

## Counter Terrorism Simulation: A New Breed of Federation

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

Keywords:  
Terrorism, Federation, System Dynamics, FOM

**ABSTRACT:** *In this paper we will explore the need for a suite of simulation tools that can be used to analyze, predict, and prevent terrorist activities. Simulation technology and tools can be applied directly to the war against terrorism, but custom solutions for this mission do not yet exist.*

*A simulation of terrorism must address each of the components of a terrorist network – the command nucleus, field cell, group communications, national host, sympathizers, and support assets. Together these components create a network that enables a small group to conduct guerilla warfare against any target in the world. Simulating our response to these components will require more than traditional interactive or analytical simulations. An appropriate simulation must represent the assets and missions of 1) the surgical application of military special forces - to include helicopter insertion and support, infantry operations in an urban environment, and search and rescue teams; 2) intelligence collection against urban and guerilla forces - particularly focused on communications and human intelligence and moving target surveillance; 3) political actions to decrease the ability of an organization to operate in specific countries; 4) legal actions against non-governmental sympathizers that support terrorists; 5) financial and economic sanctions targeted at assets belonging to terrorists and at national that host them; and 6) the cultural influences on potential recruits and supports of terrorists. These activities cover a very broad spectrum and it is probably not feasible to include all of them in a single simulation system. Depicting and analyzing this entire spectrum calls for a specialized suite of interoperable simulation tools, each of which focuses on one or two aspects of the problem.*

*Terrorism will likely remain the focus of international politics and homeland defense for the next twenty years. It is essential that simulation technology be adapted and invented to support these actions.*

### 1. Introduction

The terrorist attacks on the World Trade Center demonstrated that we are not completely safe from foreign attacks on our home soil. For decades, the United States has focused its military and intelligence capabilities on enemies beyond its own borders. But, it has become incredibly clear that our enemies have the ability and the determination to reach through our defenses and strike at critical assets here at home. Our political, military, and intelligence resources are now defending our interests by defending our own homeland.

Homeland security has already taken on a new importance in government. Prior to September 11<sup>th</sup> most people on American soil felt safe from foreign attack. Today, we look to our government for protection from attacks like those on the World Trade Center and Pentagon. Our government in turn looks to its servicemen and contractors to create and operate those defenses.

Modeling and simulation can be part of this new mission. It can provide knowledge, understanding, and preparation against future attacks. From 1945 until 1995, the M&S community has devised algorithms and systems to help us understand the threat from large-scale conventional, nuclear, chemical, and biological attack. These algorithms and systems were not laying on the shelf waiting to be put into service, but rather, had to be created piece by piece over a period of many years. We now face the need for a new set of tools and must begin creating those tools now if we are to be prepared for future terrorist threats. Within the M&S community our responsibility is to create algorithms and systems that can contribute to this fight, because terrorism will be to the 21<sup>st</sup> century what the Cold War was to the 20<sup>th</sup>.

### 2. The Evolution of New Simulation Models and Tools

The simulations necessary to address the complexity of the terrorist threat must evolve just as the current simulations of traditional combat have evolved over decades. A few organizations have been heavily involved

in quantifying the terrorist threat and identifying the relationships that hold it together. But, the largest part of the simulation community has been focusing on Desert Storm-like scenarios. Therefore, most of the military and intelligence modeling profession faces a steep learning curve in shifting to this new mission.

**Wargames.** Creating manual wargames allows us to identify objects, attributes, events, and relationships that are relevant to the problem we are trying to solve. Working with maps tables, documents, and counters allows modelers to focus on the structure of the problem rather than the structure of a computer language of software tool.

**System Dynamics.** System dynamics models are designed to capture nuggets of knowledge and hold them together so the complexities of their relationships can emerge. Since Jay Forrester pioneered this concept in the 1950's, models have been created to help us understand the complexities inherent in all types of dynamic systems. The key here is gaining an understanding of how terrorist organizations work.

**Operations Research.** Once we understand how a dynamic organization works, OR can be used to identify the optimum methods of countering it. We can use these models to identify its weakest points and to quantify our responses to its actions.

**Training Simulations.** Understanding how the target operates and how best to respond to it, we will then be in a position to capture this in interactive training simulations that can be used to teach people to take action against the new terrorist threat.

Each of the model classes above contribute essential information to our understanding of a problem and to our ability to accurately capture it in a simulation.

### 3. Terrorist Organizations and Actions

Like a foreign nation, a terrorist organization is a complex system composed of many different interlocking components. Each component and each relationship between components is a potential target for our countermeasures. A key part of creating M&S tools to address terrorism will be determining which actions work best against which targets.

