Complexities of Simulating Domestic Infrastructure Protection

Roger Smith
Titan Systems Corporation
Orlando, Florida 32765
rdsmith@titan.com

Keywords:
Infrastructure Protection, Terrorism, Homeland Security, System Complexity

ABSTRACT: *The war on terrorism includes a broad range of military, political, intelligence, legal, and social actions. In a previous paper we explored several of these domains and their relationships to each other. We argued for the creation of a federation of simulation tools to represent all of these domains. In this paper, we explore the concept of modeling the national infrastructure, one part of the physical domain described in the previous paper. The interest is in understanding how attacks on that infrastructure will impact the services provided, economy supported, and lifestyles enabled by it.*

The national infrastructure includes air transportation, ground transportation (e.g. interstate trucking, railroads, highways, bridges), water, power, telephone, cellular telephone, Internet, sewers, food distribution, and social events (e.g. shopping, sports, entertainment). Each of these is defended by the specific commercial or government organization that provides the service. There is no unified system of protection or warning across these systems. The impact of disrupting one or more of these services is not fully understood by national decision makers. Models and analytical tools can be used to explore multiple combinations of interactions and the collective impact of disrupting one or more of these systems. A modeling tool and environment sufficient to study these assets is a significant challenge, but one that our industry and country may find necessary to cope with the complexities of 21st Century homeland security.

This paper explores concepts for creating a simulation of the national infrastructure and the protective measures that are currently in place. Such a model would include terrorist attacks on these networks and the native defenses, emergency management, counter-terrorism, and anti-terrorism responses to these attacks. The number of assets and points of vulnerability within the national infrastructure are so high that protection cannot be provided to all of them, but must be assigned to the most critical. The necessary rankings cannot be performed without a clear understanding of the value of each asset, an understanding that can be improved through the use of models and simulations.

1. From Counter-terrorism to Infrastructure Protection

"[Al-Qaeda] has regrouped and will expand its war to include assassinations and attacks on 'the enemy's weak infrastructure.'"
- Abu-Leith al-Libi, Al-Qaeda Spokesman

Al-Qaeda is just one of many organizations that want to disrupt Western governments, businesses, and economies. This decade will require the reorientation of civil and military assets on the terrorist threat. These assets include models and simulations that are used to understand, predict, and rehearse these threats.

The services that tie society together form an infrastructure that spans the entire geography of the country and provides interfaces through which we communicate with the rest of the world. This infrastructure enables the style and standard of living for the country. In many ways, the infrastructure is the physical manifestation of what it means to be a member of the country. Advanced countries are supported by hundreds of distinct and interacting service infrastructures. Protecting these from destruction, disruption, and corruption is a vital part of national security.

National infrastructures are so large, complex, and intertwined that understanding how they work, how they fail, and how best to protect them is a significant problem. Modeling and simulation is one tool that can be used to explore these problems. Simulation tools that capture the behaviors of the systems, the relationships within and between the systems, and that have some ability to measure the impacts of disrupting these systems are an essential part of an effective plan for protecting the infrastructure.

In a previous paper we described the multiple dimensions of the terrorist threat and its relationship to national defense initiatives [8]. This paper builds on that work by further exploring the physical domain of the problem, specifically the protection of the national infrastructure (Figure 1-1). The value of applying simulation to this problem has also been recognized within the US government as evidenced by the recent creation of the National Infrastructure Simulation and Analysis Center at Sandia and Los Alamos National Laboratories. Together those labs have a history of modeling large systems such as the energy distribution network, national economy, and city traffic patterns [5].

