Chapter 9*

Building Analytical Support for Homeland Security

Sanjay Jain[1], Charles W. Hutchings[2], and Yung-Tsun Tina Lee[2]
[1]*The George Washington University, Washington, DC, USA*
[2]*National Institute of Standards and Technology, Gaithersburg, MD, USA*

9.1 Introduction

This chapter discusses modeling and simulation as a significant means for providing analytical support for homeland security problem solving and decision making that involves what can be considered a complex and dynamic system of systems – the current, human, domestic environment considered from a national perspective. Homeland security, in general, aims to understand the domestic environment and mitigate risks from both natural and human threats and hazards. Homeland security analyses and decisions occur at multiple levels from individuals, communities, and regions to national governments and even international organizations. Sufficient, available knowledge of the domestic environment and likely threats help decision makers at multiple levels with mitigating risks or in responding to and recovering from adverse events that occur.

Most homeland security risks involve significant unknowns and varying levels of uncertainty. An example of a natural hazard is a large hurricane approaching a coastal city, which is likely to occur each hurricane season. Coastal regions in the United States

* *Modeling and Simulation Support for System of Systems Engineering Applications*, First Edition.
Edited by Larry B. Rainey and Andreas Tolk

affected by hurricanes prepare for them and have implemented approaches such as building codes and evacuation procedures to mitigate risks to property and lives.

At the national level, organizations like the National Infrastructure Simulation and Analysis Center (NISAC) (Sandia 2013a) operated by the U. S. Department of Homeland Security (DHS) provide analyses of the potential impacts of hurricane damage to an array of critical infrastructure such as the electric power grid, telecommunications, transportation systems, water supply systems, and health care systems. NISAC analyses aid decision making at the regional or national levels in planning for, responding to, and recovering from hurricane damage (Sandia 2013b). Hurricane tracks and associated damage are not exactly predictable; however, weather patterns occur each year that lead to hurricane formation and these storms are expected to threaten many areas. Other types of disasters due to unusual natural events, accidents, or terrorism, are often unexpected and surprise decision makers and homeland security officials.

Incident management requires significant knowledge of the domestic environment, operating under normal conditions, as a basis for understanding each adverse event and its resulting interactions and impacts on multiple independent, interconnected systems. First responders and government officials often use exercises based on anticipated disaster scenarios to train for incident management, explore incident management techniques, and gain insights into organizational, logistical, and other incident management issues. The benefits of exercises include:

- Valuable experience to participants on relevant issues and responsibilities
- Testing of communications channels between first responders and higher level incident management organizations
- Improved working relationships between participants to improve responses to and management of real disasters
- Identification of gaps in capabilities and/or procedures

Exercises provide a means to explore the unknowns and uncertainties associated with various threats and hazards but have some significant limitations. Depending on the scope and complexity of an exercise, these include:

- Contrived exercise scenarios based on known prior events
- Lack of analytical capabilities to assess incident management decisions and explore different courses of action to improve learning outcomes.
- Difficulties in planning and successful orchestration
- Significant time and funding for exercise development and execution

Modeling and simulation capabilities provide an alternative means to explore unknowns and uncertainties associated with various threats and hazards, especially when coupled with exercises or serious games. Understanding the functions of one type of domestic system under abnormal operating conditions imposed by an adverse event is an

analytical challenge by itself. Understanding the functions of a system of systems under both normal and abnormal operating conditions requires advanced analytical techniques that include modeling and simulation capabilities since aspects of a domestic system of systems can respond in unexpected ways due to cascading effects of a disruption. Since a domestic system of systems cannot be re-created and experimentally studied under either normal or adverse conditions, modeling and simulation capabilities are the only available means to rigorously explore this domain and provide useful insights to analysts and decision makers.

The required modeling and simulation capabilities to support homeland security analyses are diverse, and the set of these capabilities used to analyze and manage homeland security could be considered a system of systems itself from the perspective of a government agency like DHS. For example, each critical infrastructure sector has its own analytical approaches – critical data, analysis methods, key performance indicators, experts, models, etc. – to understand and support internal management and decision making in each sector. A homeland security agency needs to engineer an analytical system of systems that integrates diverse analytical capabilities and data to support homeland security analyses and problem solving. A framework for homeland security knowledge sharing is essential to enable this analytical system of systems and the application of models and simulations as analytical components.

This chapter proposes a knowledge sharing framework to improve modeling and simulation as an analytical capability for homeland security. The next section identifies the characteristics of the homeland security domain that identify it as a system of systems as defined in Chapter 2. Section 9.3 establishes the need for an organized approach and framework to address the homeland security domain. Section 9.4 proposes a knowledge sharing framework. Section 9.5 describes a prototype application of modeling and simulation for system of systems to analyze an emergency incident. Section 9.6 summarizes the chapter. The last section provides the list of references.

9.2 Homeland Security and System of Systems

Homeland security self-evidently involves a system of systems according to the criteria described in Chapter 2. Homeland security aims to preserve the current, human, domestic environment from disruption or damage caused by various kinds of natural phenomena or human activities. The domestic environment is an assemblage of systems which exhibit properties of operational independence, managerial independence, geographic distribution, emergent behavior, and evolutionary development.

- Operational Independence of the Individual Systems: The domestic environment is composed of multiple types of collaborative systems that are independent and useful

in their own right. Critical infrastructure sectors such as energy, communications, water and waste water systems, and healthcare and public health sectors are examples. Although many systems are interdependent, e.g., most systems are connected to the electric power grid, other component systems of the domestic environment are capable of performing useful operations independently of one another. Domestic environments existed well before development of the electric power grid.

- Managerial Independence of the Individual Systems: The component systems of the domestic environment not only can operate independently, they operate independently to achieve their own purposes as well as the purpose of the integrated whole. The critical infrastructure sectors such as the financial services and communications are examples.
- Geographic Distribution: The component systems of the domestic environment such as critical infrastructure sectors are distributed and networked throughout geographic boundaries. Components of the communications system, for example, extend across the globe and into space.
- Emergent Behavior: The domestic environment performs functions and carries out purposes that do not reside in any component system. For example, nations and distinctive national cultures emerge from domestic environments. In many nations, well developed critical infrastructure enhances the domestic environment and improves standards of living that in turn support national development and growth which can occur in unpredictable ways.
- Evolutionary Behavior: Domestic environments are never fully formed or complete. They evolve over time. Technological innovations, such as development of the internal combustion engine, the digital computer, and telecommunications networks for example, alter domestic environments in profound ways.

Homeland security functions involve analyzing and understanding various components of the domestic system of systems to assess potential operational risks and related impacts on the domestic environment. Understanding the domestic environment and managing risks associated with natural and man-made threats and hazards requires the collaborative assemblage and use of vast amounts of information of varying types and quality from multiple, independent sources. For example, homeland-security-related knowledge is generated by government organizations at multiple levels (e.g., town, city, county, state, federal), commercial enterprises, private sector organizations, and from physical systems.

DHS is the primary U. S. government organization assigned to coordinate and lead the enterprise effort to secure the nation. DHS is primarily a law enforcement

organization that has a unique and multifaceted role compared to all other U. S. government organizations. DHS functions include:

- Enforcing laws to ensure public safety and health
- Supporting or managing large scale incidents and catastrophes
- Securing critical infrastructure, national borders, and cyberspace
- Screening people and cargo for potential hazards
- Administration of benefits to disaster victims

In DHS, the National Protection and Programs Directorate (NPPD), Federal Emergency Management Agency (FEMA), and the Transportation Security Administration (TSA) focus on different aspects of homeland security. NPPD gathers information on and analyzes risks to the 16 critical infrastructure sectors currently identified (DHS 2013). NPPD also leads cyber security efforts for U. S. government information technology infrastructure. FEMA gathers information, assesses risks, and plans response to a variety of emergencies and disasters such as hurricanes, tornadoes, and major floods. FEMA plans and executes high level exercises each year involving multiple federal, state, and local organizations to improve incident management. FEMA stages materiel to support responses to areas overwhelmed by a catastrophe and administers benefits to victims. TSA coordinates security for transportations systems, such as the air transportation system. TSA assesses risks to these systems and implements means to mitigate identified risks.

Air transportation systems are an example of a system of systems as identified in section 2.3.2 of chapter 2. Securing air transportation systems against terrorist threats illustrates the system of systems nature and some of the challenges involved with homeland security. Commercial aviation has encountered a number of man-made threats since the 1970s as shown in Table 9.1. For explosive threats, a watershed event occurred with the Pan Am Flight 103 Lockerbie bombing in 1988, which resulted in catastrophic loss of the aircraft due to an explosive device inserted in checked baggage. This resulted in increased focus on explosives as an aviation threat including U. S. legislation to improve aviation security. The Aviation Security Improvement Act of 1990 (Public Law 101-604) (Congress 1990) defined and specified requirements for Explosives Detection Systems (EDS) including:

- Performance criteria
- Explosive type, configuration and amounts
- Detection rates
- False alarm rate
- Throughput rate

The U. S. government also began to utilize live fire explosive testing to study the effects of explosions on aircraft structures to serve as a basis for aircraft hardening

measures and explosive detection standards. After implementation of new measures, there was a decrease in the frequency of aircraft bomb blasts worldwide after 1990.