A simplified view of a terrorist organization is given in Figure 3.1. The Command Nucleus holds the organization together and is the ultimate source of

direction and orders. However, it is not the sole conduit for all information, money, and weapons. The Field Cells operate under the direction of the Command Nucleus, but also possess a good deal of autonomy in accessing financial assets and weapons. Financial Assets are provided by Sympathizers and by the Command Nucleus. These allow the field cells to function on a day-to-day basis and give them the resources necessary to carry out a mission. Weapons are purchased openly or on the illegal market. Host Nations are those political and geographic powers that protect and host the terrorist organization. This support is particularly important when an organization is small and just getting started. It is also essential for providing a location for recruiting and training operatives. Communications are an essential part of keeping the organization together and coordinating its actions.



Figure 3.1. Simplified Terrorist Organization

Each piece of the organization presents a unique target for our countermeasures. Each piece also exists in multiple domains (Figure 3.2). The Command Nucleus and Field Cells are physical assets that can be reached with traditional military and police forces. Communications exist in an information domain that is accessible to our intelligence resources. A Host Nation exists in the political domain that must be addressed by political forces. Sympathizers exist in the physical domain, but the real target of interest here is one of culture and community. Financial assets exist in a unique domain accessible only to financial organizations. Finally, captured people, organizations, and finances are delivered to the legal system to be eliminated.

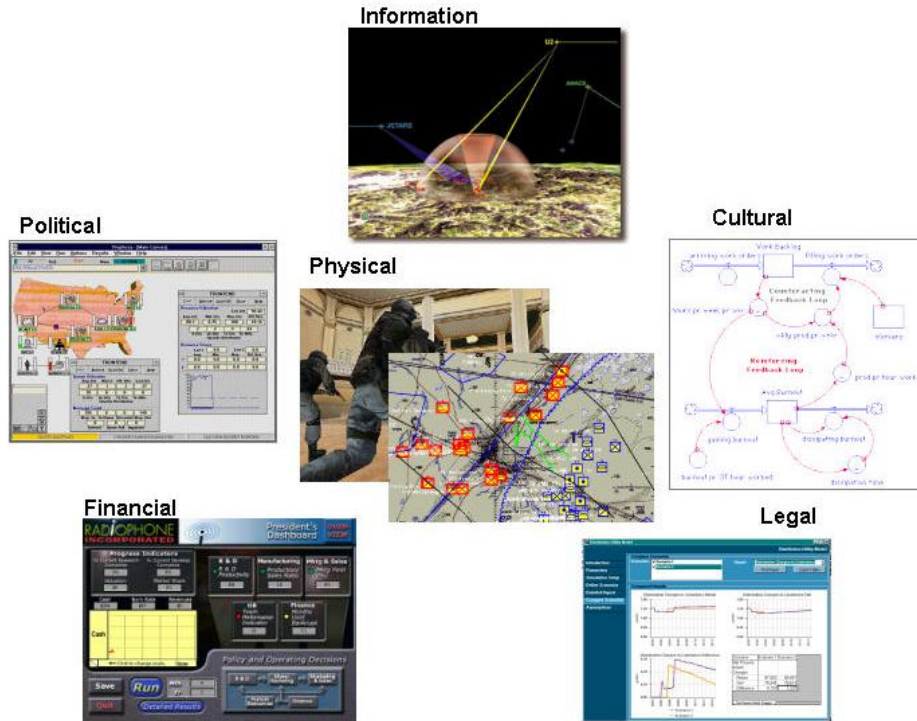


Figure 3.2. Domains of Terrorism

This diversity calls for the employment of a wide variety of assets. It is not immediately clear what all of the relationships are between these pieces or how the application of one countermeasure will impact the entire organization. There remains a great deal of research and experimentation to unveil these relationships. In the following section we will discuss some of the

countermeasures that can be taken in each domain and the impacts this will cause in other domains.

#### 4. Simulation's Application to Counter-terrorism

The different domains that must be explored through the tools and methods described above are shown in Figure 4.1 and are described in the section below.