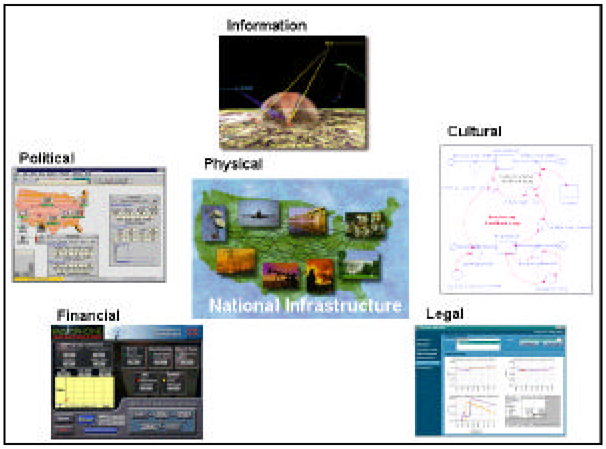

Figure 1-1. National Infrastructure in the Physical Domain

We believe that protecting the infrastructure is also a means to another end. The infrastructure is simply a mechanism for providing resources that support the national economy and provide a nation-specific lifestyle (Figure 1-2). The real goal in protecting the infrastructure is to maintain that economy and lifestyle. This change in perspective allows us to search for ways to achieve that higher-level goal. We should consider ways to change the support system for the economy and lifestyles, not just protecting the infrastructure for its own sake.

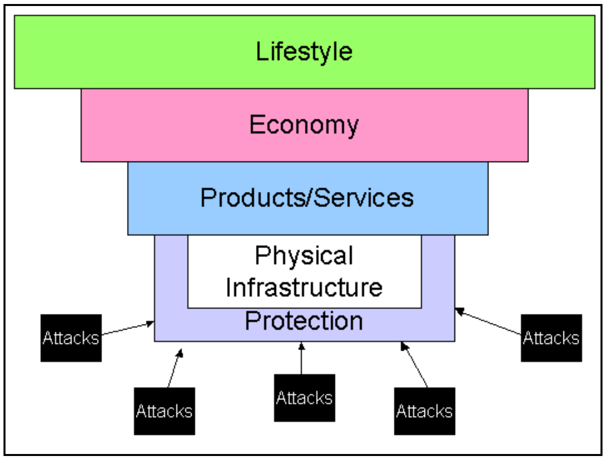

Figure 1-2. Infrastructure Role in Supporting the National Economy and Lifestyle

2. Size of the Problem

The term “national infrastructure” is a huge umbrella that covers thousands of different systems and hundreds of millions of users. The most studied of these infrastructures is the electric power generation and distribution system. The second most studied is the telephone system, followed by water processing. All of these are an essential part of the social fabric of a country and constitute assets important enough to protect. However, these are just the beginning of a long list of critical infrastructures that enable a society or country to operate. Table 2-1 lists the infrastructure sectors and systems identified by the President’s Commission on National Infrastructure Protection [4].

Table 2-1 Critical Infrastructure Sectors and Systems

Information & Communications
Telecommunications Internet Public Computers
Physical Distribution
Highways Ports Railroads Waterways Pipelines Air Transportation Mass Transit Trucking Delivery Services
Energy
Electric Power Natural Gas Oil Coal
Banking & Finance
Banks Financial Services Investment Companies Payment Systems Mutual Funds Securities Exchanges Commodities Exchanges
Vital Human Services
Water Sewer Emergency Services (Police, Fire, Medical) Government Services

The fact that so many of these systems are dependent upon electricity makes it clear why electric power generation and distribution is the most studied of these systems. Every one of the systems has experienced outages and the impacts of those outages are understood in a very general way [6]. However, an intentional attack against most of these systems has not been experienced. Neither has an attack against multiple co-dependent systems been experienced. So the cumulative impacts are not clearly understood. Recognizing the immediate effects of losing power to a geographic area for a defined number of days is clear. But, understanding the economic, health, safety, and national security impacts of outages are less clear, especially when multiple outages are experienced at the same time. Simulations can help is understand and explore such events.

We also understand that all of these systems are interrelated. The failure of one network can lead to the failure of another. In the worst case, a domino effect can develop in which multiple system failures are triggered by the initial failure of a single system. As an example, the Federal Railroad Administration estimates that cessation of rail delivery of goods would result in the cessation of automotive, paper, coal, and plastic industries within a few days or weeks [2].

