A Concept for the Use of Red Teams in Homeland Defense

Richard L. Craft

Introduction

Immediately after the attacks on 9/11, Sandia National Laboratories' management initiated the Sandia Study of the War on Terrorism (SSWOT). Run by Sandia's Advanced Concepts Group and supported by experts from all parts of the Lab, the study was organized into three teams (Red, Yellow, and Green) that focused on the following three questions, respectively:

- How do we find and stop terrorists?
- How can we protect the homeland?
- How do we address the root causes of terrorism?

The Yellow Team quickly concluded that trying to avoid ever again being successfully attacked was a losing strategy and that a more balanced, holistic approach was required as shown in *Figure 1*. In simplest terms, the strategy articulated in this framework is "watch for the punch and do all that you can to keep it from landing; if it does land make sure that it will never knock you out and that you can quickly recover; then, make sure that punching you always presents a risk to the one throwing the punch." In the months that followed the SSWOT work, Sandia's Advanced Concepts Group along with staff from a number of other Sandia organizations pursued further

development of specific ideas that had emerged in the study. These included:

- **IRIS (Intelligent, Robust Infrastructure Systems)** – This effort looked at what was required to create infrastructure that was aware of events in its environment, could protect itself against attack, and could automatically reconstitute after an attack. It also looked at approaches for rapidly replacing or augmenting infrastructure that had been completely or partially destroyed by an attack.

Figure 1. Yellow Homeland Defense Framework

- **FACETS (Fractal Approach for Clarifying and Enabling Timely Support)** – This effort looked at issues involved in anticipating an attack and effectively responding once an attack had been launched. The primary emphasis here was on local emergency preparedness and mechanisms for enabling intelligent, coordinated response.

- **SSB (Smart, Secure Borders)** – This effort looked at architectural approaches and point solutions for controlling the entry of bad actors and dangerous materials into the nation while, at the same time, not harming (and possibly improving) the flow associated with international trade.

- **DICTUM (Dynamic Integrated Capability for Threat Understanding and Mastery)** – The goal of this effort is to explore the development of a socio-psychological conceptual framework represented through a computational model that can be exercised to help understand and influence terrorist behavior.

- **SDAC (Sense, Decide, Act, Communicate)** – A recurrent theme in much of the SSWOT work and subsequent efforts was the need for vastly improved awareness. This effort focused on how recent technological advances might be used to deliver a new generation of smart sensor networks and how these might be applied in a range of settings related to the war on terrorism.

- **Dotology ("The Science of Connecting the Dots")** – One of the most talked about needs in the wake of 9/11 is the ability to better utilize the data that is collected within the nation's intelligence and law enforcement communities. The

perception is that, due to inadequate data management and communication systems and the extreme amount of data generated by the communities' collection resources, key needles are missed in the haystack of available intelligence. This effort focused on approaches to addressing this problem.

As these follow-on efforts progressed, it became apparent that a coherent constellation of concepts was emerging. At the center of this constellation was a cluster of ideas related to red teams and how they might benefit the war on terrorism. The goal of this paper is to capture Sandia's thinking in this area. Clearly, refining and bringing these ideas to fruition will require the expertise and involvement of many organizations. Even though much of this paper is written in a definitive tone—"We will do X, then Y, then Z"—the ideas in this paper should be seen as nothing more than Sandia's current opinions on this subject. While Sandia's expertise in certain areas addressed by this paper (e.g., system attack methodologies) is quite deep, in other areas (e.g., war gaming) Sandia is a relative novice, and feedback from more expert organizations is needed to strengthen the concepts and approaches articulated in this document.

What Is a Red Team?

As used in the context of the discussions that followed 9/11, a red team is a set of individuals who are experts at playing the role of terrorist organizations. They are "bad actors" who revel in figuring out how to attack and cripple or destroy things and people. Typically, these teams are composed of "strategists"—generalists who innately understand how to approach undermining systems—and "domain experts"—specialists intimately familiar with the inner workings of the types of targets to be attacked or

methods to be employed in an attack. In this partnership, the strategists sketch out the *what:* "Wipe out the capabilities and population of this region by destroying this dam," and the domain experts color in the details of *how:* "Defeat local defenses and place large charges at the submerged west interface of the dam and the canyon." An effective red team must be able to effectively "think like a terrorist" and plan actions and make decisions in the same ways that specific adversaries would. This depends on the red team being able to analyze and characterize these adversaries in a dispassionate way—understanding not just what they do but also why.

How Red Teams Could Help

As Sandia pursued each of the SSWOT follow-on efforts, a number of needs that could be supported by red teams were identified. These included:

- helping organizations think through the ways in which terrorists might attack their assets, the likely impact of these attacks, the various ways that these organizations might harden themselves against attacks, and effective ways of responding to the attacks when they occur;
- training defenders and responders at all levels inside and outside the government through the use of realistic adversaries;
- developing and codifying attack scenarios in a way that helps the intelligence community and others implement manual and automated "scenario-driven data mining";
- evaluating new policies, doctrine, strategies, and tactics for handling terrorism;
- augmenting battle staff and emergency operation teams during operations immediately following the initial phase of an attack; and

- enabling others to come to understand the terrorists.

Preparing Organizations

In a balanced approach to homeland defense, the national government cannot responsible for everything, nor should it be. While certain functions, such as intelligence, are best conducted at the national level, others, such as local surveillance, preparedness, and first response, are primarily the responsibility of both private and public state and local entities. These entities own much of what will be impacted by an attack and must be adequately prepared to watch for indications of attack, interdict if possible, and to respond if an attack is launched. Being prepared is contingent on self-awareness—having thought through what to look for and what could go wrong, and good advance planning—knowing when to interdict when possible and who will respond in a given situation and how and with what resources.

One of the ideas generated in the FACETS effort is that red teams can help with this process both by sharing tools that help non-experts think like expert adversaries and expert defenders and by helping organizations exercise their plans. While the nature of these tools is discussed later in this paper, the central notion that the reader should take away right now is that these tools allow an organization to explicitly model their missions, assets, and operating environment and to then systematically assess this world through the eyes of an adversary. Vulnerabilities and potential attack plans thus identified then drive the development of defense and response planning based on a companion set of tools that help the organization think more expertly about how to handle these potential problems. One program underway right now at Sandia is already heading in this direction

with the development of the Community Vulnerability Assessment Methodology (CVAM). These tools also help local agencies think through what "signatures" might be presented by a group trying to attack a given target in their area.

