Chapter 1

VISUALIZING CASCADING FAILURES IN CRITICAL CYBER INFRASTRUCTURE

Jason K. Kopylec, Anita D. D'Amico and John R. Goodall

Abstract This article explores the relationship between physical and cyber critical infrastructures, focusing on how threats and disruptions in the physical infrastructures can cascade into failures within cyber infrastructure. Through interviews with critical infrastructure protection experts and practitioners, we examined the issues in dealing with cyber infrastructure, including challenges with the management and organization of massive amounts of data that is geographically and logically disparate. Based on that understanding, we designed a system, named Cascade, for visualizing the cascading effects of physical infrastructure failures into the cyber infrastructure. Cascade will provide situational awareness to people who plan for and respond to crises related to Information and Communication Technology. Cascade shows how threats to physical infrastructures such as power, transportation, and communications can affect the networked enterprises that comprise the cyber infrastructure. Our approach applies the concept of punctualization from Actor-Network Theory to expose only the relevant disruptive effects and as an organizing principle for large collections of disparate infrastructure data. In particular, we show how to expose the critical relationships between the physical and cyber infrastructures. We discuss the availability of infrastructure data, and how this information can be depicted visually to maximize comprehension. This article also addresses the issue of representing both the logical and geospatial relationships within the cyber infrastructure. The resulting system design provides access to the cyber infrastructure's dependencies on other critical infrastructures, for use during disaster planning or crisis response.

Keywords: Critical infrastructure protection, cyber infrastructure, infrastructure dependencies, situational awareness, Actor-Network Theory, visualization, geographic information systems

1. Introduction

Within the Critical Infrastructure Protection (CIP) community, attention to the cyber infrastructure is directed at vulnerabilities that expose cyber assets to software-based attacks by outsiders, such as hackers, viruses or denial-of-service attacks, and the effects of those digital threats on physical infrastructures. Less attention, however, is directed at the impact of physical infrastructures on the cyber infrastructure [**?**]. Here, we explore how disruptions to physical infrastructures can *cascade* into disruptions to the cyber infrastructure, examine how the cyber infrastructure can be better incorporated into the larger context of CIP, and present the design of a software system that integrates information from both physical and cyber infrastructures.

There is a intricate web of dependencies between networked cyber assets and the external physical infrastructures that enable those assets to function and communicate. From the power grid that delivers electricity, to roads that deliver workers to the data center, a complex orchestration of services exists to keep a network up and running [**?**]. In addition, there are categories of vulnerabilities that are tied to geographic locations (e.g. earthquake faults, flood plains) that must be considered when assessing risk and planning for recovery. Those responsible for maintaining critical Information Technology (IT) systems must understand both the internal (i.e. cyber) and external (i.e. physical) infrastructures on which the cyber assets rely.

We studied how IT disaster planners and crisis responders examine the effects of other infrastructures on the cyber infrastructure. In addition to reviewing existing technologies and literature, we interviewed CIP experts and IT professionals, analyzing their current work practices and the challenges they face. These informants were drawn from county, state, and federal government agencies as well as from the academic and commercial sectors. They need to make time-sensitive decisions based on critical infrastructure data and diverse sensor data, both for proactive disaster planning as well as reactive crisis response. Although they have different primary job responsibilities, these diverse actors are linked by the shared concern with the planning, protection, and recovery of critical cyber infrastructures. Collectively, we refer to this group of practitioners as *IT crisis managers*.

IT crisis managers need to protect large-scale computer networks from both cyber threats – such as viruses, worms, and targeted cyber attacks – as well as physical threats – such as hurricanes or acts of terror. Despite this, we found that these practitioners focused their efforts almost exclusively on cyber threats, for the most part ignoring the effects that

physical infrastructure disruption could have on their IT systems. They had a poor understanding of the dependencies between infrastructures, which are complex and difficult to comprehend, especially under time pressure. IT crisis managers do not adequately understand the cascading effects on the cyber infrastructure from disruptions in other critical infrastructures. In addition, the data sources required during crisis planning and response are disparate and voluminous.

These challenges guided requirements and use cases for the design of a software system named *Cascade* that visually depicts the physical vulnerabilities of a network, the dependencies of those vulnerabilities, and how those vulnerabilities can propagate due to a computer network's dependence on other critical infrastructures (e.g. power). Our design includes the geographic location of critical computing resources and man-made or natural threats specific to the geographic region that could affect the computing resources. Our goal was to present information to IT crisis managers to support rapid vulnerability analysis and course-of-action evaluation when planning responses to potential threats, as well as an adjunct to command and control for those engaged in crisis management.

