SANDIA REPORT

SAND2004-0438
Unlimited Release
Printed February 2004

Red Gaming in Support of the War on Terrorism: Sandia Red Game Report

Summary of Red Game held July 22-24, 2003

Judy Moore, John Whitley and Rick Craft

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

Sandia is a multiprogram laboratory operated by Sandia Corporation,
a Lockheed Martin Company, for the United States Department of Energy's
National Nuclear Security Administration under Contract DE-AC04-94AL85000.

Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

Available to DOE and DOE contractors from

U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865)576-8401
Facsimile: (865)576-5728
E-Mail: reports@adonis.osti.gov
Online ordering: http://www.doe.gov/bridge

Available to the public from

U.S. Department of Commerce
National Technical Information Service
5285 Port Royal Rd
Springfield, VA 22161

Telephone: (800)553-6847
Facsimile: (703)605-6900
E-Mail: orders@ntis.fedworld.gov
Online order: http://www.ntis.gov/help/ordermethods.asp?loc=7-4-0#online

SAND2004-0438
Unlimited Release
Printed January 2004

Red Gaming in Support of the War on Terrorism:

Sandia Red Game Report

Summary of Red Game
Held July 22-24, 2003

Judy Moore, John Whitley, and Rick Craft
Advanced Concepts Group
Sandia National Laboratories
P. O. Box 5800
Albuquerque, NM 87185-0839

Abstract

The Advanced Concepts Group (ACG) at Sandia National Laboratories is exploring the use of Red Teaming to help intelligence analysts with two key processes: determining what a piece or pieces of information might imply and deciding what other pieces of information need to be found to support or refute hypotheses about what actions a suspected terrorist organization might be pursuing. In support of this effort, the ACG hosted a terrorism red gaming event in Albuquerque on July 22 –24, 2003. The game involved two "red teams" playing the roles of two terrorist cells – one focused on implementing an RDD attack on the DC subway system and one focused on a bio attack against the same target – and two "black teams" playing the role of the intelligence collection system and of intelligence analysts trying to decide what plans the red teams might be pursuing. This exercise successfully engaged human experts to seed a proposed compute engine with detailed operational plans for hypothetical terrorist scenarios.

This page intentionally left blank

Table of Contents

This page intentionally left blank

Executive Summary

In considering how to address the problem of "connecting the dots", Sandia National Laboratories' Advanced Concepts Group (ACG) has been exploring the use of Red Teaming to help analysts with two key processes: determining what a piece or pieces of information might imply and deciding what other pieces of information need to be found to support or refute hypotheses about what actions a suspected terrorist organization might be pursuing.

In support of this effort, the ACG hosted a KDD-funded terrorism red gaming event in Albuquerque on July 22 –24, 2003. The goals of this effort were to engage human experts to seed a prototype compute engine with detailed operational plans for hypothetical terrorist scenarios and to demonstrate the ability to:

- produce valid scenarios consisting of detailed actions to complete a terrorist objective,
- identify multiple options to completing some aspects of the terrorist operational plans,
- associate intelligence indicators with these operational actions including meta-data consisting of rules, constraints, and self-scoring with each action,
- capture and translate this information into a computerized knowledge base for subsequent manipulation,
- evaluate the usefulness of a "gaming" environment for producing scenarios and fragments,
- test a few hypotheses about this environment, and
- allow tool developers to test their concepts for tools for red, white or black teams.

The game involved two "red teams" playing the roles of two terrorist cells – one focused on implementing an RDD attack on the DC subway system and one focused on a bio attack against the same target – and two "black teams" playing the role of the intelligence collection system and of intelligence analysts trying to decide what plans the red teams might be pursuing.

The exercise produced a number of results of value to the research in this domain. The event showed that gaming has some significant strengths relative to simple analytic exercises and is most likely a preferable approach to scenario development in certain settings. At the same time, the games seemed to point out the value of pure analysis in the fleshing out of the most detailed parts of operational plans. The event also highlighted the importance of an adequate infrastructure (especially those mechanisms focused on capture of plan elements generated by game participants) to this process. Difficulties encountered by the analysis-oriented black team also suggested that there may be value in exploring the development of tools aimed at automated hypothesis generation based on the operational information harvested from Red Gaming.

This page intentionally left blank

Introduction

As the nation struggled to understand why Al Qaeda's attacks on 9/11, were so successful, the question of the intelligence community's ability to "connect the dots" became a focal point of discussion. Early indications were that we had sufficient evidence in hand to have warranted deeper investigation into the activities of the individuals who eventually carried out the attacks, sufficient perhaps to have discovered and interdicted the plot.

So why didn't we? Subsequent detailed investigations into the situation revealed that while we did have key pieces of the puzzle, they were scattered across a wide range of locations and organizations such that no one group in the federal government had enough pieces to put together a reasonable picture. Even if they had, these investigations have made it exceedingly clear that the analysts who are charged with turning raw information into actionable intelligence are faced with another significant challenge – how to sift through huge volumes of "chaff" to find the few kernels of "wheat" that will make the difference in this war on terrorism.

In considering how to address this problem, Sandia National Labs Advanced Concepts Group (ACG) began to explore the use of Red Teaming to help analysts with two key processes: determining what a piece of information might imply and deciding what other pieces of information need to be found to support or refute hypotheses about what actions a suspected terrorist organization might be pursuing.

The Knowledge Discovery and Dissemination (KDD) Program of the Intelligence Technology Innovation Center (ITIC) – an intelligence community research and development activity – became interested in this line of thinking and underwrote a project to explore a specific aspect of this concept. As part of this project, a "Red Game" was staged in July of this year to explore the processes that red teams use in developing scenarios and to investigate the value of a gaming environment to these processes. This is a report on this game.

The Hypothesizer Concept

In many ways, the process of intelligence analysis is much like building a puzzle in which many of the pieces are missing and in which the pieces that *are* present are hidden amongst pieces to many other puzzles. The tasks then for the analyst are to first identify when a piece being inspected is significant, to then find other available pieces belonging to the same puzzle, to try to put these pieces into their proper place in the puzzle, and to then try to understand the full picture that the puzzle presents – either by hunting elsewhere for additional pieces or by imagining what the missing pieces might look like. To add this problem, intelligence analysis is almost always a time-sensitive activity. Not only must the puzzle be built, but this must be done quickly enough to allow an adequate response to whatever threat the puzzle indicates.

First, the process that allows a piece of the puzzle to be recognized as potentially significant depends on knowledge of the subject to which the piece of the puzzle relates. Figuring out how various pieces relate and what the missing pieces of the puzzle might

show is also knowledge-intensive. The number and kinds of ways that an analyst can imagine for accomplishing a given objective are limited by the analyst's experience base. In this area, even veteran analysts can stumble because no one can know all things.

Second, analysts that have worked a given area for extended periods run the danger of becoming blind to new things, thereby rejecting potential interpretations of the picture that could possibly emerge from the puzzle.

Finally, there is only so much information that an analyst can process in a given time frame, only so much information that they can absorb, only so many facts that they can track at one time in their heads. This fact can mean that some available puzzle pieces receive only cursory treatment, if they are studied at all; that not everything studied will be retained; and that not all of those things retained will be effectively correlated.

The use of automated tools or analytic processes to help address these problems is not a new idea; however, the question is how to do this. An idea being explored by Sandia's Advanced Concepts Group is the use of a "Hypothesizer" (Figure 1). Operating as an adjunct to existing mechanisms for browsing and searching intelligence databases, the Hypothesizer allows an analyst to explore the possible implications of one or more pieces of data (i.e., to hypothesize what kinds of operational scenarios the data might imply) and to then determine what other pieces of data might be found if these operational scenarios were being played out in specific settings by certain actors.

In order to support these activities, the Hypothesizer requires a knowledge base of operational methods that can be employed in various scenarios and a means of composing the methods into plans that satisfy analyst-specified criteria. A key question then is how to generate the information required for this knowledge base. The approach being explored by Sandia is the use of Red Teams to generate specific hypothetical scenarios that can then be distilled into their component parts to deliver the desired operational methods. These operational details would be stored in a data warehouse in a format that lends itself of computer manipulation.