The U. S. enhanced aviation security again as a result of the September 11, 2001 attacks with enactment of the Aviation Transportation Security Act (Public Law 107-71), passed in November 2001 (Congress 2001). This identified a comprehensive set of security requirements for all modes of transportation. Suicide bombing attempts by Reid in December 2001 and Abdulmutallab in December 2009 using improvised explosive devices created new security challenges that require improved approaches and technologies for screening passengers and carry-on baggage.

U. S. stakeholders in aviation security include the TSA, DHS Science & Technology (S&T) Directorate, airports, airlines, and airline passengers/users of commercial aviation. Roles for each of these stakeholders include:

- TSA
    - Establish policy
    - Identify and assess threats
    - Issue and enforce regulations
    - Approve security plans and programs
    - Inspect and monitor operations for compliance
    - Provide operational direction
    - Initiate necessary changes
    - Screen passengers and baggage
- DHS S&T Directorate
    - Implement R&D to enhance aviation security
    - Provide paths to commercialization of technology for explosives detection and mitigation
- Airlines
    - Secure baggage and cargo
    - Protect aircraft
- Airports
    - Protect air operations area
    - Provide automated access control
    - Provide law enforcement support
- Airline Passengers/Users
    - Use commercial aviation as necessary
    - Comply with laws and regulations

Potential attackers will attempt to evade security procedures and explosive detection technologies to carry out an attack. Several means or vectors exist for introducing explosives onto an aircraft. These threat vectors include:

- Flight crew carry-on bags
- Flight crew
- Catering and cleaning services
- Cargo
- Mail
- Ground crew services
- Passenger introduction through carry-on, checked, gate checked, transfer baggage, or personnel borne devices.

Since security procedures limit the number of threat vectors available for introduction of explosives on aircraft and are continually evolving based on new threats, adversaries must continually modify their tactics and techniques. For example, this includes use of suicide bombing devices using homemade explosives and/or improvised explosive devices, which evade screening and detection technologies. Homeland security organizations, such as DHS, must understand the air transportation system, continually assess the risks, and implement actions to mitigate potential dangers.

Homeland security concerns extend well beyond air transportation systems and encompass multiple security concerns in the domestic environment. Government and other organizations that lead and coordinate homeland security need a framework or architecture to understand the domestic environments in normal operating conditions, evaluate and assess threats, and mitigate risks for disruptions. If a significant disruption does occur, they need the appropriate situational awareness and understanding to intervene and provide the necessary capabilities to cope with the damage and restore the domestic environment to its normal operating condition as quickly as possible, ideally with minimal losses. Integral to the homeland security analytical architecture is an ability to share knowledge and support the development and use of analytical tools and capabilities such as all types of models, simulations, and associated data.

9.3 Modeling, Simulation, and Analysis for Homeland Security

Modeling, simulation, and analysis (MSA) techniques and capabilities are extensively developed and used for strategic planning, operations analysis, and systems development for national defense. MSA techniques and capabilities can potentially support problem solving across many homeland security domains by providing insights to analysts and decision makers in many important, complex areas of importance such as social behavior, natural phenomena, environments, economy and finance, organizational performance, critical infrastructure, and other systems (McLean, Jain, & Lee 2008). Science-based MSA capabilities, judiciously applied to homeland security domains, can enhance risk analyses and support response planning for natural and man-made threats and hazards.

Currently, modeling and simulation capabilities are being developed in an ad hoc manner within DHS to address specific problems identified by a few homeland security "customers" such as first responders (Hutchings 2009). For example, national laboratories, industry partners, and universities are working on a number of DHS sponsored MSA developments. Laboratories, private firms, and academic researchers are developing MSA capabilities to support needs and provide analytical capabilities and management tools for various homeland security sponsors in other organizations; e.g., at regional, state, or city levels, independently. MSA developments should be coordinated to efficiently identify gaps to advance capabilities and avoid duplication of effort. A DHS Critical Infrastructure Modeling & Simulation Workshop (Adam 2008) recognized a variety of MSA activities and recommended:

- Developing and regularly updating a master compendium of available models and related research from labs, academia, and industry.
- Conducting research to define the model attributes and characteristics that must be included for the entries in the compendium.
- Developing methods for communicating the scope and limitations of models in a manner as transparent as possible.

A knowledge sharing framework for homeland security MSA can promote a common understanding of current analytical tools and techniques and support development of a model compendium. A suitable knowledge sharing framework provides a classification schema that defines a set of categories into which various concepts or artifacts can be arranged, understood, and evaluated. Homeland security analysts can use such a framework to logically organize knowledge assets, including MSA assets and capabilities, and identify research and development gaps and needs. A knowledge sharing framework, as described in the next section, provides structure for MSA development and use. This framework differs from enterprise architecture schemes developed by Zachman (2013) or Department of Defense Architectural Framework (DoD CIO 2010).

Homeland security stakeholders – domain experts, capability sponsors, developers, and managers, analytical and operational communities – should collaborate to create a common body of knowledge and reach consensus on homeland security issues, concepts, analytical methodology, and existing and needed MSA capabilities. A sufficient knowledge sharing framework should provide the necessary structure to support stakeholder collaboration and address significant homeland security problems and decision making. A purpose built framework supporting homeland security decision makers to address problems can guide framework development. For example, rational problem solving and decision support typically proceed in distinct phases. These might include identification of a problem situation, problem definition and formulation, creation

of an evaluation model, problem analysis, and creation of results or recommendations for action. An appropriate MSA development approach might be analogous to the rational problem solving methodology and include the following major phases:

- Problem identification
- Analytical requirements definition and specification
- Capability development
- Capability evaluation
- Capability application

This approach provides a common means to guide MSA development and is applicable across homeland security domains of interest.

9.4 Knowledge Sharing Framework

A knowledge sharing framework that integrates MSA research and development efforts is shown in Figure 9.1. The framework identifies knowledge asset needs and requirements based on input from key stakeholders – the subject matter experts, researchers and users – and provides a number of benefits.

- Users capture and share known research, development, and implementation issues.
- Developers identify currently available capabilities, ongoing projects, and facilities to avoid duplication of efforts which ensures the best use of constrained resources for developing useful MSA tools.
- Best practices are shared to allow dissemination of lessons learned from experiences of others.
- Current and needed standards are identified to ensure interoperability of developed MSA tools.

MSA developers should be able to access the knowledge and insights captured in the framework in a report or on-line using mechanisms such as a secure portal or Wiki. The following subsections describe the elements of the knowledge sharing framework shown in Figure 9.1.

9.4.1 Scope of the Framework

A knowledge sharing framework for a coherent area of homeland security MSA needs to include the sub-areas that are considered relevant by each corresponding community or technical interest group. For critical infrastructure (CI), for instance, the scope should include cross-cutting concerns with modeling, simulation, and analysis in all sixteen CI sectors currently identified by DHS (DHS 2013). The framework needs to incorporate information across all phases of infrastructure lifecycle including planning,

designing, building, operating, and decommissioning. As CI MSA capabilities evolve, separate knowledge sharing frameworks may be needed for each CI sector to reflect sector-specific needs and concerns. Similarly, for the Hazardous Material Release (HMR) area, the scope may include modeling and simulation for release of chemical, biological, nuclear, and radiological agents, as well as natural occurring releases such as volcanoes and wild fires. Associated models and simulations may involve the release of materials into the atmosphere, within buildings and other structures including heating ventilation and air conditioning (HVAC) systems, bodies of water and watershed systems, as well as ground contamination.

The scope for the healthcare systems technical area would include simulation and modeling activities that support analysis, planning, and training needs for the healthcare institutions, epidemics, and other healthcare-related emergencies. Simulation models may be used to understand healthcare systems, interdependencies with other systems, their vulnerabilities, and the impact of emergency incidents on the population and healthcare community.

For all the technical areas identified, the MSA tools may be used for all the application types defined in McLean, Jain, & Lee (2008) to inform analysis and decision support, planning and operations, systems engineering and acquisition, and training, exercises and performance measurement.

9.4.2 Needs Analysis Overview

Stakeholders at all levels need analytical tools and methods to address problems and support decision making. The purpose of this section of the framework would be to capture problem situations that are commonly encountered by stakeholders across each identified technical area and how M&S capabilities are used to support the problem solving/decision making processes at more than one level. For example in the case of CI, given a major hurricane and potential impacts, FEMA will have a set of concerns, state and local officials in potentially affected areas another set of concerns, and power generating facilities still other concerns. This will promote a common understanding of analytical issues from multiple perspectives and support the development and sharing of analytical tools and M&S capabilities across stakeholder organizations.

This section of the framework will identify, document, and catalogue problems that are most likely to be faced in the particular technical area. It will help define the relevant analytical needs and determine the right decision-relevant questions that need to be addressed, establishing the purpose and objectives for MSA capabilities. Examples of questions that may be captured as needs for using MSA for CI include:

- How will the impact of a natural disaster such as hurricane, tornado, or violent lightning storms striking parts of the power grid affect outage management?
- What will be the impact of disruption in one critical infrastructure on other co-located or connected critical infrastructure systems? For example, how will disruption in the power grid affect the water delivery infrastructure for a city?

Brase and Brown (2009) identified research questions for complex network questions. Since CI systems are networked systems, the identified questions contribute to needs analysis as indicated by examples below.