Training Defenders

While planning is a critical step in preparing an organization for possible attack, by itself it is not adequate. Plans must be exercised and evaluated in realistic settings before the people charged with implementing the plans can be said to own them and before the plans themselves can be proven effective. Given this, once an organization has assessed itself and identified both its vulnerabilities and its approaches for addressing these vulnerabilities, red teams can be used to exercise the organization's plans.

This exercising can be done war-game style: red and blue teams battling in a make-believe world governed by a white team (*Figure 2*), or in real-world exercises

conducted at the sites identified by the organization. In these games, red represents terrorist cells and their partners. Blue represents defenders at all levels of government and industry. The white team plays three roles: they work with players and game sponsors to frame the game to be played; they govern the execution of the game as it is being played, determining what is possible (e.g., "Could blue see red do this?"), what is allowed, and how red and blue moves impact the state of the game; and they evaluate the game after the fact to understand exactly what happened during play and why.

In addition to addressing concerns identified by the host organization, red teams may use the models developed by the organization to identify other objectives or different strategies for achieving attack objectives established by the organization. The goal in doing this is to strengthen the organization's plan by filling in holes that the red team perceives that the terrorist group they are playing would pursue.
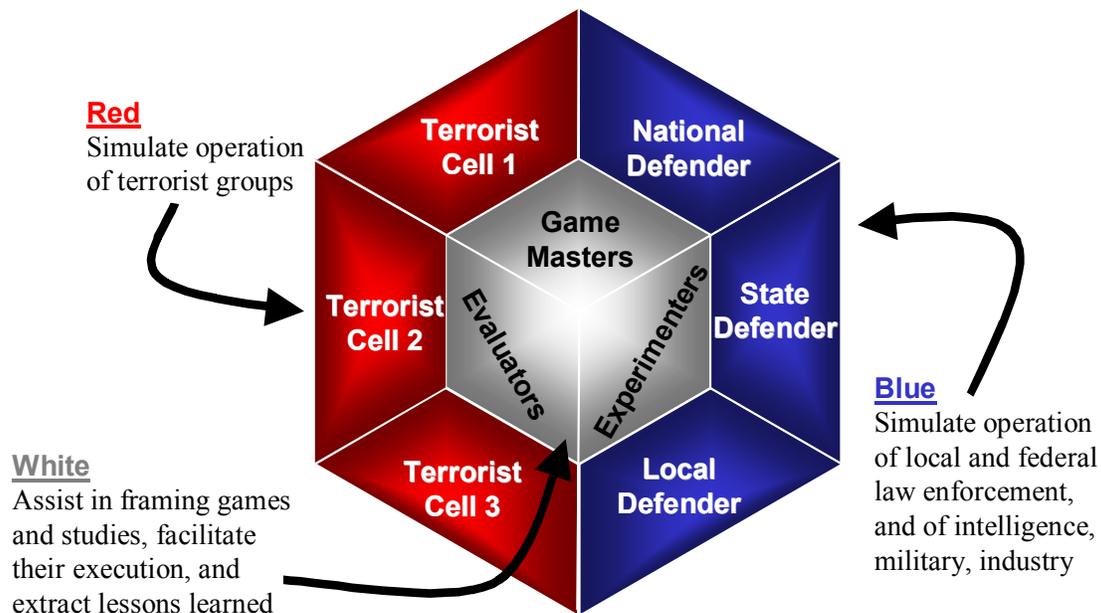

Red
Simulate operation of terrorist groups

White
Assist in framing games and studies, facilitate their execution, and extract lessons learned

Terrorist Cell 1
Terrorist Cell 2
Terrorist Cell 3

Game Masters
Evaluators
Experimenters

National Defender
State Defender
Local Defender

Blue
Simulate operation of local and federal law enforcement, and of intelligence, military, industry

Figure 2. **Terror Room Concept**

Although the organization may play the blue team role all by itself in these games, expert blue team members can also be brought to the table to play alongside the organization's staff, advising them with regard to potential response options as the game unfolds. As with the red team, the blue team can also be used to independently evaluate the organization's self-assessment and defense and response plans and to supplement or improve these plans as needed.

Developing Scenarios

In thinking through the intelligence community's challenges, it began to appear that a concept the Dotology team called "scenario driven data analysis and mining" (SDDAM) might be of use. Specifically, when individuals try to make sense of what they are observing in their world, they draw on conceptual frameworks that they have developed over years of experience and ask, "Does what I am seeing look like anything I have seen before?" Given this, it seemed that there would be value in creating computer-based systems in which "paranoid agents"—software entities that understand the particulars of given attack scenarios—constantly monitor the data being collected by intelligence looking for evidence that their own scenarios are being played out in the real world and for evidence that would refute this. Running constantly in the background, usually out of sight of the intelligence analysts who do the day-to-day sifting and interpretation of data flowing into the intelligence system, these agents would occasionally announce themselves to the analysts when they believed that they had gathered enough evidence to validate their "paranoia." The analysts would then be able to follow both the positive and negative evidence chains developed by the agents.

Assuming that this is possible, one of the key questions is how the scenarios are

developed to begin with. The use of standing red teams is one reasonable solution. A team would be given the task of thinking through how to accomplish a given objective (e.g., "wreak havoc at Disney World") and would then begin to establish specific goals within this context ("kill thousands of people" or "gut the facility's economic viability") and strategies for accomplishing these goals ("Implement a coordinated attack during one of their peak events with chemical canisters hidden in baby strollers"). Next, plans would be developed for implementing each strategy. The specific steps of each plan and the ways in which these steps could be executed would constitute a "signature" that could be codified using computer-based tools and used to drive a given paranoid agent. In all of this, steps would need to be taken to ensure that the attack scenarios developed in this way faithfully represent the approaches that would be used by groups that might launch the attacks.

Evaluating Concepts

In a very real sense, the war on terrorism is new territory for the United States. While there have been certain specialized organizations that have considered how to deal with this threat in certain narrow settings, the events of 9/11 elevated the problem to a new level and expanded the scope of things that we need to consider. Currently, we have many more questions regarding how we should prepare and respond than we have answers. Given this, providing policy makers and other leaders in various branches of government with tools that help them grapple with the issues in their own areas of responsibility would be tremendously valuable. To this end, war gaming in which red teams realistically play the role of terrorist organizations would allow policy makers to consider "what-if" with various policy options.

Augmenting Staff

As an incident is unfolding, the leaders managing the incident face a number of critical questions. While they cannot help address all of these questions, standing red team members will have expertise in critical areas that exceeds anything that local responders are likely to be able to bring to the table. Given this, there would be real benefit in putting in place an infrastructure that would allow red team members to serve as expert advisers attached to state and local emergency operations and to national response teams whenever a real attack is launched. In this capacity they could help assess what has happened, postulate what might happen next, and help in planning a response strategy.

