available at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/ijcip

Interactive visualizations for critical infrastructure analysis

*William J. Tolone**

Department of Software and Information Systems, College of Computing and Informatics, University of North Carolina at Charlotte, 9201 University City Boulevard, Charlotte, North Carolina 28223-0001, United States

ARTICLE INFO

Article history:
Received 7 July 2009
Accepted 8 July 2009

Keywords:
Critical infrastructure modeling and simulation
Critical infrastructure analysis
Visual analytics

ABSTRACT

Critical infrastructure analysis often involves overwhelming volumes of complex, heterogeneous, interdependent information. Human judgment is essential to the analysis as insights and understandings are synthesized from information that is often complex, dynamic, incomplete, diverse, conflicting and even deceptive. Yet, our ability to collect information is increasing at rates far beyond our ability to analyze it. Visual analytics – the science of analytical reasoning facilitated by interactive visual interfaces – can help analysts obtain better insights and understanding with greater efficiency. This paper discusses the research challenges involved in applying interactive visualization to critical infrastructure analysis. The research challenges are organized around three dimensions that are adapted from metrics proposed by Scholtz (2006) [8] for evaluating human information interaction systems. The challenges are illustrated using examples from the integrated modeling and simulation of critical infrastructures.

1. Introduction

Critical infrastructures are infrastructures that, if disrupted, can undermine public safety and security, public health, the economy and the way of life [1]. Notable examples in the United States include the attacks of September 11, 2001, the blackout in the Northeastern United States and Southeastern Canada in 2003, and the hurricanes in Louisiana and Texas in 2005. While it is unlikely that disruptions can be uniformly prevented, the practice of critical infrastructure analysis can reduce their impact by improving vulnerability assessments, protection planning, decision-making and strategies for response and recovery.

However, critical infrastructures have two fundamental characteristics that complicate analysis. First, critical infrastructures involve complex, multi-dimensional collections of technologies, information, processes and people. As such, each infrastructure is a system-of-systems with engineering and behavioral properties. Engineering properties include the underlying physics-based properties of the physical components and technologies that comprise the infrastructure. Behavioral properties, on the other hand, include the relational properties of the observed behavior of an infrastructure, and properties that emerge from factors such as business processes, decision points, human intervention and information generation, availability and flow. In order to be effective, critical infrastructure analysis must consider the engineering and behavioral properties of infrastructures.

The second characteristic is the high degree of dependence between critical infrastructures [2]. The dependencies, which include inter-infrastructure and intra-infrastructure dependencies, can be categorized by the type of the resulting failure (i.e., common cause, cascading, escalating); infrastructure characteristics (i.e., organizational, operational, temporal, spatial); state of operation (e.g., normal, distressed); dependency type (i.e., physical, cyber, logical, geographic);

* *Corresponding address:* Department of Computer Science, University of North Carolina at Charlotte, 9201 University City Boulevard, North Carolina 28223-0001 Charlotte, United States. Tel.: +1 704 547 4880; fax: +1 704 547 3516.
E-mail address: wjtolone@uncc.edu.

1874-5482/$ - see front matter © 2009 Elsevier B.V. All rights reserved.
doi:10.1016/j.ijcip.2009.07.004

environment (e.g., business, security, social/political); and, coupling and response behavior (i.e., adaptive, inflexible, loose/tight, linear/complex). As a result of these dependencies, disruptions in one infrastructure frequently cascade and escalate across multiple infrastructures. Cascading effects are reflected in the migration of disruptions from one infrastructure to another. Escalating effects impact the causal chain of disruptions in terms of scale, scope and consequence. Critical infrastructure analysis requires a proper understanding of these complex dependencies.