- Can we use, understand, and quantify the efficacy of new security approaches for computer networks?
- Can we improve the design of computer or communication networks to be more robust against partial failures or intentional attacks?
- Can we understand how populations will respond to the availability of new energy sources, or to changes in energy policy?

Similarly for the HMR area, on the occurrence of a release, officials want to know - What is the hazard? Where is it going? Who is at risk? How do we respond? Specific questions that may be answered using simulation include the following.

- What is the forecasted transport direction of the plume and what areas may be under hazard?
- What are the estimated potential damages, casualties, illnesses, and fatalities?
- What are the estimated emergency assistance requirements?
- What are the areas where buildings, land, agricultural crops, bodies of water, and other man-made or natural resources are or will be contaminated?

9.4.3 MSA Requirements Specifications

The high level needs analysis should form the basis for requirements specifications for the technical area. To address the analytical needs, each MSA capability needs clearly defined requirements. This section of the framework will include:

- Intended Use
- Data and Metadata Requirements
    - Quality
    - Provenance
    - Timeliness
    - Management
    - Interoperability
    - Security
- Functional Requirements

- Interactions with other MSA capabilities
- User Interface Requirements
- Performance Requirements
- Credibility and Evaluation Requirements
    - Theoretical corroboration
    - Model components verification
    - Corroboration (independent data)
    - Sensitivity analysis
    - Uncertainty analysis
    - Robustness determination
    - Comparison to evaluation criteria

  Examples of functional requirements for HMR are provided below.
- Predict the initial direction, travel, and dispersion of a plume over time from a single or multiple sources taking into account the type of source, material/chemical properties, release location, weather conditions, terrain, urban areas, and other man-made structures.
- Predict the concentration of the chemical or biological agent within the plume and flow through drainage areas over time.
- Estimate deposition and contamination levels for air, water, ground, and building surfaces.
- Identify exposed population and predict exposure levels over time.

9.4.4 Identification of Existing MSA Resources

This section of the framework will capture MSA resources available for systems analyses for each technical area. These are categorized into the following sub-sections.

Projects, Facilities, and Capabilities. The sub-section will identify the ongoing projects, facilities, and capabilities focused on the relevant technical areas. Examples for the CI sector include NISAC (Sandia 2013a) and Chemical Sector Supply Chain and Economics Project and are discussed in the following paragraphs.

NISAC is a modeling, simulation, and analysis program within DHS comprising personnel in the Washington, D.C., area as well as from Sandia National Laboratories (Sandia) and Los Alamos National Laboratory (LANL). A facility dedicated to NISAC is located at Sandia National Laboratory, Albuquerque, NM. Congress mandated that NISAC serve as a "source of national expertise to address critical infrastructure protection research and analysis." NISAC prepares and shares analyses of critical infrastructure and key resources (CIKR), including their interdependencies,

vulnerabilities, consequences, and other complexities, under the direction of the Office of Infrastructure Protection (IP), Infrastructure Analysis and Strategy Division (IASD). As of September 2008, NISAC had conducted and published 11 analyses of hurricanes covering the entire U.S. Gulf and Atlantic coast (DHS 2008).

The Chemical Sector Supply Chain and Economics Project is a key component of a larger effort to deliver Enabling Homeland Security Capabilities (EHCs) for the Modeling, Mapping, and Simulation program. The first goal of this project is to populate a detailed dataset of the chemical and petrochemical manufacturing, supply and distribution components that comprise the chemical infrastructure supply chain. The second goal is to develop a means to mathematically analyze not only the consequence of significant threats, but also the resiliency of the supply chain to recover from these impacts. This project was part of the Critical Infrastructure Protection Thrust Area and the Modeling, Simulation & Analysis Program of the Infrastructure and Geophysical Division of DHS.

Ongoing projects will also include efforts in academia as described in research literature. For example, recent reported efforts on infrastructure simulations in academia include energy distribution (Baxevanos and Labridis 2007) and water supply (Qiao et al. 2007).

Examples for the HMR area include National Atmospheric Release Advisory Capability and the National Exposure Research Lab (NERL) and are briefly described below.

National Atmospheric Release Advisory Capability (NARAC) – The NARAC facility is located at Lawrence Livermore National Laboratory in Livermore, CA. It provides tools and expert services to map the spread of hazardous material accidentally or intentionally released into the atmosphere (LLNL 2012).

EPA’s National Exposure Research Lab (NERL) - located in Research Triangle Park, North Carolina provides scientific understanding, information and assessment tools to reduce and quantify the uncertainty in the Agency's exposure and risk assessments for all environmental stressors. The Atmospheric Sciences Modeling Division provides numerical and physical modeling support to the homeland security mission in protecting against the environmental and health effects of terrorist acts (EPA 2013). This involves numerical modeling complemented by physical modeling in the Division's wind tunnel. For example, a 1:600 scale model of lower Manhattan was built and the dispersion of material from the collapse of the World Trade Center towers was studied under various meteorological conditions. Also, dispersion of airborne material around the Pentagon was simulated in the wind tunnel.

MSA Tools Summary. This sub-section will provide a collection of available MSA tools (the tools under development are identified in the preceding sub-section as projects). The tools will be briefly described to provide an overview of their capabilities. In the long term, this information should be enhanced to grow the collection to the compendium of models called for in the workshop focused on CI (Adam 2008). The brief tool descriptions will provide a useful resource until the research issues related to the proposed compendium are addressed. An interested reader can use the description to quickly develop a shortlist of tools that may be applicable for their purpose and can then follow-up to find more details. Examples of such descriptions of MSA tools for CI area are provided in the following paragraphs.

Critical Infrastructure Protection Decision Support System (CIPDSS) (LANL 2013a) has been developed jointly by LANL, Sandia National Laboratories, and Argonne National Laboratory (ANL) the set of tools under the CIPDSS program models the impact of CI on the economy, government, and population. LANL developed the city level models, Sandia developed the national level models while ANL provided the decision support part. The set of tools is intended to provide "orders of magnitude" results quickly. It was used for the analysis underlying NISAC's report on potential impact of pandemic influenza (DHS 2007).

Critical Infrastructure Protection and Resiliency Simulator (CIPR/sim) has been developed by Idaho National Labs (INL) CIPR/sim allows emergency planners to visualize the real-time cascading effects of multiple infrastructure failures before an actual emergency occurs. It uses a common operating framework that allows the tool to import real-time data from numerous existing analysis modules, including RTDS (Real Time Digital Simulator) for electric grid analysis, QualNet for telecommunications analysis, and PC Tide for wind speed and flood surge analysis (INL 2013).

Examples of MSA tools for healthcare systems area include EpiSimS (LANL 2013b) and MedModel (ProModel 2013). EpiSimS is an epidemic simulation engine. It is a C++ application that runs on high-performance computing clusters. It is a stochastic agent-based discrete event model that explicitly represents every person in a city, and every place within the city where people interact. A city or region is represented physically by a set of road segment locations and a set of business locations. EpiSimS can simulate various pharmaceutical and non-pharmaceutical interventions, including panic-based stay-home behavior, therapeutic and prophylactic use of antivirals, contact tracing, vaccination, wearing of masks, social distancing behaviors (increased inter-personal separation, hand washing, cough etiquette, etc.), household quarantine, and closures of schools. More information is available in Stroud et al. (2007).

MedModel is a simulation tool designed specifically for the healthcare industry. MedModel is used in the evaluation, planning and redesign of hospitals, clinics, and other

healthcare systems. In the hands of a trained and experienced analyst, MedModel models can be used to identify inefficiencies in an existing process and test a variety of scenarios. The animation and graphic output results show the behavior of the system under any set of circumstances (ProModel 2013).

Relevant Standards and Guidelines. This sub-section will identify the known applicable standards and guidelines. A few examples for this sub-section for CI area are presented next.

National Infrastructure Protection Plan (NIPP) is a coordinated strategy that defines CIKR protection roles and responsibilities for federal, state, local, tribal, and private sector security partners. The NIPP sets national priorities, goals, and requirements for effective distribution of resources which will enable the government, economy, and public services to continue in the event of a terrorist attack or other disaster. Sector-Specific Plans (SSPs) have been developed for each of the identified CI sectors supporting the NIPP.

Chemical Facility Anti-Terrorism Standards (CFATS) is a regulatory program to secure national high-risk chemical facilities. At the outset of the program, DHS expected that roughly 30 000 facilities would require registration and regulatory compliance to monitoring standards of which approximately 6 000 facilities would fall into one of the four high risk categories that require further regulation. As of March 2011, almost 40 000 chemical facilities had registered with DHS and completed the Top-Screen process. Of these facilities, DHS considered more than 8 064 as high-risk and required them to complete and submit site vulnerability assessments (Congress 2011).

Examples of standards and guidelines for healthcare systems include those for smallpox response and mass prophylaxis. The “Smallpox Response Plan & Guidelines” document from Centers for Disease Control and Prevention (CDC) outlines the public health strategies that would guide the public health response to a smallpox emergency and many of the federal, state, and local public health activities that must be undertaken in a smallpox outbreak.

The “Community-Based Mass Prophylaxis: A Planning Guide for Public Health Preparedness” has been developed by Agency of Healthcare Research & Quality (AHRQ) to help state, county, and local officials meet federal requirements to prepare for public health emergencies (AHRQ 2013). It outlines five components of mass prophylaxis response to epidemic outbreaks and addresses dispensing operations using a comprehensive operational structure for Dispensing/Vaccination Centers (DVCs) based on the National Incident Management System (NIMS) (FEMA 2013).

