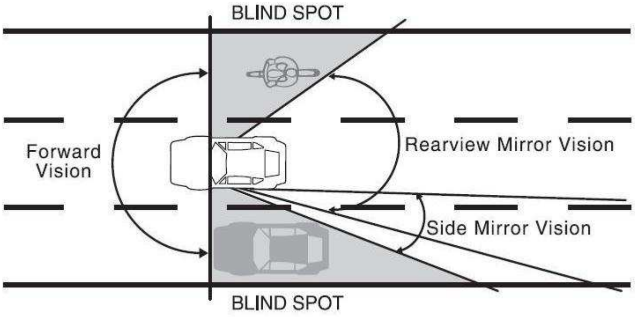

Fig. 1 A driver's blind spot

Similarly, in CIP planning, blind spots refer to certain aspects of the interrelationships among different critical infrastructures (CI systems, hereafter) that could trigger catastrophe across CI systems but are concealed from CIP planners, and discovered only in the aftermath of a crisis. The 2003 blackout is one of many examples of blind spots. Yet, not all of the interrelationships among CI systems are blind spots. In a recent study, McNally et. al. [8] examined the interrelationships among different CI systems (that is, CI interdependencies) under a quadruple framework. This study demonstrates an asymmetry in the accumulated knowledge about, and attention toward, CI interdependencies across the four quadrants of their framework. More specifically, (1) knowledge is generally available about CI interdependencies among CI systems that are directly connected by functional and geographically proximate to one another (quadrant A); (2) little attention has been paid to the CI interdependencies among CI systems indirectly connected by function regardless of their geographic location, i.e., proximate or distant (quadrants B and C); (3) although knowledge is readily available about CI interdependencies among CI systems that are directly connected by function but geographically distant (quadrant

D), the segmented nature of CI service delivery often constitutes a ”corporate firewall” that prevents knowledge exchange and communications across different CI systems about potential vulnerabilities caused by the CI interdependencies in other quadrants (that is, A, B, and C). Clearly, under this quadruple framework, CI interdependencies in quadrants B and C are more likely to become blind spots than those in quadrant D, and especially those in quadrant A. In the next section, we extend the work of McNally et. al. to the explore of sources of blind spots in CIP. That is, where do blind spots come from?

3 Sources of Blind Spots in CIP

Among possible sources of blind spots in the practice of critical infrastructure protection are complexity; imperfections in information, heuristics, and tools; and the lack of cross-domain knowledge.

3.1 Complexity of CI Systems

Complexity in CI systems stems from at least three sources: CI interdependencies, spatial and temporal variations and scale dependence of observation. Characterized by McNally et. al.'s four quadrant framework, CI interdependencies amongst CI objects can be span CI systems, i.e., inter-domain dependencies, or occur within CI systems, i.e., intra-domain dependencies. CI interdependencies can also be spatially proximate or distant. Furthermore, there are emergent features that arise when looking at a system of CIs that are not present when examining an individual CI system [8]. For example HVAC systems depend on electric power to provide cooling; if power is lost then although HVAC systems are sound, they no longer can operate. Though a simple example, this effect is only recognized with a system of systems perspective. Given the complexity of a system of CIs and the general awareness CI interdependencies as reported by McNally et. al., it is unlikely for a CIP Planner to understand properly all relevant CI interdependencies.

Furthermore, spatial and temporal variations occur among CI systems. CI systems are located, in part, based on natural and unique environmental characteristics, which impacts CI interdependencies. Therefore, our understanding CI interdependencies is not necessarily transferrable from one region to the next. In addition, our understanding may also be temporally dependent as CI behavior, and the subsequent interdependencies, can change over time (e.g., time of day, time of year, etc.)