3. Sustainment vs. Protection

A simulation that demonstrates the vulnerability of the infrastructure systems listed above is useful in understanding how the system works today. It can be used to identify key nodes that must be protected and key users of the infrastructure that need to be supported by back-up systems and special protection. However, a simulation should also be used to search for better ways to operate and protect the systems and the consumers that depend upon them. The defined purpose of “infrastructure protection” is to erect a defensive barrier around critical resources such that they cannot be penetrated [4]. Given the extreme distribution of these networks, it is unlikely that such a barrier can be constructed. Well-known examples of this problem involve the security of oil pipelines in Alaska and South America. Dissident groups attack these lines at random points across thousands of miles of pipe. Protecting such a distributed network has proven impossible. Oil companies have found that the best solution is to install warning systems that alert the infrastructure owner that a breach has occurred, enabling them to minimize the time to respond to the problem.

Table 3-1. Sample of the Magnitude of the National Infrastructure

137 Major Cities
2,800 Powerplants
    10X Power Sub-stations
463 Skyscrapers
600,000 Bridges
123,000 miles of Railroad Tracks
190,000 miles of Oil & Gas Pipeline
20,000 miles of National Borders

Sources: RAND, FEMA, FRA

Similar issues will exist with all of the systems that make up the national infrastructure, a small portion of which is characterized in Table 3-1. A comprehensive solution should include defense, deception, redundancy, self-healing, alternative services, emergency responses, trained consumers, resource stockpiles, and new expectations from customers. Taken together, all of these actions create a plan for critical service sustainment rather than infrastructure protection. Under this concept, services are sustained by a number of changes to the entire system, such as those shown in Table 3-2. A simulation that can study the different combinations of changes that can be applied and the effectiveness of each of them is a much more valuable tool [1]. Such a simulation could play an important role in restructuring and augmenting infrastructure systems such that customers experience a minimal loss of service.

Table 3-2 Critical Services Sustainment

Solution	**Description**
Defense	Barriers that prevent attackers for accessing or damaging the system
Deception	Decoys that lead attackers to the wrong targets.
Redundancy	Multiple paths and resources for providing services to customers.
Self-healing	Enabling the system to repair itself.
Alternative Services	Providing replacements for primary services.
Emergency Response	Establishing resources and plans for recovering from an attack.
Trained Customers	Teaching the customer how to handle outages and to execute their own recovery plan.
Resource Stockpiles	Identifying the necessary stockpiles to continue operations during an outage.
Modify Expectations	Changing the customer’s expectations for service reliability.

Creating a network of sustainment that includes all of the solutions shown in Table 3-2 is a very complex problem. It is more complex than understanding the system as it exists now. Modeling this problem will require the creation of new ways to represent systems. Many of the existing system dynamics tools can combine generic components to create models of specific systems [6]. But, a more comprehensive view of the systems is necessary to represent service sustainment. In such a model, alternative sources of services and the actions of the customer must be represented. Sandia analysts have created generic services modules that takes advantage of commonalities within many of the systems (Figure 3-1). Their goal is to create a modeling structure and software modules that can capture the interdependencies between each of the pieces by customizing generic models and linking them together to form a complex system.

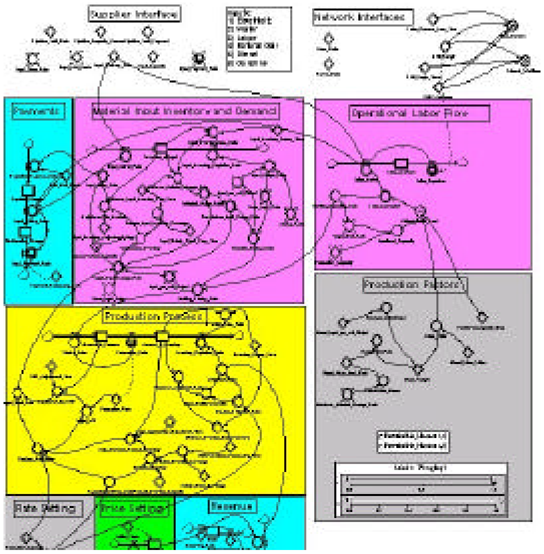

Figure 3-1. Sandia's Generic Service Module

4. Modeling Sustainment

A traditional system model represents a node as an algorithm that responds to stimuli from various sources (Figure 4-1). These algorithms can take the form of a simple equation of growth rates, an index into a table of prepared data, or a reference to an external model. An infrastructure sustainment model should combine contributions from all of the categories listed in Table 3-1. The infrastructure does not standalone against the attack. Instead a node would represent the infrastructure and its own native ability for self-healing. This would be supplemented with defenses available to that node and the deception that is available to divert the threat. If each of these is defeated, then the degradation of the node would trigger the application of redundant resources such that the customer is minimally aware of the attack. It would also draw upon available emergency response resources to restore operations.

