The Homeland Security Simulation (HLS-Sim)

George Stone
JSIMS PM Office
Alexandria, VA
George.Stone@OSD.PENTAGON.MIL

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

Abstract

American federal, state and local governments are reexamining their standards, procedures and preparedness in light of the shocking events on Sept. 11th. Hundreds of contingency scenarios must be examined to prioritize resources and time. One of the most effective ways to do so is with a simulation of the Homeland Security (HLS) environment.

Such a simulation could be constructed from a combination of existing military simulations and the development of new simulations with domain-specific algorithms to address HLS issues. The data requirements for military systems are just as exhaustive and similar in many ways as the civilian systems. Military simulation architectures, databases, and models provide a useful foundation from which to student HLS problems and upon which to construct HLS-specific tools.

1.0 Introduction

Time continues to flow forward from the milestone attack that permeated the world with the realization of hostilities on a serene homeland environment. People at work expecting just another day at the office were shocked into a sense of disbelief and surreal surroundings on this tragic day.

With this event behind us, we need to look to the future for ways and means to prevent such attacks from recurring. From security measures to preparation, our government has issued several calls to industry and academia for their cooperation, intellect and talents. The federal, state and local governments are reexamining their standards, procedures and preparedness in light of the shocking events on Sept. 11th. However, new organizations enhanced with better security and regulations do not always guarantee insight and proactive measures. There are hundreds of contingency scenarios to prepare for while the resources and time to examine and prioritize against these would cost billions of dollars. So, is there a risk-mitigation plan for these? How can we have the national, state and local governments "test out" their abilities and plans to react to such contingencies?

One way to do so is with a simulation of the world that we fear using current simulation techniques and architectures. The simulations being created now for several DoD agencies could be retrofitted to accommodate such a process. Having already spent hundreds of millions of taxpayer dollars on these systems, the US could model their important players in Homeland Security, take on the bad guys and assess preparedness in a simulated environment. Many of the activities such as sensing/detecting of certain key intelligence requirements are coded in existing models and

algorithms. The data requirements for military systems are just as exhaustive and similar in many ways as the civilian systems. We use vehicles, aircraft and watercraft in our models as do the police, fire departments, and Coast Guard. Once the system is identified, many surrogate models can be tested and then copied over to their civilian counterpart. Interactions and reactions to conditions would then be converted over to HLS-type activities. HLSim could then reuse the architecture, databases and rules established and in use by the US Department of Defense. Federal, state and local governments from many nations are reexamining their standards, procedures and preparedness in light of the shocking events on Sept. 11th.

Hundreds of contingency scenarios must be examined to prioritize resources and time. One way to do so is with a simulation of the Homeland Security (HLS) environment using "tried and true" simulation techniques and programs. DoD simulations can be retrofitted to accommodate such a process. The data requirements for military systems are just as exhaustive and similar in many ways as the civilian systems. A Homeland Security Simulation (HLS-Sim) would reuse military architecture, databases and models. It would also require the creation of a set of specialized modules to represent unique assets and behaviors in this scenario.

2.0 Homeland Security

Homeland Security is one of the newest challenges facing today's military. The impact of collaboration between local, state and national governments with other organizations is challenging. We will focus on Prevention (deterrence or reduction in vulnerabilites), Response (first on the scene and all the jurisdictional problems associated), and Recovery. There is also coordination underway between various agencies in and out of the government to consider cases where weapons of mass destruction (WMD) and other forms of terrorism may be employed in U.S. urban environments. By bringing multiple players and representatives together in this process, we can focus on our nation's and the military's vulnerabilities. Leaders, managers and players are from governmental and non-governmental agencies with representation at all levels (local, state and national). The timely *exchange* of important state-of-the-art information within Homeland Security can be represented within a simulation. The objectives of HLS-Sim will be to educate military participants on the terminology, players, and threats to Homeland Security while identifying ways for interagency organizations and their representatives to coordinate, cooperate and collaborate in a threatening or hostile in-country environment (manmade or natural disasters).

Domestic Preparedness organizations in the U.S. include the President, National Security Council, Departments of Transportation, State, Energy, Justice, Defense, DCI, FEMA, and the Defense Threat Reduction Agency (DTRA). The simulation will bring together multiple participants and organizations to share and gather information on their roles and responsibilities in Homeland Security. The HLS community needs to share scarce analytical and modeling resources to improve and protect US national interests.

The problem space is divided into multiple domains because each is unique and may require unique models and abstractions to represent the objects and events within it. In addition to models for the internal representation of objects and events, a multi-domain model will influence those abstractions such that they can be made interoperable across the domains [6].

3.0 Multi-domain Modeling

America's response to terrorist actions must bring together multiple networks of previously independent systems for defense, attack, and emergency response. Each of these can be categorized as a domain and the interactions between them represent interactions across these domains. Within the United States critical pieces of the country's infrastructure are being protected while terrorist networks attack and sometimes penetrate those defenses. This leads to the application of Emergency Response networks and the beginnings of retaliation by counter-terrorism networks. The effectiveness of these networks and the discovery of the optimal configuration of each is a task well suited for modeling and simulation.