Data Sources and Formats. The sources of data relevant to MSA technical areas and their identified formats will be provided in this sub-section.

An example for CI sector is as below is the Constellation/Automated Critical Asset Management System (C/ACAMS) (CAL EMA 2013). It is a web-enabled information services portal that helps state and local governments build critical protection programs in their local jurisdictions. ACAMS is a secure, online database, and database management platform that allows for the collection and management of CI asset data; the cataloguing, screening, and sorting of this data; the production of tailored infrastructure reports; and the development of a variety of pre- and post-incident response plans useful to strategic and operational planners and tactical commanders.

An example for healthcare systems area is provided by the National Emergency Medical Services (EMS) Information System (NEMSIS) (NEMSIS TAC 2013). The system is the national repository that will be used to potentially store EMS data from every state in the nation. Since the 1970s, the need for EMS information systems and databases has been well established, and many statewide data systems have been created. The involved organizations include National Highway Traffic Safety Administration (NHTSA), Health Resources and Services Administration (HRSA), CDC, University of Utah, and University of North Carolina.

9.4.5 Discussions and Recommendations

The discussion and recommendations section in the framework will include identified best practices, limitations, cautions, and warnings, and research, development, standards and implementation issues. Government or other sponsors can then consider recommendations for funding and execution.

Best Practices for Development and Use of MSA Tools. The development and use of MSA tools can benefit through development and use of lessons learned and sharing of best practices. This sub-section would document and capture lessons learned and best practices acquired in development, evaluation, and use of MSA tools for the technical area. Some examples of best practices include:

- Conceptual modeling practice
- Innovative approaches
- Software engineering practice

Limitations, Cautions, and Warnings. Models provide results with varying levels of error and uncertainty. This sub-section is intended to highlight and document the limitations

associated with MSA applications to minimize improper use and highlight potential areas for further development.

Research, Development, Standards and Implementation Issues. This section of the framework is intended to capture challenges and issues related to MSA tools. The challenges and issues should be prioritized for maximum value.

A number of research and development challenges need to be addressed in modeling potential threats for the technical area and impact of disruptions due to involved phenomena. Common challenges across the technical areas should be identified such as the development of simulation application architectures and integration of models and simulations for the technical area. In addition, challenges need to be identified and prioritized for each technical area. For example for CI area, computational modeling to understand the vulnerability of a dam to explosions would be useful in mitigating this threat. Physical models are necessary to collect data on impact of explosions to support evaluation of the modeling capability to ensure credibility of result. However, a physical model of a dam cannot be scaled down to laboratory settings since the physics changes based on the scale. Hence, expensive large scale experiments may be required for the purpose. An initial straw man list of such challenges for the healthcare systems area may include, increasing reality in healthcare M&S training exercises and devices, access to and usage of healthcare M&S applications by system personnel.

The success of a coordinated approach will largely depend on the ability to apply data-driven MSA tools across a range of scenarios. This ability in turn depends on use of standards. Gaps in available standards should be identified and prioritized to guide standardization efforts. At times the issue may be to identify a common standard from among multiple ones available. For example, issues with multiple Geographic Information System (GIS) standards should be identified and an approach to identify one common GIS standard to be followed for outputs by all MSA tools for a particular area should be identified or developed.

Deployment of new MSA tools for homeland security has to follow a carefully organized approach. The approach may vary across the technical areas depending on the state of technology, the familiarity of the end users with MSA, and the interfaces with the end users. Common implementation challenges across the technical areas include return on investment to stakeholders and sponsors for research projects, and ownership and usage of publicly versus privately developed tools. For example, the eighteen identified CI domains involve a myriad of stakeholders including government, quasi-government, and private sector operators, a number of oversight agencies across federal, state, and local levels, a range of jurisdictions involved in normal operation, and another range of jurisdiction that may be affected under disrupted or interrupted operations. Some sectors

may require use of “reachback” centers, i.e., entities with expertise available to guide the users in interpretation of results. Other sectors may have sophisticated users who can be trained to use the MSA tools independently.

9.4.6 Framework Reference Materials

The knowledge sharing framework will need to be supported by a number of reference materials provided via appendices. While every attempt should be made to use standard terminology, more often than not, this may not be possible due to its absence. A technical interest group should guide the generation of standard terminology that should be defined in a glossary.

The framework is expected to include technical discussions and build on existing current literature. A reference section should be included to capture the relevant publications.

Potential and existing users of MSA tools may need guidance from experts in respective areas. A list of identified experts for each major aspect of each technical area should be captured. The list may be restricted to authorized personnel and the names on the list may be included only with permission. The experts may need support for the time they may have to spend fielding questions.

This section described a knowledge sharing framework for MSA for homeland security. It is suggested that the wide area of homeland security be divided into several technical areas based on existing communities of researchers. The knowledge sharing framework can then be used to pull together and create an information source for each technical area. The collection and maintenance of information, identification of research challenges, and development of the research agenda should be coordinated by technical interest groups. Establishing such a framework for MSA capabilities is one approach to encourage collaboration and coordination for systems analysis, problem solving, and decision making for each of the technical areas. The framework should be documented and made available to stakeholders as an on-line resource such as a secure portal or Wiki to enable development and progress of MSA for homeland security purposes.

9.5 A Prototype System of Systems Application

The utility of a knowledge sharing framework for developing and using MSA capabilities for analyzing incident management is illustrated by a homeland security training scenario, which uses a variety of virtual reality, simulation, and gaming capabilities. A conceptual architecture for integrating these capabilities is shown in Figure 9.2.

The integrated simulation modules are intended to provide technically correct solutions. The gaming modules are included to provide the interaction required for training. The simulation and gaming modules should be integrated together through a data synchronization and transfer processor. The integrated capability will allow joint training of first responders and the management level personnel in the preparedness phase. The integrated simulation modules by themselves can be used throughout the incident management lifecycle including the phases of prevention, preparedness, response, recovery and mitigation.

A prototype was developed to demonstrate the concept to potential users. A prototype helps explain MSA concepts to those who are not familiar with simulation and gaming and demonstrates MSA applicability to incident management. A hypothetical scenario involving a dirty bomb explosion in Washington DC was created, and selected aspects of the incident and the response were modeled to demonstrate the capabilities of simulation and gaming. Integration of various modules highlights the advantages of this approach.

The next sub-section briefly describes the hypothetical scenario. A number of simulation and gaming modules were developed to help understand the issues involved in modeling and integration. The following sub-sections discuss the simulation and gaming modules that have been included in the concept demonstration. Each of the implemented module is discussed below with the full capability desired and the subset implemented for the demonstration. The proposed approach for integration including a test implementation for two of the modules is discussed next. The data needs for building and executing the simulations are briefly discussed. The issues identified from this experience of developing the prototype are discussed.

9.5.1 Hypothetical Scenario

The scenario for the concept prototype is based on a dirty bomb attack in Washington DC on the evening of July 4. The fireworks on the National Mall on July 4 attract a large crowd. A large number of people utilize the metro rail system to get to the National Mall. The metro rail authorities actually close the Smithsonian metro station that is nearest to the National Mall to allow better management of the crowd flow on July 4. It does not take much imagination to identify streets nearby metro station entrances as potential targets for terrorists. The selection of public places like a street as the incident location also avoids any concerns that may be raised on selecting privately owned location such as stadiums for such a study.

The scenario uses the area outside Federal Triangle metro station, that is the second closest station to the National Mall, as the target for detonation of a dirty bomb by

terrorists. The scenario did not consider the feasibility or means of getting a dirty bomb to the identified location. The probability of such an occurrence is expected to be very low with the typical high security surrounding such an event. The focus of the scenario was on the consequences if such an incident occurs.

The near term consequences of a dirty bomb explosion include the casualties and radiation exposure among the crowd in the immediate vicinity and in the area covered by the plume, and response by police, fire department, and emergency medical technicians. The major consequences of the incident and the response need to be modeled for incident management purposes.

9.5.2 Simulation modules

The simulation modules included in this effort are as below.

Plume Simulation. This module falls in the category of physical phenomena simulators shown in Figure 9.2. It should model the dispersion of plumes of various kinds including chemical, bio-logical and radiological agents. Inputs may include the characteristics of the agent released, release mechanism used, the location of release point, terrain and structures around the release point, and weather conditions. Inputs may alternately be based on the sensor readings over time in the area of interest indicating the presence of an agent and the direction(s) of the spreading plume. Outputs may include time profile of the plume, and exposure profile for the population in the region affected by the plume over time.

This module was implemented using CT-Analyst software from Naval Research Labs (NRL 2013). This tool provides the desired capabilities for modeling plume dispersion as described in the preceding paragraphs. It models the spread of the plume from the identified location taking into account the weather and the geometry of the buildings in the surrounding areas.