Enabling Understanding

It is one thing for a red team to develop an understanding of a terrorist group and to help others view their own world in light of this understanding, but it is another thing altogether to help this people understand the terrorist as well as the red team does. Even so, there are people, such as intelligence analysts, who could benefit from this level of understanding. For this reason, another function of a red team would be to codify its knowledge in a set of tools that make this knowledge accessible to certain specialized communities where insight of this sort is both essential and able to be protected.

Making the Red Team a Reality

In setting up a national red team capability, there are a number of questions to be addressed:

- How should the group be staffed and how would it be organized?
- How would it be tasked and how would it operate?
- With what other organizations would it need to interact and what would be the nature of those interactions?

- What resources would be required to support this activity and how would it be funded?
- Where would it reside organizationally and physically?

Staffing and Organization

As currently envisioned, the red teaming organization would be structured as follows:

- **Office of the Director** – This group is responsible for negotiating tasks with external customers, managing budget and facilities, establishing organizational operating procedures, and for developing and selling overall red team program. It consists of the Director and as many staff as required to manage these functions.
- **Administration Department** – This group handles the details required to keep the organization functioning on a day-to-day basis. Its responsibilities include accounting, procurement, facilities maintenance, security, and technical support and system administration for the organization's computers and networks.
- **Training Department** – This group is responsible for development of curricula and training materials used in educating customers served by the red team and for running training sessions whenever they are held. In time, it will eventually have primary responsibility for any publishing (e.g., journals, reports) done by the red team organization. Staff in this group includes people with a background in education, people with a background in the disciplines used in the *War Game Department*, and people with a background in writing.
- **Terror Science Department** – This department consists of two groups responsible for supporting the department's two functions. The first,

the *Terrorism Research Group,* is responsible for doing background research on different terrorist organizations and for the development of catalogs of attack objectives, strategies, tactics, and techniques. This group is home to the organization's red teams as well as a number of intelligence analyst-quality researchers who serve the needs of their own department as well as those of the *Training Department* and the *Tools Department*. The second, the *War Games Group*, is home to the organization's white teams and blue teams. This group manages the planning, implementation, and analysis of war games held for the red team organization's customer set and engages its sister group's red team staff as required to support these missions.

- **Tools Department** – This group is responsible for providing the tool suite used by the red team organization and its customers. This suite will include both commercial-off-the-shelf and government-off-the-shelf products as well as custom tools developed in-house by this department or developed under contract by external organizations under the supervision of the *Tools Department*. Its staff is composed largely of individuals with expertise in software development, networking, and technologies for human-to-human communication.

While the red team organization may be instantiated as a traditional entity with all staff collocated in one facility, it might also come into a being as a "virtual organization" with those functions that do not require continuous interactions with other functions being moved off to other locations. In this latter model, contract staff may provide specific functions. In the start-up phase of the organization, this virtual approach may be favorable inasmuch as certain services can be contracted with organizations already having the expertise and infrastructure needed to support the contracted functions.

Once the red team organization starts to find its feet, it will begin to seek and accept interns both from the organizations that it serves and from those organizations with which it collaborates. This internship process will help the red team organization disseminate to appropriate groups much of what it has learned and will keep the organization vital through the infusion of new experiences and new points of view. Ideally, once the red team organization has reached full flower, the interns may make up a sizeable portion of the organization's staff, with each "class" being drawn from a diverse set of external organizations and backgrounds.

Tasking and Operation

While interrelated, the red team functions described above target different customer sets. Given this, the organization is likely to negotiate services with a range of organizations rather than simply serving the needs of a single organization. It is expected that in the earliest stages, the organization will focus on developing its expertise with respect to the nature of specific terrorist organizations (this is the work of the *Terrorism Research Group*) and on exercising its red teams in war games. Initially, these red teams may cut their teeth in games run by other organizations; however, the long-term plan must be to grow the organization to the point that it can plan, run, and analyze its own games. Early games hosted by the organization will problem focus on the needs of a single type of customer (e.g., games oriented toward national leadership and exploration of

alternative approaches to policy). As the organization gains competence and reputation, this can be expanded to include other customer sets.

Alternatively, if the organization finds a home in an organization with an expansive charter, such as the Homeland Security Department, and adequate resources, the *War Games Group* might launch parallel pilot efforts focused on each of the kinds games that the organization wants to be able to run.

As the *Terrorism Research Group* is in the process of getting to know its initial set of terrorist groups, the *Tools Department* will begin work on compiling tool suites for the red, white, and blue teams, as well as for the *Training Group*. The first activities of this group will consist of working with the other groups to create documents that describe the kinds of tool suites to be produced, surveying the commercial-off-the-shelf and government-off-the-shelf worlds to see what is already available and what must be custom-built, and acquiring and evaluating those tools that are readily available.

Once the *Terror Science Department* begins to mature, the *Training Department* will be created to develop educational materials that formalize and help make transferable, as appropriate, those things that need to be imparted to the red team organization's customer base, both in the form of self-study materials and courses. It will also begin to create classes that will be used in the context of other red team organization events.

Over time, each of the departments will grow their capabilities and capacity to the point where they can fulfill the reason for which the red team organization was originally chartered. The *Terrorism Research Group* will have fully

characterized all known terrorist organizations and constantly be researching and characterizing new ones as they emerge. The *War Games Group* will be able to rapidly formulate, implement, and analyze games for any customer of the type that they have targeted. The *Training Department* will have created all of the materials required for formalization of the red team organization's knowledge base and processes. The *Tools Department* will have created all of the infrastructure and tool suites needed to support the activities of the red, white, and blue teams.

The expectation is that, at this point, the organization will also establish itself with a broad set of client organizations and will be in the process of actively collaborating with funding organizations and those organizations requiring the red team organization's services.

Just as the red team organization will grow over time, the need for the organization's services will eventually also begin to wane. It is very likely that there will be a heyday for this organization in which it is actively meeting needs; however, there may very likely come a point at which value of the things left to be done will be perceived to be low compared to the cost of doing these things. Given this, a reasonable plan is to establish a governing board for the red team organization and to build a "sunset clause" into the red team organization's charter. Annually, the board would assemble to review the organization's work and to assess what remains to be done before the organization moves toward terminating itself. Having said this, it is important to note that, even though the cost of maintaining the staffing levels associated with the group's "golden years" will not be justifiable in the final phase of the organization's lifecycle, the need for the

functions provided by the red team organization will never completely disappear. Given this, an end game built on completely codifying the organization's knowledge base and on making this knowledge base and the organization's capabilities accessible to external organizations is key. The *Training Department* and *Tool Department* may play the central role in making this happen. Once the organization begins to sunset, a skeleton staff needed to support on-going work will be moved to some existing organization (very likely one of the ones with which it partnered).