2. Related Work

Efforts have been made to understand how digital attacks disrupt the cyber infrastructure, and how those disruptions cause failures in other critical infrastructures [**?**, **?**]. Additional work has been done to provide quantitative metrics for measuring risk associated with these digital threats, see Longstaff et al. [**?**] and Lamm and Haimes [**?**]. In our work, we examine the relationship between cyber and physical infrastructures from the opposite perspective, i.e. instead of investigating how cyber threats affect other critical infrastructures, we focus on how threats and disruptions at the physical infrastructure levels may cascade into and interact with the cyber infrastructure.

To situate our work in understanding the effects of disruptions within physical infrastructures on the cyber infrastructure, we will briefly review related CIP literature. To study the propagation of threat between infrastructures, one must be aware of infrastructure interdependence. Understanding and documenting infrastructure dependencies is an essential step in coordinating disaster planning and emergency response [**?**]. There are two main approaches undertaken to understanding these dependencies and their role in infrastructure failure.

The first is to survey historical disasters. Most of what is known about infrastructure failure is the result of actual disasters. Identifying the causes and effects of previous failures and the infrastructures

involved helps to better plan for the future. Zimmerman has done extensive work in this area, surveying a large number of disasters in various infrastructures [**?**]. These results support using infrastructure dependency information for decision-making. Rinaldi et al. provide a foundation for how to learn from a disaster and map it into a framework of interdependent infrastructures [**?**].

The second method is to model and simulate infrastructure disasters. The development of computer simulations for critical infrastructure dependency is a new and rapidly evolving area of research that has yielded a number of diverse capabilities ranging in maturity levels. Robinson et al. describe the benefits and outline the goals of simulation-based infrastructure models [**?**]. Dudenhoeffer has done an extensive survey of this work [**?**] as well as design a simulation framework for supporting multiple interacting infrastructures, called Critical Infrastructure Modeling System (CIMS) [**?**]. CIMS introduces disaster scenarios on the modeled infrastructure to simulate the effects of infrastructure failures.

However, this previous research has not focused on incorporating the effects of disruptions in the physical infrastructures on the cyber infrastructure. Moreover, the results of these studies and simulations rarely reach disaster planners and emergency responders that can benefit from them; the IT crisis managers we interviewed were unaware that this work existed and none utilized infrastructure simulation technologies. This is unfortunate; much of this work is directly applicable to the cyber infrastructure, and the results of these infrastructure simulation systems could help disaster planners better understand infrastructure dependencies and vulnerabilities. The Cascade system, described later, can incorporate these systems to translate simulation results into actionable information for the IT crisis manager.

3. Linking Infrastructure Data

There are key challenges to linking cyber and physical infrastructures, noting the deluge of data and the unique aspects of cyber data. To overcome these challenges, we propose the process of induced depunctualization as an organizing principle for linking cyber and physical infrastructures, and demonstrate how this principle can be used to organize and filter infrastructure data.

3.1 Physical Infrastructure Data Challenges

There is a concerted effort in federal, state, and county governments to collect data about critical physical infrastructures. Geographic Information Systems (GIS) are often used to provide the robust storage,

visualization, and analysis solutions that are required. GIS allows for the use of geographic location as a baseline for bringing data from different infrastructures together. Within these geodatabases, infrastructure information takes the form of map layers, where each layer depicts some aspect of an infrastructure. For example, when storing information about the telecommunications infrastructure, a series of map layers will separately show the locations of telephone switching stations, fiber optic lines, telephone poles, and cell phone towers. Surprisingly, there are very few layers dedicated directly to the cyber infrastructure, such as the locations of government data centers. Without such location information, it is difficult to determine whether a flood, explosion, or power outage will damage or impede access to important cyber assets.

The collection of physical infrastructure GIS layers can be thought of as a large stack of map layers, one on top of another, growing taller and taller as new ones are added. When historical data is included, the number of layers grows even faster, making it difficult to discern the historical progress or unfolding of a crisis. It is difficult, if not impossible, to view all of these layers at once, nor can one easily select those most likely to affect the cyber infrastructure. As the information density grows, potentially important information is occluded and users are overloaded with data. This data overload makes it difficult to find the information most relevant to any single infrastructure. Suppose the IT crisis manager needs to decide where to place a back-up facility, or determine which data centers are at risk of shutting down during a hurricane. When presented with hundreds of infrastructure map layers to choose from, it is an arduous task to filter out all the irrelevant information to hone in on the layers that provide relevant information.