Crowd Simulation. The capability of modeling crowd behavior is a part of the social behavior simulators group in Figure 9.2. It should model crowd status and movement at locations of interest under different event scenarios, crowd behavior and crowd management strategies. The locations of interest may include areas around actual and potential emergency incident sites, major business, commercial and residential areas that may be affected by evacuation directives, and major public transportation points such as bus and train stations, local rail transport stations, and airports. Different event scenarios may include normal, rush hour, terrorist attack, accidental fire, natural disaster, etc. The models may predict crowd movement and crowd density variations along movement

directions, predict occurrence of stampede and casualties, perform route planning through the crowd for selected individuals (such as first responders), determine location of individuals as a function of time, predict individual movement times between selected points. Inputs may include street layouts including pedestrian areas, layouts within public buildings such as train stations and public parks, crowd volumes and density data, probabilities for stampede and casualties, weather conditions, location of emergency incidents, behavioral models of individuals, sensor data, and communications. Outputs may include location and status of specific individuals in the crowd, crowd volumes and density by city block and passages within public buildings and parks, crowd movement times between selected points, and crowd management systems data.

The crowd simulation module has been implemented by researchers from University of Arizona using AnyLogic software using the agent based simulation paradigm. Individuals and small groups are defined as agents with each of them having parameters such as age, mobility, knowledge of the area, that determine their reaction to the incident and the behavior (Shendarkar et al. 2006).

Traffic Simulation. Traffic simulation is another module that falls in the group of social behavior simulators. It should provide models of general traffic flow and specific vehicle movements for a given region under different event scenarios (normal, rush hours, off-peak hours, terrorist attack, natural disaster, evacuation, etc.), driver behavioral models, and traffic management strategies. The model may perform automatic route planning for selected vehicles, generate random events that disrupt traffic flow (vehicle breakdowns, accidents, traffic management system failures), determine vehicle locations as a function of time, predict travel times between locations, etc. Inputs may include road network layout and characteristics, traffic management system description and status, individual vehicle locations and status, driver moods, historical traffic volume and vehicle density data, pedestrian data, probabilities for accidents, incidents, weather conditions, location of emergency incidents, behavioral models of vehicle operators, sensor data, and communications. Outputs may include locations and status of specific vehicles, traffic volume and densities by area or road segment, travel times between selected locations, accident data, and traffic management system data.

This capability has been implemented using two modules that simulate traffic at different levels of detail. The Emergency Response Vehicle Simulator models the traffic at a macro level. It has been developed by NIST researchers using Java and Geotools, an open source GIS toolkit (GeoTools 2013). It mimics the movement of the response vehicles from their initial locations to the site of the incident. While individual response vehicles are modeled, the effect of the rest of the traffic is modeled using congestion

factors for each road segment that they go through. The travel route is determined using Dijkstra's algorithm.

The micro level traffic simulation capability has been implemented using Traffic Software Integrated System (TSIS) developed at the University of Florida and available through the Center for Microcomputers in Transportation (McTrans) (UOF TRC 2012). The model simulates movement of individual vehicles in the immediate area around the National Mall before and after the incident. Following the incident, a number of vehicles come out of parking garages in the area and attempt to leave resulting in traffic jams. The software allows capturing the congestion factors for each road segment defined. The congestion factors determined through micro-level simulation of one area can be used to estimate congestion factors for the wider area modeled in the macro-level traffic simulation.

Health Care Simulation. Health care simulation module is part of the organizational simulator category in Figure 9.2. It should model the actions of the health care organizations (including emergency medical technicians, hospitals) in response to an emergency incident including the deployment of resources and actions for triage and treatment of injured at the incident site, movement of casualties to hospitals, and treatment at the hospitals. The model logic will include relevant policies and procedures for emergency situations including calling in medical staff, using temporary accommodations for the injured, acquiring needed supplies and equipment. Inputs may include the number, location and type of casualties from an emergency incident, the availability of staff at work and off (on-call), the availability of resources (own and those that can be acquired quickly from surrounding jurisdictions), the time and resources required for attending to each casualty type, and the probabilities of death from different casualty types over time. Outputs may include the operation of the health care system over time including the number of people treated and released, admitted, dead, waiting for treatment, and the state of the staff and facilities (to determine their capability to deal with another incident).

The concept demonstration includes a model for only one part of the health care system, namely, the emergency department. The operation of a hypothetical emergency department for handling the casualties from the incident is simulated. It was developed by NIST researchers using ProModel. Casualties arriving at the emergency department include serious cases of trauma and cardiac cases brought in by ambulances and walk-ins with minor injuries and the worried well. The model indicates the build up of queues for the walk ins. The ambulances carrying serious cases are occasionally diverted to other hospitals based on the status at the hospital modeled.

Transportation Simulation. Transportation Simulation is a part of the infrastructure systems simulators group in Figure 9.2. It should mimic the transportation system infrastructure including highways and road network, rail network, waterways, marine and air transport. It should model the impact of man-made or natural disasters on the transportation infrastructure components. Inputs may include the description of the transportation system infrastructure together with its network, characteristics of node points, traffic volumes across arcs and through the nodes, traffic control mechanisms, failure characteristics of major control mechanism and equipment, operation and maintenance resources, multi-modal links and links to other critical infrastructure. Outputs may include the impact of modeled emergency events on the operation of the transportation infrastructure over time.

A metro rail simulation model was developed for the purpose of demonstrating the concept of transportation simulation. The model was developed using AutoMod by NIST researchers with active support from the vendor, Brooks Software. It models the evacuation of people from the incident area using metro rail system. The metro system lines passing through the incident area are modeled. The model helps determine the rate at which the crowd can disperse using the metro system.

9.5.3 Gaming modules

The gaming modules would be especially useful for incident management training applications. Two of the modules were implemented, one at responder level and the other at the management level.

Triage Application. Triage is part of the On-Scene Response group of gaming applications in Figure 9.2. This application allows trainees to play the role of emergency medical technicians conducting triage following a dirty bomb explosion. This module was developed through collaboration between researchers from NIST and the Institute of Security Technology Studies (ISTS) at Dartmouth College. The ISTS researchers had previously developed the triage application for a airplane crash scenario (ISTS 2013) (McGrath and Hill 2004) (McGrath and Carella 2005). The NIST researchers created the 3-D geometry of the incident location and worked with ISTS researchers to set up the application.

The gaming application allows a user to move around in the 3-D space representing the incident site. The user can see the fire caused by the explosion, the casualties lying on the ground, the fire trucks, other responders, objects and structures on the street and the surrounding buildings. They can go to each victim and perform triage by looking for the vital signs and asking specific questions if possible. The victims requiring

immediate attention can be carried away on stretchers through a gross decontamination station created using hoses from two fire trucks. The application includes audio effects to make the experience closer to reality. A user has to contend with sounds of sirens, victims, limited lighting conditions in performing his/her responsibilities for conducting triage.

Incident Management Strategy Gaming. The strategy gaming application would fall under the Response Management category of gaming applications shown in Figure 9.2 and is targeted at the management level personnel for the responding agencies. This may be used by personnel at the Emergency Operations Center (EOC) to plan out the response resource deployments. The module was developed by NIST researchers using C#. The module shows a map of the incident site together with the locations of response resource providers including police stations, fire stations, and hospitals. The map also shows the important buildings around the incident site. The interface provides the capability to place icons representing response resources on the map thus making and visualizing the deployments. The map can be updated based on reports from the incident site. All the icons used are based on standards defined by the Homeland Security Working Group (HSWG 2012).

The application allows decision makers to develop an awareness of the situation and make decisions for resource deployment. These decisions can then be communicated to the responding teams. The strategy board can be updated with locations and damage information as reports are received from the incident. The board can be used with a real incident or with a simulated incident modeled using the concept demonstration prototype.

9.5.4 Integration of Simulation Modules

The benefit of the individual simulation and gaming modules can be synergistically increased through integration. In the absence of integration, each simulation will have to either make assumptions about the phenomenon modeled by other simulations or utilize summary statistics from the other simulations. For example, the emergency department simulation will have to utilize the arrival rate of ambulances determined by the emergency vehicle response simulation model. Utilizing a distribution based on results from other simulations will result in piecewise simulations of the overall system. Integrating the simulations together such that they can exchange entity information will allow modeling the whole system together. The integrated set will thus allow increased accuracy.

The integration of simulation modules can be accomplished using the High Level Architecture (Kuhl et al. 1999) (IEEE 2010). However, the traditional approach of

integrating the simulation using the High Level Architecture (HLA) is quite resource intensive and requires major coordination among the developers of the simulations being integrated. A modified approach involving adapters developed at NIST (McLean et al. 2000) was used for the integration. Two of the simulation modules, the emergency department simulation and the emergency response vehicle simulation, were integrated together using the adapters. Figure 9.3 shows a screen shot of the integrated execution of the two modules. As the simulated ambulance arrives at the hospital location in the emergency vehicle response simulation window shown in the right half of the screen, it enters the emergency department simulation window shown in the left half of the screen. The ambulance discharges casualties at the hospital and leaves. Again, the movement between the two simulations is coordinated. The two simulations are integrated using a conservative approach with a simulation time step of 30 seconds.

The integration of gaming and simulation modules allows joint training of personnel from multiple levels of organizations. The first responders and management level personnel can be trained together on the same simulated incident. This allows them to share experiences leading to better teamwork and performance. Strategies for addressing the significant technical challenges in the integration of the gaming and simulation modules are topics for future research. The challenges include:

- Synchronization of time between gaming modules that should execute in real time and simulation modules that have the capability to execute in accelerated time.
- Re-synchronization of gaming and simulation modules after a fast forward or "jump" in simulated time.
- Establishing communications with gaming soft-ware since they have generally been developed with proprietary architecture.
- Affecting the event flow in simulation based on actions taken in gaming clients and vice versa.
- Achieving agreement between results of simulations executed at an abstract level and games executed at a detailed level.