Partnerships and Interactions

Because of the nature of its mission, the *Terrorism Research Group* will have strong ties to the intelligence community, most likely being closely aligned with whatever inter-agency working groups on terrorism may exist. The group may also be affiliated with related research activities at the various war colleges and other organizations in academia, government, and the private sector possessing special expertise in the area of particular terrorist groups. This group will also support its sister, the *War Games Group*, during the planning and execution of specific war games and will interact with them in the course of red-on-white games run for red team training and for experimenting with certain aspects of red team operation.

The *War Games Group* will maintain relationships with other organizations specializing in war gaming, such as the war colleges, and especially with those with any background in terrorism-oriented games. It will also be the primary interface between the red team organization and the customers that it serves.

Like the *Terror Sciences Department*, the *Training Department* will very likely maintain liaison with counterparts in the war college community. As the organization's publishers, they are also very likely to maintain contact with other organizations writing in this subject area. For the purposes of course and materials development, this department will interact frequently with both the *Terror Sciences* and *Tools Departments*.

The *Tools Department* will relate to its internal peers as described above and to external suppliers of tools and development services. Depending on how things progress, the department may also interact with development organizations in other agencies with the goal of integrating the red team organization's tool suites into the automation environments of these other agencies.

Resources and Funding

To run the organization, the minimum requirements will include a place to live, access to whatever infrastructure (e.g., secure networks) is required to link the organization to its partners and its clients, furnishings and equipment, and funding.

Given where the organization will head in terms of the functions that it will provide and how it will provide them (as described earlier and in more detail below in section on red team tools), there is something to be said for creating an organization that is somewhat distributed from its inception. Locating the various staff elements, especially those in the *Training* and *Terror Sciences Departments*, in a way that forces them to become comfortable with remote collaboration will be a good thing. This does not necessarily mean putting different groups in different cities but may mean separating them enough within a single building or on a single campus that

interacting electronically is less trouble than walking to wherever the other groups may be located.

Much of the data with which the red team organization deals is likely to be extremely sensitive (SCI or SAP); therefore, there is an advantage in setting up shop in a place in which the facilities needed to protect this kind of data are not a rarity. At the same time, it is likely that a large number of the organizations and individuals with which the red team organization interacts will not have access to the kinds of clearances needed for access to this kind of data if they have any clearances at all. For the purposes of training and war gaming conducted at the red team organization's facility, the educational and game spaces need to be able to accommodate the needs of events run at everything from unclassified to SAP. In practice, this may require separate facilities for different kinds of sensitivities.

Because of the necessary relationship to the intelligence community, the organization's infrastructure must support secure data and voice communications to outside organizations. Likewise, the internal network must support classified computing at whatever level is required by the organization's work. At the same time, the ability for red team organization's staff to access the Internet, to send and receive unclassified mail, and to hold unclassified discussions over public phone systems is paramount. Finally, when the organization exercises with external organizations that hold no clearances, there will still be a need to set up secure communications between these organizations and whatever elements of the red team organization are operating at a distance. Since these organizations are unlikely to possess such capabilities, the red team organization needs to be ready to deploy this infrastructure at the

organizations' locations whenever the need arises.

As with communications, the equipment used by red team organizational units must be easily transported to and set up at remote customer sites. Again, the question of classification must be addressed here. This requirement applies equally to the hardware that the units carry to the field and to the tool suites that this hardware hosts. It will very likely be necessary to maintain different configurations for different uses (e.g., a tool might use a sanitized red team knowledge base when taken to uncleared sites and a SAP knowledge base when operated in the most secure settings), possibly implemented through the use of different hard drives that are easily removed from the computing platforms.

Finally, in the earliest stages of this organization's lifecycle, it is likely that no reimbursable work will be done; therefore, a guaranteed funding source will be required until the organization is able to reach critical mass. From that point on, the organization will market its services and will exist on a mix of dedicated funding and fees collected for service. In the case of the first, the funding is likely to be associated with specific programs developed by the red team organization and its partner organizations (e.g., DoD, HHS, FEMA, HSD). In the final stages of its lifecycle, the funding stream will once again consist exclusively of dedicated funds, most likely associated with programs aimed at moving the red team organization's capabilities into whatever organization is tapped to be the custodian to its final capabilities.

Ownership and Location

There are several potential candidates for initial ownership of this organization. Inasmuch as the goal of this effort is to stand

up a technical capability unlike any that currently exists and given that this organization's capabilities would have direct relevance to the DoD, DARPA is one option, possibly in the context of the existing mission of its IAO organization and its TIA program or as sister to this program. A second possibility is to engage FEMA, NIST, HSS, or any of the other agencies involved in addressing issues related to emergency response. A third possibility, one—or a federation of—federal research labs would offer the technical wherewithal to deliver the tools needed by the organization.

The most promising option may be to find a home for this effort in the Homeland Security Department but to also establish a board representing the organization's intended constituency and to allow this board to exercise oversight authority, approving or disapproving in periodic meetings the priorities and plans set by the red team organization. A home in HSD will guarantee the organization access to the kinds of resources needed to make the work and to the kinds of private and governmental customer sets that it is designed to serve.

In weighing all of the factors that affect where such an organization might be sited, a strong case can be made for collocating with an organization already experienced in war gaming, such as the Naval War College. The fact that the war gaming experts will already have the facilities and processes in place means that the red team organization can begin to become productive much more quickly and less expensively than if it first had to create its own infrastructure.

One possible exception to this would be the *Terror Science Group*. Because of this group's necessarily intimate ties with the intelligence community, housing this

organization in Washington, DC, where it has ready face-to-face access with this community, might make the most sense. In addition, establishing this satellite office would provide the red team organization with ready access to many of the group's other potential partners in the federal government.

The Team's Facilities and Tools

The facilities and tools used by the red team will include, among other things:

- The physical rooms that support the team's functions
- The technological infrastructure that exists in these rooms
- The tools suites that are used by each of the team's within the organization

War Gaming Rooms

A centerpiece in the war-gaming mission is the *terror room*, a sophisticated war-gaming environment used both for training and for experimentation (*Figure 3*). As currently envisioned, the *terror room* will be used in several ways. First, traditional war games will be run with human players for the purposes of equipping these players for real-world operations. Since different kinds of blue players have different real-world responsibilities (e.g., the functions of a local emergency operations management team differ from those of a national intelligence organization), different types of games can be developed and played out again and again with various blue teams in order to benefit the organizations and locations that these players serve.

