IDA

INSTITUTE FOR DEFENSE ANALYSES

Defender's Edge: Utilizing Intelligent Agent Technology To Anticipate Terrorist Acts

L. B. Scheiber, Project Leader

June 2003

Approved for public release; distribution unlimited.

IDA Document D-2849

Log : H 03-000891

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
00 JUN 2003	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Defender's Edge: Utilizing Intelligent Agent Technology to Anticipate Terrorist Acts	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Institute for Defense Analyses, 4850 Mark Center Drive, Alexandria, VA 22311-1882**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**UU**	**118**	

This work was conducted under IDA's independent research program, CRP 1089. The publication of this IDA document does not indicate endorsement by the Department of Defense, nor should the contents be construed as reflecting the official position of that Agency.

INSTITUTE FOR DEFENSE ANALYSES

IDA Document D-2849

Defender's Edge: Utilizing Intelligent Agent Technology To Anticipate Terrorist Acts

L. B. Scheiber, Project Leader
J. E. Hartka
R. S. Murch

PREFACE

The events of September 2001 dramatically demonstrated the need for the Nation to greatly improve its counterterrorism activities. IDA has shown that intelligent agents have the potential to process available data into knowledge that commanders could use to dramatically change the outcome of battlefield campaigns [Ref.1]. This same technology has significant potential to aid in the war on terrorism. However, the war on terrorism is new and is only beginning to be defined. Further, terrorism has many forms. Its elements seem to be everywhere; yet they are difficult to identify. Terrorists' intentions and plans are even harder to uncover.

On the other hand, the Nation has a significant number of organizations working on different aspects of counterterrorism. Most of these organizations maintain significant databases in support of their efforts. In general, these organizations do not share the contents of their databases with each other. The Nation is just beginning to examine the potential benefits of conducting integrated analyses utilizing data maintained by different organizations. One objective is to be able to anticipate and stop terrorist acts before they can be carried out. However, a coherent strategy to accomplish this does not yet exist. This briefing provides some initial ideas on how intelligent agent technology might aid that process.

This task was accomplished by the Institute for Defense Analyses (IDA). The study team consisted of Dr. Lane B. Scheiber (Project Leader), Dr. Joseph E. Hartka, and Dr. Randall S. Murch.

The study team would like to thank the reviewers, Dr. Joan F. Cartier, Dr. Dale E. Lichtblau, Dr. Thomas L. Allen, Dr. Ronald A. Enlow, Dr. Alfred I. Kaufman, Dr. Stephen M. Ouellettte, and Dr. Victor Z. Utgoff, for their insightful comments.

CONTENTS

Appendixes

INTELLIGENT AGENTS

SOFTWARE PROGRAMS THAT CARRY OUT FUNCTIONS, WHICH, IF DONE BY HUMANS, WOULD BE CONSIDERED TO EXHIBIT INTELLIGENCE[1]

[1] Professor Marvin Minsky, MIT, 1964.

OBJECTIVE

THE OBJECTIVE OF THIS EFFORT WAS TO CONDUCT SOME INITIAL RESEARCH AIMED AT IDENTIFYING POTENTIALLY IMPORTANT ROLES FOR INTELLIGENT-AGENT TECHNOLOGY TO AID IN THE WAR AGAINST TERRORISM. TWO AREAS IN WHICH INTELLIGENT AGENTS COULD SEEMINGLY PLAY SIGNIFICANT ROLES ARE:

- **DEVELOPMENT AND MAINTENANCE OF A REAL-TIME PICTURE OF TERRORIST ACTIVITY**
- **PREDICTING POTENTIAL OCCURRENCES OF TERRORIST ACTS SUFFICIENTLY WELL IN ADVANCE SO THAT THEY CAN BE PREVENTED**

THE SITUATION

- **BACKGROUND**
- **ISSUES**
- **AN EXAMPLE**

BACKGROUND

"Who are the terrorists?" is a very good question. They don't look significantly different from other people and, in general, they blend into society. It is what they are trying to do that makes them different. Simply put, terrorists seek to injure or destroy our country, our economy, and our way of life. They believe they can reach these objectives by attacking our citizens and infrastructure and by creating mass fear. As we saw on 9/11, and with other attacks, their weapon of choice is anything that is capable of bringing about these objectives. As we also saw, they obtain the needed resources in many different ways, including acquiring them in-country or importing them, if necessary. Their planning, preparation, training, and practice efforts are generally designed not to attract attention although they may conduct trials to see if we do, in fact, observe specific activities. Their organizations are usually small and disciplined—often called cells. The cells are, at most, loosely coupled. Orders come from above—at times by nonstandard means like clandestine communications or specific words imbedded in a speech by a ranking principal.

The United States has many organizations working on counterterrorism including the FBI, the CIA, and the newly formed Department of Homeland Security with its Customs Service, the Immigration and Naturalization Service (INS), and the U. S. Coast Guard. The Department of State also has a role as do many organizations in the Department of Defense.

BACKGROUND

- **KEY QUESTIONS**
  - **Who are the terrorists?**
  - **What are they trying to do?**
  - **What personal and other resources, information, and opportunities do they need to perform their mission?**
  - **How do they get what they need?**
  - **How do they organize, plan, train, practice, and execute?**
- **MANY ORGANIZATIONS ALREADY ASSIGNED COUNTERTERRORISM MISSIONS**

BACKGROUND (continued)

The execution of a terrorist act is an integrated, multi-faceted process with at least four elements: (1) organization, intentions, plans, and motivation; (2) resources, including people and funding; (3) weapons, or material to make them, and appropriate delivery system; (4) opportunity including an appropriate target and a timeframe that will result in the desired impact.

However, our current intelligence-gathering and crime-fighting organizations have not been set up to analyze or even obtain appropriate data to cover the full range of activities that take place during the period from the conceptualization of a terrorist act to its execution. Further, many of these organizations are relegated to reacting to terrorism rather than anticipating or predicting it, largely because systems, tools, and training do not exist to enable then to operate differently.

What then are the problems? A number were illustrated by 9/11. For example, each counter-terrorism organization has a different set of responsibilities. Each organization collects data related to its mission and area of responsibility. Data collected by one organization is generally stored in that organization's stove-piped repository system and are not readily available. For the most part, these systems are not connected to the systems of other organizations. Further, the data are not adequately mined, exploited, or shared across organizations in a synergistic way. In some cases, the laws do now allow sharing. although this problem has been lessened by the Patriot Act [Ref. 2]. Finally, there is no approved concept for an integrated approach to collect and analyze the data required to counter terrorism. Simply merging organizations or requiring integration is insufficient. A clearly defined game plan is needed with organizational responsibility explicitly defined such that intelligence gathering is combined and analyzed as a whole with results expeditiously delivered to those responsible for taking action.

BACKGROUND (continued)

- **EXECUTION OF A TERRORIST ACT IS AN INTEGRATED, SEQUENTIAL, MULTI-FACETED PROCESS**
- **U.S. EFFORTS TO COUNTER THIS TYPE OF CRIME HAVE BEEN SEGMENTED—DIFFERENT PARTS OF THE PROCESS ARE THE RESPONSIBILITY OF DIFFERENT INTELLIGENCE GATHERING AND CRIME FIGHTING ORGANIZATIONS:**
  - **No single organization responsible for all aspects of the process**
  - **Segmented, uncoordinated data collection**
  - **Data stored in stovepiped systems**
  - **Data not adequately mined, analyzed, or shared**
  - **No integrated view or approach**
  - **Quality and perspective of analyses may vary between organizations**

OPERATIONAL ISSUES

Terrorism against U.S. assets has occurred for many years. However, the proximity and magnitude of that seen on 9/11 both here and abroad generated realization that our intelligence-gathering and crime-fighting organizations were not designed to detect and stop this type of crime—at least not in any integrated way. Rather each organization was set up with a particular set of responsibilities that, in general, do not overlap. Further, existing laws are not clear on how these organizations should work together to prevent this type of event. Some examples are shown in this viewgraph. Finally, non-overlapping areas of responsibility can create seams that terrorists may try to exploit to reduce detection.

Another significant problem in fighting terrorism is the orientation of our crime-fighting organizations. Many, if not most, of our crime-fighting organizations are reactive rather than proactive. That is, they are trained to respond to a criminal act and extract all relevant data from the scene after the crime has occurred. They use these data to help track down and prosecute criminals under rules of engagement that are determined by the criminal justice system. Terrorists must be stopped before they can commit their acts. In the war on terrorism, the normal crime scene may not exist. While it is normal for criminals to try to hide their crimes, terrorists want to publicize their acts to obtain the maximum terror response. While some criminals might not carry out a crime if it means going to jail, some terrorists are even willing to die to carry out their acts. While criminals generally act at the level of people, local business, etc., terrorists act at a level to impact society, national economy, etc. This suggests that, while reactive law enforcement may be adequate to deal with the common or even sophisticated criminals, proactive, anticipatory law enforcement is required to adequately fight terrorism.

OPERATIONAL ISSUES

- **TERRORISM CROSSES OPERATIONAL AND MISSION BOUNDARIES OF THE ORGANIZATIONS ESTABLISHED TO COUNTER IT. FOR EXAMPLE:**
  - **CIA and cooperating foreign services focus on foreign activity, especially intelligence gathering and "special activities"**
  - **U.S. Customs attempts to prevent the inflow of contraband**
  - **U.S. Immigration and Naturalization Service attempts to prevent illegal and questionable immigration, as well as monitor visits by foreign nationals**
  - **FBI focuses on violations of federal law involving U.S. national security and cooperates with police and security service of cooperating foreign nations**
  - **Many other federal organizations, such as Secret Service, Department of State, Department of Defense, Department of Homeland Security, etc., also have counterterrorism roles**
  - **Many state and local agencies also have roles most associated with public safety**
- **CRIME FIGHTING ORGANIZATIONS ARE REACTIVE, CRIME INVESTIGATION AND PROSECUTION ORIENTED. TERRORISM REQUIRES A PREDICTIVE, ANTICIPATORY, AND PREVENTATIVE ORIENTATION.**

ANALYTICAL ISSUES

As our information-gathering and crime-fighting organizations developed, so did their character and methodology—within the prescribed "rules of engagement" (laws, regulations, and policies). How they operate and the ways in which they measure their effectiveness developed as well. Today, each has its own data collection process and database(s) for storing those results. Each also has its own approach to analyzing its data as well as long-standing internal procedures and products for identifying threats according to its areas of responsibility. However, there has been little, if any, requirement for one organization to share data with another such that an integrated view can be developed and provided to the decision makers as well as appropriate law enforcement organizations. In some cases, sharing of data between organizations has been prohibited by law or by the current interpretation of the law.

The solution to this problem is not just sharing more data. The solution also needs to address what needs to be shared, when it needs to be shared and with what other organizations. Answering these questions requires a clear understanding of what the receiving organizations will do with the data when they receive it.

ANALYTICAL ISSUES

- **EACH ORGANIZATION PURSUES ITS OWN MISSION IN THE CONTEXT OF ITS OWN MEASURES OF EFFECTIVENESS (MOE) AND CULTURE.**
  - **FBI & DoJ Example: Because of its charter and history, the FBI and the Department of Justice might reasonably approach their analyses from the standpoint of building a legal case, and their primary MOE might well be the expected probability of getting a conviction in a U.S. trial.**
  - **CIA Example: Because of its charter and history, the CIA might reasonably approach its analysis from the standpoint of assessing all dimensions of a threat to prepare for an overseas counter-terrorist operation. The primary MOE might be the extent and accuracy of the data that supported the operation.**
- **EACH ORGANIZATION HAS ITS OWN COLLECTION PROCESSES, DATABASES, AND ANALYSIS PLANS, PROCEDURES, AND PRODUCTS FOR IDENTIFYING THREATS OR OTHER ELEMENTS THAT NEED SCRUTINY.**
- **FEW, IF ANY, REQUIREMENTS TO SHARE DATA OR METHODS WITH OTHER ORGANIZATIONS TO ENABLE THE DEVELOPMENT OF AN INTEGRATED VIEW. IN SOME CASES, SHARING IS PROHIBITED BY CURRENT LAWS.**

AN EXAMPLE

None of our current intelligence-gathering and crime-fighting organizations have been set up to analyze or even obtain data that cover the full range of activities that take place from the time a terrorist act is conceived until it is executed.