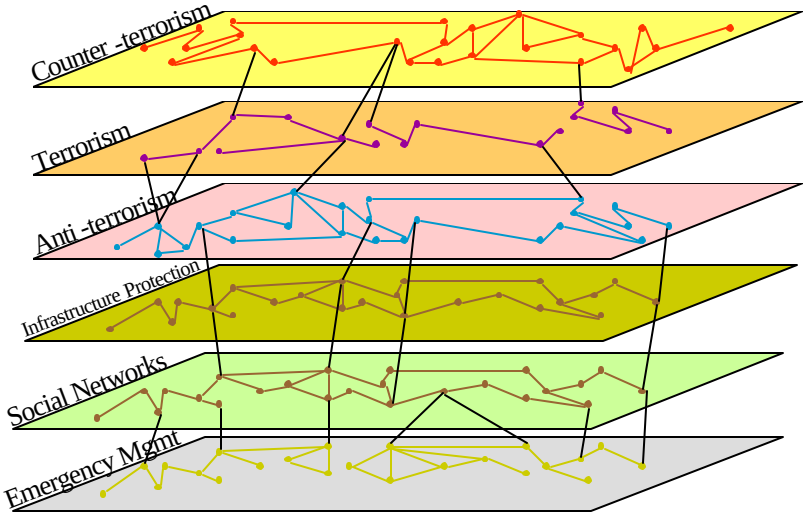

Figure 1. Multi-domain Infrastructure Relationships

3.1 Infrastructure Protection

All advanced countries are supported by a large number of very complex networks providing product and service delivery. The financial network housed in the World Trade Centers and the air transportation networks that were attacked on September 11th are just two of these networked services. Within in the United States additional networks include:

- Water
- Power
- Telephone
- Cellular Telephone
- Internet Serivices
- Highways
- Sewers,
- Food Distribution
- Interstate and Local Mass Transportation,
- Interstate and Local Trucking,
- Shopping Centers,
- Sporting Events, and
- Social Events.

Each of these provides a potential target for attack and each is protected to a different degree by difference government and commercial organizations. In the extreme case, it is desirable to protect every piece of this infrastructure. But, a more realistic approach is to provide a level of protection commensurate with the network's criticality to society, the concentration of its resources, its image in the political and social eye, and its perceived importance to an attacker.

These same criteria can be used in designing a simulation to represent them. It is impractical and probably unaffordable to create a simulation that represents all of the nodes and flows of all of these networks. But, it may be possible to represent the most critical networks and nodes. It is also important to consider the interrelationships of all of the networks and those with networks in the domains described below.

In order to protect these resources it is necessary to first understand how they operate, how they are related to other networks, and where their weaknesses lie. Professionals who work in these systems often implicitly understand these issues for their own networks. However, this expertise is difficult to organize and collect so that it can be understood and studied by people in other networks or by national leaders who are seeking a systemic solution to a national problem. An HLS simulation would be one useful tool for capturing expertise from all of the networks and presenting it such that a national-level solution could be explored.

3.2 Terrorism Networks

The networks we are trying to protect are threatened and attacked by networks of terrorist organizations. Those organizations are not simply individuals or small groups acting independently. Terrorists in the 21st century are international organizations with extensive internal resources and external supporters. In a previous paper [4] one of the authors presented one perspective of these terrorist networks. That paper described the role of the command nucleus, field cells, communications networks, weapons technologies, financial assets, national hosts, and sympathizers. Like modern advanced societies, all of these resources must be available and coordinated in order to enable international terrorist groups like the Al Quaeda [1].

3.3 Emergency Management

Once a terrorist attack occurs, most infrastructure protection systems and networks turn to the emergency management domain for assistance and solutions. This network includes the police, fire, ambulance, rescue, hospital, FEMA, National Guard, and state and local government resources designed to handle these situations. Each of these provides a number of nodes and flows within its own organization and is required to cooperate with all of the other assets in this domain.

The HLS simulation would include the number, location, and connectivity of each of these networks and their capabilities to exchange information and to coordinate with other networks. All of these systems are currently exercised through the use of live rehearsals of emergency situations and through table-top discussions in a classroom environment. These manual forms of simulation are very useful but they rely too heavily upon manual calculations and estimates that are better handled by a computer. They also provide few tools for automatic data collections and analysis. An HLS simulation would be an excellent supplemental tool for studying these problems.

Many of the assets and actions within the emergency management domain have similarities with military assets and actions. This may allow the adaptation of military tools to represent this domain. There have been several attempts to demonstrate this type of adaptation. The best known of these is the Plowshares project in which the JANUS combat model was modified to represent hurricanes, tornadoes, fires, and the emergency response assets that would handle such events. A more recent project entitled EPICS has attempted a similar transformation of the JANUS simulation. Companies such as Raytheon have also converted some of their internal wargaming tools into emergency management tools and PC combat games like Real War by OCI are being modified to include cooperation between different organizations.