A second use for the *terror room* is as a laboratory for perfecting red team theory. While potentially quite sensitive, there is much to be gained in thinking through the question of what terrorists might do to improve their operations. Given this, the *terror room* could be used to allow the red

and white teams to play through a scenario with a view to allowing red to learn from white what can be observed and why. In response, red would rethink the kinds of strategies and tactics that it can employ to achieve a given objective and replay the scenario to determine whether or not the innovations have helped. Findings from this process are used to drive blue team missions ("How would you defend against X if they were doing Y?") and to drive requirements for new capabilities.

The t*error room* will also be used to evaluate new defensive concepts. These can include new ways of employing existing capabilities in order to address specific concerns and ideas for use of capabilities that are yet to be developed. Lessons learned from these blue-on-white games are used to build catalogs of defensives strategies and tactics. They also contribute to the development of doctrine and help in evaluating the potential value of hypothetical defensive capabilities.

Finally, the *terror room* will provide an environment for understanding the details of how a given terrorist group might carry out

an operation against a particular target. Given a specific objective, a red team will develop detailed plans for how to implement the objective. Both the plans and the thought processes leading to the plans are recorded in detail with a view to deriving the principles employed by the red team in its operations. In turn, these principles are codified in software agents (as discussed next) that can be used in support of various red team organization activities.

The notional organization of the war-gaming facilities is depicted in *Figure 3*. The lion's share of the facility is dedicated to the **main war rooms**, physical spaces used for the central aspects of any game. **Auxiliary war rooms** allow for teams playing different roles within the red or blue organizations to be physically separated from one another. **Observation rooms** allow white team evaluators to monitor the conversations, actions, and decision-making processes of red and blue players. The **control room** is manned by the game masters who manage the flow of interactions, dictating what can and what does occur as red and blue play out their respective roles.
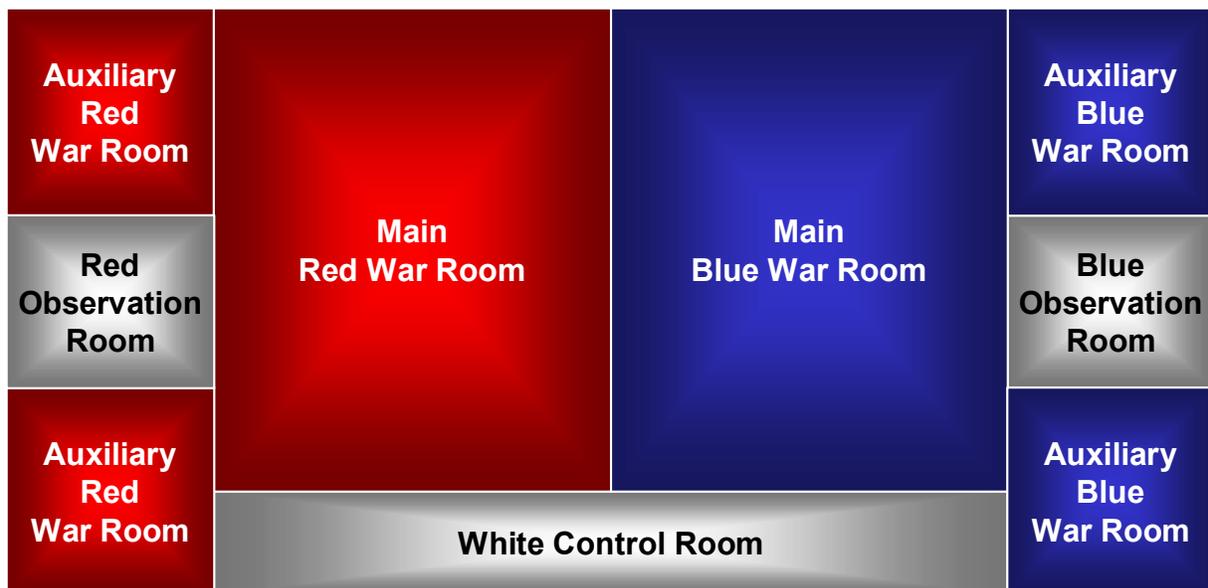

Figure 3. **Terror Room Facility Elements**

Technological Infrastructure

In the early days of the t*error room*, while the red team organization is in the process of perfecting its craft, the t*error room* may be little more than physical spaces; however, the long term goal for the room is to create a highly automated facility capable of supporting complex, distributed war games through the use of computing and communication technologies. When this evolution is complete, the central functions of the white team will be embodied in software, allowing red-on-white, blue-on-white, and red-on-blue games to be rapidly framed, implemented, and analyzed. Likewise, agent-based blue and red software

components will allow the organization to host games in which some or all of the "players" on either the red team or the blue team or both are simulated. Inasmuch as the exclusive focus on this red team organization is terrorism, a key goal in creating the red "sims" is that they faithfully replicate the ways in which specific terrorist groups would behave. To this end, one of the chief goals of the research conducted by the *Terror Science Department* will be to codify in this way all that it learns about each terrorist group studied and one of the chief goals of the *Tools Department* will be to make this codification easy.
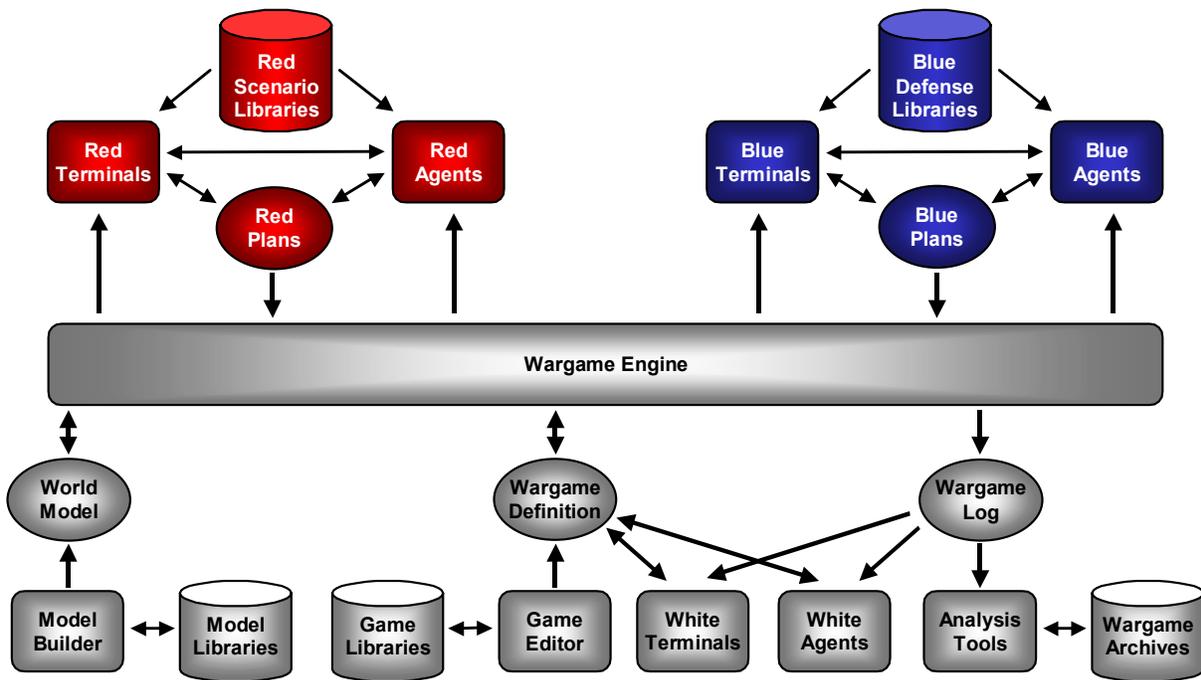