One means a terrorist organization might use to bring weapons or weapon material into the United States is to hide it in a shipping container. About 17,000 shipping containers arrive in the United States every day, only a small percentage of which can be searched. Many people have at least some access to the containers as they move from the original shippers to the ultimate recipients. Thus, identifying the best containers to search for contraband is a complex task. As shown on the viewgraph, a number of U.S. intelligence gathering, homeland security, and crime-fighting organizations have responsibility for collecting information that might be helpful in making that selection, but there is no current system for collaboratively integrating and analyzing that data and providing the results to organizations responsible for acting on it.

AN EXAMPLE

IDENTIFYING SHIPPING CONTAINERS THAT MIGHT CONTAIN TERRORIST WEAPONS OR EXPLOSIVE MATERIAL IS ONE STEP IN THE COUNTERTERRORISM PROCESS. HOWEVER, DIFFERENT ORGANIZATIONS ARE RESPONSIBLE FOR DIFFERENT PARTS OF THIS PROCESS. FOR EXAMPLE:

- **U. S. Customs Service is responsible for assuring containers do not contain any illegal material.**
- **CIA is a likely source of data about the background and threat profile of the original shipper as well as the other organizations (and their people) that have access to the container as it is packed and moves along its path to the United States.**
- **CIA is also likely to have information on the source and characterization of weapons and other material that terrorists are likely to try to ship, including shipping timeframe.**
- **FBI is generally responsible for identifying the threat potential of various people and organizations handling the container after it arrives in the United States.**
- **Knowing who has had or is expected to have access to the different containers could provide the cues needed to identify which containers to inspect. However, all of the data necessary to make these decisions are not currently contained in the customs database [Ref. 3].**

A WAY FORWARD

- **WHAT'S NEEDED?**
- **THE CONCEPT**
- **AN EXAMPLE**
- **EMPLOYING INTELLIGENT AGENTS**
- **A COMPARISON OF THE CHALLENGES**
- **NEXT STEP**

WHAT'S NEEDED ?

- **AN INTEGRATED VIEW WITH**
  - **Real-Time Picture**
  - **Prediction**
- **INFORMED DECISION MAKERS**
- **LINKED LAW ENFORCEMENT**

NEED AN INTEGRATED VIEW

As already discussed, the carrying out of a terrorist act involves a significant number of activities such as developing an organization; planning the act; setting up adequate communications; acquiring appropriate skills, weapons material, and funding; and providing training, housing, and transportation for terrorist personnel. Generally, each activity is conducted in such a way as to minimize the potential to generate any suspicious characteristics.

As the events of 9/11 showed, data collected by individual organizations did not sufficiently raise concerns within the collecting organizations to initiative preventative action. Further, the data were not generally shared with organizations outside of the collecting organization. However, analyses since 9/11 have indicated that a correlation of the data across these organizations might have provided an early indication of the pending terrorist attacks. As we move forward in the development of the organizations that have counter-terrorism responsibilities, we must be sure that our approach to collecting and analyzing data leads to an integrated view—one that not only provides a near-real-time picture of the terrorists' activities, but also provides predictions of pending terrorist acts sufficiently well in advance that they can be prevented.

NEED AN INTEGRATED VIEW

- GENERALLY, EXECUTING A TERRORIST ACT INVOLVES A SPECTRUM OF ACTIVITIES ACCORDING TO A TIME SEQUENCE.
- EACH IS USUALLY CONDUCTED IN SUCH A WAY AS TO MINIMIZE ATTENTION.
- OBSERVATIONS ON MOST ACTIVITIES, WHEN TAKEN ALONE, ARE DESIGNED NOT TO APPEAR SUSPICIOUS.
- GLOBAL ACTIVITY PATTERNS, DERIVED FROM DATA ACQUIRED FROM MULTIPLE ACTIVITIES ARE NEEDED TO GENERATE A PICTURE THAT CAN REVEAL TERRORIST ORGANIZATIONS, INTENSIONS, PLANS, PERSONNEL CAPABILITIES, TARGET OPPORTUNITIES, MEANS, METHODS, ETC., SUFFICIENTLY WELL TO PREDICT A TERRORIST ACT FAR ENOUGH IN ADVANCE THAT IT CAN BE PREVENTED.

OBTAINING AND UTILIZING AN INTEGRATED VIEW

One of the first steps is to identify the questions that need to be answered. Certainly characteristics of a pending act like what, when, where, how, why, and by whom are high on the list. Each of these questions leads to a more detailed set and so on. Whether or not these, as well as other, pertinent questions can be answered depends to a large degree on the data being collected, which leads to the next question. What are the data requirements? That is, what data are necessary to answer the questions? Are they part of the current data collection plan? Are they being collected? If not, can they be collected with current means? If not, what means can be developed to collect them?

Further, an organization must be assigned responsibility for carrying out the analyses that will provide the integrated view. This leads to another very important question—data access. Assuming that the right data are being collected, where is it stored and how does the "new"[2] organization obtain timely access to it? Further, are the data stored in a usable form and can different "pieces of data" be correlated among the different databases?

Given timely access, the data need to be processed. Processing in this sense means transforming the data into information and knowledge. It means finding the relationships among the data and translating those relationships into patterns that can be quickly recognized by humans as potential indicators of pending terrorist acts. It means doing it in near-real-time or at least quickly enough so that the results can be used to prevent attacks rather than just contribute to knowledge of how they occurred. This may require the development of advanced data-processing techniques and the software to automatically carry out the processing in such a way that predictive analysis is preformed. It also means identifying gaps in the data being collected and the knowledge that can be drawn from it so that improved collection efforts can be developed and put into place.

Given that timely access can be made available in the physical sense, can it be made available in the legal sense, e.g., will public policy permit it? Even with the Patriot Act, current laws still appear to limit the sharing of information among Government agencies, for example, data collected abroad by the CIA and the data collected within the United States by the FBI. Are additional changes to the laws required? If so, to what degree? Can a reasonable balance be maintained between the data needed and the privacy American citizens expect, or does the new war mean our presumptions need to be changed?

Further, there is the question of what the "new" organization does with its findings—especially the predictions. It must certainly keep the decision makers informed—probably on a near-real-time basis—given that they will need to make decisions based on the results of the integrated analyses. Further, the law enforcement organizations need to be linked because these findings will be fundamental to their task of preventing the terrorists' acts, as well as to all of the planning that is required to do that and to carry out the effort necessary to convict the terrorist. However, not every law enforcement

[2] "New" refers to the organization doing the integrated analyses.

OBTAINING AND UTILIZING AN INTEGRATED VIEW

- FORMULATE QUESTIONS AND DATA REQUIREMENTS TO ADDRESS THEM
- DEVELOP STRATEGIC PLAN TO BEST ACQUIRE THE DATA
- ASSIGN RESPONSIBILITY
- PROVIDE ADEQUATE ACCESS TO THE DATA
- DEVELOP ADEQUATE DATA PROCESSING CAPABILITIES
- MODIFY LAWS PROHIBITING DATA SHARING
- KEEP DECISION MAKERS INFORMED
- LINK-IN LAW ENFORCEMENT

OBTAINING AND UTILIZING AN INTEGRATED VIEW (continued)

organization needs every piece of data. Establishing which ones need what data, the means by which the findings are to be transmitted to the designated organizations, and the responsibility of the different law enforcement organization(s) to act on these findings as well as establishing safeguards for the data itself remain as challenges [Refs. 4-6].

Finally, is there an organization responsible for carrying out the integrated analyses? The Homeland Security Act of 2002 charges the Under Secretary of Homeland Security for Information Analyses and Infrastructure Protection with responsibility of analyzing information from various sources to identify threats of terrorism against the United States. However, it does not specify how these analyses are to be carried out or what organization is to do it. In his State of the Union address on January 28, 2003 [Ref. 7], President Bush announced plans for a new organization, the Terrorist Threat Integration Center, to be set up to integrate intelligence on terrorism collected at home and aboard. Details on this organization are just being developed such as its relationship with the Department of Homeland Security, from whom does it take direction, how and from whom does it get its data, what processing it is expected or required to perform, and what reports it will produce and to whom they will go.

A WAY FORWARD

- WHAT'S NEEDED?
- ➢ THE CONCEPT
- AN EXAMPLE
- EMPLOYING INTELLIGENT AGENTS
- A COMPARISON OF THE CHALLENGES
- NEXT STEP

THE CONCEPT

The objective is to develop indications of pending terrorists acts so that they can be stopped before the terrorists can carry them out.

As each counter-terrorism organization carries out its mission, it collects data associated with that mission. Although any one set of stand-alone data may not provide details of pending terrorist attacks, it may provide early indications of them. Some of these early indications could be used to trigger searches for collaborating data in other organization's databases. Data obtained from such searches could provide valuable insight into terrorist's plans and capabilities.

For example, analyzing terrorist material found in a shipping container and following it might enable Customs and the FBI to identify the terrorist who is to receive it. A search of the FBI's Foreign Terrorist Threat Task Force (FTTTF) database might indicate associates of the terrorist. A search of the INS database could indicate the origin and backgrounds of foreign visitors involved and their expertise.

The CIA may also be able to provide information on foreign nationals. The type of material intercepted along with the physical location and expertise of the group could be used to search the infrastructure databases [Refs. 8-10] to provide an indication of potential terrorist targets. It could also be used to focus the intelligence resources.

Arrival of terrorist material and/or imported expertise to use it or scheduled high profile events planned for the local area could provide an indication of the timeframe of the planned act.

THE CONCEPT

- **DESCRIPTION**
  - **Use correlations within stand-alone or stovepiped databases to provide indications of terrorist activity.**
  - **Use analyses across currently unconnected databases to identify terrorists' intentions, plans, organization membership, personnel capabilities, sources of support, opportunities, etc.**
- **EXAMPLE:**
  - **Detection and forensic exploitation of terrorist material in a shipping container could trigger search for terrorist connections as the container moves to its ultimate destination.**
  - **This information combined with other data could lead to an understanding of the terrorists' intentions, plans, and capabilities.**

(This page is intentionally blank.)

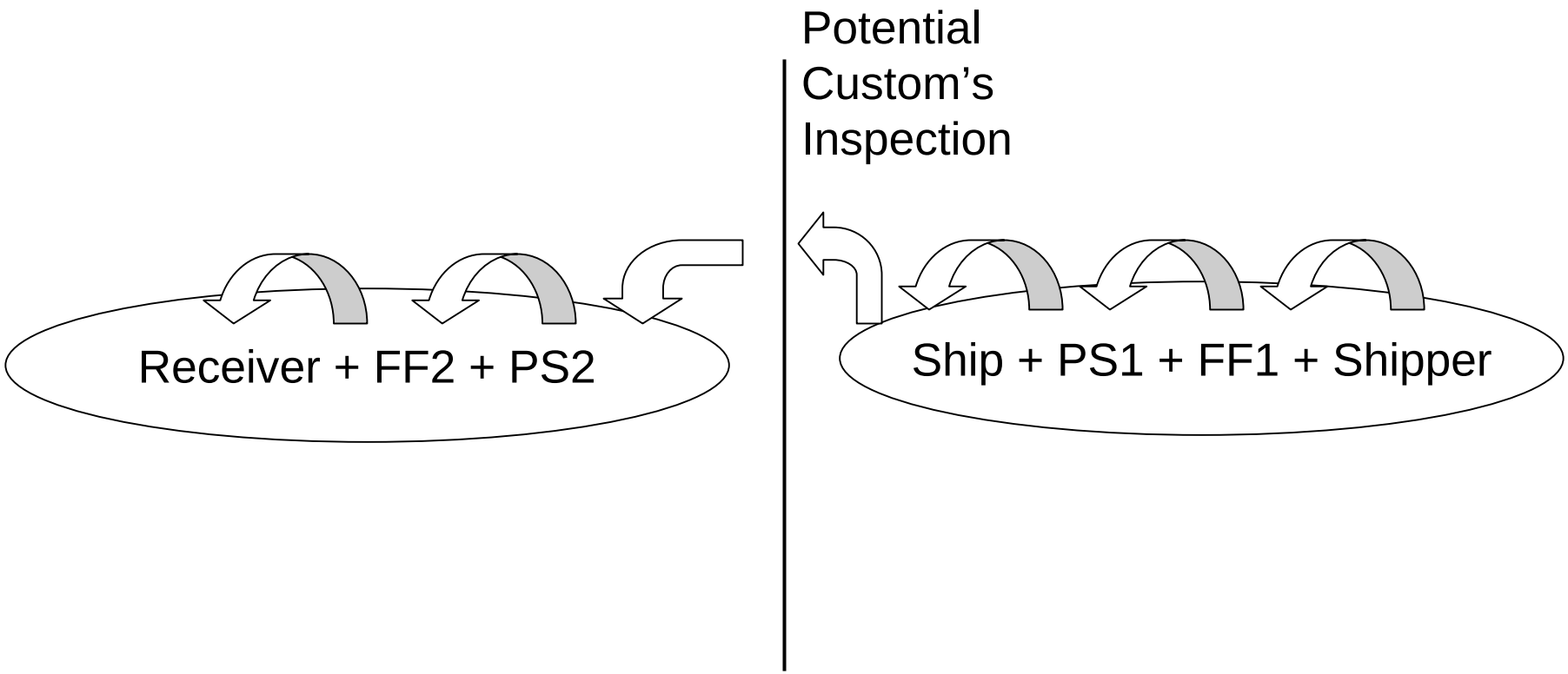
A WAY FORWARD

- **WHAT'S NEEDED?**
- **THE CONCEPT**
- **AN EXAMPLE**
  - **Shipping Container Problem**
  - **Need for Integrated Approach**
  - **Need for Automated Approach**
- **EMPLOYING INTELLIGENT AGENTS**
- **A COMPARISON OF THE CHALLENGES**
- **NEXT STEP**

THE SHIPPING CONTAINER SITUATION

In broad terms, the shipper packs a container and gives it to a freight forwarder (FF) to take it to the port. Port security (PS) guards it until it is loaded onto the ship. The ship carries it to a U.S. port where, if selected, it is inspected by U.S. Customs. It is then moved to the port holding area where port security guards it until another freight forwarder transports it to the receiving organization. A much more complete view of this can be found in References 3 and 11.