Within the national security community, efforts to explore possible terrorist scenarios occur on a regular basis. The hypotheses developed in those events tend to be locally kept, thereby limiting their usefulness to intelligence analysis, and the focus is usually on identifying high level objectives, targets, and/or methods of terrorists and seldom on operational details required for interdiction. In contrast, this effort is exploring what would be required to create a national "red gaming" capability to engage a broad range of experts drawn from a diverse set of knowledge domains in the generation and collection

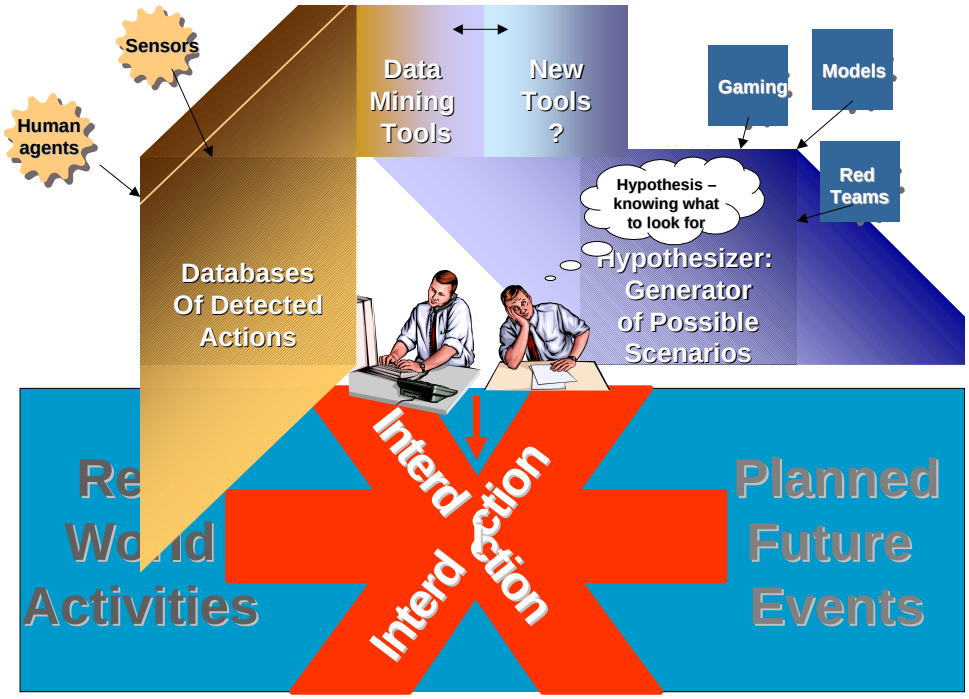


Figure 1. The intersection of analysis with real world data and the hypothetical world of the "hypothesizer" leading to successful interdiction.

of hypothetical scenarios and to make the knowledge aggregated from this process available to analysts throughout the intelligence community via the proposed Hypothesizer. This process would utilize existing work on red teaming and vulnerability studies, but would add one or more standing Red Team operations working in a gaming environment to develop potential terrorist scenarios. The Red Teaming process would consist of:

- drawing together appropriate red team members for the planned effort,
- using this team to generate the base ideas and operational plans,
- capturing and parameterizing this data,
- perturbing the data to generate still more scenarios, and filtering these by validating their plausibility.

Successfully representing an adversary requires not only that the team have a fundamental understanding of the adversary's operational methods, constraints, and basic motives but that they experience, as much as possible, the planning/operational environment. However, many of the operational methods that might be used to carry out a plot are "reusable": for example, there is a limited number of ways to enter the country or obtain funds that would be "reused" by any number of terrorist scenarios that require entry into the country. Therefore, we propose developing computerized tools that will free teams up to concentrate on the essential themes of the scenarios, with the repertoire of operational details automatically drawn upon as needed.

In addition to the Red Team, this process requires that the actions required by the scenario be translated into signatures such as data entries or intelligence reports that could be matched to data base entries. A Black team consisting of intelligence and signal processing experts would perform this translation process.

In addition to improving the analysts' toolset, the enhanced terrorist red cell capability and the generated data sets would be beneficial for terrorism war gaming. As such, it should become a pivotal element of a full time, on-going war-gaming effort to support the national strategies for the War on Terrorism and Homeland Security. These games would allow the exploration of improved policies, tools and strategies for interdicting terrorists, defending against potential attacks, and improving first responder capabilities.

The Plan for the Game

In support of this effort, the Advanced Concepts Group of Sandia National Laboratories hosted a terrorism red gaming event in Albuquerque on July 22 –24, 2003. The goals of this effort were to engage human experts to seed a prototype compute engine with detailed operational plans for hypothetical terrorist scenarios and to demonstrate the ability to:

- produce valid scenarios consisting of detailed actions to complete a terrorist objective,
- identify multiple options to completing some aspects of the terrorist operational plans,
- associate intelligence indicators with these operational actions associates meta-data consisting of rules, constraints, and self-scoring with each action,
- capture and translate this information into a computerized knowledge base for subsequent manipulation,
- evaluate the usefulness of a "gaming" environment for producing scenarios and fragments,
- test a few hypotheses about this environment, and
- allow tool developers to test their concepts for tools for red, white or black teams

The following sections describe structure and conduct of this game in more detail.

Overview

While run as a single event, the "game" actually consisted of three distinct, yet interrelated exercises (Figure 2). In the first, two red teams each played the role of a terrorist cell assigned the task of planning and executing an attack on the Washington, D.C., subway system ("the Metro"). Red Team 1 was directed to implement an attack using an RDD device while Red Team 2 was to use bio-agents.

This exercise was played in stages (Figure 3). During the "setup phase", the two red teams framed their problem. This included, among other things, establishing the identities of team members and setting ground rules for how the team would conduct itself in this exercise. The teams then developed skeleton plans that framed the overall strategies that they proposed to pursue. This was followed by detailed planning in which the red teams researched and selected specific options for realizing their strategies. These plans were to be detailed down to observable actions. Once detailed plans were laid, the red teams were presented with specific events meant to challenge these plans and were asked to identify how they would modify their plans, if required, to handle these perturbations.

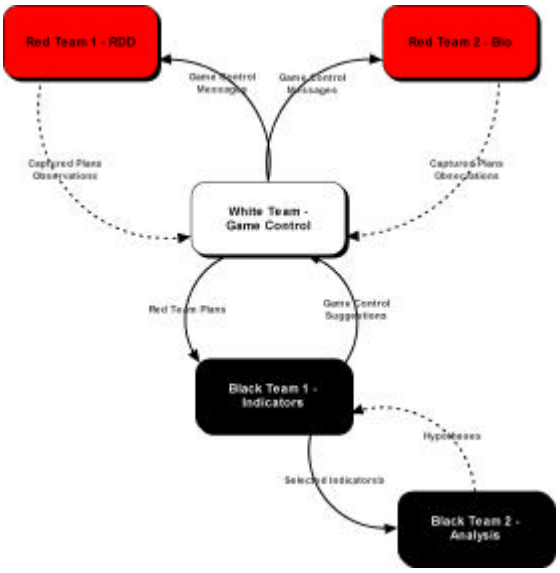


Figure 2. Overview of Team Interactions.

In the second of the three exercises, a Black Team 1 had a "god's eye" view of the red team planning sessions. They would receive the work of the red teams in near real time and have as their primary task the development of potential indicators and the relationships among such indicators. They

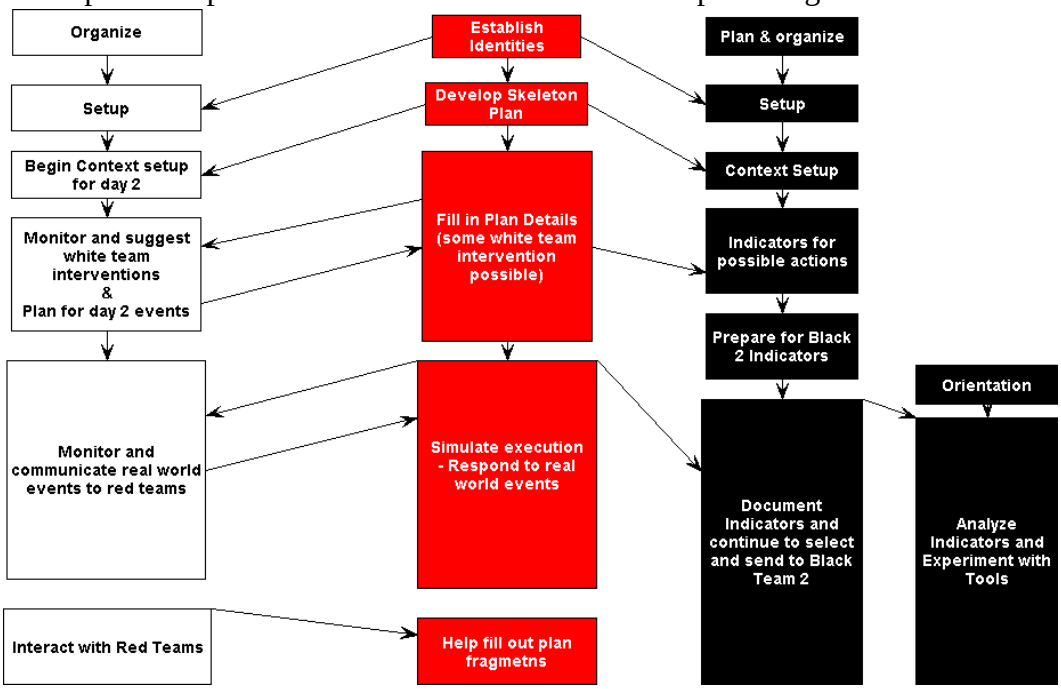


Figure 3. The Structure of the Game

could also influence the White Team which will be controlling the game to insert changes into the red team environments to force the exploration of operational alternatives and to force the level of detail generated to be appropriate for the testing of our concept.

In the final exercise, Black Team 1 transmitted to Black Team 2 messages meant to simulate some of the traffic that analysts might see during an on-going operation. Working in "blind mode" – receiving only those indicators selected by Black Team 1 and lacking any operational context – Black Team 2 used the evidence contained in these messages, and attempted to play the role of intelligence analysts and to decide exactly to what scenario the indicators might be pointing. In doing this, Black Team 2 was forced to use a small collection of "nonstandard" tools for their analysis of the unfolding plans. The chief goal in this exercise was not successfully divining the red teams' plans but exploring language and working style barriers. The findings of this work would help shape the development of future analyst tools, such as the Hypothesizer discussed above.