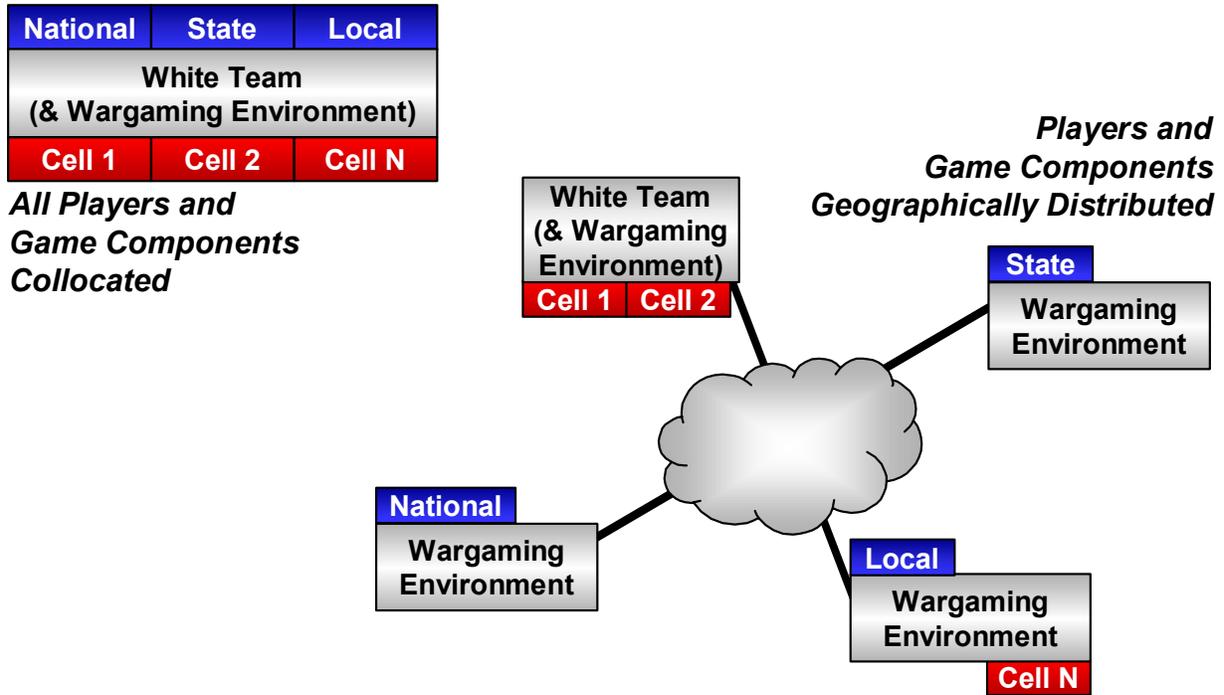*Figure 4.* **Terror Room Infrastructure and Tools**

Figure 5. Centralized And Distributed Games

Figure 4 depicts a notional view of the *terror room* infrastructure. The centerpiece of the infrastructure is the war game engine, a suite of software components that execute the simulation that supports each game and that monitor and moderate all interactions (including conversations between players located in different rooms). The bottom of the figure shows the kinds of tools that the white team will use in creating and executing a game. The model builder allows the white team to describe the locations in which the games are set, the kinds of people (including the terrorists) that populate these places, etc. The game editor allows the white team to frame the nature of the game to be played—what questions are to be explored, what assumptions are being made (i.e., what bounds are placed on the game), what aspects of the game are to be monitored for later analysis. The analysis tools are used to digest, both in real-time and after the fact, the data that is collected

during the course of the war game. The red team tools include libraries of "moves" that can be used by the red team during play. Likewise, the blue team's libraries catalog defensive strategies and tactics for addressing specific situations. Specific actions taken by either team are expressed as "plans" that are to be implemented during the next step of the game. The red, white and blue terminals represent the means by which human players interact with the system in various roles defined by the game. Red, white, and blue agents represent the simulated players (or, in the case of white, certain automated functions that would otherwise be performed by humans) that have been assigned specific roles in the game.

Given this infrastructure, nothing constrains a game to be played in a single facility. The same infrastructure elements that allow teams in different rooms within a given

14

facility to interact will allow remotely located groups to play together in a common simulation environment (*Figure 5*). Pursuing this capability provides the red team organization with a number of advantages. Early on, as the organization relies on existing war gaming expertise such as that found at the war colleges, this capability to distribute the game will make it possible to host games in the red team organization's own facilities even though the bulk of the work is being supported by experts at other locations (note that the implication of this statement is that the earliest distributed infrastructure may focus largely on human-to-human communication and on extending white team capabilities of the expert organization to the red team organization's facilities. In its heyday, this infrastructure will make it easy for the organization to bring its capabilities to its customers rather than the other way around. In the end, the proper design of this infrastructure will ease the process of transitioning the organization's capabilities into whatever organizations are tapped to be the on-going custodians of these capabilities.

White Team Tools

The full tool suite to be used by the white team once all automation is in place is likely to consist of tools to assist in defining and planning a game, tools that enable the implementation of a game, and tools that assist in the observation and analysis of a game. While not a complete list, some of the tools in the white team suite may include:

- **Game characterization tool** – This tool allows "experimenters" to define the nature of the game to be played, including a statement of what is to be learned/explored, the timeline and pace of the game, the nature of the world in which this game will be played, the nature of the players in this world (their capabilities, motivations,

resources, etc.), and any objectives/constraints that must be met (e.g., what facilities to use or clearance levels to exclude).