Making sense of critical infrastructures is aptly described as a "wicked problem" [3]. Wicked problems are nonlinear in nature; they are without a definitive formulation; they have an open solution space where solutions have relative quality; they are problems for which each instance is arguably unique and for which analysts have no right to be wrong. Critical infrastructure analysis is a wicked problem that involves overwhelming volumes of complex, heterogeneous interdependent information, and one that depends on human judgment to synthesize insights and understandings, particularly when the available information is dynamic, incomplete and/or deceptive.

Visual analytics, "the science of analytical reasoning facilitated by interactive visual interfaces" [4], can help address this challenge. Visual analytics enables analytical discourse and, in particular, the activity of "sensemaking" through interactive visualization. The goal of sensemaking is to produce insights that lead to timely and correct judgments — judgments that are essential to enhancing the efficiency, security and resilience of critical infrastructures.

Unfortunately, despite the broad understanding of the value of sensemaking in interactive visualization, many research challenges remain to be addressed before the anticipated benefits to the practice of critical infrastructure analysis can be realized. Several researchers (see, e.g., [6,5,7]) have described the activity of sensemaking; all the descriptions emphasize that sensemaking is a "process" not a "product". The work of Pirolli and Card [5] illustrates this emphasis (Fig. 1). This view of sensemaking has several important implications to the design of interactive visualizations for critical infrastructure analysis. First, sensemaking is an iterative process with numerous feedback loops; this suggests that interactive visualizations must support the refinement of analyses. Second, sensemaking involves forging and analysis; this suggests that interactive visualizations must facilitate the transformation of forged data into knowledge that will lead to proper understanding. Third, sensemaking is human-centric; this suggests that interactive visualizations for critical infrastructure analysis should not be designed to give answers, but rather to enable human insight and facilitate discernment. Finally, sensemaking involves the construction and refinement of implicit and explicit cognitive representations; this suggests that interactive visualizations should help users bridge these representations by linking past understandings to new understandings.

This paper discusses some of these research challenges. The discussion is organized around three dimensions adapted from the metrics proposed by Scholtz [8] to evaluate human information interaction systems. The visual analytics research challenges are discussed in the context of our work on the integrated modeling and simulation of critical infrastructures [9–12].

2. Organizing the challenges

The complexity of critical infrastructures necessitate tool support to facilitate effective vulnerability assessments, protection planning, decision-making and strategies for response and recovery. All these activities involve substantial analytical discourse around large, complex information spaces. Unfortunately, existing tool support for critical infrastructure analysis is limited.

Scholtz [8] has examined evaluation methodologies and metrics for human information interaction systems. These systems are designed to support the exploration and analysis of large, complex information spaces. In her examination, Scholtz suggests that evaluation must extend beyond the use of traditional usability metrics, which focus primarily on issues of perception, interaction and performance, to include new metrics that focus on the effectiveness and/or efficacy of analytic tasks. In other words, these new metrics should examine the impact of a system on the analytical practice of its users and the analytical products that the users produce.

We draw on Scholtz's work to organize the research challenges in the area of interactive visualization for critical infrastructure analysis. The challenges are organized along three dimensions based on Scholtz's evaluation metrics of usability, utility and impact. In the context of human information interaction systems, usability metrics help evaluate perception, interaction and performance. Utility metrics, on the other hand, help evaluate changes in work practice. Impact metrics help evaluate changes to work products. Adapting these metrics to interactive visualizations for critical infrastructure analysis leads to the following three dimensions.

- **Usability challenges:** Visual analytics research challenges that focus on issues of perception and/or interaction for critical infrastructure analysis.
- **Utility challenges:** Visual analytics research challenges that focus on issues related to the analytical practice of critical infrastructure analysis.
- **Impact challenges:** Visual analytics research challenges that focus on issues related to the analytical products of critical infrastructure analysis.

We describe these categories as dimensions because many of the research challenges possess characteristics from multiple categories. Nevertheless, for clarity of presentation, we associate each identified research challenge with its dominant dimension in our discussion.