9.5.5 Simulation Data Needs

Development and execution of simulations such as those discussed in this chapter require a large and varied set of data. Two databases have been developed to indicate the kind of data that will be needed to support the simulations. One database includes reference information that may be useful for any incident while the other is specific to the incident. The example databases are developed as two units for illustrative purposes only. It is recognized that the real data may reside in a number of databases spread at different organizations. It may be worthwhile to read some of the data directly from the

existing databases while other parts of the data may be read in and stored locally depending on the communication and storage infrastructure available to a community. The reference database may include information such as natural disaster intensity scales for earthquakes and hurricanes, characteristics of biological and chemical agents, triage categories and tags, capabilities of emergency response equipment such as police cars, fire trucks, and personal protective devices. Such a database will provide the information for modeling the behaviors of the various entities and physical phenomena. It can also serve as the reference for decision makers.

The incident database may include information specific to the incident. Such information would comprise of the map of the area, locations of nearby responding agencies, sites of local, state or national importance in the area, current status, traffic densities on the streets in the area, etc. The information in the incident databases will be utilized to populate and update the simulation models. For example, the incident database may indicate that two fire trucks of type A are close to the scene. The corresponding simulation model will be initialized with that information. The information on capabilities and features of fire trucks of type A will be retrieved from the reference database to correctly model their actions.

9.5.6 Issues Identified

The development of the concept demonstration prototype helped identify the issues involved in building a system with integrated simulation and gaming modules. The issues are summarized below.

- The numerical data inputs for the simulators were generally in proprietary formats. Some of the data had to be entered using input screens of the simulators. The tools developed internally at NIST allowed XML inputs.
- The GIS data inputs could be in a number of several GIS “standard formats.” There are multiple file formats defined with different versions, multiple earth models and multiple projections. There is no best combination of these factors and translation errors between the formats are common.
- The imported graphics required varied formats also. For an earlier version of the strategy board, the map had to be downloaded as a bitmap and then converted into Targa (.tga) format. Another tool required the bitmap to be converted to Jpeg (.jpg) format. Yet another required conversion to AutoCAD format.
- The open source software used was not found to be as robust or well documented as commercial software. The lack of documentation such as UML diagrams made it difficult to comprehend the code.

- Communication with some of the proprietary tools was hard to implement as they were not de-signed to interact with external programs.
- One of the tools was restricted to use by government personnel only.

There were some instances of default standards that helped the process. For example, inputs of 3D models for the two different gaming software used was possible using 3D Studio Max format.

The experience underlined the need for standards for data inputs and outputs for the simulation and gaming modules. Standards are also needed to enable plug and play interfacing of the modules.

The demonstration prototype helped illustrate explain concepts for integrated gaming and simulation for incident management to the user community since the responder community associates simulations with live exercises and table top models. The concept demonstration prototype helped elucidate the value computer simulation and gaming may provide to them. The demonstration prototype development process also helped verify some of the major issues that were anticipated in realizing the use of simulation and gaming in incident management. Further work is needed to identify and build the infrastructure required for enabling integrated gaming and simulation using independently developed modules. Such infrastructure will include defined standard architecture, interfaces and data formats that allow bringing together desired modules for incident management for different scenarios.

9.6 Chapter Summary

This chapter presents an approach for enabling modeling and simulation capabilities to analyze and understand the current, human, domestic environment and support homeland security concerns using a knowledge sharing framework. Homeland security concerns encompass a large number of diverse, interacting systems, organizations, and individuals, which form complex and interwoven systems of systems. A large incident causes significant disruption of the domestic system of systems and can damage multiple components, such as critical infrastructure, that adversely impact a significant population. Effective management of a large incident requires appropriate actions from a range of government agencies, non-governmental organizations, private sector organizations, and individuals. Homeland security analysts and decision makers need to understand the nature of an incident on the domestic environment, the cascading damage resulting from the incident, the related impacts of cascading damage, and carefully coordinate actions to address the damage and restore the domestic environment.

Analyzing the domestic system of systems requires the use of advanced modeling and simulation capabilities and techniques, which need development. A suitable knowledge

sharing framework can enable a coherent body of knowledge and the use of a wide variety of data and modeling and simulation capabilities to understand the functions and performance of individual systems and the integrated components of a system of systems. An appropriate framework would support organized development of modeling and simulation capabilities for a wide range of incidents over large geographical areas by coordinating knowledge and guiding the work of personnel involved in research, development and practice of modeling and simulation for homeland security applications.

This chapter presents a knowledge sharing framework to support homeland security modeling and simulation development and use. The framework provides for necessary knowledge assets to set up and maintain the ability to develop and deploy homeland security modeling and simulation capabilities. Framework development involves stakeholders, subject matter experts, and modeling and simulation researchers in building and maintaining essential knowledge assets.

A prototype system of systems example shows how such an analytical capability can be implemented to understand and plan for a large incident such as a bomb explosion during the Fourth of July celebrations at the National Mall in Washington, D. C. Models of crowd behavior, vehicular traffic, emergency response deployment, and emergency health care system, are all integrated together to create a system of systems model for study and analysis. Such a capability is useful for identifying poorly understood aspects of an incident or incident response and can serve as a basis for further study, data acquisition, or experimentation to improve knowledge. The demonstration prototype also highlighted some of the technical challenges that need to be addressed to integrate a diverse set of modeling and simulation capabilities and data.

Homeland security issues are especially challenging because they are grounded in lack of knowledge or uncertainty about physical phenomena or human intentions related to potential threats and hazards. Risk analysis and management focus on adverse effects of known unknowns; however, homeland security organizations are often unprepared for unforeseen disasters or catastrophes such as the 9/11 attacks, the impact of Hurricane Katrina, and the Deepwater Horizon disaster in the U. S. over the past decade. Homeland security analysis needs to employ strategies and capabilities to deal with known unknowns and unknown unknowns. A sufficiently rich body of knowledge augmented by modeling, simulation, and analysis capabilities in an appropriate knowledge sharing framework may help analysts to better explore uncertainties and discover unknowns to address this problem.

Acknowledgments

The Science and Technology Directorate of the U.S. Department of Homeland Security (DHS) sponsored the production of part of this material under Interagency Agreement HSHQDC-08-X-00418 with the National Institute of Standards and Technology (NIST). NIST sponsored a part of this work to the George Washington University under grant number 707NANB8H8167. The work described was funded by the United States Government and is not subject to copyright.

The work reported here gained from substantial technical and leadership contributions by the late Charles R. McLean. The concept prototype was developed through contribution of several people including the following NIST researchers: Damien Bertot, Swee Leong, Yan Luo, Guillaume Radde, Benjamin Raverdy, Frank Riddick, and Guodong Shao. External collaborators include Dr. Dennis McGrath, Douglas Hill and Jenny Bodwell of Institute of Security Technology Studies at Dartmouth College, Dr. Gopal Patnaik of Naval Research Labs, Dr. Young Jun Son and his graduate students from University of Arizona, and personnel from Brooks Software.

Disclaimer

The material discussed and views expressed in this chapter are the authors' personal perspectives and do not reflect official views or policies of the U. S. Department of Commerce or DHS.

Some software products or services may have been identified in the context in this paper. This does not imply a recommendation or endorsement of such products or services by the authors, NIST, or DHS; nor does it imply that such products or services are necessarily the best available for the purpose.

9. 7 References

1. Adam, N. 2008. Workshop on Future Directions in Critical Infrastructure Modeling and Simulation, Final Report. U. S. Department of Homeland Security, Infrastructure & Geophysical Division, Science and Technology Directorate, Washington, DC.
2. AHRQ (Agency for Healthcare Research and Quality of U.S. Department of Health & Human Services). 2013. Community-Based Mass Prophylaxis. Available via: <http://archive.ahrq.gov/research/cbmprophyl/> [accessed December 22, 2013].