THE SHIPPING CONTAINER SITUATION



THE SHIPPING CONTAINER PROBLEM

Some of the containers shipped to the United States may contain terrorist material. Due to U.S. Customs resource constraints only a small number of the containers can be inspected. Thus, the problem is to identify those containers that have the highest probability of containing terrorist material.

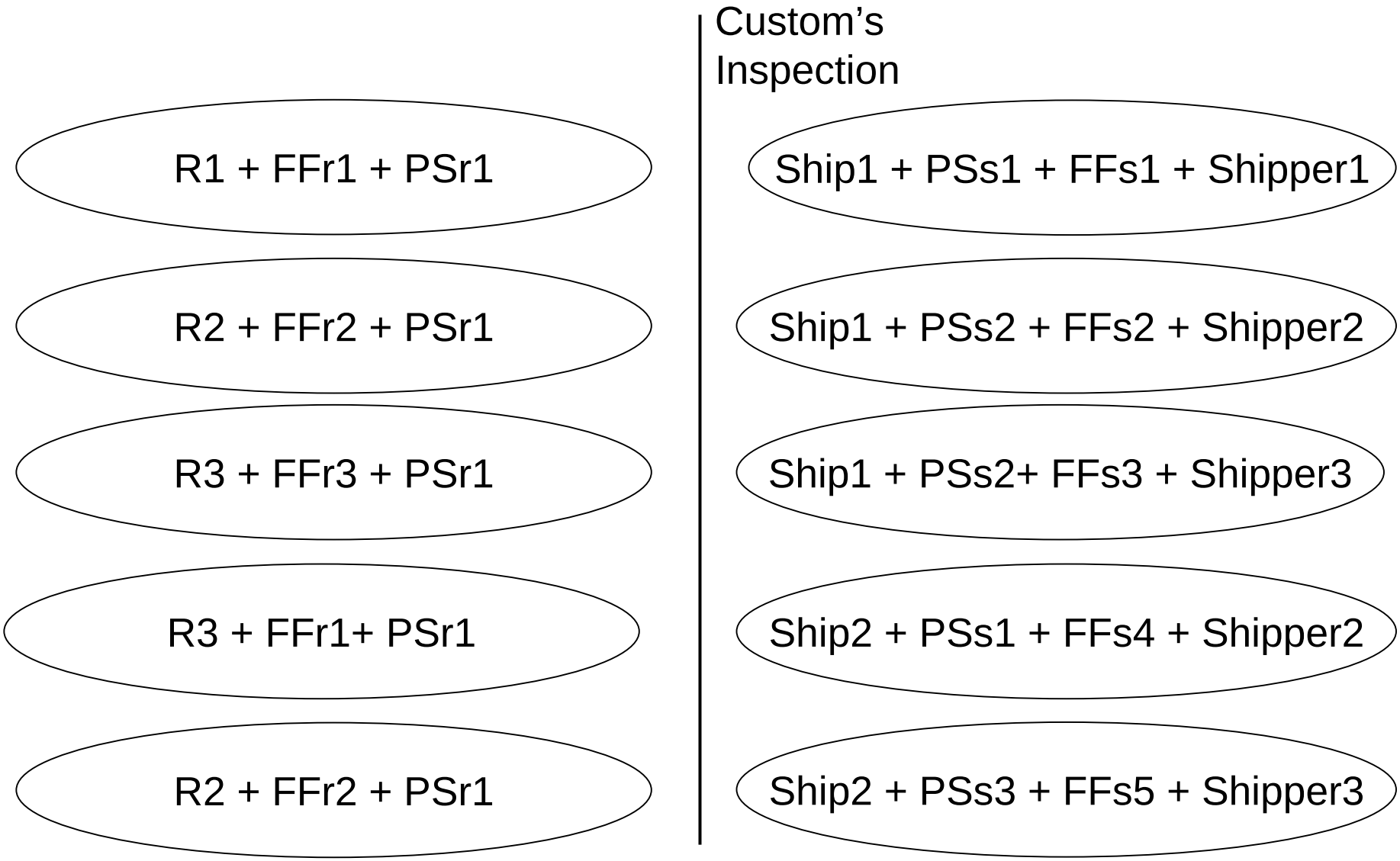
Using information about each of the organizations that has an opportunity to insert material into or remove material from a particular container, the likelihood of a given container carrying terrorist material can be calculated in a rather straightforward manner. Then, those with the highest score would give the highest probably of yielding terrorist's material.

This is a very simplistic view of the problem. Again, a more complete and general view is given in References 3 and 11. However, both views are oriented toward stopping the flow of inappropriate material into the United States. Since the simple view is sufficient for the current effort, we will use it here.

Just because the approach is simple does not mean that the task is insignificant. With some 500 container ships around the world, some able to carry more than 6,000 containers, trying to keep track of every person and every organization that has had access to every container that will eventually arrive in the United States is a formidable task.

Note: FFs1 = freight forwarder for shipper 1, PSr1 = security organization at port 1 that is receiving container, R = intended recipient, FFr1 = freight forwarder for recipient 1, PSS1 = security organization at shipper port 1.

THE SHIPPING CONTAINER PROBLEM

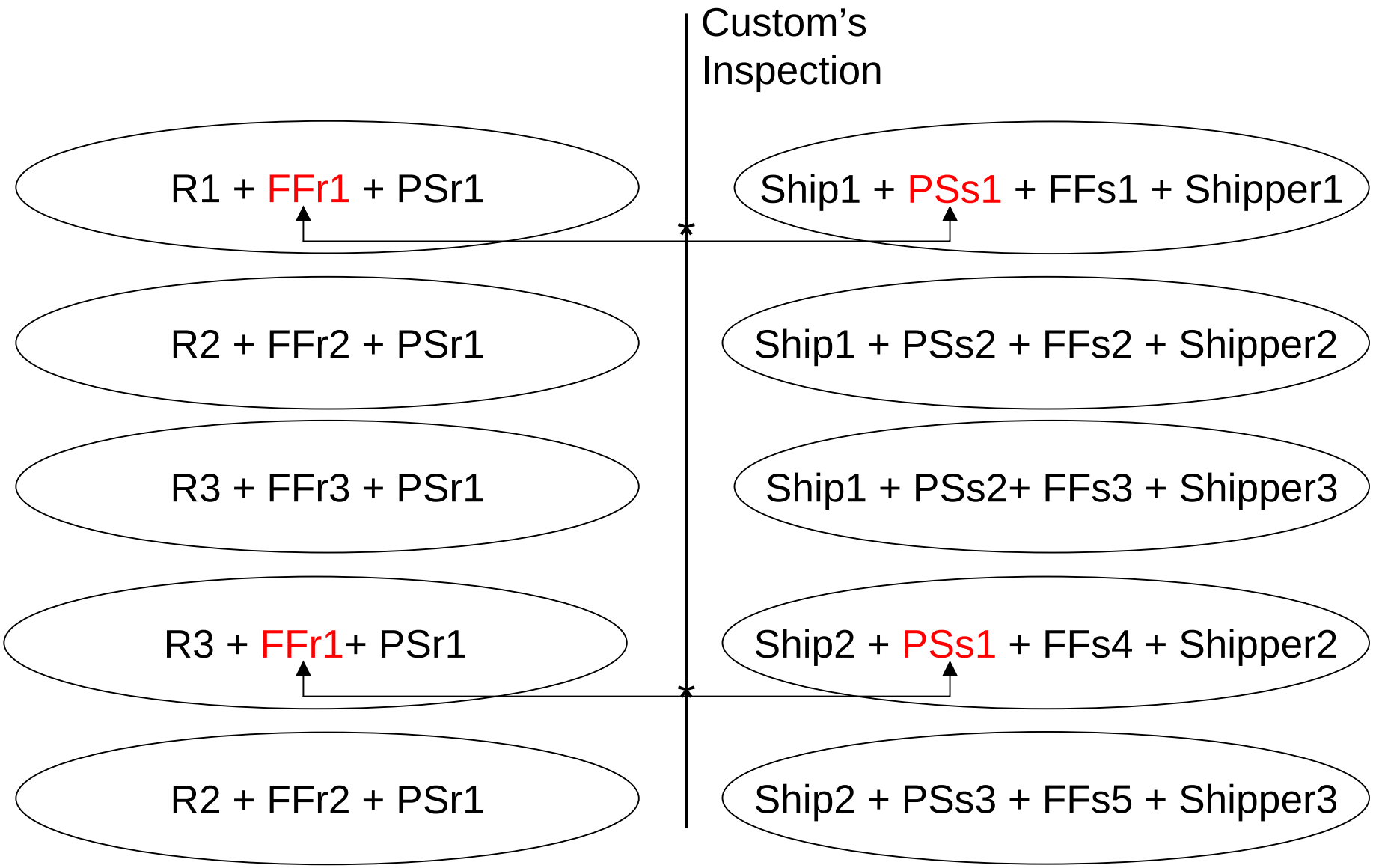


THE SHIPPING CONTAINER PROBLEM (continued)

Assuming that adequate means of identifying the containers to be searched as well as the resources to carry out the searches are available and that inappropriate material is being shipped, there is a high expectation that at least some of that material will be found. Removing terrorist material may very well slow up a terrorist operation, but it does not necessarily put the terrorist organization out of business. That requires, as a minimum, identifying the organization (person) that was to remove it. It may also be helpful to identify the organization (person) that inserted it. How might this be done?

One approach to identifying the involved individuals is to keep track of all of the shipping container data and to sort through the data to identify the common elements. As shown in the viewgraph, material was found in containers on ship 1 and ship 2. An analysis of the common elements shows that both containers were guarded by the same organization at the shipping port and were to be transferred to their respective receiving organizations by the same freight forwarding organization. Given the increased probability that these sending- and receiving-side organizations might be involved could add a degree of learning to the process.

THE SHIPPING CONTAINER PROBLEM (continued)



* Terrorist material found

OPTIONS AFTER DETECTING TERRORIST MATERIAL

Stopping the flow of contraband requires more than inspecting selected containers. The interest in it must be eliminated. Thus, finding those who have the interest may be the next step. Those interested might be divided into two categories—those that retrieve the material and transport it to the users and the users themselves. In general, the latter are of more interest than the former.

This chart shows some of the options that might be employed once terrorist material has been located in a container. To locate the intended users, one might leave the material in place, tag it, and follow it to its destination. One might also apprehend those who remove the material from the container and interrogate them. If the nature of the material poses an unacceptable risk, one might be able to replace the material with a non-useful look-alike. On the other hand, the situation might be such that the only timely alternative is to remove the material from the container and dispose of it in an appropriate manner.