Another problem is that there is no straightforward method for connecting map layers, and therefore no way to relate different infrastructures. States like New York [**?**] and Montana [**?**] have amassed expansive databases of infrastructure map layers and begun efforts to provide simple search capabilities for map layers of interest. Still, these systems lack support for associating map layers from different infrastructures.

3.2 Cyber Infrastructure Data Challenges

The cyber infrastructure has characteristics that challenge its total representation within a GIS: it is geographically dispersed, incorporates components beyond the IT crisis manager's control, and is often dynamically reconfigured. Large enterprise networks will have many mission-critical servers geographically distributed. These servers may be logically related and support one organizational mission, yet they are housed

in different locations and may be vulnerable to quite different physical threats (e.g. hurricanes on the Gulf Coast, earthquakes on the Pacific Coast). Displaying such dispersed assets within one GIS display would require a scale that affords little space for details. The other side of this issue is that a single building may incorporate computing devices with very different missions. Separate database servers containing medical records and transportation records – each serving different missions – may be co-located and therefore share a common physical vulnerability even though they have no logical relationship. Furthermore, these large enterprise networks also rely on components such as an Internet Service Provider or a backbone provider that is outside the network owner's control and their location and status may be unknown. Finally, large enterprise networks are dynamic. Networks are reconfigured with new hardware, software is updated or replaced, and file content is changed at a frequency that far exceeds any configuration document or disaster plan. Thus, the current state of the system is often partially unknown. Because of this it is important to allow for frequent display refreshes and to provide the IT crisis manager with information about the age and reliability of the network-related data.

Whereas physical infrastructure data is collected and managed as GIS map layers, cyber data is collected through sensors – such as intrusion detection, network monitoring, or vulnerability assessment systems. This data is collected at different rates from the various sensors and often stored in multiple formats. Some of these systems can generate huge amounts of data. To fully understand threats to the cyber infrastructure, this data must be linked to the physical infrastructure; however, the cyber data is typically not stored in the GIS format of physical data.

3.3 Infrastructure as Actor-Network

In this section we describe a methodology for organizing the massive, complex data discussed in the previous section in a way that highlights only the relevant interaction effects between infrastructures. This principle forms the basis for our design and allows IT crisis managers to rapidly hone in on the data they require while filtering out irrelevant details. Malone and Crowston's coordination theory support these requirements, describing the importance and pervasive need to study the dependence between interacting systems [**?**]. We apply concepts from Actor-Network Theory (ANT) [**?**, **?**] to critical infrastructures to better meet these challenges. ANT provides perspective on how to view and analyze complex systems and interactions with disparate, yet coordinated, parts. A goal of ANT is to combine processes seamlessly with

the objects and interactions that constitute them. Law shows how ANT can be used to study disasters [**?**] and system failures [**?**] .

A key concept of ANT is punctualization [**?**], where many different, interacting parts of a complex system become abstracted and named by their collective emergent behavior [**?**]. In a punctualized system, the individual parts are hidden. We can apply this concept of punctualization to the problem of infrastructure protection. For example, the IT crisis manager views the electrical infrastructure as a single entity whose mission is to serve reliable power. In actuality, it is made up of thousands of power lines, generators, and transformers, all working together to provide the desired effect of electricity supply, but as long these individual parts work seamlessly to provide the power needed, they remain concealed.

This process of hiding the parts and only acknowledging a larger whole contributes to the challenge of studying infrastructure interactions and dependencies. Due to punctualization, interactions within and between infrastructures are hidden, so identifying vulnerabilities and threats to these invisible systems is extremely difficult. Perrow defines the complexities of such physical systems, outlining the visible and hidden interactions among them, motivating the question of how to make these hidden interactions visible [**?**]. Our work also attempts to understand why we cannot see some interactions and what we can do to make them visible. Returning to our example, when there is a power outage at a critical data center, the IT crisis manager no longer sees the electrical infrastructure as a single entity. Downed power lines, back-up generators, utility companies, and repairmen that go unseen during normal operation all become visible, exposing the infrastructure's parts, couplings, and dependencies. The hidden elements are rediscovered when an actor-network suffers from disruption or failure.