3. Baxevanos, L.S., and D. P. Labridis. 2007. Implementing Multiagent Systems Technology for Power Distribution Network Control and Protection Management. IEEE Transactions on Power Delivery, 22(1):433-443.
4. Brase, J.M., and D.L. Brown. 2009. Modeling, Simulation and Analysis of Complex Networked Systems: A Program Plan. Livermore, CA: Lawrence Livermore National Laboratory. Available via http://science.energy.gov/~/media/ascr/pdf/program-documents/docs/Complex_networked_systems_program_final.pdf [accessed September 19, 2014].
5. CAL EMA (California Emergency Management Agency). 2013. Constellation/Automated Critical Asset Management System (C/ACAMS). Available via: < http://develop.oes.ca.gov/WebPage/oeswebsite.nsf/Content/D290C3544ECABEF788257561006A1812?OpenDocument> [accessed December 22, 2013].
6. Congress (U.S. Congress, House of Representatives). 2011. Full Implementation of the Chemical Facility Anti-Terrorism Standards Act. House Report 112-211. U.S. Government Printing Office. Available via: <http://www.gpo.gov/fdsys/pkg/CRPT-112hrpt211/html/CRPT-112hrpt211.htm> [accessed December 22, 2013].
7. Congress (U.S. Congress, Senate and House of Representatives). 1990. Public Law 101-604 – Nov 16, 1990. Available via: < http://www.gpo.gov/fdsys/pkg/STATUTE-104/pdf/STATUTE-104-Pg3066.pdf> [accessed December 22, 2013].
8. Congress (U.S. Congress, Senate and House of Representatives). 2001. Public Law 107-71 – Nov. 19, 2001. Available via: http://www.gpo.gov/fdsys/pkg/PLAW-107publ71/content-detail.html [accessed September 19, 2014].
9. DHS (U.S. Department of Homeland Security). 2007. National Population, Economic, and Infrastructure Impacts of Pandemic Influenza with Strategic Recommendations. Available via: <http://info.publicintelligence.net/PI%20FINAL%20-%2012-21-07.pdf> [accessed December 21, 2013].
10. DHS (U.S. Department of Homeland Security). 2008. Fact Sheet: Critical Infrastructure and Homeland Security Protection Accomplishments. Available via: < https://www.hsdl.org/?view&did=235174> [accessed December 21, 2013].
11. DHS (U.S. Department of Homeland Security). 2013. Critical Infrastructure Sectors. Available via: < http://www.dhs.gov/critical-infrastructure-sectors> [accessed December 22, 2013].
12. DoD CIO (U.S. Department of Defense Chief Information Officer). 2010. The DoDAF Architecture Framework Version 2.02. Available via:

<http://dodcio.defense.gov/Portals/0/Documents/DODAF/DoDAF_v2-02_web.pdf> [accessed December 21, 2013].

13. EPA (U.S. Environmental Protection Agency). 2013. Atmospheric Modeling and Analysis research. Available via: <http://www.epa.gov/AMD/> [accessed December 21, 2013].
14. FEMA (Federal Emergency Management Agency of U.S. Department of Homeland Security). 2013. National Incident Management System (NIMS). Available via: < http://www.fema.gov/national-incident-management-system> [accessed December 22, 2013].
15. GeoTools. 2013. GeoTools: The Open Source Java GIS Toolkit. Available online via < http://www.geotools.org/ >[accessed December 2013].
16. HSWG. 2012. Homeland Security Working Group: Symbology Reference. Available online via: <http://www.fgdc.gov/HSWG/index.html> [accessed December 19, 2013].
17. Hutchings, C.W. 2009. Enabling Homeland Security with Modeling & Simulation (M&S). Interservice/Industry Training, Simulation, and Education Conference (I/ITSEC), Paper ID# 9512, Orlando, FL, Nov. 30-Dec. 3.
18. IEEE. 2010. IEEE 1516-2010 – IEEE Standard for Modeling and Simulation (M&S) High Level Architecture (HLA) – Framework and Rules. Available via: <http://standards.ieee.org/findstds/standard/1516-2010.html> [accessed December 19, 2013].
19. INL (Idaho National Laboratory). 2013. Modeling and Simulation: Critical Infrastructure Protection and Resiliency Simulator (CIPR/sim). Available via: <https://inlportal.inl.gov/portal/server.pt/community/national_and_homeland_security/273/modeling_and_simulation/1707> [accessed December 21, 2013].
20. ISTS (Institute for Security, Technology, and Society). 2013. Synthetic Environment for Emergency Response Simulation. Available via: <http://www.ists.dartmouth.edu/projects/archives/synth.html> [accessed December 19, 2013].
21. Jain, S. and C.R. McLean. 2003. Modeling and Simulation of Emergency Response: Workshop Report, Relevant Standards and Tools. National Institute of Standards and Technology Internal Report, NISTIR-7071. Available online via <http://www.nist.gov/msidlibrary/doc/nistir7071.pdf> [accessed December 22, 2013].
22. Kuhl, F., R. Weatherly, and J. Dahmann, 1999, Creating Computer Simulations: An Introduction to the High Level Architecture, Prentice Hall, Upper Saddle River, NJ.

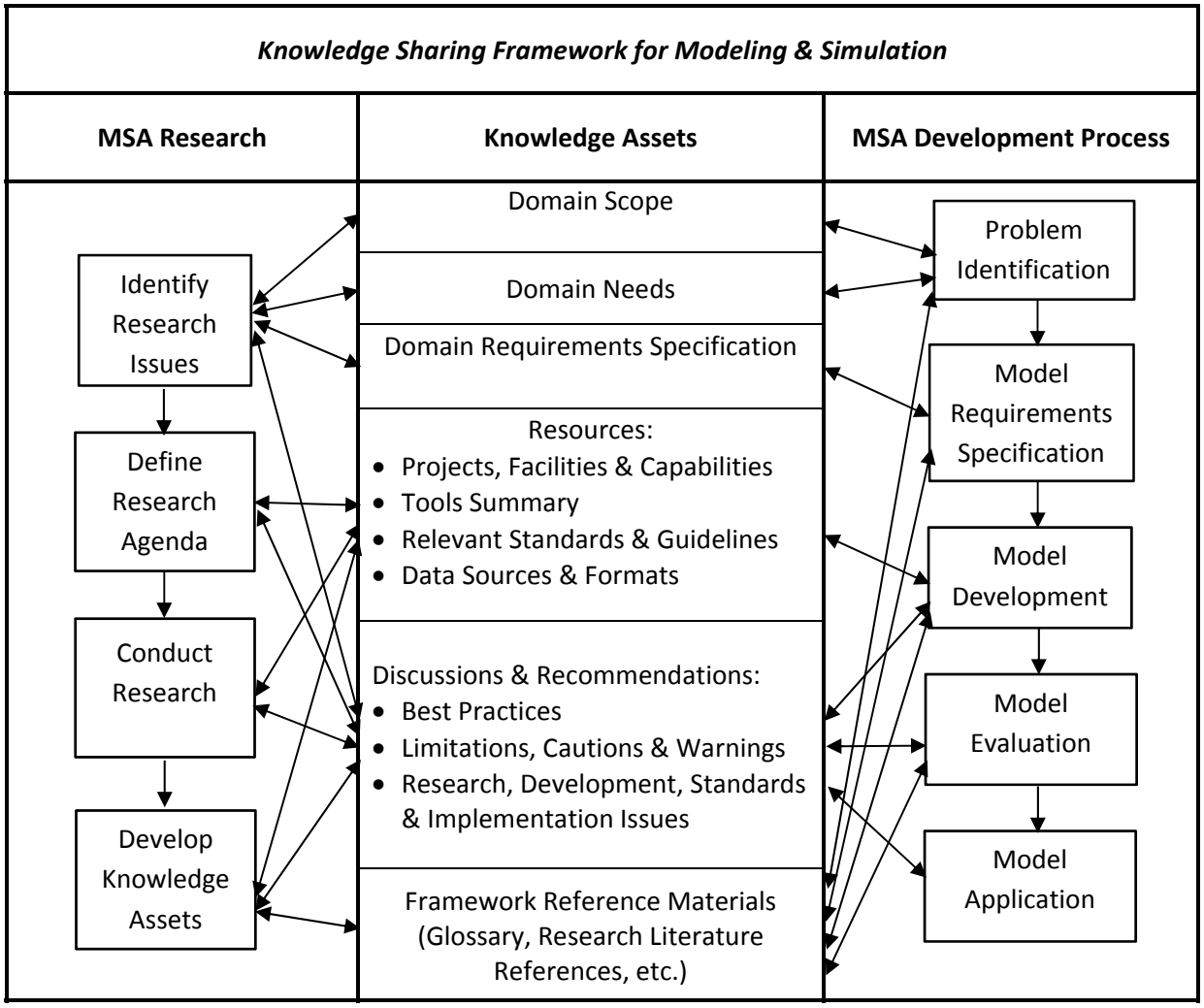
23. LANL (Los Alamos National Laboratory). 2013a. CIPDSS: Critical Infrastructure Protection Decision Support System. Available via: < http://www.lanl.gov/programs/nisac/cipdss.shtml> [accessed December 22, 2013].
24. LANL (Los Alamos National Laboratory). 2013b. EpiSimS: Epidemic Simulation System. Available via: < http://www.lanl.gov/programs/nisac/episims.shtml> [accessed December 22, 2013].
25. LLNL (Lawrence Livermore National Laboratory). 2012. National Atmospheric Release Advisory Center. Available via: <https://narac.llnl.gov/> [accessed December 21, 2013].
26. McGrath, D., and D. Hill. 2004. Unreal Triage: A Game-Based Simulation for Emergency Response, Proceedings of the Huntsville Simulation Conference, Huntsville, AL. Available via: < http://www.ists.dartmouth.edu/library/58.pdf> [accessed December 19, 2013].
27. McGrath, D. and C. Carella. 2005. Synthetic Environments for Emergency Response Simulation, Proceedings of the 2005 Game Developers Conference, San Jose, CA. Available via: <http://www.ists.dartmouth.edu/library/118.pdf > [accessed December 19, 2013].
28. McLean, C. R., S. Jain, and Y. T. Lee. 2008. A Taxonomy of Homeland Security Modeling, Simulation, and Analysis Applications. Simulation Interoperability Workshop (SIW), Paper No. 08S-SIW-098, Providence, RI.
29. McLean, C. R., S. Leong, and F. Riddick, 2000, Integration of Manufacturing Simulations using High Level Architecture (HLA), Proceedings of the 2000 Advanced Simulation Technologies Conference, April 16-20, Washington DC.
30. NEMSIS TAC (NEMSIS Technical Assistance Center, University of Utah School of Medicine). 2013. National EMS Information System (NEMSIS), Version 3. Available via: <http://www.nemsis.org/v3/> [accessed December 22, 2013].
31. NRL (Naval Research Laboratory). 2013. CT-Analyst. Available via: <http://www.lcp.nrl.navy.mil/ct-analyst/Home.html> [accessed December 19, 2013].
32. ProModel Corporation. 2013. MedModel - The Industry Standard for Healthcare Simulations. Available via: <http://www.promodel.com/products/medmodel/> [accessed December 22, 2013].
33. Qiao, J., D. Jeong, M. Lawley, J. P. Richard, D. M. Abraham, and Y. Yih. 2007. Allocating Security Resources to a Water Supply Network. IIE Transactions, 39(1):95-109.
34. Sandia (Sandia National Laboratories). 2013a. National Infrastructure Simulation and Analysis Center (NISAC). Available via: <http://www.sandia.gov/nisac/> [accessed December 21, 2013].