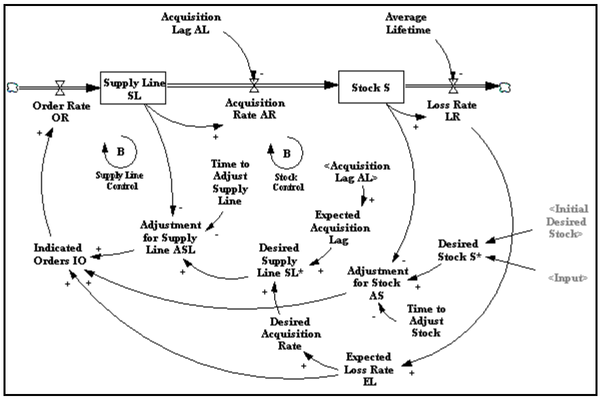

Figure 4-1. System Dynamics Model Algorithm Examples

In this environment, the customer may experience no loss of services. Or they may need to turn to alternative services to continue their economic operations or maintain their lifestyle. The customer may also require emergency services and may turn to resource stockpiles to continue operations. The model should also include modified customer expectations and an increased reliance on alternatives and stockpiles. Figure 4-2 graphically represents these factors and their relationships to each other.

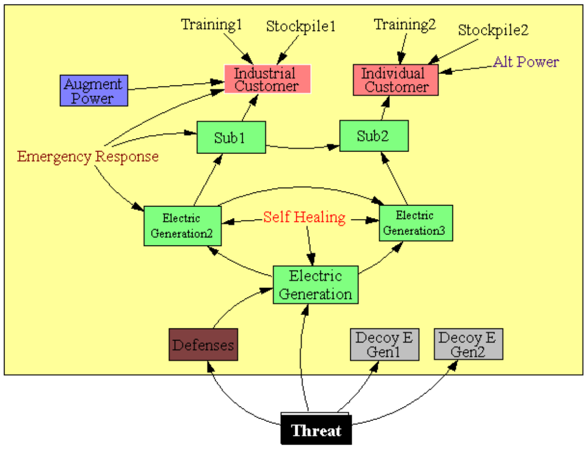

Figure 4-2. Model of Critical Service Sustainment.

5. Measures of Effectiveness

A model of all of the cross-dependent systems described in the previous section must include measures of effectiveness (MOEs) that capture the strengths and weaknesses of the aggregated system. The composite system performance may be measured using criteria concerning the performance of the entire system. Some of these MOEs are described in the following sections.

Nodes Down

The number of nodes that are disabled by the attack is an important MOE. It demonstrates both the magnitude of the attack and its effectiveness against protective measures that may have been taken. Since a system can be made inoperable through the destruction of a single key node or by eliminating a number of interrelated nodes, this MOE must include identifications of the nodes affected, their locations, and their degree of connectedness to other nodes and infrastructure sectors.

Time Down

The time that the nodes are not able to provide products or services to their customers is another useful MOE. This measure should focus on the experience of the customer, not on the technical status of the infrastructure nodes. There are many conditions under which the nodes can be considered operational, but the customer still receives no products or services. The important effect is denial of service to the customer, so the health of individual nodes is of less interest than the ability of the entire system to provide services.

Trickle Down

A failure in one system may trigger failure in another. For example, the loss of electrical power can severely impact systems for transportation and communication. So trickledown is a measure of the interdependencies among systems. It may also be important to understand whether a local failure was triggered by trickledown from a single outside system of from the cumulative effects of multiple systems.

Users Down

The number of users that lose service is a good measure of the effectiveness of an attack. This number may be a combination of both direct attack effects and safety shutdowns initiated within the system. This is effectively an internal trickledown effect. The identity and capacity of a specific user is important in measuring the impact of an attack.