Although not explicitly described in ANT, but essential to the study of infrastructure dependency, is that when failure is introduced into a punctualized system, not all the parts are revealed. For example, if a critical data center loses power, only those systems that rely on that power become important. The status of back-up generators and possible failure of critical computer hardware are brought to attention. The data center operations may also rely on other elements, such as staff and telecommunications, but those remain hidden during the failure to the power infrastructure. Failure causes a partial depunctualization of the system, where the parts that become visible are those directly relevant to and affected by the failure; the rest of the punctualized system remains hidden.

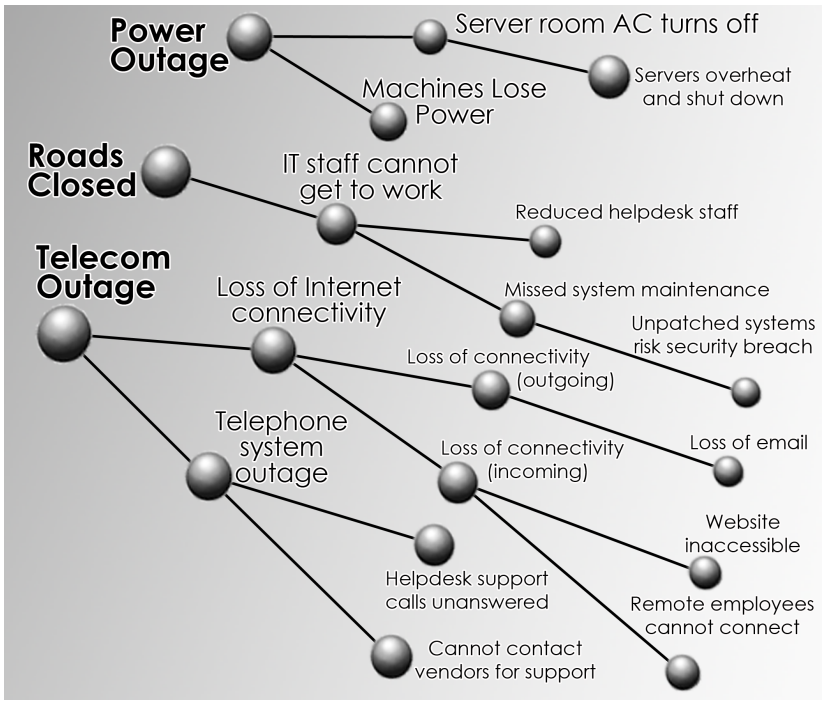

Figure 1. Cascading effects on a data center from disruptions to the power, transportation, and telecommunications infrastructures resulting from a hurricane.

Applied to CIP, this partial depunctualization is useful because even though the infrastructure interactions may be too complex to fully understand, the most relevant interactions are exposed. So although all the interactions between complex infrastructures may be difficult to define, we can learn those that are of most interest to CIP by studying and simulating failures in these systems. By purposefully inducing or simulating failure into these punctualized systems, we can uncover the relevant facets and connections between infrastructures, keeping the non-relevant portions hidden.

We propose to call this process that purposefully deconstructs an entity into its separate, dependent parts *induced depunctualization*. This process can be accomplished through either of the two methods discussed previously – surveying historical disasters or computer simulation. To illustrate the use of induced depunctualization to reveal cascading effects of other infrastructures affecting the cyber infrastructure, take the example of a hurricane hitting a critical data center. Figure **??** shows cascading infrastructure failures that can result from such a crisis.

This portion of a disaster scenario shows how three separate physical infrastructure failures, namely electrical, transportation, and telecommunications, can affect an enterprise computer network. Failures propagate across infrastructures, exposing otherwise hidden portions of those infrastructures in the process. For example, a common vulnerability in critical data centers is to connect critical servers to back-up power supplies, but not providing back-up power to the air-conditioning units that cool the servers. When a power failure occurs, the air conditioning systems shut off, causing the servers to overheat and shutdown, reducing the effectiveness of the back-up power. Depunctualization reveals this otherwise hidden dependency. Induced depunctualization provides a method for determining the relevant component dependencies and cascading disruptions of a physical infrastructure failure.

3.4 Organizing Infrastructure Data

As discussed earlier, there are huge collections of infrastructure data and, as more and more sensors are added to critical computing networks and other infrastructures, this deluge of incoming data will grow even faster. Missing from these collections is a filtering mechanism or organizing principle that can guide an IT crisis manager to the right information at the right time. The results of induced depunctualization analysis are useful in showing the potential disruptions that could cascade from an infrastructure failure.