Scale dependence of observation refers to the level of detail represented. Due to their inherent complexity, CI systems are often examined or observed at various scales analysis. CI interdependencies are naturally associated with these scales of analysis. Examining CI systems at a particular scale necessarily obscures both detail and context. Furthermore, our understanding of CI interdependencies is scale dependent - i.e., assessing geographic proximity depends on scale; assessing direct v. indirect functional dependence also depends on scale. Consequently, macro-scale and micro-scale CI interdependencies can be occluded due to the scale of observation. Likewise, CI interdependencies may be misunderstood due to the scale of observation.

3.2 *Imperfect Information*

Much of the information needed for CIP planning is not within the public domain. It is estimated that 85 percent of all CI data in the U.S is maintained by the private sector. Owing to their confidential, proprietary and business sensitive nature, these data are not accessible to the public [9]. In the United States, the Protected Critical Infrastructure Program under the U.S. Department of Homeland Security, with provisions from the Critical Infrastructure Information Act, only encourages private sector data sources to submit information/knowledge/data voluntarily to the U.S. federal government. Nevertheless, even if the U.S. were to comply, the data are often large, extensive, even entrapping [10].

3.3 *Imperfect Heuristics*

Human thinking is affected by two common effects that set limits on our cognitive abilities. These affects can be a source of blind spots. The availability heuristic occurs when a human uses the most available pieces of information to assess the frequency of an object class or the probability of an event [12]. Salience also contributes to minds ability to retrieve available information. If one was to witness an event rather than just hear about it, one is more likely to remember and retrieve that as a process that occurs [12]. People are also biased when it comes to assessing situations they have not seen before. Their bias of imaginability leads them to generate an answer according to some rule if there are no known instances to reference [12]. Risk can be evaluated incorrectly or not seen if a person cannot fathom the type of risk that exists in a situation given the rules that the person already has in place.

People start from a value point that is known and then adjust it to meet the situation being evaluated. However, the result is always tied to the initial value point. This is known as the anchoring effect [12]. When the adjustment from this value point is not sufficient to lead to an accurate conclusion of the events or objects in question, a misconception is left and an error can occur [12]. It is important to understand the limitations of these heuristics so that judgment and decision making in critical situations can improve.

3.4 Imperfect Tools

Modelers of CI systems should consider the capabilities and limitations of the tools that they use to understand CI systems. Often, it is possible for tools to under represent or even worse misrepresent critical information necessary to understand real world CI phenomena. For example a geographic information system is capable of displaying CI systems in visual displays with colors to represent functionality and type. It can easily display spatial proximity as different scales of observation. However it cannot easily display the functional connectedness or nature of the functional relationships amongst those objects. On the other hand, ontological modeling tools, that can easily represent functional relationships, do not effectively depict spatial proximity.

3.5 Lack of Cross-Domain Knowledge

As society and its organizations become more specialized, human knowledge tends to be more domain-specific. People who have cross-domain knowledge are usually are in senior positions and less accessible. This is especially the case in organizations that operate and/or manage CI systems due to the security and business-sensitivity concerns in the arena of CIP. The shortage of subject matter experts with cross-domain knowledge further contributes to the problem of blind spots.

It should be noted that the above discussion of possible sources of blind spots in CIP is by no means inclusive. An in-depth investigation that systematically studies the phenomena is beyond the scope of this paper. However, in the next section we discuss the potential role of information technology and modeling in revealing blind spots.

4 Information Technologies, Modeling and Blind Spot Revelation

It is well established that driver blind spots can be revealed by adjusting the rear-view mirrors or incorporating additional mirrors as well as the protocol of ”looking back over your shoulder”. In CIP planning, we claim that blind spots can be revealed through the innovative use of information technology, modeling, and associated operational protocols. In this section, we highlight several general approaches to blind spot revelation that demonstrate potential promise.

To facilitate blind spot revelation, it is necessary to articulate various methods and tools together under an overarching framework. We propose a spatial decision support system (SDSS) to serve the purpose. More specifically, by combining the strength of an ontology-based knowledge engine and GIS, cross-domain knowledge solicited from human experts [10] can be represented, visualized, and further applied to reasoning and modeling; by coupling several methods in a model base, the SDSS provides CIP planners with tools in revealing blind spots and preparing for disaster management. Briefly discussed below are these methods.