The Teams

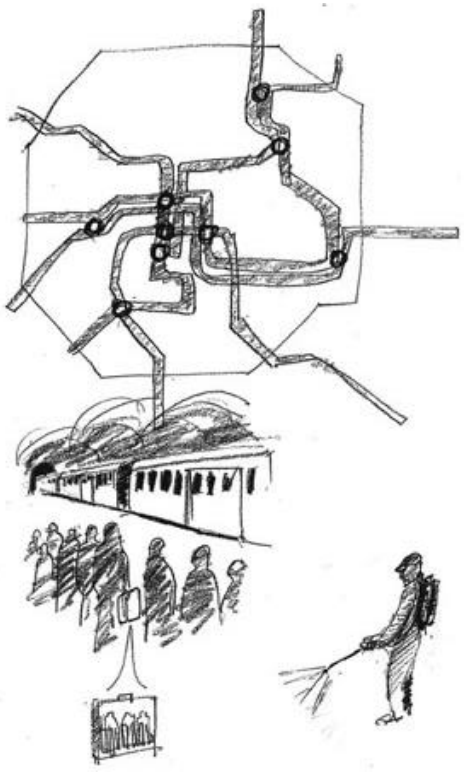
In all five teams were required to support the exercises – the two red teams, the two black teams, and a white team that served as game masters and observers. Each of these teams was composed with the goal of learning certain things about the process.

The two red teams each had a leader who was aware of what the game event was trying to accomplish and teams members who were chosen to provide certain skills of use to such a planning exercise. The assignments for the teams were alike in the following ways:

- Each team would represent a sleeper Al Qaeda cell in the US that had been tasked to pull off a major terrorist event in the DC subway in a two year time window. The initial constraints were:
  - ***People***: Teams were allowed to recruit others in country and out of country – but if they were going to assume the presence of resources from out of country, they would have to plan for getting them into the country.
  - ***Risk***: Their cell could be completely destroyed but leaving a trail to other Al Qaeda leaders was not acceptable. They would want to get credit for Al Qaeda for the event but they didn't want to be detected before completion.
  - ***Money***: $100,000 was available from overseas to support the cell's effort, but they would need to communicate to get it. Making money was allowed. Charitable fund raising was also allowed.
  - ***Communications***: open source information was assumed, no special means of communication was assumed.
  - ***Skills***: the team could assume that they had whatever knowledge or skills that the real players had. At the end of the game the Game Masters would query the teams about how any specialized knowledge could have been gained – in particular what actions would be required. There were some specialized skills in the each of the red teams which both teams can call upon.
  - ***Context for the Individuals***: The team would assume that most of them had only been here for a few years and had tried to maintain a low profile. They

were not citizens and were here on visas. All were extremely loyal and dedicated to the cause of Al Qaeda.

The differences in the two teams were:



- One team was hand picked by the leader and all members knew that leader very well. They were focused on an RDD event and had domain expertise on RDDs and money laundering. The objective for their terrorist attack was to cause enough damage that the news media will compare the effects with those of Chernobyl. Most members of this team came from a background of intelligence operations.

- The other team was picked for various expertise and they had not previously met. They were focused on a biological event and possessed domain expertise on bio threats and the DC subways. The objective for their terrorist attack was to cause the workforce in DC to be unable to or refuse to use the subway. Team members came from Sandia, Argonne, DHS, DIA, NSA, DTRA and retired military. While all of the team members were strangers to one another, both the team's leader and the team member who took on the role of his executive officer had extensive experience in military operations planning.

Black Team 1 (the indicators team) was formed largely by the KDD sponsors and consisted of analysts from CIA, NSA and CNO supplemented by Sandians who regularly support the intelligence community.

Black Team 2 (the analysis team) was also handpicked by the KDD sponsors. It was made up of two junior-level analysts from NSA and CIA plus a program manager from the KDD community.

The White Team consisted of the Sandia game designers, the KDD sponsor, and observers from Sandia and DTRA interested in the application of gaming to countering terrorism. Members of the White Team were assigned several roles. A single Game Master was assigned as the final decision maker and had responsibility for the overall conduct of the event. Two assistants to the Game Master served as points of contact for the two red teams and were meant to manage issues arising in each team as their games progressed.

All of the red and black teams were assigned a White Team member, called the Communicator, who handled all messaging back and forth between the appropriate teams. The Communicator also captured unstructured notes of the team activities. Both red teams and Black Team 1 were also assigned White Team members, called Notetakers, whose job it was to record the information being produced by each of these teams. The notes gathered by these individuals were meant to give the Game Masters and Black Team 1 a "god's eye view" of the progress being made by these teams. Black Team 2 had only a Communicator who monitored the flow of information with the Game Master and with Black Team 1 as well as helping the Black Team 2 with the possible use of pre-determined templates for analysis. Finally, there were also Observers who watched team behaviors to understand idea creation processes.

In preparation for the event, a complete collection of assignment descriptions and possible templates for capture of red team scenario fragments was generated. These are attached in the appendices of this report.

The Infrastructure

The game environment consisted of five separate spaces for the teams linked together by a classified computer support system. Four of these spaces were contiguous and were occupied by the red teams, Black Team 1, and the majority of the White Team members. The fifth space, occupied by Black Team 2 and its White Team Communicator, was located in a different building in Sandia's security compound, in part to keep the isolated analysts from being "contaminated" by direct contact with the rest of the game players.

The computer support system was made up of thin client computers connected via secure network to a classified server that was used for the common location of game files. Communications among the teams was facilitated through classified email and the notes of team activities were captured and stored on a classified file server.

The meeting was held at the Secret National Security Information level and the classified file server was capable of handling information at the level of Secret Restricted Data level. Since not all in the meeting were cleared for Restricted Data, any files printed for the teams from the file server were reviewed in real time for proper classification before distribution to the players.

The Schedule

The entire Red Game event took place over a period of four days. On the evening of the first day, attendees met for a dinner that gave the Sandia hosts a chance to prepare the players for what was to start the next day. As all members of a given team (excluding Black Team 2) were seated together at the same table, the event gave team members a chance to become acquainted. It was hoped that this would enable team members to more readily address the tasks at hand first thing the next day.

The plan for the morning of the second day was to allow the red teams to conduct their "setup" and strategic planning activities (Figure 3). During this time, Black Team 1

would be developing its strategy for developing indicators and would start framing specifics as soon as the results of the red teams' setup exercises were ready.

During the afternoon of the second day, the red teams would develop their detailed plans. At the same time, Black Team 1 would be analyzing the strategies developed by these two teams and framing the kinds of messages that the planned to send to Black Team 2. As the detailed plans of the red teams began to be fleshed out, Black Team 1 would begin to develop associated indicators and to create detailed messages for Black Team 2.

The red team's detailed planning process would continue through the morning of the third day and Black Team 1 would continue to develop indicators and to prepare messages from Black Team 2. At the same time, Black Team 1 would begin sending to Black Team 2 the messages that it had queued up the previous day. As they received these messages, the analysts on Black Team 2 would attempt to use various "non-traditional" analysis methods as vehicles for divining to what kinds of events the messages might point.

By lunchtime on the third day, the red teams would be through with their scenario development. That afternoon, the red team members and the White Team would take part in a series of activities aimed at exploring specific issues related to the development of scenarios in the context of gaming. These included:

- considering how exhaustive catalogs of specific kinds of operational methods might be developed,
- looking at the role of culture in scenario development,
- examining the importance of role playing in this process, and
- brainstorming approaches that might be used in scoring plans.

The morning of the fourth day would be dedicated to a "hotwash" where all players would participate in developing lessons learned from the event. The intent was to take advantage of the collective expertise to enhance the study of which this game is a part.

The Game's Results

While the overall design of the gamed worked well, it quickly became clear that the red teams were progressing slower than had originally been planned. To accommodate this, the red team scenario development activities were extended through the end of third day and the post-game exercises moved to the start of the final day.

The balance of this section provides an overview of how each of the team's activities played out. Details of the specific products produced by these activities can be found in the appendices.

Red Teams

The objective of both red teams was to execute a major attack on the Washington DC subway system. The final scenarios of these teams are detailed in full in the classified appendices of this report. In both cases they were judged to be plausible, workable, and likely to have succeeded in causing major loss of life or economic disruption. Given the time constraints of the exercise, many of the operation details were not specified but were within the capabilities of the teams assembled. The team scenarios were both fairly rugged and adaptable to the perturbations given by the white team.

Black Team 1

Black 1 Team, given a "god's eye view" of the unfolding plans of the red teams, faced the challenge of translating those plans into indicators. They developed some high level principles about the general nature of indicators and observables:

1. Each indicator would be described by the usual detail – answering the "who, what, when and where" questions.
2. It would also be important to associate the phase of the scenario with each indicator. These phases would include planning (gathering information and target selection), travel, financial transactions, communications, training and education, and acquisition of tools and technology. It was noted that some of these categories might have specific types of indicators more commonly associated with specific terrorist organizations – such as financial methods common to Islamic cultures.
3. Other qualifiers might need to be associated with each indicator – such as the likelihood of the visibility of this indicator, required associations with other indicators for relevance (including required timing or sequencing), or significance in world context.
4. Finally, the likelihood of a particular indicator to pique the interest of subject matter experts such as intelligence analysts, counterintelligence specialists, bank tellers, customs agents, law enforcement officers or security guards, might need to be assessed.

This team of intelligence analysts noted that the general associations of individuals involved in terrorist activities are currently the indicators used in intelligence operations to interdict terrorist acts – especially if the terrorists were associated with specific religions or political movements, indicators of specialized associations might be important. Examples might be religious schools, visible religious practices, common training camps or other educational institutions, points of origin of foreign players, memberships in special organizations, associations with individuals on watch lists, and family ties.