Table 1 lists the visual analytics research challenges for critical infrastructure analysis. The challenges are organized according to the three dimensions of usability, utility and impact. The list is by no means comprehensive; rather, it is illustrative of the research challenges that we have encountered during our extensive work on the integrated modeling and simulation of critical infrastructures [9–12]. The categorization provides an organized way to characterize and

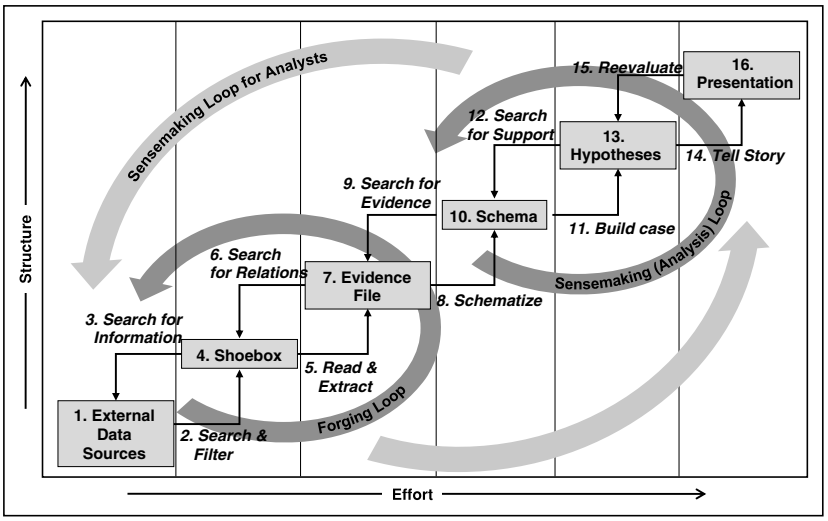


Fig. 1 – Pirolli–Card sensemaking process [5].

Table 1 – Visual analytics research challenges for critical infrastructure analysis.	
Usability challenges	Exposing and Exploring Context Bridging Visual Representations Registering and Managing Abstraction Exposing and Exploring Uncertainty
Utility challenges	Facilitating Reasoning in Context Moving Beyond the Technical Enabling Integrated Cognition Increasing Transparency of Analysis
Impact challenges	Uncovering Blind Spots Increasing Situational Understanding Building Shared Understanding among Disparate Viewpoints Facilitating Trust

explore the research challenges. The discussion of specific research challenges also provides insight and a roadmap for visual analytics research applied to critical infrastructure analysis.

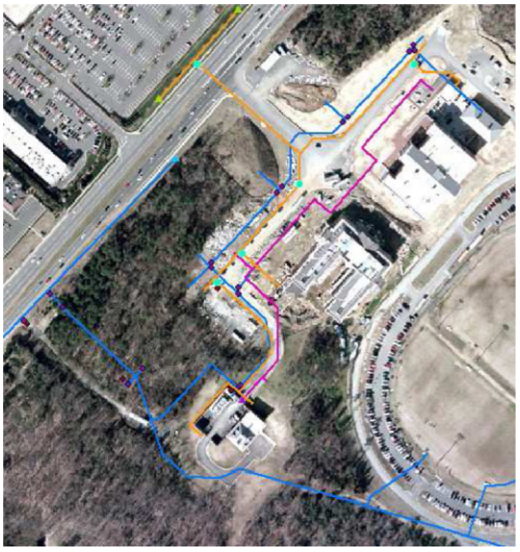


Fig. 2 – Spatial visualization with weak functional context.

3. Visual analytics usability challenges

Visual analytics usability challenges for critical infrastructure analysis focus on issues of perception and/or interaction. To illustrate this dimension, we examine four research challenges: (i) exposing and exploring context; (ii) bridging visual representations; (iii) registering and managing abstraction; and (iv) exposing and exploring uncertainty.