Using the cascading effects from an induced depunctualization of the hurricane scenario that was depicted in Figure **??**, each step in this type of scenario can then be paired with infrastructure GIS map layers or network sensor data. Table **??** shows each of the failures from the hurricane disaster scenario with potential associated map layers or cyber sensor data sources. For example, an electrical outage map, which can be provided by the utility company, shows if a data center is in danger of losing power, which can be coupled with the status of back-up power supply and generator sensors to provide greater situational awareness. On their own, these individual physical or cyber components do not describe the power outage threat, but in combination they can help define the threat to IT systems.

Table **??** shows that at each possible disruption point, there are map layers or cyber sensors that can provide insight about how a network could be, or is being, affected. In addition, there is a way to organize the large number of data sources by pairing them only with the relevant failure entries. Combining both the physical and cyber infrastructure data allows IT crisis managers to fully understand the threats to their

Table 1. Infrastructure disruptions and associated physical map layers or cyber sensor data.

Infrastructure Disruption	Associated Data Source
Power outage occurs	Outage location map Backup generator status sensor UPS status sensor
Server room AC turns off	Server room temperature sensor
Servers overheat and shut down	Server status sensor
Machines lose power	Network status sensor Router status sensor
Roads are blocked	Snow accumulation map Traffic map
IT staff cannot get to work	IT staff house locations map IT staff route to work map Traffic map
Help desk staff is reduced	Trouble ticket status Help desk on-hold wait time
System maintenance is missed	System maintenance schedule
Unpatched systems risk security breach	Intrusion detection sensor

critical cyber assets. However, the data can be difficult to comprehend without visual aids. In the next section, we demonstrate how to display the data using the organizing principle of induced punctualization to enable IT crisis managers to plan for and respond to threats to their cyber assets.

4. Visualizing Cyber & Physical Infrastructures

Presenting cyber and physical infrastructure information to an IT crisis manager intuitively to allow for planning or provide situational awareness is paramount. Here we describe our design for providing this capability; Figure **??** shows the proposed organization for our Cascade user interface. The system design provides multiple coordinated views that present potential infrastructure disruptions and their cascading effects, and supporting GIS infrastructure map layers and network topology.

Combining physical and cyber infrastructure data within these views enables IT crisis managers to easily determine if a threat or disruption is occurring or may occur. Our design incorporates: cascading infrastructure failures – shows cause-effect of what can go wrong; disaster plan documents – suggests what to do when failures occur; infrastructure GIS

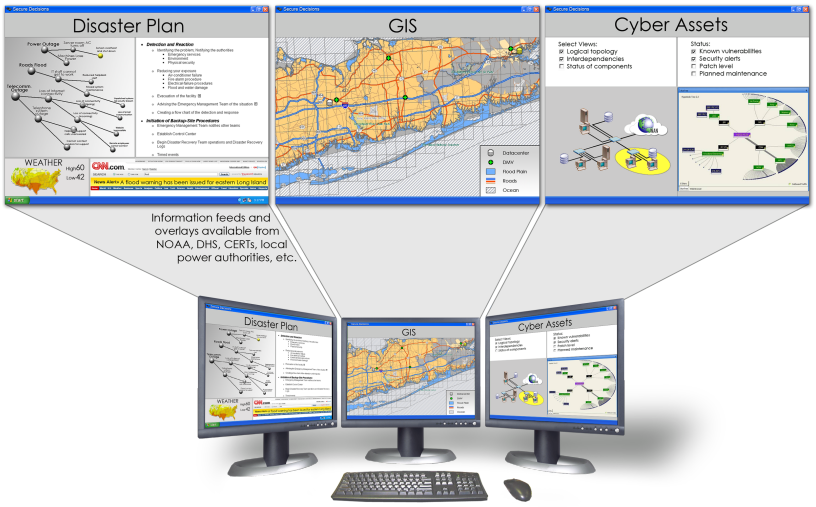

Figure 2. Coordinated views of cascading effects relate GIS infrastructure map layers to network topology.

data – provides status of physical threats to the network; and network topology – connects infrastructure data to affected network function.

4.1 Cascading Effects & Disaster Plans

The first view, shown in Figure **??**, provides information about what can fail and what to do about it. Presenting the cascading effects of vulnerabilities on network operations illuminates the possible failures. Specific scenarios – such as hurricane, fire, or pandemic – can be chosen and displayed. These scenarios can either be hand-crafted or generated from underlying infrastructure dependency simulation.