The team then applied their ideas to the development of "clues" to send to the second black team. They decided to include some noise as well as signal and send observations that hinted to facts of the scenario. Since the red teams lagged behind the work of the black teams, Black Team 1 generated clues based on the knowledge of the plans still under development by the red teams but filled in the required details for indicators themselves. The actual flow of information between the black teams is included in the classified appendices.

Once the red teams had produced enough details, Black Team 1 started associating indicators with these actions. One major issue around the creation of indicators for this game was the question of how the indictor came to the attention of the Black Team 2. To get the analysts on this second team started, Black Team 1 picked some indictors to feed them in a rather arbitrary fashion. This technique was successful in getting them information to start the analysis and was deemed to be not unlike the real world where attention is often created by the systematic probing of common information. Overall, Black Team 1 found it straightforward to associate indicators with the red team actions.

Black Team 2

The use of Black 2 team as a test bed was deemed a success. Black 2 team started work on day 2 of the event. After some initial problems with email, the game between Black Team 1 and Black 2 flowed very well. Since Black Team 2 had very little access to technical expertise during the game, they relied mainly on social analysis to build links and deduce the details of the scenarios. They were actively engaged in conversations with the Black Team 1 and successfully probed for many details. In the end, they zeroed in on the RDD scenario, but seemed to reach an impasse with the Bio scenario. One of the reasons for this lack of progress was due to the lack of access to tools to help them work through the implications of the evidence they possessed.

White Team

In the early phases of the game, the White Team's role was mainly to deal with communications and data recording issues and to encourage the red teams to generate initial plans to feed to Black Team 1. As the red team dynamics progressed, the White Team moved a player from one of the red teams to the White Team to increase team participation in the process. In general, the processes worked well even though the Notetakers were worn by the end of each day.

On the afternoon of the third day, the White Team began injecting perturbations into the game with a view to seeing if the scenarios generated were "rugged" against disruptions. The specific perturbations used were developed in light of the scenarios that each red team had generated by noon of the third day. As the red teams received messages specifying that some event had occurred, they would respond back with adaptations to their plans. Overall, this exercise did help reveal weaknesses in the plans but, more importantly for the purposes of the exercise, demonstrated that this process could help a standing red team generate alternative methods of carrying out plan steps.

The Post-Game Exercises

On the morning of the fourth day, members from all of the teams were split into four groups in order to discuss the post-game questions. The results of their discussions follow.

All the Ways to Do X

One of the facts that the ACG had recognized about building a database of plans was that thinking at different levels of abstraction would be required. At the highest level, experts would be involved in thinking about strategies that might be pursued in order to achieve specified objectives. Below this, players in a game would think through specific tactics that might be employed in order to implement given strategies. At the lowest level, experts would articulate specific sequences of concrete actions that can be taken to realize particular tactics. Whereas the upper levels are more abstract and lend themselves well to group brainstorming activities, the bottom level is quite concrete and, it was expected, would require specific knowledge from experts who traffic in particular fields.

To explore this notion, this breakout session had as its goal enumerating and describing as many ways as could be imagined of transferring funds between parties in an organization. While the session was framed as described, participants quickly voiced their discomfort with the limited scope and advocated expanding the discussion to include mechanisms for acquiring finances and ways of consuming it. Given the limited time, what emerged was a handful of ways to deal with funds. A brief analysis of these methods indicated that, while each method might have a distinct structure and employ method-unique resources, common roles and processes could still be identified across all methods, lending credence to the notion that it would be possible to create abstract operational patterns that could be elaborated in different ways to create unique operational plans.

The Role of Culture and How to Manage This in a Game

In developing their plans, the red teams specifically chose to generate logistics without attention to the cultural bias of the players as a constraint. This decision was not without risk. The long range goal of the Hypothesizer effort is not to simply to collect all possible ways to accomplish any logistical plan for terror attacks but also to do so in a way that reflects how specific terrorist groups might carry out these operations. Prior to the Red Game, it was Sandia's premise that the role of culture in such terrorist planning would be greatest in strategies, objectives and target selection— with smaller impact on tactical details. In order to explore these beliefs, the second post-game exercise focused on the role of culture on this kind of gaming.

Cultural experts in this session felt that the premise was weak and discussed ways in which cultural bias might impact tactical details. It was clear that the organizational structure of terrorist teams would be different than that created by the red teams. A major influence would come from strong family ties in that the choice of what to do might be made largely by who would be a trusted member of the team and what skills they could acquire rather than by what shills were needed and then who might have those skills. The command and control structure for the red teams was pretty much a hierarchical, western structure with large concern for operation security. It was noted that the almost fatalistic belief in their cause due to religious convictions might cause much less contingency or back up planning in actual terrorist cells, and that their command and control structure is very fluid. There was also disagreement about the shape of the cultural figure. One observation was that the terrorist have given us their overall objectives and hence there is

no cultural understanding necessary. We do not, however, know how they will approach their operation planning without understanding their cultural viewpoints. In summary, this seems to be an open point that needs much more discussion.

The Role of Identities in Red Gaming

This red game was not designed to be a role playing game in that the game organizers did not assign each participant a specific persona to maintain throughout the game. At the same time, each team was asked to create identities for the terrorist cell and its support network (i.e., the group was create a representative set of actors who would be carrying out the planned event and would frame all subsequent plans in terms of these actors). This third post-game session was asked to discuss in detail the role of identities in the game and how the process could be improved.

A number of key points were surfaced in this discussion. The first observation was that understanding the person is critical. If you don't have information on people, what do you have? You can't track ideas. This became a significant issue at the start of Black Team 2 analysis efforts in that they didn't know that they were dealing with two cells. Once the team's processes were in place, the team's later discovery that there were two scenarios in effect did not impact their progress.

Second, the red teams needed to be able to identify the attributes of the person(s) necessary to carry out each of the tasks in a plan. This would be done by identifying the skills needed, creating paths by which persons could get those skills, and finally considering how viable it would be to assemble a group possessing all of the requisite skills. Alternatively, it was felt that starting with people with certain skills and letting that define the scenario might be useful – an approach that could significantly alter the kinds of scenarios that a red team would entertain. Other details, such as date of entry into the U.S., were also seen as important to specify since profiles could be generated from such data.

Issues around unique ID were discussed. Identity disambiguation is a difficult problem due to:

- borrowing identities
- AKA's
- could have 90% of person's identifying characteristics, but 10% could be wrong.
- different spellings/pronunciations.

In games that play out specific scenarios with specific roles, this factor would need to be considered.

The group discussed various gaming options and suggested that there would be value in constraining the biographies of the roles and in identifying the types of people needed to carry out a task. One example of this would be to identify a specific game, and then have the team choose some specified number of people from a deck of personas for various scenarios. It should not be possible to invent "ideal" people that instantly appear. Part of the exercise could then be to investigate why they chose certain people.

Scoring Plans

One of the important features of the database of scenarios envisioned in this project will be the scoring of the scenarios in various dimensions. One possible score would involve some measure of the likelihood of success of the plan. In this session, variations on success measures were discussed. It was felt that success is a value judgment which is based on cultural factors. This raises come interesting questions for scoring since the measure of success used in our database would likely be from our point of view and yet the terrorist might treat some smaller part of the plan as successful. Regardless, this issue points to the need for scoring of fragments of a plan and for evolving measures of success. Some new categories for possible differentiation measures were discussed, such as the complexity of a plan, the size of a terrorist team, the style (hierarchical versus distributed) of planning and operation of the team, and the likelihood for retaliation. When discussing the particular plans developed in the game, a smaller size team with simpler means of acquisition of deadly material was the critical criteria. The difficulty of containment and of recovery from a particular attack was the critical things to consider.

Observations and Lessons Learned

Relative to the objectives set for it, the Red Game produced a number of useful findings and lessons learned. The following briefly summarizes a number of these:

About Teams

With respect to the operation of the teams, several interesting observations were made (see the appendices for a more detailed discussion of team dynamics). First, a fair portion of what the teams did involved brainstorming-style discussions in which the goal was to generate a broad range of options relative to whatever question was on the table. Ideally this process would draw on the collective expertise of all team members. On several occasions, dominant team members were seen to be controlling the "air time", thereby limiting the potential synergies that could be obtained from multi-minded exchanges.

Second, the approaches used by both teams were radically different. While one team was very structured in its approaches and presented a more disciplined, leader-centric feel, the other appeared much more chaotic, with the leader encouraging debate and then harvesting from these discussions the plan that the team would pursue. As noted earlier, one team was made up of professionals accustomed to the conduct of real-world operations, while the second was much more eclectic in its composition with only its leadership having any real-world experience in this arena and the balance of the team coming from more theoretically-oriented backgrounds. This latter team was also much more given to researching information on-line than was the team of professionals. The

professionals were much more cautious about mapping out their attacks (evidenced by actual reconnaissance of the D.C. Metro system that the team had done prior to arriving at the Red Game) and planned measures laid to ensure a low operational signature.

The question of cultural biases was an interesting one. While individual team members did not play specific roles, the team as a whole was aware that they were supposed to be planning an Al Qaeda-like operation. Even so, the question of whether or not specific methods were faithful to the culture of this organization seemed to impact the team's thinking in some portions of the discussion but then disappear totally in others. There was little effort invested in creating fictitious roles (particularly in the RDD team) and not much in maintaining them.