35. Sandia (Sandia National Laboratories). 2013b. Sandia Labs New Release: Hurricane Season: Predicting in advance what could happen. Available via: < https://share.sandia.gov/news/resources/news_releases/hurricane_nisac/#.UraEEvRDs1M> [accessed December 22, 2013].
36. Shendarkar, A., K. Vasudevan, S. Lee, and Y.J. Son, 2008. Crowd Simulation for Emergency Response using BDI Agents Based on Immersive Virtual Reality, Simulation Modelling Practice and Theory, 16, 2008, 1415-1429.
37. Stroud P.D., S.Y. Del Valle, S.J. Sydoriak, J.M. Riese, and S.M. Mniszewski. 2007. Spatial Dynamics of Pandemic Influenza in a Massive Artificial Society. Journal of Artificial Societies and Social Simulation 10(4):9.
38. UOF TRC (University of Florida Transportation Research Center). 2012. Traffic Software Integrated System - Corridor Simulation (TSIS-CORSIM). Available via: < http://mctrans.ce.ufl.edu/featured/tsis/> [accessed December 22, 2013].
39. Zachman, J. A. 2013. The Zachman Framework: The Official Concise Definition. Available via: <http://www.zachmaninternational.com/index.php/the-zachman-framework> [accessed December 22, 2013].

Table 9.1: Aviation Security Threats and Responses

Time Period	**Event/Threat**	**Vulnerability**	**Response**
1970s	Traditional hostage/hijacking	Guns, weapons	Magnetometers
December 1988	PanAm 103, Lockerbie	Bomb in baggage	Baggage scans
September 2001	World Trade Center, Pentagon attacks	Box Cutters, small knives, etc. on person or in carry-ons	Aviation and Transportation Security Act (ATSA)
December 2001	Reid hijacking attempt	Shoe bomb	Shoes removed
August 2004	Chechen suicide attacks	Vests	Pat-downs, backscatter
August 2006	Heathrow liquids plot	Novel liquid bomb	Liquids ban
June 2007	Glasgow airport attack	Vehicle-borne improvised explosive device (VBIED) to soft target	Increased awareness and focus on emerging threats to physical transportation infrastructures
December 2009	Non-metallic body bomb	Body bomb in sensitive area	Explosive trace detection, sensitive pat-down, whole body Imaging

Figure 9.1: Overview of Knowledge Sharing Framework for Homeland Security Modeling and Simulation technical areas



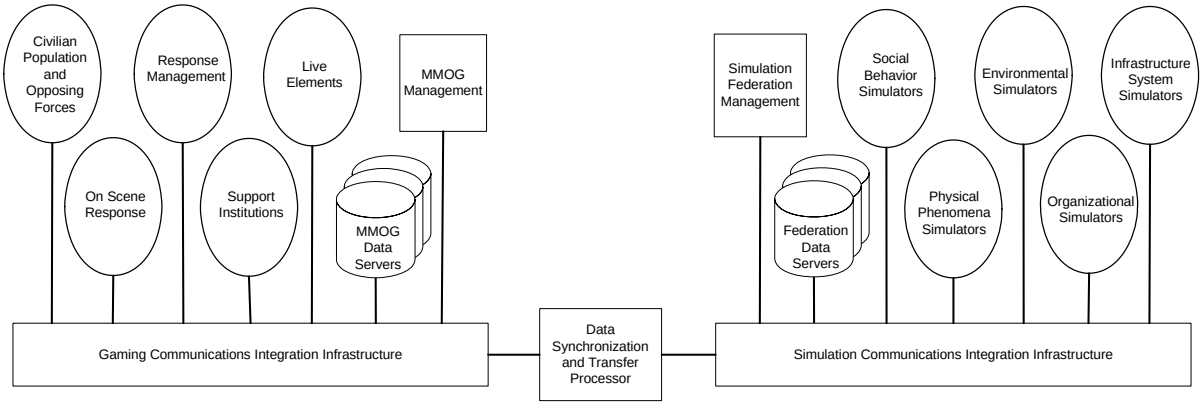


Figure 9.2: Architecture Concept for Simulation and Gaming for Incident Management

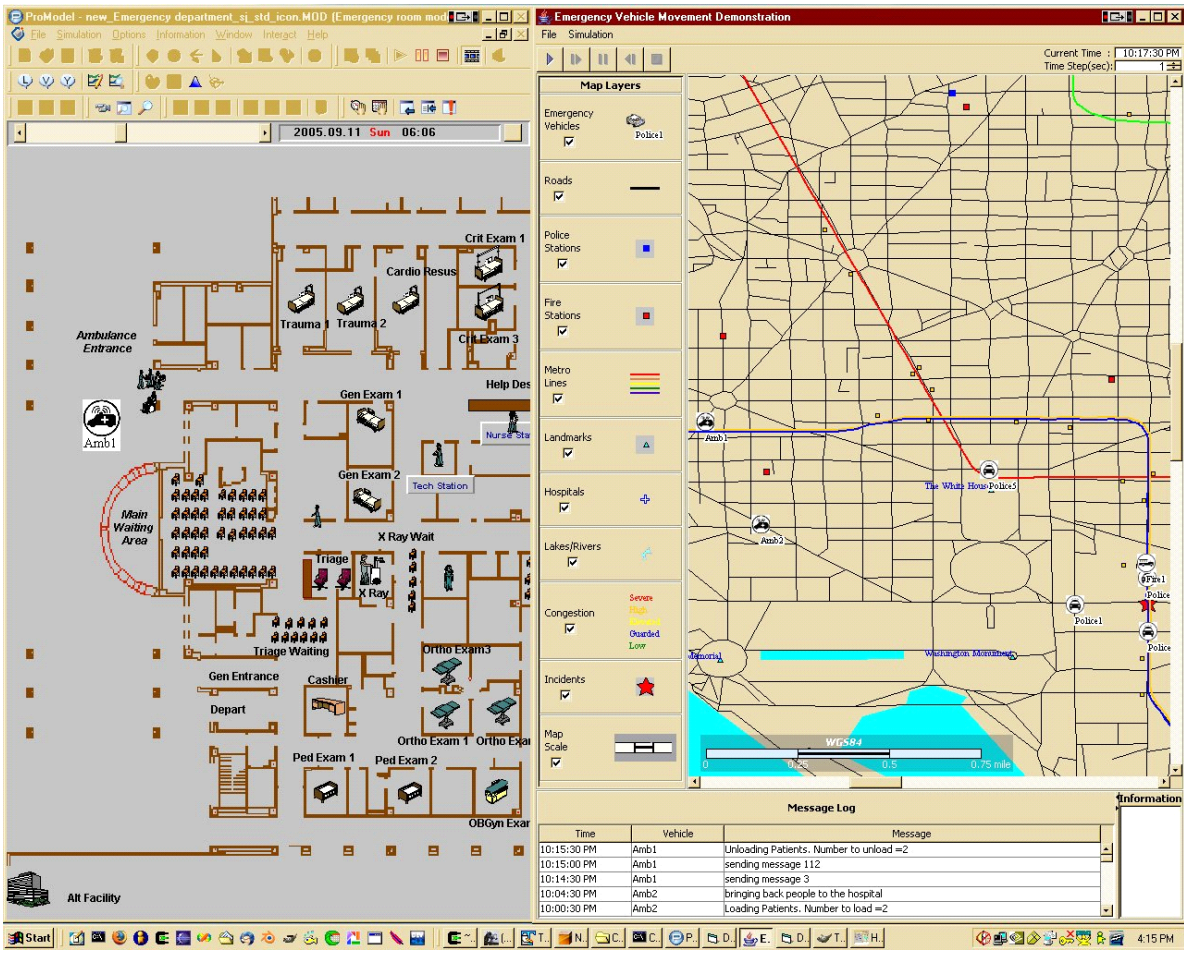


Figure 9.3: Screenshot of Integrated Execution of Emergency Department Simulation (left half) and the Emergency Vehicle Response Simulation (right half). Added Annotations Show the Corresponding Ambulances in the Two Simulations.