3.1. *Exposing and exploring context*

Critical infrastructure analysis must be conducted in context [10]. Examining critical infrastructures in isolation ignores the complex dependencies that exist between infrastructures and the contextual factors that shape and constrain infrastructure behavior. Furthermore, because context gives meaning to action [13], analyzing critical infrastructures in isolation can lead to a loss in the meaning or implications of infrastructure behavior. When this occurs, the resulting analysis is at best incomplete and at worst invalid.

The notion of context is rich and multi-dimensional. To our knowledge, current visual analytics capabilities do not adequately allow analysts to perceive space, time and function simultaneously. For example, the ability to analyze cross-infrastructure versus intra-infrastructure dependencies in spatial and temporal context is required for critical infrastructure analysis, but is very difficult with current visual analytics capabilities. Spatial analysis typically involves map overlays. However, overlaying infrastructure data onto map displays tends to obscure important dependency data. For example, in Fig. 2, orthophotographs are overlaid with natural gas distribution data (depicted in orange), water

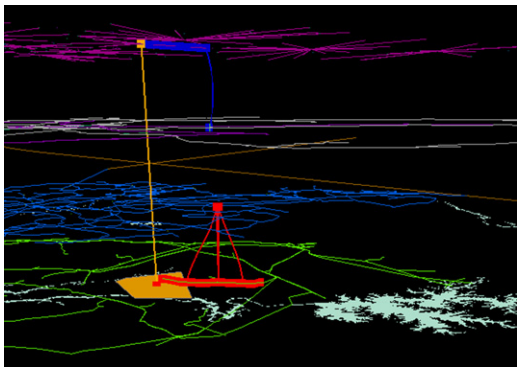


Fig. 3 – Cross-infrastructure dependency visualization with weak spatial context.

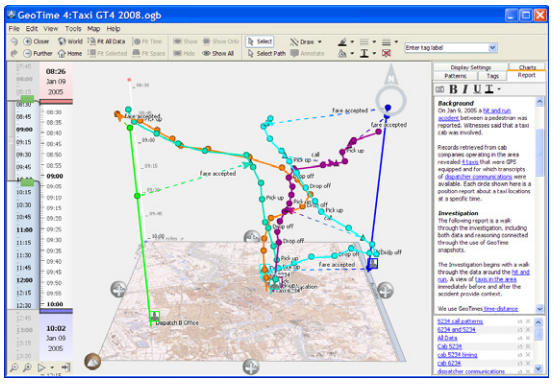


Fig. 4 – GeoTime visualization [14].

distribution data (depicted in blue) and steam distribution data (depicted in fuchsia). While spatial context is preserved, cross-infrastructure dependencies are difficult to identify.

On the other hand, visualization techniques that highlight cross-infrastructure versus intra-infrastructure dependencies do not adequately visualize spatial context. For example, in Fig. 3, data about each infrastructure are partitioned along the z-axis (i.e., each infrastructure is depicted at a different elevation). Cross-infrastructure dependencies are readily perceived when the data are viewed at the proper angle. Unfortunately, exploring the data at such an angle obscures the spatial context.

The interactive visualizations in Figs. 2 and 3 do not adequately depict the temporal context. While techniques for spatial analysis have been extended to include support for temporal analysis, these techniques often obscure important functional data. Fig. 4 presents a GeoTime visualization [15]. The ground plane provides the spatial context and marks the "instant of focus" along the temporal dimension of the z-axis. Events that occur after the instant of focus are marked on the positive z-axis. Events that occurred before the instant of focus are depicted on the negative z-axis. Basic relationships among events are expressed; however, exploring the meaning of the events in a functional context is more difficult.