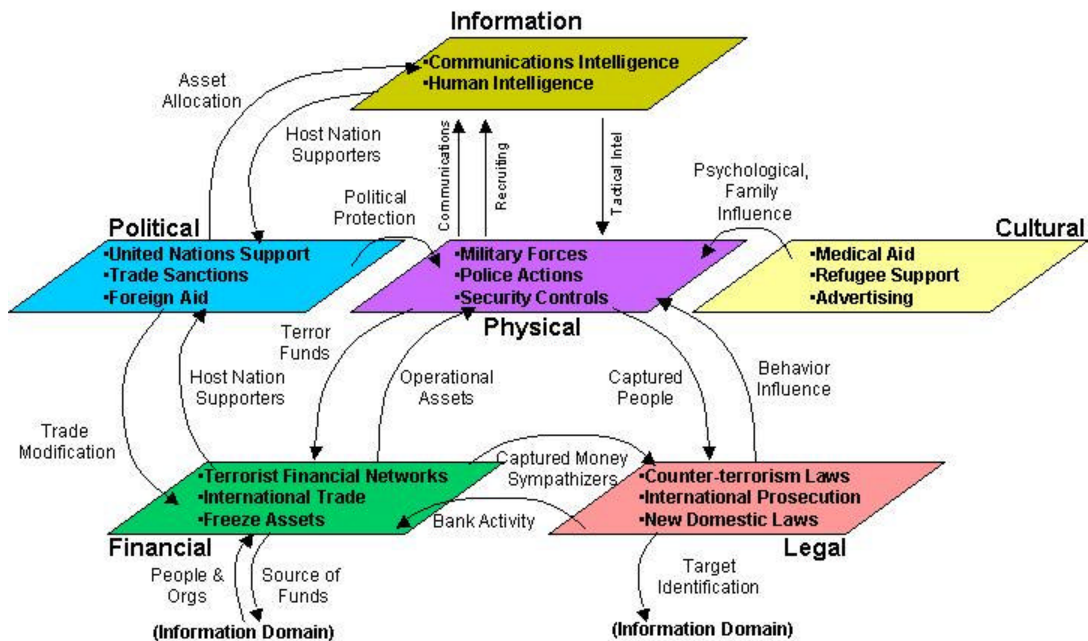


Figure 4.1. Cross-Domain Interactions

#### **4.1 Military Simulation**

The military portion of the scenario includes actions like those conducted in Afghanistan in search of Al Qaeda. A traditional combat simulation in which aircraft bomb targets, helicopters deliver special forces, infantry engage in firefights, and surveillance aircraft search for targets can be used for the military portion of the mission. Existing wargames and semi-automated forces systems can be adopted to meet this need.

But such a system does not represent the intelligence assets and activities that have gathered clues to the identity, location, activities, and plans of the targets. This must be carried out in a different federate.

#### **4.2 Intelligence Simulation**

Intelligence simulations represent all of the intelligence, surveillance, and reconnaissance assets available to the United States. This includes the processing, collating, and fusing capabilities of different organizations and identifies what can be known about the target. This simulation narrows perfect knowledge of the battlefield down to what is really knowable and actionable at specific times in the scenario. Some wargames use human role players to manually narrow perfect knowledge of the real world to what is accessible to our forces. This is effective for small vignettes, but is impractical for large scenarios and long timelines. Neither does it provide the technical accuracy, consistency, and traceability that are necessary for consistent, realistic representation.

Intelligence simulations access the physical battlefield to extract potential targets. They return reports containing the identities, locations, activities, and intentions of enemy forces. This information is used by the Military Simulation to direct its forces and to target precision weapons. This information may also be provided to Political and Financial Simulations to focus their own actions.

#### **4.3 Political Simulation**

Political Simulations are often conducted as human role-playing exercises. When these are assisted by computers that track decisions and provide information about the world scenario, they can also be integrated into the larger mission against terrorist networks. Actions in the political domain may include garnering support from the United Nations and from countries like Pakistan. They may also impose trade sanctions and withhold foreign aid to induce host countries to take steps against terrorist organizations. The goal is to deny terrorists the safe

homeland that they need to maintain training facilities and command bases.

Intelligence simulations provide the data necessary to focus political actions and to convince coalition partners that certain parties are involved in terrorist actions. Political actions should have a direct impact on the ease and strength of operations being conducted in the Military Simulation and may influence the tasking of Intelligence assets.

#### **4.4 Financial Simulation**

Terrorist networks rely on international money transfers to support their field cells around the world. Political Simulations may provide the evidence necessary to persuade international banks to take actions against specific customers. The political domain is the conduit through which intelligence information is released to the Financial Simulation. The Financial Simulation is where specific aspects of trade and financial sanctions are executed. It also controls the flow of money to field cells, thus impacting their effectiveness.

Financial action against identified groups can lead to information about relationships that identify previously unknown collaborators that can become targets for Military and Intelligence actions. They also provide evidence that can be used to prosecute terrorists in the Legal Simulation.

#### **4.5 Legal Simulation**

Legal Simulation is a new domain of wargaming. In it, new laws are passed and prosecutions are made against terrorists. These insure that people captured in the Military Simulation and identified in the Financial Simulation are removed from active participation in terrorist activities. This simulation can be used to extract information during plea-bargaining concerning terrorist groups, individuals, and activities that are as yet unknown to our counter-terrorist groups. This information can be fed back into the Military, Financial, Political, and Intelligence simulations to assist them in locating more terrorists.

This simulation may also influence the activities of terrorist groups by intimidating individuals to the point that they do not join the group or are reluctant to carry out missions within the borders of countries that are aggressively capturing and punishing people.