A more important influence seemed to be the interactions that team members had or did not have prior to the game. Once play began, team members quickly fell into 'real-life' roles, defined either by personality styles or by personal histories. In the bio team, players generally interacted according to personality styles. In the RDD team, players naturally adopted the occupational roles they filled in real life (note that these team members generally knew each other outside of the game environment - minimally, the team leader knew all participants outside the game environment and so was able to assign them roles appropriate to experience).

Neither the observers nor the presence of other teams seemed to affect the dynamics of the red teams.

About Infrastructure

The infrastructure (or lack thereof) expressed itself in a number of ways during the game. First, there was a strong desire on some number of the team members to have access to the internet. As set up, each team had access only to a single open computer with a view to providing them with Internet access. During the teams' research phases, having a larger number of computers might have been useful. If this idea is pursued in further games, software should also be put in place that makes it easier for the White Team to capture the teams' searchers. Following the game, the White Team harvested the browser logs for this exact purpose but this proved to be a tedious process, as no mechanism for exporting these logs was available.

Second, while certain forms were created in advance of the event that were aimed at helping the Notetakers capture the plans generated by the red teams (both those plans that were accepted and those options that were considered but rejected), a better mechanism for capturing this information is needed. The manual processes used placed a very heavy burden on the Notetakers.

Beyond simply allowing the Game Masters to capture the scenario elements that are the focus of this kind of game, making this information available to the red teams as they are playing would have also been useful. The teams could have tracked actual and potential plans more readily than was done in this first experimental game. Also, being able to

more formally capture this information in real-time would help both the White and black teams better track the progress of the red play.

At points the activities were quite intense. Tracking via computer everything that was happening during these periods was difficult for to the White Team. Having three terminals – one for email and two more for monitoring each of the two teams – would have been helpful.

For lack of interactive ways of viewing current plans and given the limited number of computers available for researching topics, printers became a dominant mechanism for reviewing content. Bottlenecks in printing (this was more of an issue on the classified side of the game) suggest that more printers would be needed if alternative means of reviewing data were not provided.

Related to this issue is the question of how to handle classification of printouts. Before being released, every document was reviewed for classification to ensure that it did not contain data that should not be released to the players. This process was a second bottleneck and could have been alleviated by adding another person to staff this position as their only job (the classifier in this game also played other roles) or by creating an infrastructure that mechanistically ensures that data could not migrate from other sources to the players.

Black Team 2 reported that they would have preferred to have access to additional computer-based tools.

In general, the use of classified email for game monitoring worked very well with each team assigned a communications person. The use of shared documents on the classified file space also worked well and made it possible to easily track recorded information. One issue was the lack of really good tools to capture the scenario generation work of the red teams. Our prepared spreadsheet forms turned out to be of limited value for this process.

In framing the game, one of the questions had been whether or not a game like this could be done in distributed fashion with team members being geographically dispersed and team interactions facilitated by electronic communication. Observers noted that the team dynamics were quite fluid. Often side conversations or small groups would form that would be precluded by an electronic format. Distributing players, it was felt, would lead to completely different team dynamics.

About the Game Plan

With respect to the structure of the game and the process of planning for it, the following were observed.

Time duration was just about right. As noted earlier, the red teams needed an extra half day beyond what had originally been planned but extra room in the agenda and players travel plans allowed for the accommodation of this.

The red team planning process was essentially a top-down drill where the objectives were elaborated into strategies which, in turn, were further elaborated into operational specifics. By contrast, the second half of Black Team 1's tasks – feeding indicators to Black Team 2 – was necessarily chronological in nature. Because both the red teams and Black Team 2 began working on the same day, all of the red team data needed by Black Team 1 was not ready when required. To compensate, Black Team 2 "filled in" details and used the resulting picture to drive the process of generating indicators. In retrospect, it would have been better to let the red teams run for a day before beginning black team operations. This would have allowed the red team scenarios to have been developed in sufficient detail to be played out sequentially by the black team.

One of the goals of the exercise was to get the red teams to produce sufficiently detailed task descriptions to permit ready analysis by Black Team 1. In many parts of the proposed plans, this level of detail was never achieved. To address this, there might be value in splitting the red teams into two groups. One would focus on operational strategies and the second on operation details. It is worth noting that of these two, the perturbations suggested by the White Team would largely affect the former.

Next, timelines presented a problem during this exercise. Since the White Team did not force the exercise to proceed on a timeline, it was unclear how the teams should handle any perturbations that were introduced. In at least one case, it became clear that *when* a given event occurred would significantly impact how the team would need to respond to the perturbation. In future events, it was felt that enforcing a game timeline during this part of the game would alleviate this confusion.

It was suggested that better role definitions would have been helpful. One idea for improving the establishment of this operational context was to have the red teams fill out "Visa applications" for each of the characters that they decided would be part of the their cell. It was felt that the process of answering the questions would do much to establish a persona for each of the characters involved.

Finally, at end of the game, the red teams briefed each other on the plans that each had developed. The process of formally documenting the results proved useful in pointing out fuzziness in thinking and strengthened the overall process of capturing the teams' plans.

About the Value of Gaming

One of the central questions being addressed by this Red Game was whether or not a gaming construct adds anything to the process of scenario development relative to what might be done in a purely analytic exercise. The answer from the players was "yes".

First, the gaming environment lent a degree of reality to the process. It engendered a feeling of urgency that would have been totally lacking in a simple analytic process.

Second, the perturbations, though played out in a relatively short timeframe, proved to be good mechanisms for exploring other ways of doing things. Allowing teams more time to address specific perturbations would have been useful.

As much as anything, the games played during this event focused on operational strategy. It appears from what was observed in the game play that details may be better worked offline. At the same time, working to some level the details in the gaming environment contributed to a deeper sense of the complexity of these plans.

Unlike an analytic drill that engages a specified set of experts to consider a given topic, a gaming environment is much more forgiving to changes in team dynamics when these are required. If egos begin to conflict or certain players are being too quiet, it is easier in the context of a game to argue for a change in the world that impacts the team in ways meant to address these needs.

Black Team 2's difficultly in assessing the significance of certain details about the bio scenario argues for the possibility that subsequent games utilizing a hypothesizer could test the usefulness of this concept in relatively well controlled conditions.

Lastly, the dynamics of teams – the joint sense of ownership of the problem at hand and the synergistic playing off of each other's ideas – argues for the use of gaming in at least some aspects of scenario development if creation of a robust scenarios repository is ever to be instantiated at the national level.

Next Steps

The Red Game was never intended to be an end unto itself but is part of a larger activity aimed at exploring what will be required to implement the Hypothesizer and the national red team that would shepherd the development of its underlying scenarios knowledge base. The Game was designed to help answer a number of outstanding questions about the potential for interactive gaming as one technique for developing scenarios and the various pieces of information related to them. There are still more questions to be answered before the idea of the national red team capability is widely socialized.

Additional Games and Exercises

Consideration is also being given to holding one or more additional games that would focus on issues entailed in different aspects of the Hypothesizer concept. Some of the ideas being considered include:

- an analyst game that would explore the use of a prototypical version of a Hypothesizer in support of an analysis game very much like that in which Black Team 2 was involved,
- an "indicators" exercise in which the question of how a given plan might express itself as observables is addressed,
- an operational details exercise in which experts with deep knowledge in a narrow domain work to define all of the ways that a given set of things might be done (such as the covert movement of personnel),

- a “scoring” game aimed at determining how experts would evaluate scenarios in a wide range of dimensions,
- a “targets” exercise aimed at exploring the relevant characteristics of targets from an operational perspective and at the development of a taxonomy based on these characteristics,
- an “objectives” exercise that would seek to develop a taxonomy for describing things that groups might try to accomplish and things that they might try to avoid,
- a taxonomy exercise focused on “resources” that can be used to support terrorist operations,
- an exercise that cuts across all of these dimensions by considering how target selection is influenced by desired outcomes and available resources,
- an implementation game focused at exploring the impact that variations in the operational environment have on observables that might be seen by intelligence systems (e.g., what happens when roles in a given plan are allocated differently in an organization or when members of the organization are deployed in various ways or how a given plan might play out differently in different cultures), and
- a “logistics” game that forces analysts to explore whether it is possible to detect and characterize operation *without* the benefit of social network analysis and related techniques.
- A non-expert game in which team members are asked to devise a plan outside their areas of expertise.

Lessons Learned

Given the lessons learned and the possibility that other games will be played, the following improvements are recommended.

If the same kind of “red game” were to be played in a standing red team environment, it should follow a slightly different timeline. To start, a day and a half to two days should be spent developing plans to the level done in this game. Following this, another day and a half to two days should be spent working out specific details of how each element in the plan could possibly be implemented. Finally, one to two more days would then be given to playing out one or more times against a timeline (as is typically done in war games) the detailed plans developed in the second phase of this process.

In each of the three phases, a White Team could perturb the plans being developed. In the first phase, the focus would be on harvesting a rich set of strategies and on ensuring that the specific strategies being laid are robust. In the second, the focus would be on cataloging specific techniques for achieving particular operational sub-objectives (e.g., moving funds, acquiring resources, and recruiting operatives) and on preparing the red teams for the war gaming phase. In the final phase, perturbations would be injected in real-time and red team actions would be assessed continuously by a black team. The goal here is to evaluate the robustness of specific strategies and the detectability of specific actions used to implement these strategies. One key result of this would be an ever-growing catalog of indicators and the actions with which they might be associated.