Picking among the options necessitates a tradeoff of the risks involved versus the need to identify the intended users, and to some degree the supplier. While option 3 might seem to eliminate the risk, it might not. The terrorists may simply believe that the material got lost and order more. The next shipment might not be intercepted. This may also happen in option 2 if the terrorists believe that they were shipped faulty material. On the other hand, if the material is reordered, Customs will have another chance to identify the source.

OPTIONS AFTER DETECTING TERRORIST MATERIAL

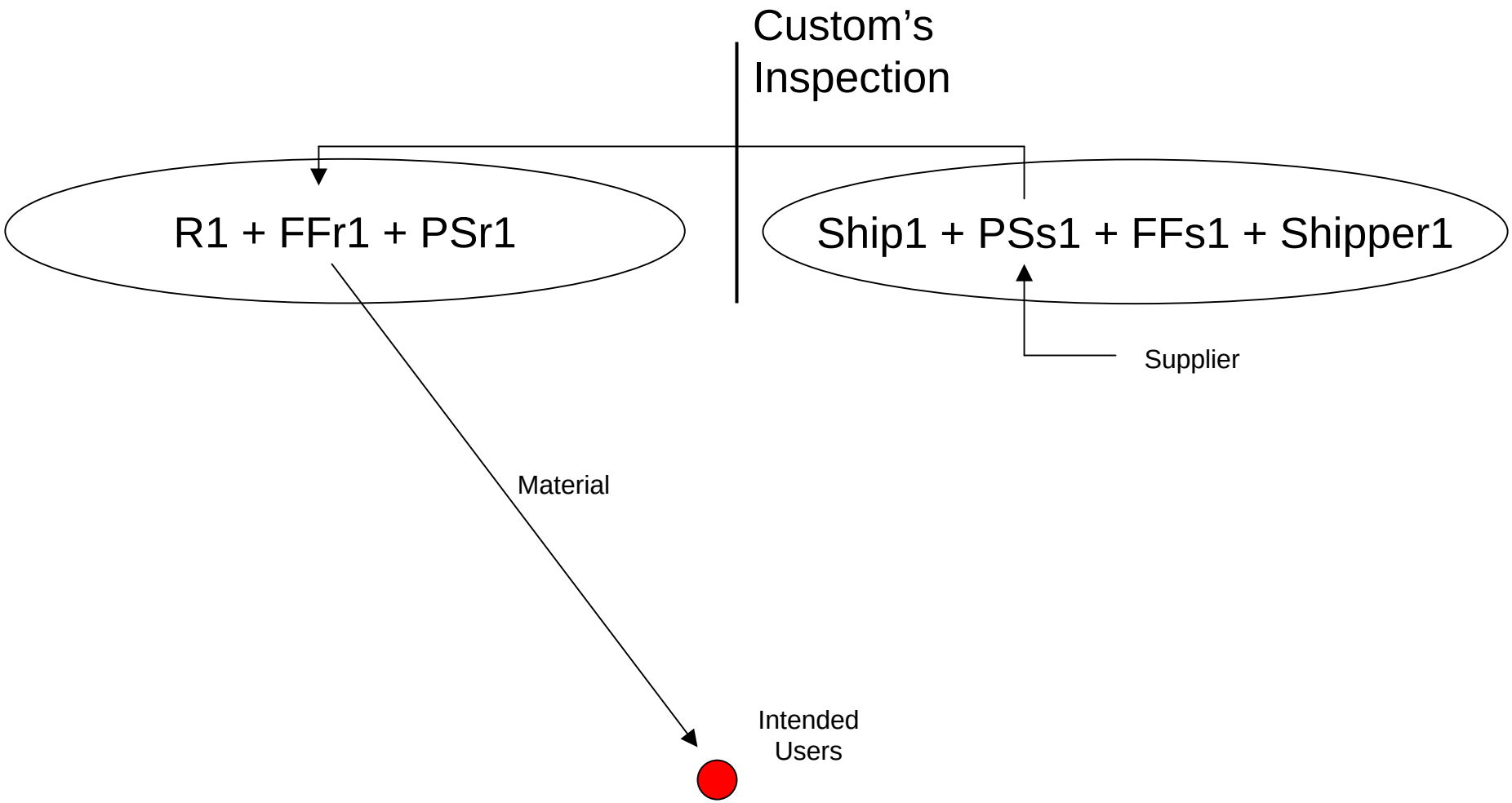
1. **IF NOT LETHAL, TAG IT, LEAVE IT IN PLACE AND:**
    a. **Apprehend and interrogate those who collect it**
    b. **Follow it to its intended users**
2. **IF LETHAL, REPLACE WITH NON-LETHAL LOOK-ALIKE, TAG IT AND:**
    a. **Apprehend and interrogate those who collect it**
    b. **Follow it to its intended users**
3. **REMOVE AND DISPOSE OF THE MATERIAL**

LIMITATIONS OF A STOVEPIPE APPROACH

However, as helpful as locating the supplier and recipient of the terrorist material might be, it does not ensure that the terrorist cell can be made ineffective or even identified. If a particular terrorist is eliminated, a replacement may be obtained. If a specific cell is eliminated, the job of carrying out the act may just be moved to another, yet to be discovered, cell.

To adequately understand the terrorist's intentions, additional data may be required, such as the identities of other terrorists in the cell, what they plan to attack, and the status of their resources. Further, to neutralize interest in the intended targets, the targets themselves need to be identified and provided with appropriate protection. Other similar targets may also need additional protection. These data may be contained in databases other than those maintained by the U.S. Customs Service. This reinforces the need for an integrated approach—the integrated analyses of data from many, if not all, of the organizations that collect data related to terrorists and their activities. However, collaboration is not part of a mandate in any federal agency's current mission [Ref. 12].

LIMITATIONS OF A STOVEPIPE APPROACH

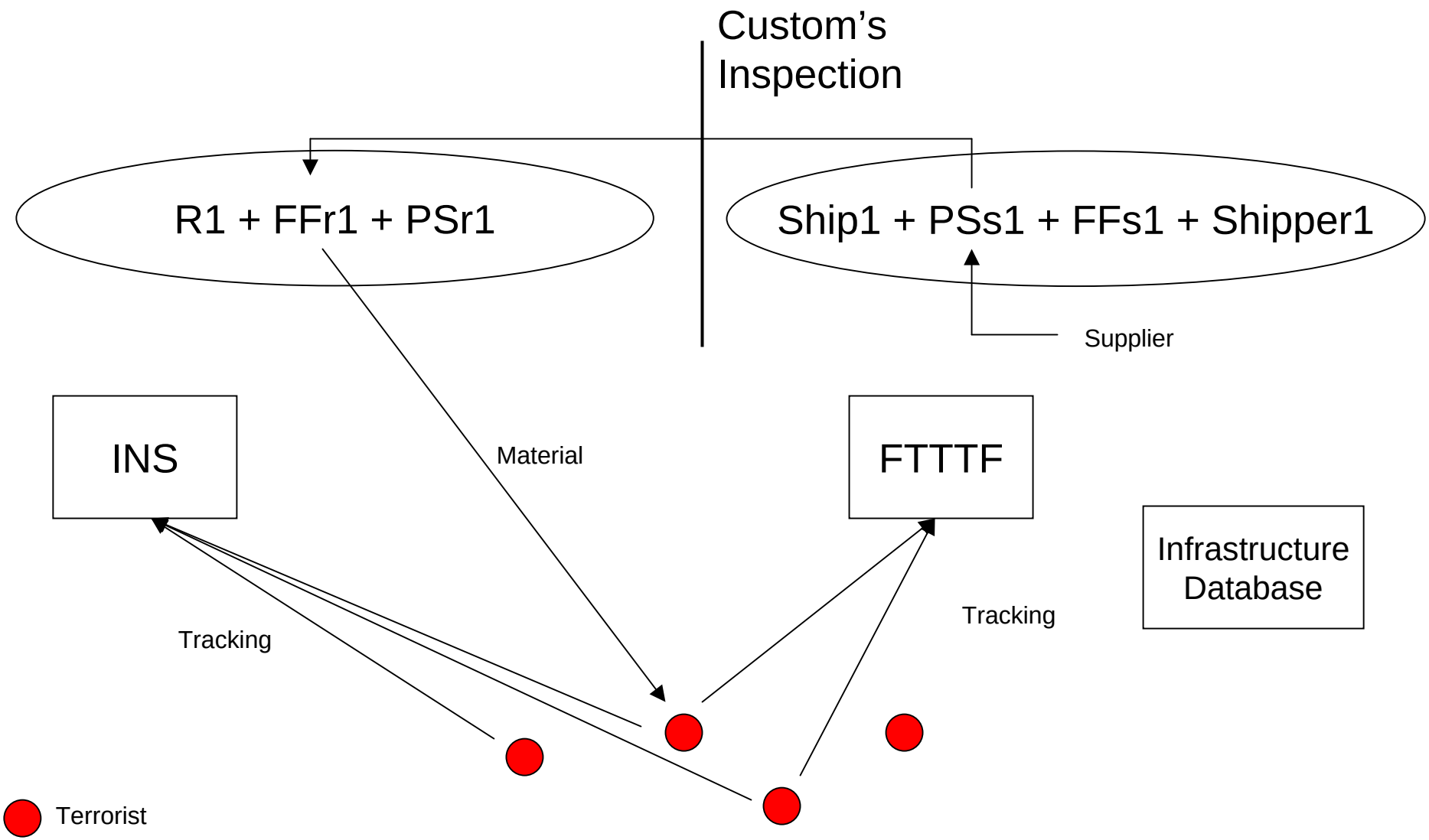


NEED FOR AN INTEGRATED APPROACH

As an example of the need for an integrated approach, consider the following. The Customs agents might note that a person from FFr1 delivered the terrorist's material to another person and note that in their database. However, they may not have information on this recipient. On the other hand, the FTTTF may know this person and that he belongs to a particular terrorist cell. It may also know others in the cell, some of whom may have only recently arrived in the United States. Their purpose might be to add specific expertise that the cell needs to carry out its pending mission. The INS system may have relevant information on their areas of expertise. Infrastructure databases [Refs. 8-10] have data on potential targets that could include how terrorists might plan to attack them and what resources would be required.

Each of these sets of data alone might be of limited utility in addressing the terrorist problem. However, when taken together and analyzed properly, a picture of a particular act might begin to emerge. The existence of a cell is of fundamental importance. The nature of the material and the fact that it has been delivered might indicate the type of attack and a timeframe. Likewise, the arrival of additional people with certain skills may add an indication of an emerging capability. Matching the type of targets in the area along with the resources needed to attack them might make the picture clear enough to identify the potential targets and a timeframe for the attack. If these elements are identified prior to the attack, the attack might be prevented.