Including disaster planning documents directly into the interface puts them at the fingertips of the IT crisis manager and affords coordination with the other views. For example, a user can link to staff contact lists, news feeds, or weather reports. If the user clicks on a node in the scenario for the failure "reduced help desk staff", he or she can be directed to the portion of the disaster plan that outlines how to deal with this problem.

4.2 GIS Infrastructure Data

As discussed earlier, much of the critical infrastructure data is stored in the form of large collections of GIS map layers. The second view incorporates these, as shown in Figure **??**. The advantage to map displays lies in the ability to overlay very different kinds of information in the

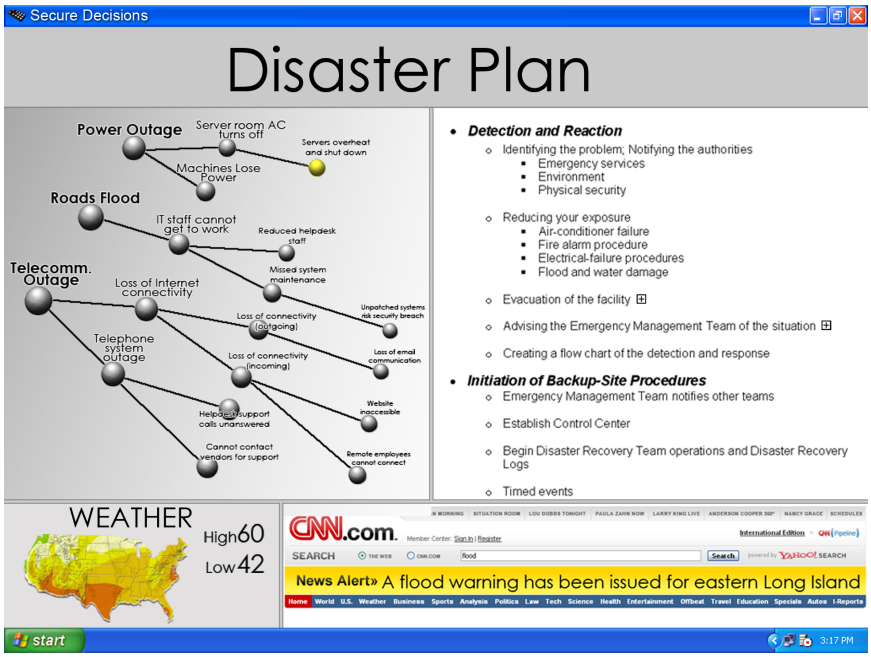

Figure 3. Cascade view depicting cascading failures and disaster plans.

same space, using their physical location as the underlying connection. GIS displays and analysis tools play a central role in collecting and using critical infrastructure information.

Cascade leverages GIS to present a familiar view of infrastructure data. By coordinating the disaster plan view with the GIS view, we can use the failure-to-data associations to organize which map layers to look at. This provides the fundamental mechanism for organizing large catalogs of map layers and implicitly shows the dependencies between infrastructures.

4.3 Coordinating the Physical and Cyber

The final view, pictured in Figure **??**, closes the loop between the physical locations of critical cyber assets and where they function within the network topology by showing the logical layout of the network. This view depicts how workstations, servers and network hardware are organized and connectioned into logical subnets, showing how connections can be made between machines and to internet gateways. Additional information can be visually layered onto this logical network base view,