#### **4.6 Cultural Simulation**

One reason that terrorists can persuade people to join them and to take violent actions against certain targets is

that they control the culture in which people are raised. A Cultural Simulation can be used to explore ways to influence this environment. The goal is to persuade these people to take non-violent courses of action to address their grievances. The cultural simulation will represent the influence of media such as the radio and television within a culture. As an example, the Taliban's restrictions against media created an environment in which they could mold people's minds in the absence of contradicting evidence. This simulation would also provide medical and nutritional support to citizens and refugees in target countries. This conveys a distinct message about the supposed enemy – one that contradicts propaganda.

This simulation will have a psychological influence on the people encountered in the Military Simulation. The goal is to influence the populous to support our actions and to sever their ties with terrorist organizations. Assets providing medical support can also gather information useful to the Intelligence simulations in searching for targets or anticipating future activity.

#### **4.7 The Gestalt**

The federation of simulations described above does not exist at this time. In fact, we are at such a primitive stage in our understanding of all domains of the problem that we are not prepared to begin creating computer software of this problem. At this point we need to approach the problem by manually defining and exercising a wargame that can capture all of the interactions and provide a laboratory for discovering additional resources, events, interactions, and relationships that are important across the entire problem. Then we will be in a position to move on to system dynamics models, operations research, and training systems.

In some cases, the domains and simulations described above are significantly separated along a timeline such that it would be very difficult to include them in an interactive exchange. A scenario spanning several months would be required to pull in all of the assets and events described above.

#### **5. Interoperability Across Domains of Terrorism**

As stated earlier, all of the activities and interests of a terrorist organization cannot be represented in a single homogeneous model – the problem is too big and too diverse. Such a complex organization is better represented in a suite of models that exchange information that is generated in one dimension of the problem and that also impacts another dimension.

A federation object model (FOM) for such a federation would be very different from a FOM designed to join simulations of object-on-object combat operations. This FOM would contain many objects and interactions that represent a unique relationship between just two federates. For example, the identification of terrorist sympathizers may be of no interest to the combat simulation, but may be essential to the financial simulation. This identification would lead financial institutions to specific accounts for confiscation. Financial evidence may then be a crucial part of the legal actions that can be taken against the organization, removing it from the terrorist's support network, and limiting their ability to purchase airplane tickets or to move about the country. Some of the objects and interactions that must exist in a counter-terrorism FOM are shown in Figure 5.1. The figure also illustrates the need for object attributes that are able to respond to influences from these unconventional external federates.

|              | Physical  | Information  | Political                                      | Cultural  | Financial  | Legal   |
|--------------|---|--|--|---|--|---|
| Objects      | Terror Command<br>Terror Field Cells<br>Military Forces<br>Special Forces<br>Law Enforcement<br>Customs | Sensor Platforms<br>Sensors<br>Analysts<br>Distribution Cells      | National Govt<br>United Nations<br>Tribal Govt | Aid Workers<br>Food<br>Medicine<br>Media<br>Education | Finance Institutions<br>Finance Networks<br>Account Holders<br>Money | Justice System<br>Military Tribunals                  |
| Modifiers    | Fear<br>Loyalty<br>Duty<br>Org Visibility   | Cultural Coop<br>Legal Position                                    | Power<br>Attention                             | Political Enviro<br>Cultural Mind                     | Self-interest<br>Asset Access  | Political Positions<br>Financial Info<br>Mental State |
| Interactions | Prisoners<br>Communications<br>Intel Reports  | Tactical Intel<br>Cultural Intel<br>Financial Intel<br>Immigration | Trade Sanctions<br>Foreign Aid<br>Protection   | Lives Saved<br>Media Images                           | Money Transfer<br>Transfer Source                                    | Trials/Convictions<br>Immigration<br>Prosecutions     |

Figure 5.1 Multi-Domain Terrorism FOM Concept

## 6. Welcome to the Next 20 Years

Over the next 20 years, America's arsenal against terrorism will expand dramatically and simulations will be part of that arsenal. Though a need will remain for more traditional models of combat, we are faced with a huge vacuum of tools to address this new threat. We must construct tools that allow our military, political, financial, legal, intelligence, and cultural agencies to understand all of the aspects of this new threat and to become prepared to address it.

Simulation scenarios will no longer focus solely on foreign countries and their topography. In the future, they will include domestic locations and all-to-familiar cultural features.

## 7. 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] Perla, Peter. (1990). *The Art of Wargaming*. Naval Institute Press. Annapolis, MD.
- [4] Rashid, Ahmed. (2001). *Taliban: Militant Islam, Oil & Fundamentalism in Central Asia*. Yale University Press. New Haven: CT.
- [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<sup>n</sup>: 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 Biography

**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.