4.1 Abstraction

Abstraction can be used to assist in blind spot revelation. In order for CIP Planners to understand further the sources of blind spots within their CI systems it is necessary to assess their CI systems from different levels of abstraction [7, 15]. This will promote a learning cycle in which domain assessment leads to an enrichment of the domain data, which, in turn, will necessitate further domain assessment. Through abstraction methods enabled by a SDSS, Planners will better understand where the sources of blind spots originate and determine if the blind spots are located under the planner's control or outside the planners control in a larger world domain.

4.2 CI System Specification

McNally et. al. [8] describe a method for the specification of individual CI systems as well as a system of CIs. A system of CIs is a collective group of CI systems that provides commodities integral to maintaining normal operations for a given region. There are four iterative steps to this method for CI system specification.

(1) *Identify the CI systems*: identify the CIs, their boundaries and structures. (2) *Specify the CI systems*: place all CI objects into the model. Identify and specify properties and characteristics of each object in the model. Specify inherent functionalities and model relationships between objects in the same system (intra-domain interdependencies). (3) *Specify the system of CIs*: define cross-domain interdependencies amongst objects from different CI systems. (4) *Verification and Validation*: evaluate and refine the model to direct future iterations of these steps.

Integrating into a SDSS support for such methods can facilitate the discovery of blinds spots by CIP Planners.

4.3 Scenarios

Scenarios, potentially built based on data and knowledge included in a SDSS, can be used to reveal blind spots. Scenarios can demonstrate how over time interdependencies amongst CI systems and systems of CIs can change. Each scenario connects an initial state and initiating event(s), to desired and undesired end states (different levels of damage), with a sequence of events linking the two.

When modeling, the scenarist compiles information together into chunks. Then, the scenarist can bring these chunks together with other experts to form larger pieces of information (larger chunks) that can potentially lead to goals or plans. In this way, a scenario functions as a bridge to connect the communities of modeling and planning [16]. Thus, scenarios can expand knowledge.

While scenarios can be designed from a vulnerability or risk assessment mindset, they also can be designed from a red team mindset [8, 11]. ”Red Team” has been used by the Department of Homeland Security (DHS) and the Institute for Defense Analyses Advanced War Fighting Program to describe the creation of a scenario from the mindset of the enemy [3, 8, 11]. This is much like Altshuller’s theory of inventive problem solving in which the scenario composer develops a state of mind rather just composing scenarios for risk assessment [2].

4.4 Verification and Validation

To refine the model and enrich the knowledge base, we employ techniques that reveal blind spots as well as methods to verify and validate those blind spots. Verification asks if a model behaves according to its specification. Validation asks if model behavior reflects the represented phenomenon. By verifying and validating CI models better information and understanding is gained, and blind spots are revealed. Case-based verification, face validation and Delphi questioning have been used to verify and validate critical infrastructure models [14]. Case-based verification compares actual events to modeled events to assess model accuracy. It allows us to reflect upon how well the model represents the real world. Face validation asks experts to look at the model as a whole, including data representation, and offer their opinion as to the accuracy of representation. Delphi questioning asks subject matter experts a series of questions designed to elaborate on the data quality and representative accuracy. Each of these three techniques is used continually to refine the knowledge base in search of blind spots.

5 Conclusions

The sources of blind spots in CIP are potentially endless. A SDSS can incorporate known data/knowledge into a model base which visualizes the CI data/knowledge. Sources of blind spot can be investigated using modeling techniques as we have described. These different tools and techniques will allow the planner to assess and resolve vulnerabilities thereby circumventing potential emergencies. In addition, the planner can develop response plans for emergencies within their domain that can minimize the cascading effects.