NEED FOR AN INTEGRATED APPROACH



NEED NEW AUTOMATED APPROACH

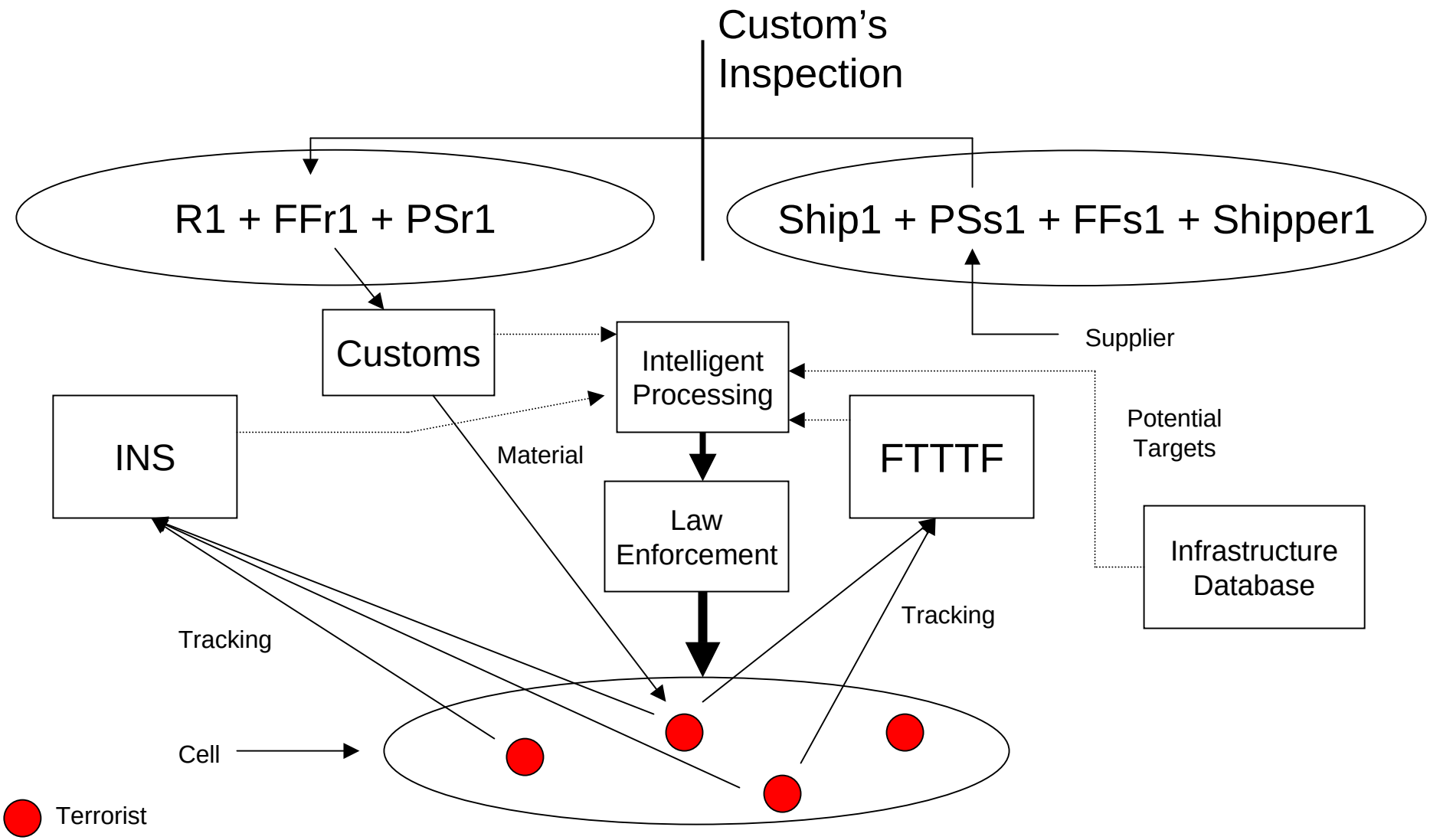
The sheer magnitude of all of the data being collected along with the classification and privacy issues would probably make a single database approach impractical. Further, even the stand-alone databases can be extremely large and are ever growing.

The processing necessary to locate and extract the relevant facts and to correlate these facts across the span and magnitude of the data necessary to develop the desired picture is beyond manual (human) capability. Further, the analysis needs to be done not once, but nearly continuously—generally as often as relevant data arrives, which could be on a second-by-second basis, 24 hours a day, 7 days a week.

Clearly some form of intelligent automation is required to continuously search such a large amount of ever-changing data to locate patterns that will not only help generate the desired picture, but also provide insight into terrorist intentions. Intelligent automation will also provide the capability needed to predict terrorist acts and prevent their occurrence.

Given adequate access to the necessary data, it should be no more difficult to do the final processing centrally, while the data itself is housed distributively in the databases of the collection organizations, than to have all of the data at the integration center itself. Having all of the relevant data at one location might make it a terrorist target. Additional automation may be required to provide a timely distribution of the results of these analyses to the organizations that are charged with using them, such as the decision makers and the law enforcement organizations.

NEED NEW AUTOMATED APPROACH



(This page is intentionally blank.)

A WAY FORWARD

- **WHAT'S NEEDED?**
- **THE CONCEPT**
- **AN EXAMPLE**
- **EMPLOYING INTELLIGENT AGENTS**
  - **Real-Time Picture**
  - **Prediction**
  - **Developing an Employment Concept**
  - **Other Potential Areas of Application**
- **A COMPARISON OF THE CHALLENGES**
- **NEXT STEP**

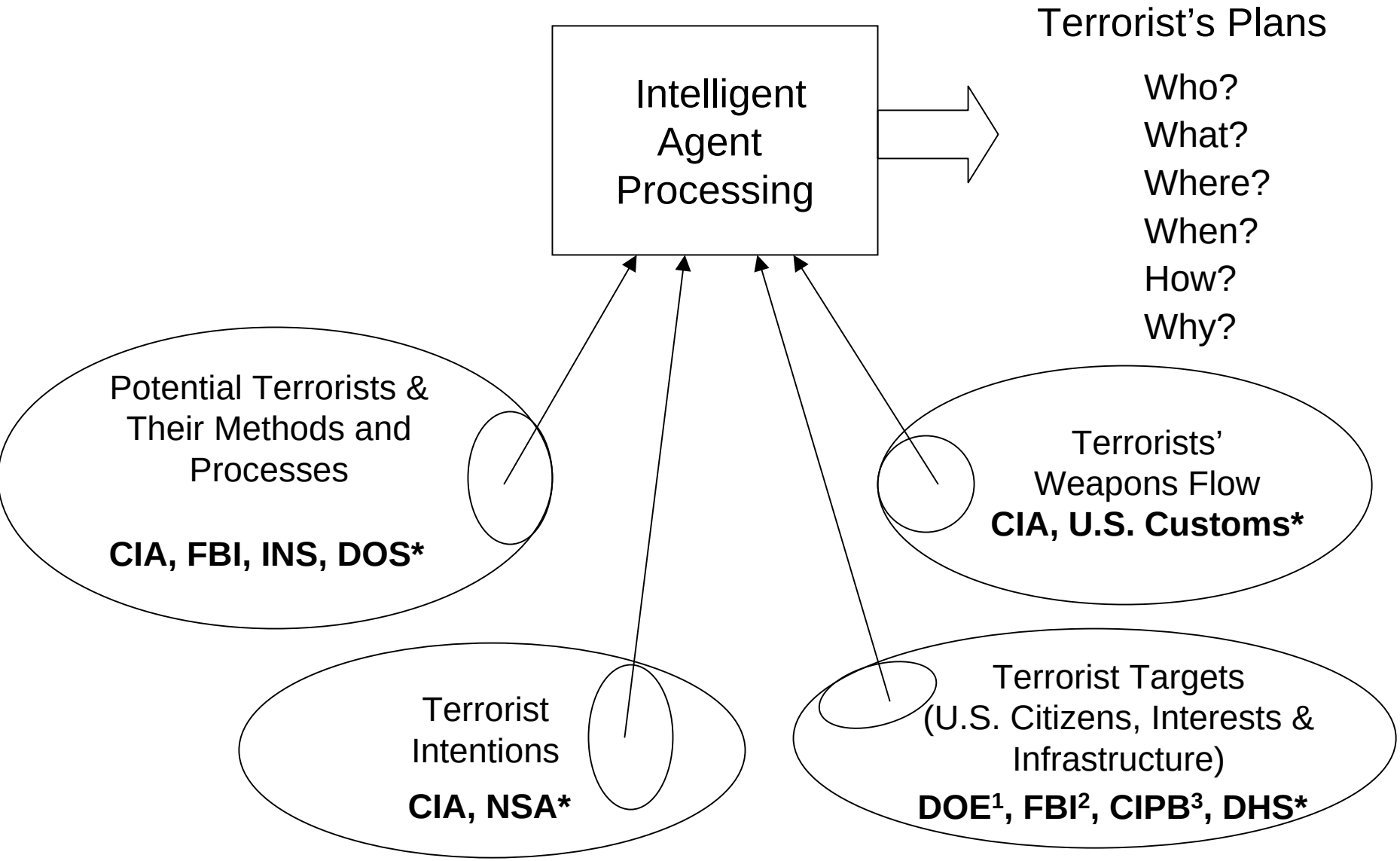
POTENTIAL APPLICATION OF INTELLIGENT AGENTS

There are many ways to analyze terrorist operations. One is to consider the process by which they aggregate the necessary elements. The example shown here divides the information into four major areas: the terrorists themselves, their intentions, their resources such as weapons or bombs, and target opportunities and vulnerabilities. The data about each of these elements are likely to be found in databases that are assembled and maintained by different organizations. Furthermore, cross-checks and collaboration will be necessary to fully exploit the potential of the data to reveal the terrorists' plans and capabilities.

The key issue is how to find patterns in the data that are consistent with an aggregation of the critical elements at a particular time and place. Given the large amount of data to continuously process, its ever-changing nature, and the desire for a near-real-time picture coupled with an indication (i.e., prediction) of the terrorists' plans and capabilities leads one to consider a form of intelligent processing. As noted above, intelligent agent technology has been shown to be able to quickly transform large amounts of data into information that humans can more easily and more quickly assimilate and act upon.

Finally, as has already been noted, it is not necessary to collect all the data in one place. It may even be counter-productive, given the number of organizations collecting data and the amount of data they are collecting. It is not even necessary that the databases be used to store the data of the same type. The key to an effective intelligent automation process is access. That is, it matters less where the data physically resides and what database system it is stored in than the degree of access the intelligent processing has to the data. In the current situation, it would appear preferable to keep the data distributed and only centralize the transformation of the data into the information needed to combat the terrorists. A center established to have all terrorism data might itself become a target.

POTENTIAL APPLICATION OF INTELLIGENT AGENTS



* Example of collector organizations

[1] Critical Infrastructure Protection Program
[2] National Infrastructure Protection Center (NIPC)
[3] President's Critical Infrastructure Protection Board

OPERATORS' VIEW

Intelligent agent technology has been applied to a number of different sets of data. The next three viewgraph show results from an application that utilized data generated in an experiment conducted by the Joint Forces Command in 1999 [Ref. 1]. The experiment was a large human-in-the-loop effort that examined new approaches along with technology expected in 2015 for locating critical mobile targets on the battlefield, such as enemy mobile missile launchers (called TELs) and the vehicles (called MTTs) that resupplied the TELs with missiles. The experiment generated multiple sets of data. The main set used by the intelligent agents contained data about vehicles on the battlefield.

More than 10,000 vehicles were on the battlefield, only 360 of which were military. All military vehicles belonged to the enemy force. The vehicular data were collected by multiple sensors and arrived at a rapid rate. It soon became voluminous. Sensor coverage was incomplete and data on any particular vehicle were intermittent and ambiguous. At times it was incorrect and misleading. These characteristics made the data extremely difficult for the human to handle.

This viewgraph provides an example of the view of the battlefield as seen by the operators. The yellow squares represent the vehicles "seen" by the sensors. Screen notations added by the operators are shown in black.