Once the immediate emergency has been handled, we generally turn to counter-terrorism resources for retaliation.

3.4 Counter-terrorism

Counter-terrorism models and networks include military forces, intelligence organizations, logistics, political leaders, and diplomatic intermediaries. The primary focus of these assets is not to protect the infrastructure or to respond to the emergency, though they may participate in these to a limited degree. Instead, their focus is to locate those responsible for the attacks and deal with them. These networks of assets must be able to interact with certain of the assets in the terrorism networks. Military forces would probably be focused on the command nucleus, field cells, and weapons caches. Intelligence assets would focus on the command nucleus, communications, finances, and social networks. Political and diplomatic assets would focus on the national hosts, sympathizers, and the cultural or social environment in which the terrorists live [5].

This domain is the most amenable to the reuse of existing military simulation models and tools. The actions of the assets involved are adaptations of more traditional combat scenarios for which the military models were constructed.

3.5 Anti-terrorism

Anti-terrorism is classified as unique from counter-terrorism. Anti-terrorism are the actions performed to prevent future attacks, while counter-terrorism is focused on responding to an attack that has occurred.

Following a terrorist attack, many organizations adopt new operating policies designed to prevent a second occurrence. When these measures become a permanent part of the protective practices they would be considered part of the infrastructure protection domain described earlier. However, many of these measures are temporary and do not fit within the long-term structure of the networks being protected or the mission of the organization providing the services. The addition of the National Guard at every airport security point is a practice that can only be maintained for a limited time. This must eventually be transformed into a more sustainable and permanent measure. The use of financial intelligence to search for specific money transfers identifying participants in the attacks are another of these measures. Special screening by the immigration and customs offices are another.

International organizations also provide humanitarian and emergency support to the citizens displaced by attacks on terrorist organizations. The media turns its attention to the issue and sometimes dedicates an entire channel to discussions of the topic.

The goal of these actions is not to capture or punish those who conducted the initial terrorist attack, but to thwart others who may be planning another attack or who simply seize upon the event to release their own wave of evil.

4.0 Conclusion

Homeland Security is now a permanent part of our national defense. It will remain the primary focus of our diplomatic, justice, intelligence, and military policies for at least the next decade, and probably for several decades. In spite of this attention, our enemies will continue to attack our homeland and will occasionally succeed in their missions. Modeling, simulation, and analysis of this situation will contribute to our understanding of this threat, our preparedness for it, and our ability to recover from the events it creates. Just as models of traditional combat have helped us understand and prepare for major warfare engagements, homeland security simulations will prepare us for these new threats. Hopefully, they will also contribute to a future in which the peaceful nations of the world are so well prepared for terrorist threats that the terrorists are no longer able to pose a threat.

5.0 References

[1] Bodansky, Yossef. (2001). *Bin Laden: The Man Who Declared War on America*. Prima Publishing. Roseville: CA.

[2] Hughes, Wayne P. (1997). *Military Modeling for Decision Making*. Military Operations Research Society. Alexandria, VA.

[3] Rashid, Ahmed. (2001). *Taliban: Militant Islam, Oil & Fundamentalism in Central Asia*. Yale University Press. New Haven: CT.

[4] Smith, Roger. (2002). "Counter-terrorism Simulation: A New Breed of Federation". *Proceedings of the Spring 2002 Simulation Interoperability Workshop*. Orlando, FL.

[5] Smith, Roger. (2001). "Modeling and Simulation Adds Insight on Terrorism". *Signal Magazine*. December, 2001. Armed Forces Communications and Electronics Association (AFCEA).

[6] 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.

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

Author Biographies

LTC GEORGE F. STONE received his doctorate in Industrial Engineering in 1996 from the University of Central Florida, master in Industrial Engineering at Texas A&M in 1989 and bachelor of science in general science at the US Military Academy in 1980. He is currently the senior Army representative for the Department of Defense's Joint Warfare System. Prior to this assignment, George directed the Army's Warfighting Analysis and Integration Center. He has been the technical director for the JWARS program, deputy project manager at the Joint Simulation System Program Office and system manager for the Warfighter's Simulation program. George participated a civil-military operations simulation, the Plowshares program in 1995 and led a Military Operations Research symposium on Homeland Security in March 2001. An active duty Army lieutenant colonel, George has served in numerous field artillery assignments, including two battery commands in Germany, and was an Assistant Professor for the Systems Engineering Department at West Point.

ROGER D. SMITH is a Vice President of Technology for Titan Systems Corporation working on next-generation simulation applications and distributed computing technologies. His most current work has been studying information operations and counter-terrorism as well as the development of new intelligence simulations. He is the creator and instructor for 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.