- **Model libraries and editors** – These libraries contain drop-in components (the "bricks" used to build this "house") that are used to create a game description along with model fragments (pre-fabricated "brick walls") that collect these components into collections that have meaning in the larger context. These components and model fragments consist of both descriptions that are used by the game characterization tool and functional elements that are used by the game builder to compile the overall game model. Editors allow new "bricks" and "walls" to be defined or existing ones modified to meet the needs of specific games.

- **Game builder** – This tool compiles the profile created by the game characterization tool into the world models and simulated player models needed to execute the game.

- **Observers tool** – This tool allows observers and experimenters to define, before the game begins, which specific conditions the war gaming engine needs to monitor (e.g., interactions between a human playing a given role and that role's tools, interactions between specific simulated entities in the game, or the state of one of these entities). It also allows these people to define how these phenomena are to be monitored (i.e., stored in an archive, displayed on a specific screen in "raw" format, or sent to a preprocessor before being routed to one of these destinations). The tool is also used in real-time by observers during game play to capture and display specific items of interest.

- **Resource planning tool** – This tool uses a game profile generated by the game builder tool in order to estimate the kinds and amount of resources needed during each phase of the game. Among other things, these resources can include required computing resources, voice and data communications, people, and facilities. Once estimated, the tool helps the game developers identify and "reserve" specific resources, decide on how specific functions and roles in the game will be allocated to these resources and estimate how much these resources will cost. In turn, this information can be used to refine original game specifications in the event that resource requirements exceed expectations.

- **After-action reporting tool** – This tool guides players and observers through the process of reviewing and analyzing game play from their own perspectives. Its goal is to capture some of the perception and decision-making issues that are not amenable to automated capture during the game.

- **Data analysis tools** – This collection of tools allows data collected during the game to be dissected and interpreted both after the fact and in real-time.

- **Presentation tool** – This tool allows observations/lessons learned from a game to be codified so results are readily briefed to players and others.

- **Permutation engine** – This tool enables experimenters and evaluators to "what if" a game that has already been played by altering key elements of a game's threads of execution and using agents to play out the N different ways that the game might have evolved differently from the point of change.

- **Research issues log** – In the course of planning, implementing, and analyzing a game, the participants will identify other issues that are candidates for further research. This tool allows these issues to be characterized according to some uniform scheme and logged into a common repository.

Red Team Tools

One of the central weaknesses of traditional red teams is a lack of rigor in thinking through how to achieve a given objective. Consequently, team members can fall into the trap of using the same techniques over and over again, even when the details of the objectives to be achieved are changing. One way of addressing this is through the use of model-based assessment. In this approach, red team members model the target that is to be attacked, placing particular emphasis on how things in the world of the target relate to one another. This modeling is multi-dimensional, taking into account the target's physical structure, functions, environment, and behavior. The analysis of how to achieve the desired objective then proceeds by systematically examining how interdependencies in the world can be traced from the desired outcome back to actions that terrorists would be able to execute. If done correctly, this sort of analysis will produce a number of attack options. The red team can then weigh the relative difficulty, cost, risk, and "rewards" of each such attack.

Given this, the red team tool suite will contain, among other things:

- **Target modeling tools** – This family of tools allows the many aspects of a given target to be described in computer- and human-understandable formats using a suite of interrelated "views." Depending on the task at hand, this tool will be used in either of two ways. When the red team is

16

working on the assessment of a specific target, it will have access to a rich suite of data about the target and will use this tool to codify everything that it learns about the target. In the context of war gaming, the terrorist group that the red team is portraying may have very fragmented knowledge of a given target and have to work at gaining insight into the details of the target's structure, function, etc. In this case, this tool serves as a notebook for what is learned in the course of the game and, at successive phases, may be automatically populated by the game engine.

- **Attack objectives analysis tool** – How you pursue a given target or how you even select a target to pursue depends on what you want to accomplish. This tool enables a red team to think through its overarching attack objectives for a mission, the hierarchy of subordinate goals that must be met in order to achieve each objective, and the relative importance of each objective to the overall mission.

- **Target analysis tools** – This suite of tools enables analysis of potential targets at several levels of detail. At the coarsest level, a red team can use a tool that allows a broad-brush assessment of a system with a view to gaining a high-level understanding of a target's context, function, structure, and behavior and to identifying portions of the system that look like potential avenues of attack and that deserve more in-depth study. At finer levels of detail, the tools enable red team members to determine specific ways a given target could be attacked and to identify the resources needed to carry out each such attack.

- **Consequence and cost analysis tool** – In deciding what targets to pursue or how "good" any given attack plan is relative to others, a means of assessing the real impact of an attack and the "costs" incurred in implementing the attack is required. This tool provides red teams with this capability, taking into account the nature of the target itself along with the target's relationship to its context.

- **Offensive operation planning tool** – This tool enables a red team to plan all of the details surrounding a given attack that it hopes to implement (e.g., secure financing, deploy foot soldiers in advance of the attack, secure needed tools). The output of this tool is one "scenario" that illustrates how this operation would be carried out.

- **Scenario elaboration tool** – The job of this tool is to convert a scenario generated using the operation planning tool into a whole family of variations on this theme that could be used to implement the same "seed" plan. This family of scenarios would then become "signatures" that could be used by the intelligence community in support of a scenario-driven approach to mining intelligence data.

- **Scenario evaluation tool** – While any number of ways might be dreamed up to achieve a particular target objective, any given terrorist organization, with its culture and resources, is likely to use only a subset of the entire space of approaches. Given this, this tool vets the plans and scenarios generated by the operation planning and scenario elaboration tools to identify which approaches are consistent with a given terrorist organization's mode of operation. In human-based game play, this tool allows plans developed by the red team to be analyzed before

implementation to ensure that the red team players are not simply "mirroring" U.S. attack approaches.

- **Red team knowledge base** – This tool catalogs the full repertoire of "moves" that a given terrorist group might employ in carrying out an attack. This knowledge base is used by the scenario evaluation tool and by human red team players trying to figure out what to do next in a war game.

- **Red team groupware** – As noted earlier in the document, red teams are typically composed of many players. While work is divided up among players, typically along specialty lines, this division can sometimes hamper efforts to assess a given target as a "system", with interdependencies between different areas of responsibility often being overlooked. This tool addresses this problem by enabling team members to task one another in a way that ensures complete and adequate coverage of a given target and by ensuring that the team understands the system and not just constituent components.