Next, the quality of the gaming infrastructure showed itself to be an important factor in how easily a game can be carried out. Here a number of improvements should be considered. Among these are:

- mechanisms for real-time, structured capture of plans being considered by the red teams (these should allow red team members to view both their plan as it stands and all of the alternative accepted and rejected for any part of the plan),
- broader access to computer terminals (while having terminals for red team members might prove disruptive to team operations, it seems that some players' work styles demand access to lots of information), and
- automation for black team members that enables structured capture of indicators.

A third improvement is to associate specific deliverables with first two phases of the game. As played in the Red Game, deadlines were initially instituted as a way to force closure. These proved less effective that desired. It now seems that demanding structured reports that deliver specific information in specific formats might be a preferable approach. Note that if the scenarios capture tools covered in the first recommendation were in place, this issue would diminish in importance.

Appendices

This contains the invitation letter, instructions for the game participants, templates for black team 2 and notes from the process observers. Additional details of the game are documented in a classified Sandia report.

Invite Letter

The Knowledge Discovery and Dissemination Program of the Intelligence Technology Innovation Center is exploring the use of red teaming and gaming to systematically develop plausible terrorist scenarios and identify potential indicators of these scenarios. In support of this effort, the Advanced Concepts Group of Sandia National Laboratories is hosting a terrorism red gaming event in Albuquerque on July 22 –24, 2003. The goals of this effort require human expertise to seed a compute engine with detailed operational plans for hypothetical terrorist scenarios. Your expertise will contribute to the success of this pilot event.

Within the national security community, efforts to explore possible terrorist scenarios occur on a regular basis. The hypotheses developed in those events tend to be locally kept, thereby limiting their usefulness to intelligence analysis, and the focus is seldom on operational details required for interdiction. This event is part of a project developing the concepts for the creation of a national "red gaming" capability to generate and collect hypothetical scenarios and the creation of a data warehouse that would store of the operational details of scenarios or scenario fragments, in a computer manipulatible format.

This red game will consist of 2 red teams, a black team and a white team.

- As a red team member, you will work with other experts to develop operational details for a specified hypothetical terrorist event.
- As a black team member, you will work with other intelligence experts to assess, develop, attach, and correlate indicators with red team operational details.
- As a white team member, you will help to control and assess the environment of the game and team interactions.

We believe this concept could lead to a national capability, which would significantly improve our ability for successful interdiction in terrorist activities. Your participation is essential in assessing the feasibility of this concept.

Please plan to arrive in Albuquerque on July 21, 2003, in time for an informal dinner with the group. Additional details about travel/hotel arrangements for the workshop are attached. The meetings during the workshop will be held at an SNSI level because of the possible sensitivity of the materials generated. I have also included an "Information Request" form for you to **complete and return to, Alicia Cloer, via email (aacloer@sandia.gov) by July 7.** If you have questions about anything, please contact Ms. Cloer at 505-845-9819, or Judy Moore at 505-845-9415.

Instructions for Players

Instructions for Participants

Assignments: Your job is to contribute to the red team planning for a hypothetical terrorist event. This is not a role playing exercise, but you will be asked to put yourself into the frame of mind of a terrorist committed to a cause. You will also be required to generate some detailed information about the lives of the people in your cell to allow the proper assignment of indicators by the black team for any actions. You will be calling upon your previous knowledge and generating details behind these plans. There will be an assigned team leader that will keep the group on track for these goals.

The game will simulate a two-year operation that will span everything from initial planning to final actions taken after implementation of the attack. The game will take place in two phases over the course of two days. On the first day, you will develop a detailed plan for an operation that could take up to two years to carry out. On the second day, you play out your plan in a game that evaluates your work in various dimensions.

During the two days, your team will periodically receive unsolicited messages from the white team. During the first day, these messages will be designed to encourage you to explore certain aspects of your plan in more detail. During the second day, these messages will present your team with unexpected opportunities, changes in environment, and incidents of direct relevance to your team. As you and the rest of team decide, you can pursue your previously developed plans or alter them if you believe that these changes will deliver better results than the originals.

At the end of the first day, you will be interviewed regarding your thoughts on that day's planning exercises. On Thursday morning, you will take part in the game's "hotwash". During this time, you may be asked to fill out a questionnaire or be interviewed or both. The goal of this time is to collect your insights about the strengths and weaknesses of the gaming approach for scenario development and to get your ideas on how this approach might be used most effectively (or even if it should be used at all).

Processes: You will be equipped with flipcharts and whiteboards that can be used during the planning and are encouraged to document your discussions as thoroughly as possible using these means.

Two note takers assigned to the team will act as recorders of the plans that you develop. One of these note takers will also act as liaison between you and the white team. Any questions that you want to ask the white team will be transmitted via this note taker. Answers from the white team will come back through the same channel.

Instructions for Red Team Leader

Assignments: Your job is to organize and run the operations of your team. This includes assigning roles to your team members, keeping them on track with respect to your team's objectives, and ensuring that the products that they produce are detailed enough to enable the black team to develop indicators associated with your team's planned activities.

The game will simulate a two-year operation that will span everything from initial planning to final actions taken after implementation of the attack. The game will take place in two phases over the course of two days. On the first day, you will develop a detailed plan for an operation that could take up to two years to carry out. On the second day, you play out your plan in a game that evaluates your work in various dimensions.

During the two days, your team will periodically receive unsolicited messages from the white team. During the first day, these messages will be designed to encourage you to explore certain aspects of your plan in more detail. During the second day, these messages will present your team with unexpected opportunities, changes in environment, and incidents of direct relevance to your team. As you and the rest of team decide, you can pursue your previously developed plans or alter them if you believe that these changes will deliver better results than the originals.

At the end of the first day, you will be interviewed regarding your thoughts on that day's planning exercises. On Thursday morning, you will take part in the game's "hotwash". During this time, you may be asked to fill out a questionnaire or be interviewed or both. The goal of this time is to collect your insights about the strengths and weaknesses of the gaming approach for scenario development and to get your ideas on how this approach might be used most effectively (or even if it should be used at all).

Processes: You will be equipped with flipcharts and whiteboards that can be used during the planning and are encouraged to ***document your discussions as thoroughly as possible using these means***. There is not a facilitator for your work so you and your team will need to do all the writing. Two note takers assigned to the team will be recording your work in parallel onto the secure network. One of these, the Communicator, will also act as liaison between you and the white

team. Any questions that you want to ask the white team during game play will be transmitted via this note taker. Answers from the white team will come back through the same channel. During breaks and lunch, feel free to visit the game control room to discuss any issues that you feel need to be addressed. There are other observers in the room, but only the Communicator should be interacting with you or your team during play of the game.

Questions for Red Team Leaders

Background: The red game exercise is aimed at answering questions about the utility of red gaming and analytic drills in the development of scenarios. The red team that you are leading interacts with two other teams – a white team that monitors your progress during planning and that interacts with you during the second days' role playing and a black team that translates your planned actions into potential indicators.

In managing your team, one of your key tasks will be to ensure that the plans developed meet several criteria. The questions listed below are meant to help you assess how well you are doing at meeting these criteria.

Questions Is the plan complete? Are all of the required steps specified? Are you sure that there are no "something magic happens here" steps in your plan?

Is the plan sufficiently detailed? Does it specify what role is performing what actions in what contexts and under what conditions?

Is your plan robust? Have you identified critical elements that, if subverted, will make it impossible to carry out your plan? Have you developed contingencies to address these possibilities?

Is your plan realistic? Do you believe that it reflects the kind of operational approaches that real-world organizations would employ? Would most organizations be able to pay the "costs" associated with your plan?

Is your plan effective? How likely would it be to achieve the objectives that you have been given?

Instructions for Red Team Recorder

Assignments: Your job is to record the plan(s) developed by your team in the supplied excel spreadsheet on the SCN. You should also record any options that they may have considered in the process of developing these plans but have chosen not to pursue.

The game will simulate a two-year operation that will span everything from initial planning to final actions taken after implementation of the attack. The game will take place in two phases over the course of two days. On the first day, your team will develop a detailed plan for an operation that could take up to two years to carry out. On the second day, they play out their plan in a game that evaluates your team's plan in various dimensions.

At the end of each day, you will be asked to stay after the players have left for the day and to help the white team assess how the game is going and to plan any changes that are required for the next day. Please be ready to report on how far you believe your team has progressed on their goals and what suggestions you have for improving the game for your team.

On Thursday morning, you will take part in the game's "hotwash". During this time, you may be asked to fill out a questionnaire or be interviewed or both. The goal of this time is to collect your insights about the strengths and weaknesses of the gaming approach for scenario development and to get your ideas on how this approach might be used most effectively (or even if it should be used at all).

Processes: You will use a thin-client terminal attached to the SCN that will give you access to the Red Game directory space. You will use the templates found in your team's folder to record your findings and will store your results in the same directory. You will receive reminder messages from game control to save every half hour throughout the course of the game so that the white and black team members can track your progress. Remember that you cannot walk away from your SCN client without logging off.

During breaks and lunch, feel free to visit the game control room to discuss any issues that you feel need to be addressed.

Instructions for Red Team Communicator

Assignments: Your job is to record what you observe about the processes that your team uses to generate its plans (e.g., what questions they ask, how they resolve between multiple choices, how much they are influenced by constraints and objectives handed to them).

The game will simulate a two-year operation that will span everything from initial planning to final actions taken after implementation of the attack. The game will take place in two phases over the course of two days. On the first day, your team will develop a detailed plan for an operation that could take up to two years to carry out. On the second

day, they play out their plan in a game that evaluates your work in various dimensions.