Finances Down

Measuring the financial impact of losing pieces of the infrastructure is a very difficult thing to do in a model. There needs to be a way to represent the economic productivity of the systems and their customers. This should be separated into productivity that is recoverable and that is irrecoverable. Late delivery of frozen meat to a grocery store may be a recoverable loss because the meat can be sold the next day. But a day of lost electric or Internet service is not recoverable. In many cases this separation is heavily influenced by the duration of the loss of the infrastructure. Some customers can easily absorb the loss of Internet connectivity for an hour or even a day, but others are not able to tolerate this loss for even one minute.

Confidence Down

Successful attacks will negatively influence the confidence levels of infrastructure customers and of the general populace. This lack of confidence or security can be expressed in many different ways. It may cause people to move away from high-priority targets, to travel less, remain in their jobs longer, take more sick leave, or postpone major purchases. All of these are personal expressions of a change in confidence.

6. Conclusion

Modeling and simulation may be able to provide valuable support to National Infrastructure Protection. One of the most valuable additions would be in exploring alternative modifications to the current methods of protection and service sustainment. The extremely large size of the national infrastructure and the difficulties faced in completely protecting all of the systems involved, make it nearly impossible to prevent attacks against every part of the infrastructure. It is important to recognize that these infrastructures support the national economy and lifestyle and that those are the real assets that we want to protect and that our enemies want to disrupt. Infrastructure protection programs and studies should focus on maintaining the economy and lifestyle, and protecting the various infrastructures across the country is one factor in achieving this.

7. References

[1] Booz-Allen & Hamilton. (1997). "Critical Infrastructure Protection Strategic Simulation Report". Report to the President's Commission on Critical Infrastructure Protection. Washington D.C.

[2] Federal Railroad Administration. (1997). "Basic Characteristics of Freight Rail Transportation in the United States". Report to the President's Commission on Critical Infrastructure Protection. Washington D.C.

[3] Lofdahl, Corey. (2002). "Characterizing the Terrorist Threat". Presentation at the 70th

Military Operations Research Society Symposium. Leavenworth, Kansas.

[4] Marsh, Robert. (October, 1997). “Critical Foundations: Protecting America’s Infrastructure”. Report of the President’s Commission on Critical Infrastructure Protection. Washington D.C.

[5] Nelson, Jennifer. (2002). “Critical Infrastructure Surety Activities at Sandia National Laboratories”. http://www.sandia.gov/

[6] Robinson, C., Woodard, J., & Varando, S. (Fall 1998). “Critical Infrastructure: Interlinked and Vulnerable”. Issues in Science and Technology Online. http://www.nap.edu/issues/15.1/robins.htm

[7] Sandia National Laboratories. (1997). “US Infrastructure Assurance Prosperity Game Final Report”. Report to the President’s Commission on Critical Infrastructure Protection. Washington D.C.

[8] Smith, Roger. (2002). “Counter-terrorism Simulation: A New Breed of Federation”. *Proceedings of the Spring 2002 Simulation Interoperability Workshop*. http://www.simulationfirst.com/papers/

[9] Smith, Roger. (1996). “I^n: The N Dimensions of Interoperability”. *Proceedings of the 1996 Interservice/Industry Training Systems and Education Conference*. National Defense Industrial Association. http://www.simulationfirst.com/papers/

[10] Sterman, John. (2000). *Business Dynamics: Systems Thinking and Modeling for a Complex World*. McGraw Hill. New York: NY.

[11] U.S. Government. (2001). “National Plan for Information System Protection, Version 1.0”. Washington D.C.

Author Biography

ROGER D. SMITH is a Vice President and Group CTO at Titan Systems Corporation working on next-generation simulation applications and distributed computing technologies. His most current work has been creating techniques to model information operations, counter-terrorism, and infrastructure protection. He is the creator and instructor of a series of military simulation courses that have educated hundreds of simulation professionals. He is also the Area Editor for Distributed Simulation for *ACM Transactions on Modeling and Computer Simulation* and is actively involved in promoting the expansion of the simulation profession.