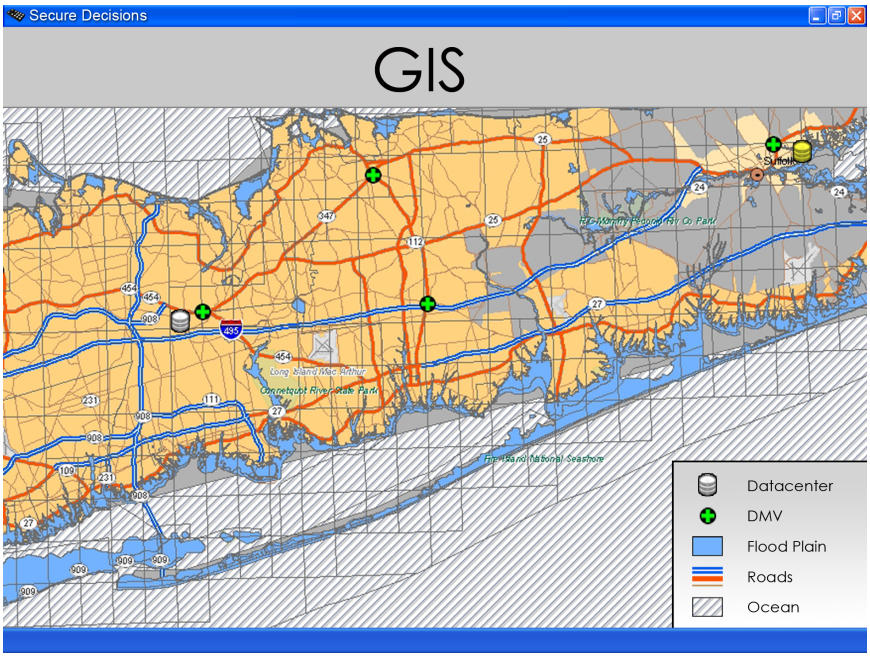

Figure 4. Incorporating GIS to view associated infrastructure map layers.

such as the status of software patches, power availability, temperature, connectivity, etc.

Cascade combines the network topology view into a coordinated application with disaster planning and infrastructure GIS, allowing interactive exploration of how infrastructure effects cascade onto both physical cyber assets and the network impact of those failures. For example, an IT manager in the middle of a hurricane crisis might click on the failure 'Server Room AC shuts off'. This brings up a GIS status map of all the data center's air conditioning systems. Spotting one that has failed in a particular building, he or she clicks on it. The corresponding critical servers in the network topology window light up, showing which are at risk for overheating. There is an intuitive and seamless integration of asset status, infrastructure data, and network information that provide an IT crisis manager with a full picture of the effects to the network when failures occur.

5. Conclusion

The Cascade system provides a mechanism for both understanding cascading failures from outside of the network and organizing massive

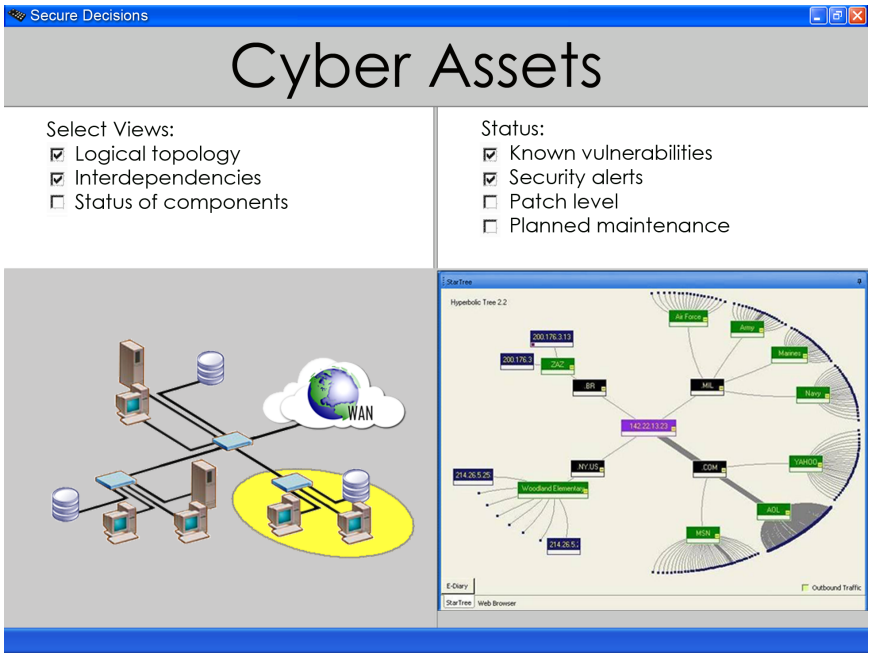

Figure 5. Showing network topology and critical cyber assets.

amounts of infrastructure sensor and GIS data. The combined and coordinated geographic and network topological views provide awareness over both the physical and logical aspects of a large-scale computer network. The intuitive, interactive visualization of disaster plans illuminates the cascading effects of infrastructure failures. Coupling these functions is essential to the stability and survivability of critical cyber assets.

Our work builds upon the current directions in CIP and highlights the importance of including traditional IT operations more fully in these endeavors. GIS systems are now being used to catalog and view the components of various infrastructures. Historical analysis and computer simulations have been performed to derive models of the dependencies between critical infrastructures. However, portions of the cyber infrastructure have been largely ignored in GIS representations and dependency modeling. IT systems are tremendously important to the functioning of physical infrastructures, and although researchers have focused on this dependency (i.e. cyber to physical), the reverse (i.e. physical to cyber) has been an understudied area.