During the two days, you will also serve as the liaison between your team and the white team. Any questions that your team wants to ask the white team will be passed by you via email. Likewise, all answers to these questions will be returned via email to you.

Your team will periodically receive unsolicited messages from the white team. During the first day, these messages will be designed to encourage your team to explore certain aspects of your plan in more detail. During the second day, these messages will present your team with unexpected opportunities, changes in environment, and incidents of direct relevance to your team. How the team handles these messages is up to them. Your job is to let the team leader know when such messages have arrived.

At the end of each day, you will be asked to stay after the players have left for the day and to help the white team assess how the game is going and to plan any changes that are required for the next day. Please be ready to report on how far you believe your team has progressed on their goals and what suggestions you have for improving the game for your team.

On Thursday morning, you will take part in the game's "hotwash". During this time, you may be asked to fill out a questionnaire or be interviewed or both. The goal of this time is to collect your insights about the strengths and weaknesses of the gaming approach for scenario development and to get your ideas on how this approach might be used most effectively (or even if it should be used at all).

Processes: You will use a thin-client terminal attached to the SCN that will give you access to the Red Game directory space. You will find a Word file in your team's folder that contains a number of questions to seed your observations. Please record your findings in this file and feel free to answer the existing questions if applicable and to add your own questions as needed. Please save your work periodically throughout the course of the game. Remember that you cannot walk away from your SCN client without logging off.

You will use an email account assigned to you for this game to communicate with the white team electronically.

During breaks and lunch, feel free to visit the game control room to discuss any issues that you feel need to be addressed.

Instructions for Red Team Process Observer

Assignments: Your job is to record what you observe about the human dimensions on your team's activities (e.g., how do they organize themselves to solve various problems, to what degrees to personalities influence game dynamics, how effective does the team seem to be at the various tasks it pursues, …)

The game will simulate a two-year operation that will span everything from initial planning to final actions taken after implementation of the attack. The game will take place in two phases over the course of two days. On the first day, your team will develop a detailed plan for an operation that could take up to two years to carry out. On the second day, they play out their plan in a game that evaluates your team's work in various dimensions.

During the two days, your team will periodically receive unsolicited messages from the white team. During the first day, these messages will be designed to encourage your team to explore certain aspects of your plan in more detail. During the second day, these messages will present your team with unexpected opportunities, changes in environment, and incidents of direct relevance to your team. How the team handles these messages is up to them. They can pursue their previously developed plans or alter them if they believe that these changes will deliver better results than the originals.

At the end of each day, you will be asked to stay after the players have left for the day and to help the white team assess how the game is going and to plan any changes that are required for the next day. Please be ready to report on how far you believe your team has progressed on their goals and what suggestions you have for improving the game for your team.

On Thursday morning, you will take part in the game's "hotwash". During this time, you may be asked to fill out a questionnaire or be interviewed or both. The goal of this time is to collect your insights about the strengths and weaknesses of the gaming approach for scenario development and to get your ideas on how this approach might be used most effectively (or even if it should be used at all).

Processes: You will use pen and paper to record your observations. If you wish to send messages to the white team during play, you can pass a message through one of your team's note takers who will have email access. During breaks and lunch, feel free to visit the game control room to discuss any issues that you feel need to be addressed.

Questions for Red Team Process Observers

Background: The red game exercise is aimed at answering questions about the utility of red gaming and analytic drills in the development of scenarios. To this end, your job is to observe the operation of the red team to which you are assigned with a view to gaining insight into a number of questions.

The **Recorder** on your team will focus on capturing the *content* of the plans developed by the team. The **Communicator** will focus on communications with the white and noting any "metadata" associated with any red task that might not be captured by the recorder. Your role is to address the *human dynamics* of the red team process.

Questions Did the red team members treat this event like a game? If so, was this approach effective?

Were there significant differences in team dynamics between Tuesday's analytic planning drill and Wednesday's role playing?

What roles did each of the members of the team assume? (e.g., leader, idea generator, critic, etc.)

Did the presence of you and the note takers impact team dynamics? If so, how?

Did your team's awareness of the other red team and of the white and black teams' impact on planning exercises?

How did the team respond to interaction with the white team?

Was the team size appropriate?

To what degree did the team members know each other beforehand? How did this (un)familiarity affect team dynamics?

Did politicking for particular plan options ever emerge? If so, what were the dynamics associated with this? Did "alliances" form within the team? To what degree did these alliances impact which ideas "won out"?

How did personality assert itself in these exercises?

Based on what you observed what impact do you believe distribution of the team and the uses of electronic collaboration have on team dynamics?

Instructions for Black Team 1 Players

Assignments: Your job is to work with the other team members to analyze planned actions proposed by two red teams in order to identify things that might be observed about these actions.

Each team's game will simulate an operation that will occur over a period lasting up to two-years and that can span everything from initial planning to final actions taken after implementation of the attack. The game will take place in two phases over the course of two days. On the first day, each red team will develop a detailed plan for an operation. On the second day, they will play out their plans in a game that evaluates their work in various dimensions.

During the two days, the teams will periodically receive unsolicited messages from the white team. During the first day, these messages will be designed to encourage them to explore certain aspects of their plan in more detail. During the second day, these messages will present the teams with unexpected opportunities, changes in environment, and incidents of direct relevance to their plans. As they decide, they can pursue their previously developed plans or alter them if they believe that these changes will deliver better results than the originals.

You will be assigning possible indicators to the planned actions developed by the red teams. ***Note that this exercise is being run at the SECRET level and hypothesizing fictitious collection capabilities and their outputs is completely acceptable. A key goal of running your team is to help the observers understand the processes that might be used in developing indicators and not the details of what any real-world system would produce.*** You are encouraged to assign indicators to all actions considered by the red teams, even if they are discarded by the red teams for use.

On the second day, you will also be passing some portion of these indicators on to a second black team, the "blind black team", whose job is to simulate a group of analysts trying to determine exactly what each red team is trying to accomplish and how. It is your job to determine which indicators you send to this team.

At the end of the first day, you will be interviewed regarding your thoughts on that day's planning exercises. On Thursday morning, you will take part in the game's "hotwash". During this time, you may be asked to fill out a questionnaire or be interviewed or both. The goal of this time is to collect your insights about the strengths and weaknesses of the gaming approach for scenario development and to get your ideas on how this approach might be used most effectively (or even if it should be used at all).

Processes: You will be equipped with flipcharts and whiteboards that can be used during the planning and are encouraged to document your discussions as thoroughly as possible using these means.

A white team member will be assigned to your team to act as liaison between you and the white and blind black teams. This person will also be responsible for updating your team on the latest red team plans and for capturing the indicator assignments that your team makes. Any questions that you want to ask the white team will be transmitted via this note taker. Answers from the white team will come back through the same channel. Indicators that you wish to pass to the second black team will be transmitted in the same way.

Questions for Black Team 1 Communicator/Recorder

Background: The red game exercise is aimed at answering questions about the utility of red gaming and analytic drills in the development of scenarios. Part of this involves the development of indicators that would be associated with plans developed in this way. To this end, one of your jobs is to observe the operation of the black team to which you are assigned with a view to gaining insight into a number of questions.

Questions How important was the level of detail delivered by the red teams to the development of indicators? Could *kinds* of actions be mapped to *kinds* of indicators or were very detailed specifications of actions required before indicators could be produced?

What kind of information was needed to develop indicators?

Was there ever ambiguity about what might be seen? How were conflicts regarding these things resolved?

To what degree did the black team members consider what collection systems might be in place in their development of indicators?

How did the black team members go about deciding which indicators to forward to Black Team 2?

Did processing inputs from two separate red teams ever present a problem?

Black Team 2 Templates

Several templates were created for possible use by Black Team 2 – mostly to force them into conversations where the terminology issues of different analysts could be explored. These were not really very useful – partly because the interface was so poor for real use. However, we include them in the report for completeness. These were actually Excel spreadsheets but these are represented as tables in this report.

The Zachman Framework: the view of the Terrorist organization						
view	*who*	*how*	*what*	*when*	*where*	*why*
	people	**process**	**technology**	**timelines**	**locations**	**goal**
Champion/ Inspirational leader						
leadership						
captain						
cell lead						
terrorist						
supporter						
casual						

Sources	*who*	*how*	*what*	*when*	*where*	*why*
	people	**process**	**technology**	**timelines**	**locations**	**goal**
public						
humINT						
photINT, imINT						
comINT, sigINT						
masINT						
financial INT						
law enforce INT						

Competing Hypothesis Table

		Hypothesis 1	Hypothesis 2	Hypothesis 3	Hypothesis 4	Hypothesis 5	Hypothesis 6
	Evidence						
1							
2							
3							
4							
5							
6							
7							
8							
9							
10							

key:
4 = evidence strongly supports hypothesis
3 = evidence consistent with hypothesis
2 = evidence could support hypothesis
1 = evidence appears unrelated to hypothesis
0 = evidence inconsistent with hypothesis

Process Observer Comments

1. **Did the red team members treat this event like a game? If so, was this approach effective?**
   RDD Team Observer: Off and on day one and most of day two. They became most engaged in it as a game in the segment where the white team was throwing the interruptions. The created identities played virtually no role in the interchanges. Every now and then someone would recall an identity, "He'll do it because he's supposed to be a business man…" Again this became most real on the afternoon of the 2nd day when the pace of play picked up.
   Bio Team Observer: Most players kept the game concept in mind during the discussion. Only rarely did any of them speak in the first person (i.e. "I could do that…").The leader most consistently modeled the first person approach. When he did this, several of the others followed suit. Much more in the overall environment would need to be controlled to help it be natural for the players to adopt, and stay in, roles.