Blue Team Tools

As a starting point, it is assumed that blue team members have access to the same *kinds* of target analysis and attack planning tools as the red team but the not same knowledge base. These tools provide the blue team with its baseline assessment of those things against which it needs to be able to defend. In addition to these red team tools, blue's suites could include:

- **Target modeling tools** – Used in the course of game play, this tool serves as a notebook for storing what the blue team knows about its world. As with the red team's tool, the contents of this notebook may be automatically updated in the course of a game to

simulate discovery of information over time.

- **Defense/response planning tool** – Given the list of viable attacks produced by the red team tools, this tool allows the blue team to explore defensive strategies for each such attack.

- **Blue team knowledge base** – This tool catalogs the full repertoire of safeguards and "moves" that defenders might employ in watching for and defending against various kinds of attacks.

War Rooms for States and Cities

As noted earlier, one mission of the red team organization is to help private and public state and local entities prepare for the possibility of attack. *Figure 6* illustrates current thinking about how this would be done. Using tools created for the red team organization, an organization (in this case, a city) would model their environment and then use the red team assessment tools to identify how they might be attacked. For each scenario developed in this way the organization uses the response planning tools to postulate and evaluate alternate defense and response approaches. The combined set of approaches selected in this way becomes the organization's response plan.

In the second phase of this process, the model of the target environment developed by the organization becomes the context for a wargame played against one of the red teams by the organization's defense force, which is aided by a professional blue team. Starting with the catalog of potential attacks developed by the organization, the red team plays through various scenarios, some of which may not have been identified at all by the organization. Under the advice of
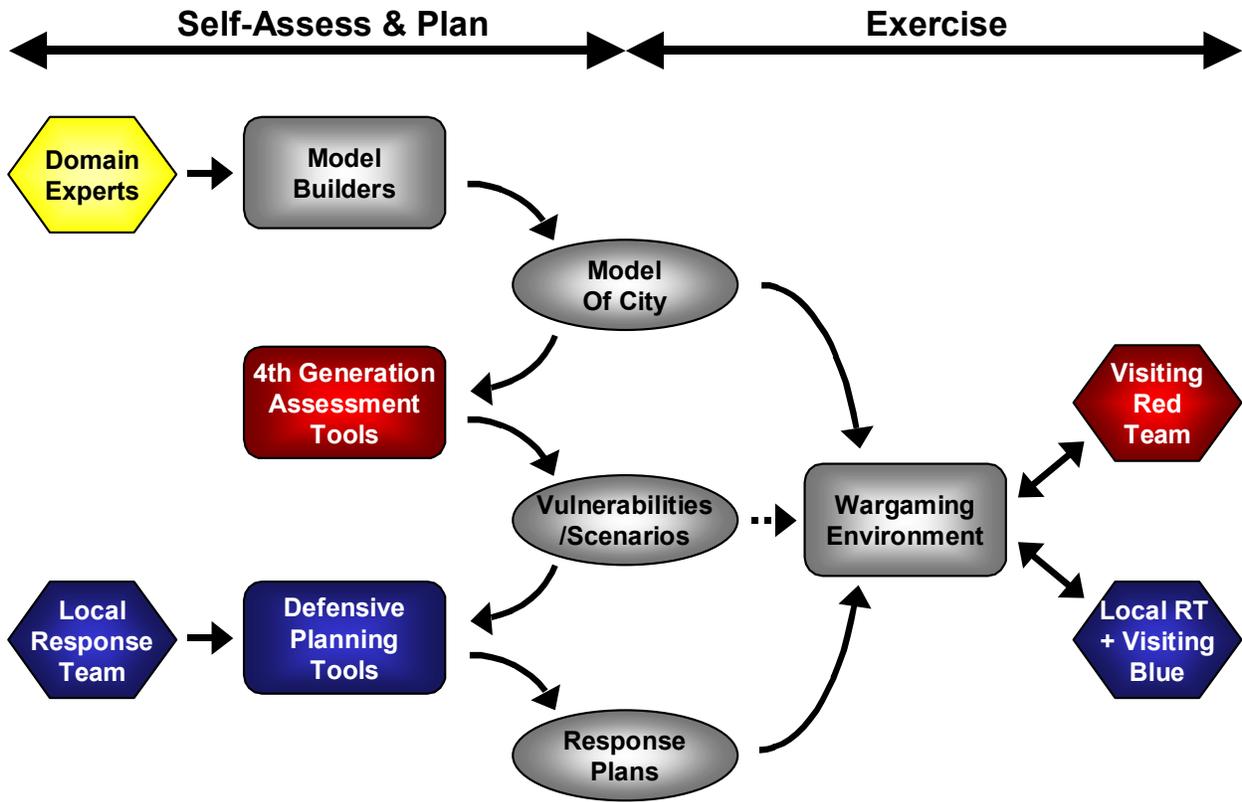
Self-Assess & Plan   **Exercise**

***Figure 6.* Terror Room Infrastructure and Tools**

the blue team, the organization tests its plans to see how well they work against real attackers and where the organization needs new strategies or simply more practice.

It is interesting to note that the infrastructure used to support this distributed war gaming may be of use to the organization for more than just this gaming. In the FACETS efforts described at the start of this document, one of the findings was that a standard emergency operations infrastructure at the city, local, and county levels was entirely lacking. Today, every organization fielding such a capability assembles it themselves or has one custom built. As a consequence, the ability to rapidly grow an emergency operations capability that allows the management of large-scale operations (like the World Trade Center response) is

extremely limited. Since the infrastructure used to support organizational self-assessment and war gaming is designed for distributed operations, it might (with some forethought) also serve as a basis for creating standardization emergency operation center and incident command post architectures.

First Steps

Given all of these things, the final question to address is where to start. As noted at the start of this paper, this document is meant to be a starting point for debate within the community of organizations that will be required to see this sort of vision realized. At this earliest of stages, a number of key questions need to be discussed:

- Are these ideas reasonable?

- How much would this kind of effort cost?
- How quickly should/could each of the capabilities described be launched and which should be pursued first and which last?
- Which organizations should be engaged and for what purpose?

At this point in time, two parallel courses of action seem desirable. An effort focused on framing this program and on developing a constituency for these concepts should be a first priority. The products of this work would be a detailed joint proposal for this effort, a fully fleshed out plan for how the organization would be launched and then grown, and a plan for marketing this effort to potential customers. Following initial discussions over the phone and email, a workshop involving interested potential collaborators might be held as a means of working through the issues to be addressed in the desired work products. An initial proof-of-principle war game involving potential partners might also be held to explore and demonstrate red team organization concepts.

Next, work could be started that would examine the specifics of what would be required to create the kinds of tools described above. The products of this effort would be an overall architecture for the technical infrastructure and associated red, white, and blue team tools and work packages that could be parceled out to other organizations for implementation as funds became available.