Future research should investigate interoperability amongst different CI Planners domain ontologies using common semantics [1]. Also, consistency constraints should be developed to help the planners understand how to make ontologies with similar descriptions of objects and properties in order to standardize the process and resulting datasets [4].

While conducting and applying this research, many observers became interested in what the resulting CI models were demonstrating. It is interesting that at this time many facilities managers and industrialists are examining ways to manage their systems. Our research draws attention to the details for which they are responsible and offers a new way of thinking about their systems. CIP is an expanding field that will continue to highlight potential dangerous issues in need of planning.

References

1. Fonseca, F., Camara, G. and Monteiro, A. (2001) ”A Framework for Measuring the Interoperability of Geo-Ontologies” Spatial Cognition and Computation, 6(4): 307-329.
2. Garrick, J. (2002) ”Perspectives on the use of risk assessment to address terrorism”, Risk Analysis, 22(3): 421-423.
3. The Naitonal Strategy for Homeland Security (2002) The office of Homeland Security, July. Accesed May 30th, 2008. http://www.whitehouse.gov/homeland/book/nat_strat_hls.pdf
4. Frank, A.U.(2001). ”Tiers of Ontology and Consistency Constraints in Geographic Information Systems” International Journal of Geographical Information Science 15 (7): 667-678.
5. ICF Consulting. ”The Economic Cost of the Blackout: An issue paper on the Northeast Blackout” August, 14, 2003. Accessed May 31, 2008 from http://www.solarstorms.org/ICFBlackout2003.pdf
6. IWS. ”NERC Welcomes U.S.-Canada Power System Task Force Final Report” Published April 6, 2004 by the North American Electric Reliability Council. Accessed May 30, 2008.
7. Kramer, J. (2007) ”Is Abstraction the Key to Computing?” Communications of the ACM, April, 50 (4): 37-42.
8. McNally, R.K., Lee, S-W, Yavagal, D., and Xiang, W-N (2007) ”Learning the Critical Infrastructure Interdependencies Through an Ontology-Based Information System”, Environment and Planning B: Planning and Design 34: 1103-1124.
9. Terner M., Sutton R., Hebert B., Bailey J., Gilbert H., Jacqz C. (2004) Protecting Critical Infrastructure GeoIntelligence, March 1, 2004 http://www.geointelmag.com/geointelligence/article/articleDetail.jsp?id=90043
10. Tolone, W.J., Xiang, W.-N., Raja, A., Wilson, D., Tang, Q., McWilliams, K., and McNally, R. (2006). Mining critical infrastructure information from municipality data sets: a knowledge-driven approach and its applications. In: Hilton, B.N. (Editor). Emerging Spatial Information Systems and Applications. Hershey, PA: Idea Group Publishing, 310-325.
11. Sandoz, J.F. (2001) ”Red Teaming: A means to Military Transformation” Report by the Institute for Defense Analyses, Alexandria Va, Advanced Warfighting Program. http://handle.dtic.mil/100.2/ADA388176
12. Tversky, A., and Kahneman, D. (1974) ”Judgment Under Uncertainty: Heuristics an Bias: Bias in Judgments Reveal Some Heuristics of Thinking Under Uncertainty” Science. 185: 1124-1131.
13. Turban E., Aronson, J.E. (2001) Decision Support Systems and Intelligent Systems (Prentice Hall Upper Saddle River, NJ)
14. Weeks, A. (2006) ”A Delphi-Case Design Method for Model Validation in Critical Infrastructure Protection Modeling and Simulation”, Masters Thesis, Dept of Geography and Earth Sciences, Univ. of North Carolina at Charlotte, May.
15. Wing, J. (2006) ”Viewpoint: Computational Thinking” CACM, March 49(3): 33-35.
16. Xiang W-N, Clarke K.C., (2003) ”The use of scenarios in land-use planning” Environment and Planning B: Planning and Design 30(6): 885-909.