OPERATORS' VIEW

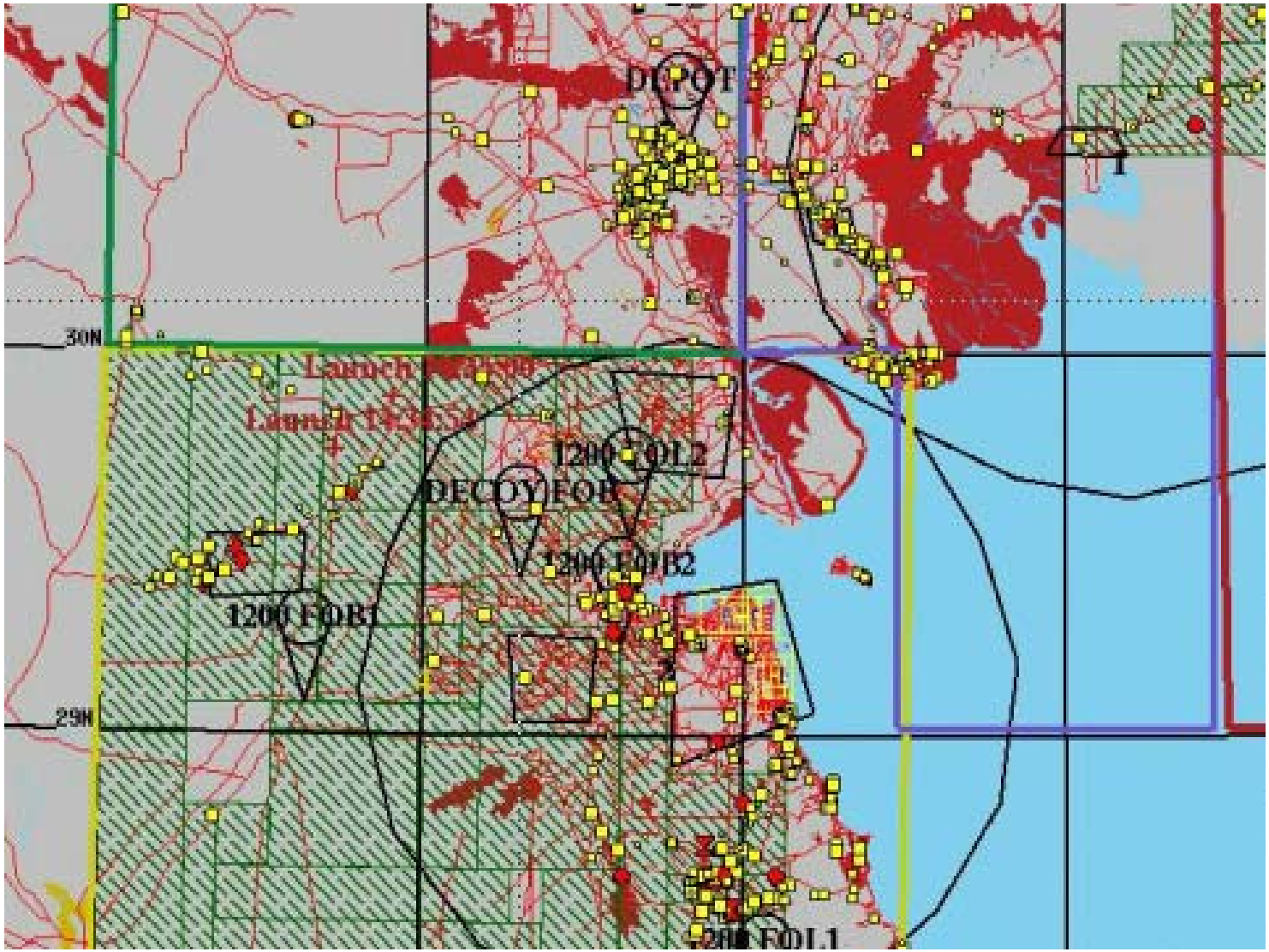


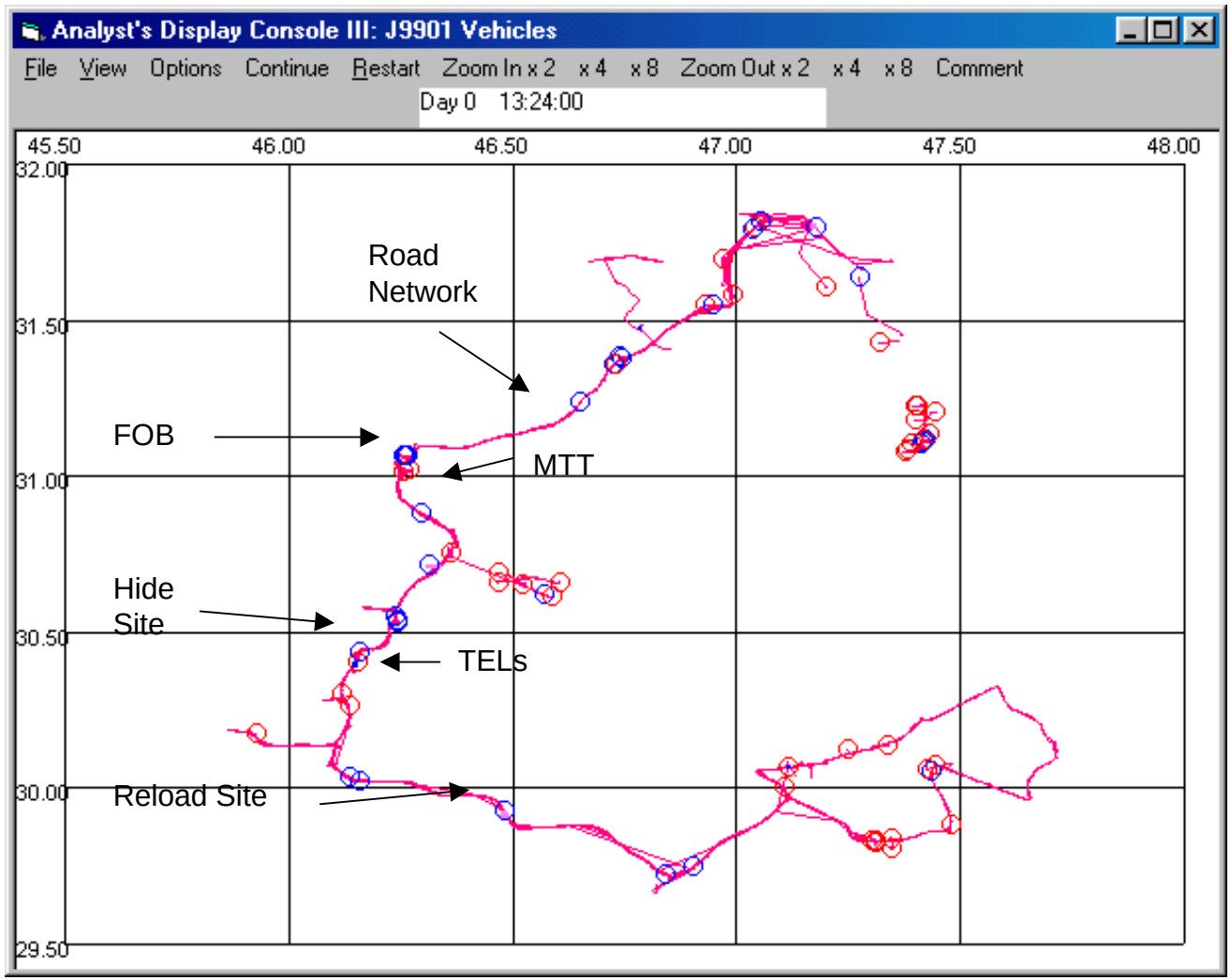
ILLUSTRATION OF AN INTELLIGENT AGENT APPLICATION
EXAMPLE OF OUTPUT

Inputs from the sensors were provided to operators at a rate of about 438 per minute. Each input was essentially a hit on a vehicle. Among other things, the input contained the vehicle's sensed position and 12 numeric values—each representing the probably of the vehicle being one of 12 types, which included cars, buses, and trucks as well as TELs and MTTs.

The intelligent agents were designed to transform these "pieces of data" into information humans could more readily use than that in the display shown on the previous viewgraph. Specifically, they were intended to identify locations of TEL hide and reload sites and the sites of forward operating bases (FOBs) (sites used to store and prepare the missiles). Operating at speeds of 20 to 100 times real-time, the intelligent agents were able to knit together the different "pieces of data" to provide a nearly seamless view of the enemy's mobile missile operation. This viewgraph shows a snapshot of that output. As shown, not only are the positions of the hide, reload, and FOB sites identified, but the current positions of the TELs and MTTs are illustrated as well. The intelligent agents even show the roads on which the TELs and MTTs are traveling. It is interesting to note that the intelligent agents needed only 0.6 of 1 percent of the data collected to provide this output.

In some ways, this example of a near-real-time picture might be considered analogous to observing terrorist activities. It tells what has happened but may not be helpful in indicating what is about to happen, such as a loaded TEL moving toward a firing location or a terrorist act that is about to take place. We must expand the analyses capability to provide results that enable us to predict hostile events.

ILLUSTRATION OF AN INTELLIGENT AGENT APPLICATION EXAMPLE OF OUTPUT



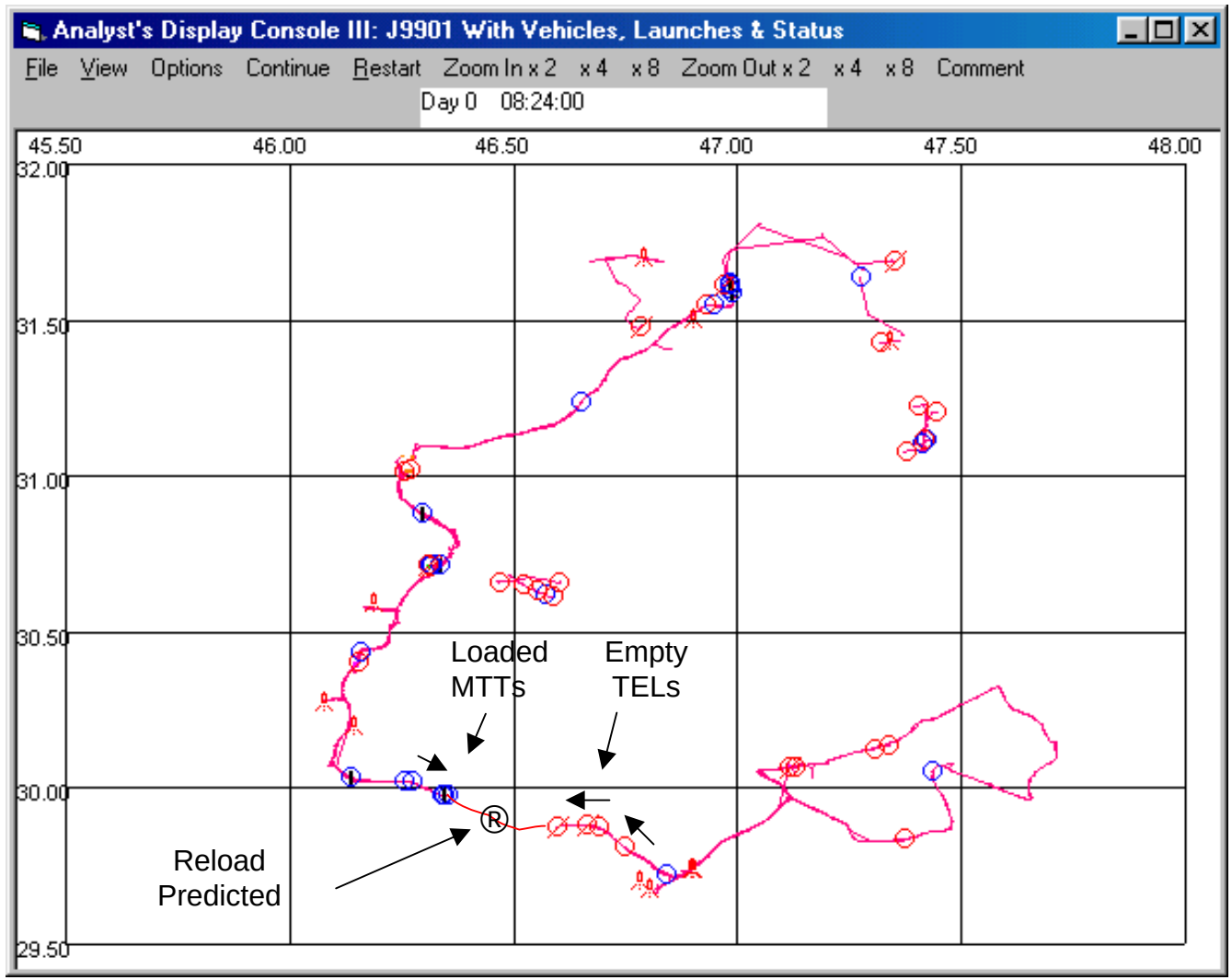
INTEGRATING DATA AND MAKING PREDICTIONS

The previous slide showed that intelligent agents have been used to extract patterns from large amounts of streaming data on vehicles. This slide shows that additional information can be obtained by utilizing additional data, that is, by combining the vehicle data with mobile missile launch data that was also available in the experiment.

Since TELs are the only vehicles that fire missiles, combining the missile firing data with the vehicle data provides vehicle type confirmation that could be used to initiate an attack. However, the firing data also serve to indicate that the TEL is now unloaded, i.e., no longer has a missile. While destroying an unloaded TEL removes one launcher from the enemy's arsenal, following it can provide an opportunity to locate a reload site and the FOB supporting it. Destroying these can significantly shorten the conflict.

Further, the knowledge that the TEL is empty can be used to predict the occurrence of a reload operation even before the site has been located. For example, the unloaded (empty) TELs shown in the viewgraph are moving down the road to the left. The loaded MTTs are coming from the left down the same road. Clearly they are going to rendezvous at a reload site. Knowing this in advance could be extremely valuable in allowing the blue force time to conduct effects-based analyses of potential attack strategies. In a similar fashion, certain information might be sufficient to indicate the potential for an act and to initiate steps to prevent its occurrence. This information includes knowing (1) a terrorist cell has a specific set of expertise, (2) the cell has material to make specific types of weapons, (3) the weapons are likely to be used against a certain set of targets, and (4) the targets are located in an area the cell can easily reach.