3.2. *Bridging visual representations*

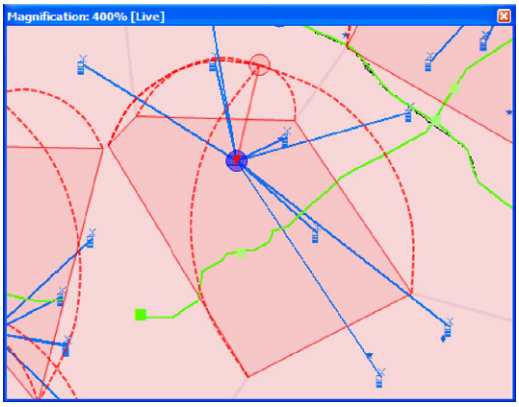
In 1690, John Locke described knowledge as the ability to distinguish concepts or ideas [16]; to paraphrase, knowledge emerges from the connections among concepts. Given this description of knowledge, sensemaking can be described, in part, as the process of discovering and understanding these connections. Klein, et al. [17] emphasize this point in describing sensemaking as "a motivated, continuous effort to understand connections … in order to anticipate their trajectories and act effectively." As such, visual analytics capabilities for critical infrastructure analysis must provide better methods to expose and explore these connections. Yet, these connections often involve heterogeneous representations that, in turn, may include multiple visual representations. This is particularly true for critical infrastructure models because their visual representations may include points, polygons, text, tables, etc. Given the need to understand the connections among these representations, effective analysis requires solutions that bridge these representations. However, these varied representations present some challenges.

For example, bridging polygons to point data or polygons to table data can be difficult. In Fig. 5(a), the region represented by the central polygon is directly connected to the larger blue point at the center of the image. Visual containment may not be an adequate visual metaphor to depict this connection because the region may not be directly connected to all the contained elements. In this case, a parachute symbology is used to identify an anchor point for the region. (The anchor point is the circle at the end of the dashed lines that connect the polygon vertices to the circle — essentially an upside down parachute.) Then, the anchor is linked to the blue point feature by the red arrow. Yet, while technically accurate, this visualization is not always visually intuitive.

An alternative approach to bridging visual representations is to use probes [18] as in Fig. 5(b). Here, the anchor point (yellow circle) is associated with the region by using a probe (vertical line). Then, the anchor point is linked to a table. While a probe is more effective than the parachute symbology in this example, probe-based visualizations present challenges when the anchor must be linked to a feature within the region that is near the base of the probe. Properly distinguishing the probe from the connection can be difficult under these circumstances.

3.3. *Registering and managing abstraction*

Critical infrastructure analysis occurs at different scales and scopes. As a result, the levels of abstraction associated with an analysis must be properly registered and managed. Russell, et al. [7] describe sensemaking as a cyclic process of searching for proper representations followed by instantiating these representations. The data ("residue"), which do not fit the instantiations, lead to the refinement of the representations, followed by re-instantiation, and so on. Mismatched levels of abstraction for representations – during their creation or instantiation – can mislead analysts. Visual analytics must address this challenge by managing the complexity of abstraction, making the level of abstraction apparent to the analyst and helping the analyst encode data properly.



(a) Parachute symbology. **(b) Probe symbology [18].**

Fig. 5 – Bridging visual representations.

(a) IT infrastructure abstraction. **(b) IT infrastructure dependencies.**

Fig. 6 – Exploring levels of abstraction.

For example, consider Fig. 6(a), which depicts a portion of the IT infrastructure of a Fortune 100 company. This interactive visualization allows IT analysts to explore the infrastructure at various levels of abstraction from the business unit level to the workflow level to multiple application levels all the way down to the hardware level (e.g., servers and routers). Fig. 6(b) depicts the same IT infrastructure with the key dependencies highlighted. Interactive visualizations such as these can help IT analysts develop a better understanding of their organization's IT infrastructure at multiple levels of abstraction.

3.4. *Exposing and exploring uncertainty*

Critical infrastructures are socio-technical systems with engineering and behavioral properties. Engineering properties are the underlying physics-based properties of physical resources and technologies that underlie an infrastructure. The behavioral properties of an infrastructure emerge from factors such as business processes, decision points, human intervention, and information generation, availability and flow.

Due to the socio-technical nature of critical infrastructures, their operation can involve substantial uncertainty.