2. **Were there significant differences in the team dynamics between Tuesday's analytic planning drill and Wednesday's role-playing?**
   RDD Team Observer: Not really. Roles and relationships were fairly well established in the first hour or two of the first day. If anything, role definitions became stronger (reinforced) as time went on.
   Bio Team Observer: The principle difference between the two days was the removal of one person from the team who had dominated the conversations on the first day. The team developed a norm in which everyone was encouraged to contribute at any time in the discussion. This worked pretty well for the first day-and-a-half. When time-sensitive events were put in play on the second day, this norm remained in place. The result was that specialists who had the subject matter expertise to solve the tactical problem couldn't get airtime to surface the logical solutions. The leader would make specific requests of individuals from time to time, but he didn't assign tasks to individuals or groups.

3. **What roles did each of the members of the team assume? (e.g., leader, idea, generator, critic, etc.)**
   RDD Team Observer:
   - The named leader initially assumed the leadership role – explicitly established it with a 5 min. speech intended to set the stage – what he (the leader) wanted, how he had planned to structure the day, etc.
   - Another team member immediately challenged the named leader for leadership position by questioning his plan for moving forward, his objective, etc. Also served as idea generator throughout both days, partially through his challenge, partially through production of new ideas.
   - Two experienced operational people brought significant operations skills to the taste and tended to participate much more as the planning process got to that stage.
   - One person served as process guy – kept the group focused on creating time lines, WBS, game deliverables, etc.

- One idea generator participated, but her ideas were so far out of the group mainstream that she "checked out" (withdrew from participation relatively early in the process) – she also provided some cultural information, which appeared to be listened to but was not incorporated into subsequent discussions. Although apparently the most knowledgeable of the group in this area her opinion was never solicited.
- Two members were clearly technical advisors. "You tell us what you want to accomplish and we'll tell you how to do it." They were listened to with respect.
- One person did not participate at all.

Bio Team Observer: The named leader's 35 years experience as a leader and commander in the Navy showed itself profoundly. He was clearly very flexible in what style of leadership he brings to the task at hand. He did not try to take this disparate group of strangers and make an efficient, cohesive team. He steered to process to the desired outcome without using his authority to control the discussion. (Had he tried, he and one other team member would have been in a power struggle from the start.) He let all the others carry the energized discussion in whatever direction any participant (usually one specific team member) wanted to take it. In time, it became clear that the leader was harvesting pieces of these discussions for later use. Sitting beside The leader was another important team member (who came a little late to the group and originally sat away from the table). He ignored much of the initial discussion of the rest of the team and outlined an operational plan on his tablet. About an hour into the exercise, he pulled his chair up next to the leader and showed him the plan (with the rest of the group continuing to talk without even noticing). The leader never tried to control the discussion of the others. Some members became exasperated at the domination of the discussion by one individual, but the leader let them take care of themselves and didn't intervene. At several intervals the leader would say, "Here's what we have so far…" Each time he did that, the team agreed. He had adequately integrated their discussion into the plan and felt like full participants. This highly non-linear way of doing things obviously made the job of the Black Team very difficult. This reality points to the near necessity of videotaping these events.

4. Did the presence of you and the note takers impact team dynamics? If so, how?

RDD Team Observer: No – Except one of our note takers began to participate part way through. He did influence team dynamics – produced some info they did not have. He was cautioned by game master.

Bio Team Observer: No – The note takers spent most of the time feverishly writing or typing. There wasn't time to interfere.

5. Did your team's awareness of the other red team and of the white and black team's impact on planning exercises?

RDD Team Observer:

- Other red team – no
- White team – only as prescribed by the game
- Black – in their requests for identities before team was ready to give them

Bio Team Observer:

- Other red team - no
- White team – within the game rules

- Black – when the black team leader came out to try to get a specific plan from the team, it broke the above described dynamic

6. **How did the team respond to interaction with the white team?**
   RDD Team Observer: Fine – until the interventions became what the team as nonsensical – then they started to fight the game
   Bio Team Observer: Fine

7. **Was the team size appropriate?**
   RDD Team Observer: It was about minimum size. Could have had up to 4 more – not more than that. Could have used more because of the method of planning – broke into compartmentalized activities
   Bio Team Observer: The answer to this depends on the desired purpose of the exercise. This team was small enough to do its planning as a committee-of-the-whole (9 people). The way that the leader managed the activity meant that the team could have been smaller or larger and not much would have changed. They did not seem to lack and specific subject matter expertise. The space allotted for this team made them too large by about 2 people.

8. **To what degree did the team members know each other beforehand? How did this (un) familiarity affect team dynamics?**
   RDD Team Observer: The leader knew everyone, some of the team members knew each other, it may have accelerated the development of their comfort with each other – without a comparison group, I can't tell.
   Bio Team Observer: The leader didn't know the team members and they didn't know each other. This meant that they would have had to have spent much more time in introductions to be able to appreciate what each individual might have brought to the plan. This contributed to the result that members did not defer to others with expertise.

9. **Did politicking for particular plan options ever emerge? If so, what were the dynamics associated with this? Did "alliances" form within the team? To what degree did these alliances impact which ideas "won out"?**
   RDD Team Observer: Most of the politicking was in the context of the sub rosa power struggle between the leader and one other member. Other members generally did not take sides, but let the two play it out.
   Bio Team Observer: One individual drove *every* topic in general discussion (remember the leader and one other member were doing their planning in parallel). In addition, the dominant conversationalist introduced *most* topics. He would defend his idea until the other person gave up. He would, from time to time, take over someone else's idea and push it as hard as his own. The result was that the number of ideas generated was much larger than the number of ideas considered. In terms of the final decisions made by the leader and his assistant planner, the dominant voice was sometimes ignored and sometimes validated. Once the leader had clearly stated the plan, the dominant voice would let go and there was never a direct challenge of the leader for leadership.

10. How did personality assert itself in these exercises?

RDD Team Observer: (see #3)

Bio Team Observer: Personality determined the process and the content.

11. Based on what you observed what impact do you believe distribution of the team and the use of electronic collaboration has on team dynamics?

RDD Team Observer: It would be a completely different process. There was a great deal of simultaneous conversation and input particularly in the early stages that would be forced into a linear format

Bio Team Observer: This team organically followed multi-level and non-linear paths throughout the game. The two times that the Black team needed explicit information that this team hadn't generated, getting that information disrupted the team flow. Their leader didn't constrain the team to linear processes. If location and electronic communication were issues that forced linear processes, then the team dynamic would be radically different.

DISTRIBUTION:

Joseph Ball
2084 State Hwy 230
Laramie, WY 82070

William M. Glanton
270 Brookshire Place SW
Ocean Isle Beach, NC 28469

Joseph Markowitz
9514 Georgetown Pike
Great Falls, VA 22066

Argonne National Laboratory
9700 S. Cass Ave.
Argonne, IL 60439
Attn: David F. Brown

Central Intelligence Agency
7036 E. Monte Ct
Mesa, AZ 85208
Attn: Martin Martinez

Central Intelligence Agency
Washington, DC 20505
Attn: Timothy Thomas
Joseph Keogh
Robert Wallace
Allison Yezril

Defense Threat Reduction Agency
8725 JJ Kingman Road Stop 6201
Ft. Belvoir, VA 22060
Attn: David Hamon
Mark Kane

Department of Homeland Security
7th & D Streets SW
Washington, DC
Attn: Steve Chase
Gary Strong

Institute for Defense Analysis
Mark Center Drive
Alexandria, VA 22311
Attn: Thomas Richards

National Security Agency
9800 Savage Road
Ft. Meade, MD 20785
Attn: Arthur H. Becker, Jr. (10)
William Butterfield, Suite 6655
Stephen Dennis
Kimberly McVaney
Michael Peters, Suite 6786
Donna Irene Walsh, Suite 6222
Elizabeth Walton, Suite 6158
David Darchicourt

U.S. Naval War College
686 Cushing Rd,
Newport, RI 02841
Attn: Charles H. Breen

U.S. Department of Defense
711 Chamberlain Ave, Bldg 24701
Ft. Gordon, GA 30905
Attn: Katherine Wilson

U.S. Department of State
2201 C Street NW
Washington, DC 20520
Attn: Mark Caudil

MS0425	Leonard Connell, 9745	
MS0784	Ray Parks, 6512	
MS0839	Curtis Johnson, 16000	
MS0839	Gerry Yonas, 16000	
MS0839	Jessica Turnley, 16000	
MS0839	John Whitley, 16000	
MS0839	Judy Moore, 16000	(10)
MS0839	Rick Craft, 16000	
MS0839	Tom Karas, 16000	
MS0839	Wendell Jones, 16000	
MS0961	Joe Harris, 14020	
MS1137	Greg Conrad, 6544	
MS1137	Marilyn Warrant, 6544	
MS1137	Olin Bray, 6544	
MS1138	Shelley Eaton, 6536	
MS1176	Dwight Miller, 15312	
MS1217	Jim Corey, 5913	
MS1219	Bill Tedeschi, 5923	
MS1219	Irene Dubricka, 5941	
MS9951	Dave Reichmuth, 8358	
MS0899	Technical Library, 9616	(2)
MS0616	Patent and Licensing Office, 15000	
MS9018	Central Technical Files, 8945-1	