INTEGRATING DATA AND MAKING PREDICTIONS



STEPS IN DEVELOPING THE INTELLIGENT AGENTS

The first step in developing the concept was to define the problem the intelligent agents were to solve. In this example, it was to locate the TEL hide and reload sites and the FOBs.

The second step was to develop an understanding of the enemy's mobile missile operation as perceived by the friendly forces. Here it was determined that the enemy was using the sequence of Hide-Fire-Hide-Reload-Hide cycle. That is, a loaded TEL would move from its hide site to a launch site and fire. It would then quickly move to another hide site where it would remain for a period of time. It would then move to a reload site where it would receive a replacement missile from an MTT, which had recently arrived from the FOB. After being reloaded, the TEL would move to another hide site, and the MTT would return to the FOB. After a period of time, the cycle would be repeated.

Since this effort used data from an exercise, the next two steps were replaced by an examination of the available data to determine what relevant indicators it contained. It was found that, with appropriate processing, the positions over a period of time could be latitude/longitude grid of the battlefield area showing the TEL and MTT movements in real-time. Also to be shown on the display were the positions of the hide, reload, and FOB sites as they are being determined by the intelligent agents.

The next step was to develop the intelligent agent concept and the rules to be applied. In examining the enemy's operation it was found that (1) TELs hid alone—no MTT or other TEL were nearby, (2) the only time TELs and MTTs stopped in the same location was to reload the TELs, and (3) only the MTTs stopped at the FOB. Based on this, it was decided to use three intelligent agents: one to examine the data for each of the different types of sites. The hide site agent would look for locations where TELs stopped alone. The reload site agent would look for locations where TELs and MTTs stopped together. The FOB agent would look for locations where only the MTTs stopped.

Transforming the concept and rule set into computer code represented a significant challenge due to the limitations associated with the data (the experiment was designed to reflect the limitations expected on the battlefield). For example, vehicle track data were limited to short unconnected segments. A tracking agent had to be developed to connect the segments together so that the intelligent agents could determine where the vehicles were stopping as opposed to being overlooked by the various sensors. Once these limitations were overcome and the intelligent agents implemented, they were run against data from the experiment. The results are as shown on the previous viewgraphs.

STEPS IN DEVELOPING THE INTELLIGENT AGENTS

- DEFINE THE PROBLEM IN TERMS THE INTELLIGENT AGENTS CAN HANDLE
- DEVELOP AN UNDERSTANDING OF THE ENEMY'S OPERATIONAL CONCEPT COVERING THE DEFINED PROBLEM
- DETERMINE OBSERVABLES IN THE ENEMY'S OPERATION THAT PROVIDE INDICATORS RELATED TO THE PROBLEM BEING ADDRESSED
- ESTABLISH DATA COLLECTION AND ANALYSES PLAN
- DETERMINE HOW THE RESULTS OF THE INTELLIGENT AGENT PROCESSING ARE TO BE DISPLAYED; DEVELOP REQUIRED DISPLAY
- DEVELOP CONCEPT AND RULES FOR INTELLIGENT AGENTS
- TRANSFORM THE INTELLIGENT AGENT CONCEPT AND RULES INTO SOFTWARE
- TEST THE INTELLIGENT AGENT SOFTWARE AGAINST THE DATA

POTENTIAL STEPS IN DEVELOPING INTELLIGENT AGENTS FOR COUNTERTERRORISM

There is considerable parallel between the development of the intelligent agents to find the mobile missile sites and that of detecting certain indications of terrorism. Some of the potential steps are listed in this viewgraph.

The first step is still to define the problem the intelligent agents are to solve. Further, the problem needs to be defined in terms that the intelligent agents can handle. Once the problem is defined, the terrorist operation can be examined to determine what actions are meaningful predictors of pending terrorist acts. In developing a detailed understanding of the terrorist operation, it might be useful to start by creating a taxonomy of questions related to the terrorist organization and its members. An initial list of such questions is included in Appendix A.

Once a list of actions is compiled, the next question is what observables are available to provide visibility into the actions. For some actions, there may be no practical way of gaining visibility. For others, there may be overlapping potential. Thus, the next step is to develop a data collection and analyses plan. These two functions need to be coordinated. That is, collecting data without a notion of how it will be used may lead to a significant amount of irrelevant data being collected with a corresponding waste of data collection resources.

The concept and rules for the intelligent agents need to be developed to work in conjunction with the data analyses plan. In addition, the entire effort will have limited utility unless the results are appropriately distributed and displayed. In this case, appropriately means not only to the right organizations and in a timely manor, but also with adequate controls to protect privacy and to keep the information from falling into the hands of those against whom it is directed—the terrorists and those that support their efforts.

POTENTIAL STEPS IN DEVELOPING INTELLIGENT AGENTS FOR COUNTERTERRORISM

- DEFINE THE PROBLEM IN TERMS THE INTELLIGENT AGENTS CAN HANDLE
- DEVELOP AN UNDERSTANDING OF THE ENEMY'S OPERATION
- ASCERTAIN WHAT ACTIONS ARE MEANINGFUL PREDICTORS OF PENDING ACTS
- DETERMINE OBSERVABLES IN THE TERRORISTS' OPERATION THAT PROVIDE INDICATORS OF ACTIONS ASSOCIATED WITH THE MEANINGFUL PREDICTORS
- ESTABLISH DATA COLLECTION AND ANALYSES PLAN
- DETERMINE HOW THE RESULTS OF THE INTELLIGENT AGENT PROCESSING ARE TO BE DISPLAYED; DEVELOP REQUIRED DISPLAY
- DEVELOP CONCEPT AND RULES FOR INTELLIGENT AGENTS
- TRANSFORM THE INTELLIGENT AGENT CONCEPT AND RULES INTO SOFTWARE
- DEVELOP REPRESENTATIVE DATA IF NONE HAS YET BEEN COLLECTED
- TEST THE INTELLIGENT AGENT SOFTWARE AGAINST THE DATA
- DEVELOP, IMPLEMENT, AND TEST THE DATA DISTRIBUTION CONCEPT

OTHER POTENTIAL AREAS OF APPLICATION

There are a large number of areas that intelligent agents might potentially be able to help. Those shown here are aimed at uncovering potential patterns of activity that might be associated with terrorists' training or testing of techniques associated with an upcoming act.

The data on airplane crashes (including those of small planes), air traffic control violations, and train derailments, all of which are frequent occurrences, could be analyzed for changes to the normal patterns. This might be indicative of terrorist tests. Tracking selective types of missing material might provide an early indication of terrorist intentions. Analyses of hospital ER visits and discovery of animal and bird carcasses might indicate terrorist experimentation with biological or chemical agents.

Tracking passengers who have become ill while or after traveling on any major carrier could help pinpoint the source of the illness. It could help separate "natural" occurring events from those of terrorist attacks. This could be especially helpful in uncovering events that are less dramatic than the recent SARS (Severe Acute Respiratory Syndrome) outbreak. It could also help identify where the people who became ill went and with whom they came in contact along the way. This might be used to identify areas where additional medical resources are needed to minimize the effects of the illness.

Tracking fake IDs may give rise to a number of potential indicators, especially when locations of use, type of ID, frequency of observations, and apparent intent of use are examined. For example, if the ID is used in an attempt to purchase material that could be used to construct weapons of mass destruction, it could be an early tip-off of a planned terrorist act.

Increasingly our computer hardware and software is being designed and manufactured by foreign companies, some of which are nationalized. This includes elements of operation systems such as Windows as well as computer circuits (see for example Refs. 13-15).

This certainly increases the possibility of someone, some company, or even some nation incorporating malicious elements into the material we purchase to support our infrastructure as well as our Government operations. Such additions are not likely to be found without extensive and directed efforts, given the difficulty of determining all potential capabilities of a complex system. Generally, testing a complex system to ensure that it functions as intended is a demanding effort.

OTHER POTENTIAL AREAS OF APPLICATION

ASSESS—NUMBER, TYPE, CAUSE, AND LOCATION

- AIRPLANE CRASHES
- AIR TRAFFIC CONTROL VIOLATIONS
- TRAIN DERAILMENTS
- MISSING OR THEFTS OF SELECTED MATERIALS OR PROPERTY
- HOSPITAL ER VISITS—ESPECIALLY ELEVATED INDICATIVE SYMPTOMS THAT COULD BE DUE TO BIO AGENTS, BURNS, CHEMICAL REACTIONS, ETC.
- ANIMAL AND BIRD CARCASSES FOUND

TRACK

- PASSENGERS THAT HAVE BECOME ILL WHILE OR AFTER TRAVELING ON SPECIFIC AIRCRAFT AND SHIPS
- LOCATIONS, TYPES, FREQUENCY, AND APPARENT INTENT OF FAKE IDs

EVALUATE

- VULNERABILITY OF INFRASTRUCTURE AND GOVERNMENT OPERATIONS TO MATERIAL OBTAINED FROM SUPPLIERS WITH FOREIGN OWNERSHIP

OTHER POTENTIAL AREAS OF APPLICATION (continued)

Knowing the total dependency of our infrastructure as well as federal and state government operations on material provided by foreign suppliers would allow the Government, DHS in particular, to determine the risk faced by the United States. should supplies from various countries or various parts of the world be interrupted due to conflict, political unrest, or other disagreements. This knowledge would be extremely valuable in identifying all of the locations where a particular item is used and the sensitivity of our operations to it should the item come under question for any reason. It would also be invaluable in uncovering efforts by a nation to set up situations in our infrastructure and Government operations that could cause us hardship whenever that nation decided to activate the situation.

Further, augmenting this knowledge with the success and problems associated with material purchased from these suppliers as well as similar information on the suppliers themselves, and providing access to that information by the organizations purchasing the material for our infrastructure and Government operations, could greatly benefit those organizations in making their future purchases.

A WAY FORWARD

- **WHAT'S NEEDED?**
- **THE CONCEPT**
- **AN EXAMPLE**
- **EMPLOYING INTELLIGENT AGENTS**
- ➢ **A COMPARISON OF THE CHALLENGES**
- **NEXT STEP**

A COMPARISON OF THE CHALLENGES

This viewgraph compares the challenges met by the intelligent agents developed to locate the sites associated with enemy critical mobile targets on the battlefield with those expected in counterterrorism.

The column on the left of the viewgraph briefly lists the challenges of finding tactical ballistic missile (TBM) mobile launchers and the vehicles that reload them. In that operational problem, a variety of sensors provided data to at least two independent databases. The quantity of data, the disparity in timeliness and accuracy, and the confusion of having valid data on a large background of innocent vehicular traffic made success for the human a matter of luck in choosing the right data to examine at the right moment in time. Intelligent agents were developed and successfully overcame these challenges. Not only could they identify and track the true target vehicles, but they could also predict the likely time and place of their rendezvous for the reloading of the launch vehicles (TELs).

The column on the right lists features of a terrorist attack process that are at least roughly analogous to the TBM problem. Certainly the specifics of the data that will support useful correlations will be different as will the operational doctrine or behavior that drives the governing rules for the intelligent agents. The key point is that the potential of intelligent agents has already been demonstrated in a meaningful operational context. Applying them to counterterrorism is not a matter of hoping for a miracle of new technology but of extending demonstrated concepts to new situations.

A COMPARISON OF THE CHALLENGES

• **Challenges met by IAs:[a]**	• **Analogous CT[b] Challenges**
– Different types of vehicles, weapons, behaviors, etc.	– Different terrorist cells, intensions, resources, etc.
– Great deal of innocent vehicular traffic making background "noise"	– Operating in U.S. society which creates large background noise
– Separate, independent data sources and databases	– Data on potential terrorists and their activities collected and analyzed by many different organizations
– Intermittent data giving partial tracks	– No single database complete or 100% accurate
– Ambiguous identity on each "hit"	– Terrorists and their support structure may consist of people with multiple "identities"
• **Results**	• **Potential Results**
– Reliable track identification	– Near-real-time portrayal of a cell's activities
– Predictions of future behavior (reloading of TELs)	– Predictions of future behavior (construction of a WMD[c])

[a] Intelligent agents; [b] Counter-terrorism; [c] Weapon of mass destruction

(This page is intentionally blank.)