IT crisis managers, who must keep critical computing networks operating during all types of natural or man-made disasters, need more

information than is currently available regarding how vulnerabilities and failures in other critical infrastructures can cascade into mission-critical enterprise networks. Because the cyber infrastructure is geographically dispersed, includes computing components outside the IT manager's control, and is often reconfigured, it is technically challenging to model its interactions with other critical infrastructures and to present this information in a comprehensible fashion to the IT crisis manager.

Our research, including interviews with individuals responsible for maintaining continuity of computer network operations during crises, led us to investigate Actor-Network Theory as a method to deconstruct how the cyber infrastructure could be affected by failures in other critical infrastructures. These interviews further informed the design of a display system to provide situational awareness to IT managers who are preparing disaster plans and responding to crises.

The proposed Cascade system is a way to not only fuse and organize the massive amounts of infrastructure information currently in use; it can display this information visually and intuitively for fast comprehension and action on the part of those managing essential computer networks. The continued implementation and operational fielding of tools like Cascade, coupled with maturing infrastructure simulation systems and risk management tools will greatly add to the resilience of critical cyber infrastructure. This resilience will have the positive cascading effect of greater reliability and trust in all critical infrastructures.

Acknowledgments

This research was funded by the Office of Naval Research, contract #N00014-06-M-0146.

References

[1] D. Dudenhoeffer, S. Hartley and M. Perman, Critical infrastructure interdependency modeling: A survey of U.S. research, *Proceedings of Third International Conference on Critical Infrastructures*, 2006.

[2] D. Dudenhoeffer, M. Permann and M. Manic, CIMS: A framework for infrastructure interdependency modeling and analysis, *Proceedings of the 2006 Winter Simulation Conference*, pp. 478–485, 2006.

[3] E. Eidswick, Montana spatial data infrastructure: Enhancing an all-hazards approach to emergency preparedness, *ESRI Homeland Security GIS Summit Proceedings*, 2006.

[4] J. Goldstein, Emergence as a construct: History and issues, *Emergence: Complexity and Organization*, 1, pp. 49–72, 1999.

[5] V. Kumar, J. Srivasta and A. Lazarevic, *Managing Cyber Threats: Issues, Approaches, and Challenges*, Springer, 2005.

[6] G. A. Lamm and Y. Y. Haimes, Assessing and managing risks to information assurance: A methodological approach, *Systems Engineering*, 5(4), pp. 286–314, 2002.

[7] B. Latour, *Reassembling the Social: An Introduction to Actor-Network Theory*, Oxford University Press, 2005.

[8] J. Law, Ladbroke Grove, or how to think about failing systems, Technical Report, Lancaster University, Lancaster, UK, 2000.

[9] J. Law, Notes on the theory of actor-network: ordering, strategy, and heterogeneity, *Systems Practice*, 5, pp. 379–393 1992.

[10] J. Law, Disasters, a/symmetries and interferences, Technical Report, Lancaster University, Lancaster, UK, 2003.

[11] T. A. Longstaff, C. Chittister, R. Pethia and Y. Y. Haimes, Are we forgetting the risks of information technology? *Computer*, 33(12), pp. 43–51, 2000.

[12] T. W. Malone and K. Crowston. Toward an interdisciplinary theory of coordination, CCS Technical Report #120, Massachusetts Institute of Technology, Cambridge, Massachusetts, 1991.

[13] National Infrastructure Protection Plan. (http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf).

[14] New York State Geographic Information Systems Clearinghouse (http://www.nysgis.state.ny.us/).

[15] C. Perrow, *Normal accidents*, Princeton University Press, 1999.

[16] S. M. Rinaldi, J. P. Peerenboom and T. K. Kelley, Identifying, understanding and analyzing critical infrastructure interdependencies, *IEEE Control Systems Magazine*, pp. 11–25, 2001.

[17] C. P. Robinson, J. B. Woodward and S. G. Varnado, Critical infrastructure: Interlinked and vulnerable, *Issues in Science and Technology*, 15(1), pp. 61–67, 1998.

[18] R. Zimmerman, Decision-making and the vulnerability of interdependent critical infrastructure, *Proceedings of IEEE International Conference on Systems, Man and Cybernetics*, pp. 4059–4063, 2004.

[19] R. Zimmerman, Critical infrastructure and interdependencies, in *McGraw Hill Handbook of Homeland Security*, David Kamien(ed.), 2005.

[20] R. Zimmerman and C. E. Restrepo, The next step: Quantifying infrastructure interdependencies to improve security, *International Journal of Critical Infrastructures*, 2006.