A WAY FORWARD

- **WHAT'S NEEDED?**
- **THE CONCEPT**
- **AN EXAMPLE**
- **EMPLOYING INTELLIGENT AGENTS**
- **A COMPARISON OF THE CHALLENGES**
- ➢ **NEXT STEP**

NEXT STEP

The next step is to develop a data collection and analyses plan. The plan starts by identifying the questions to be answered. For example, what are the intentions of the various terrorist cells, and do they have the means to carry out those intentions? The next step is to identify the data needed to answer those questions. Assuming that the data can be obtained, what organization is best positioned to collect it, and does that organization currently have the means to collect the data?

Assuming the data can be obtained in a timely manner, decisions must be made as to which organization is to analyze it, how that organization will obtain the data, how it will process the data, and to whom it will provide the results and in what form. It must also be decided if some form of real-time display is required.

While the above might seem to suggest that one organization will do all of the processing, this is not required. While examining the raw data might prove helpful from time to time, having organizations that collect the data process it in agreed to ways would considerably lessen the workload on the organization charged with doing the analyses. Further, maintaining all of the data in one location might not only be impractical, or at least cumbersome, it might make the site an unacceptably significant target, and not only for terrorists.

The first step in analyzing the data may very well be looking for patterns of activity that, when taken together, reveal intensions, plans, potential capability, organizational structure, opportunity, timeframe, etc. As previously noted, intelligent agent technology has shown promise in being able to do this type of processing and prediction.

NEXT STEP

DEVELOP A DATA COLLECTION AND ANALYSES PLAN

- **WHAT QUESTIONS ARE TO BE ANSWERED?**
- **WHAT DATA ARE NEEDED TO ANSWER THOSE QUESTIONS?**
- **HOW CAN THE DATA BE OBTAINED?**
  - **What organization is collecting/can collect each element?**
  - **Any additional collection means required?**
- **WHAT ORGANIZATION WILL PROCESS THE DATA?**
- **HOW WILL THE ORGANIZATION OBTAIN THE DATA?**
- **HOW ARE DATA TO BE PROCESSED?**
- **TO WHOM ARE THE RESULTS TO BE DELIVERED? IN WHAT FORM**?

(This page is intentionally blank.)

CONCLUSIONS

CONCLUSIONS

In general, terrorism is a covert effort involving many facets, such as people, skills, weaponry, targets, and timing. Countering such efforts is complex not only because of their covert nature, but also because the number of possible terrorist acts is so large. Although the number of organizations with counter-terrorism responsibility is also large and many of them are collecting significant amounts of data, our current ability to stop the terrorists is limited.

One problem is that, while terrorism and associated acts are multi-faceted, each of the counter-terrorism organizations has a particular area of responsibility and collects data accordingly. While some data sharing occurs, there is little integration of the data being collected across the organizations. While some of the stand-alone databases might be able to provide a real-time “picture” of selected aspects of terrorist activity, analyses of an integrated set will probably be required to reveal terrorists plans and capabilities sufficiently well to prevent their attacks.

CONCLUSIONS

- **COUNTERTERRORISM IS A VERY COMPLEX PROBLEM**
- **LARGE NUMBER OF ORGANIZATIONS WITH COUNTER-TERRORISM RESPONSIBILITIES, MANY COLLECTING SIGNIFICANT AMOUNTS OF DATA WHICH IS OFTEN NOT EFFECTIVELY EXPLOITED**
- **SOME DATA SHARING – LITTLE INTEGRATION**
- **ANALYSES OF INTEGRATED DATA ARE LIKELY NECESSARY TO PREVENT TERRORIST ATTACKS**

CONCLUSIONS (continued)

The amount of data, the rate at which it is growing and the methodologies that need to be employed to analyze it indicate that some form of intelligent automation, like intelligent agent technology, is required to transform the data into real-time information that the humans can more readily utilize.

In providing this real-time prospective on the terrorist's intentions, it is not necessary to have all of the data, nor all of the analyses, in one location. Access to the necessary data and the results of any preliminary processing along with adequate controls is the key.

Although the Homeland Security Act of 2002 charges the Under Secretary of Homeland Security for Information Analyses and Infrastructure Protection with the responsibility of analyzing information from various sources to identify threats of terrorism against the United States, it does not specify how such analyses are to be carried out or what organization is to do it. In his State of the Union address on January 28, 2003, President Bush announced plans for a new organization, the Terrorist Threat Integration Center, to be set up to integrate the intelligence on terrorism collected at home and abroad. Details on this organization are just being decided. The relationship of these two organizations in the processing of the integrated data and dissemination of the results is not yet clear.

CONCLUSIONS – (continued)

- INTELLIGENT AUTOMATION, SUCH AS THE USE OF INTELLIGENT AGENTS, IS NECESSARY TO TRANSFORM THE DATA INTO INFORMATION AND KNOWLEDGE THE HUMAN CAN MORE READILY UTILIZE
- ALL DATA NEED NOT RESIDE IN ONE PLACE. ACCESS IS THE KEY
- RELATIONSHIP OF THE DEPARTMENT OF HOMELAND SECURITY AND THE TERRORIST THREAT INTEGRATION CENTER IN CONDUCTING THE INTEGRATED ANALYSES IS NOT YET CLEAR
- DETAILS OF CONDUCTING THE ANALYSES ON AN INTEGRATED SET OF DATA AND WHERE TO SEND THE RESULTS ARE NOT YET DEFINED

CONCLUSIONS (continued)

Regardless of which organization is given the responsibility, one of the first tasks to be done is to define the questions to be answered. This is not an easy task because it depends on what data are being collected, what data could be collected, and how all of the data could be brought together and analyzed. Past experience indicates this will be an evolutionary process.

As our knowledge of the needs and data increase, the questions will be refined. As the questions evolve, we will seek better ways to collect the required data along with improved ways to analyze it.

We need to be judicious in our data collection efforts. On one hand, we need to collect only what is needed since the data are already voluminous, and collecting data that are not needed might generate privacy issues, deplete our limited collection resources, and bog down our analyses efforts. On the other hand, some additional data collection may be required to answer the evolving, and hopefully more profound, questions.

Finally, while it is true that the questions and the data are tightly coupled, the questions should drive the data collection. Collecting large quantities of data and then looking to see what questions it might answer may lead to some very interesting results, but it does not ensure that the most important questions will ever be addressed. Furthermore, it may lead to a disproportion of the available resources being devoted to data collection as opposed to the analyses and dissemination of results. The questions must be the driver.

CONCLUSIONS (continued)

- **NEED TO DEFINE QUESTIONS TO BE ADDRESSED AND TO BE SURE DATA COLLECTED SUPPORTS THE QUESTIONS. AN EVOLUTIONARY PROCESS**
- **QUESTIONS SHOULD DRIVE THE DATA COLLECTION-NOT THE OTHER WAY AROUND**

(This page is intentionally blank.)

REFERENCES

REFERENCES

1. *Warfighter's Edge: Using Intelligent Agents to Solve Warfighter Problems,* IDA Document D-2623, July 2001.

2. *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (Oct. 25, 2001), (Short Title USA Patriot Act),* H.R. 3162, In The Senate Of The United States, October 24, 2001. thomas.loc.gov/cgi-bin/query/D?c107:2:./temp/~c1070xrEXA::

3. "Pushing the Border Out: Creation of the 'Virtual' Electronic Border," Donald Quartel, ONR Workshop on "Transformation," Quantico, VA, September 18-19, 2002.

4. "Fact Sheet: Strengthening Intelligence to Better Protect America," January 28, 2003. www.whitehouse.gov/news/releases/2003/01/20030128-12.html

5. "Bush Details Threat Integration," *Federal Computer Week*, February 14, 2003. www.fcs.com/fcw/articles/2003/0210/web-threat-02-14-03.asp

6. "Threat Center Raises Questions, Concerns, Federal Computer Week, February 26, 2003. www.fcw.com/fcw/articles/2003/0224/web-ttic-02-26-03.asp

7. State of the Union Speech, President Bush, January 2003. www.whitehouse.gov/news/releases/2003/01/20030128-19.html.

8. DOE's Critical Infrasturcture Protection Program (CIPP). www.naseo.org/committees/energydata/energyassurance/stern2.pdf

9. FBI's National Ingrastruction Protection Center (NIPC) www.nipc.gov/

10. President's Critical Infrastructure Protection Board (CIPB). www.whitehouse.gov/news/releases/2001/10/20011016-12.htm

11. Donald Quartel, Testimony to the Subcommittee on Technology, Terrorism and Government Information of the U.S. Senate Judiciary Committee, February 26, 2002. (Also available in the proceedings of the ONR Workshop on "Transformation.")

12. "Homeland Security: A View Through the Eyes of Janus", Steven Cooper, Keynote Address to Homeland Security Section, ONR Workshop on "Transformation," Quantico, VA, September 18-19, 2002.

13. "Readying for a Trip Offshore," *Computerworld,* April 21, 2003, p. 42.

14. "Offshore Coding Work Raises Security Concerns," *Computerworld*, May 5, 2003, p. 1.

15. "Exporting IT Jobs," *Computerworld,* April 25, 2003, p. 39.

16. *Making The Nation Safer—The Role of Science and Technology in Countering Terrorism*, National Research Council of the National Academies, The National Academies Press, 2002.

17. *An Act to Establish the Department Of Homeland Security, and for Other Programs* (Short Title Homeland Security Act of 2002), H.R. 5005 EAS, In the Senate of the United States, November 19, 2002. thomas.loc.gov/cgi-bin/query/C?c107:./temp/~c107EBN5dN

18. *Protecting America's Freedom in the Information Age*, Markle Foundation Task Force, October 2002. www.markle.org/#

19. Counterterrorism, Section 3.1, "DARPA's Strategic Plan for 2003," February 2003. www.darpa.mil/body/strategic.html

APPENDIX A

GLOSSARY

Appendix A
GLOSSARY

CIA	Central Intelligence Agency
CIPB	Critical Infrastructure Protection Board
DHS	Department of Homeland Security
DOJ	Department of Justice
DOS	Department of State
FBI	Federal Bureau of Investigation
FF	freight forwarder
FOB	forward operating base
FTTTF	Foreign Terrorist Threat Task Force
IDA	Institute for Defense Analyses
INS	Immigration and Naturalization Service
MOE	measure of effectiveness
NIPC	National Infrastructure Protection Center
PS	port security
SARS	Severe Acute Respiratory Syndrome
TBM	tactical ballistic missile

(This page is intentionally blank.)

APPENDIX B

AN INITIAL TAXONOMY OF QUESTIONS

WHO?
(The Perpetrators and Their Organizations)

PEOPLE

A. PERSONAL

1. What are the names of the terrorists? What other names do they go by?
2. What identifying documents do they possess?
   a. Passport
   b. Green Card
   c. SSN
   d. Other
3. What are their physical features? Height, weight, hair color, eye color, observable markings, picture
4. Medical care
   a. What medical needs do they have?
   b. Where do they go to take care of them?
   c. Whom do they see?
   d. What medication do they take?

WHO (continued)

5. What vice do they have? What vices might they be susceptible to?
6. Do they have criminal histories?
   a. Types of crimes? Civil, criminal, terrorism?
   b. Nature? Violent, nonviolent?
7. Education

B. TIES

1. How long have they been in the United States?
2. Where did they come from?
3. What is their nationality?
4. What do they own? For example, car, house, stocks?
5. Who are their relatives and where do they live?
6. Do they have family here? Are they close?
7. Are the relatives part of a terrorist organization?

WHO (continued)

C. ACTIVITIES/FUNDS

1. Work/Income

a. What work experience, training, and expertise do they have?
b. Where do they work?
c. What type of work are they currently engaged in?
d. How long have they been employed? At this job? Other jobs?
e. How much do they make?
f. Do they have other income/other visible means of support?

2. Funds

a. Where do they keep their funds?
b. Whose names are on the accounts?
c. Who is authorized to withdraw the money?
d. How do they spend their money? What have they bought lately?
e. What means do they use to pay—cash, charge, checks, other?

3. How do they spend their non-working hours?

WHO (continued)

D. ASSOCIATES (outside of their organization)

1. Who do they associate with? Who do they converse with?
   a. What do they talk about?
   b. By what means? Phone, mail, e-mail, face-to-face?
   c. In U.S., outside U.S.?

E. ASSOCIATIONS

1. What other organizations do they belong to?
   a. Are they active?
      - Do they attend meetings?
      - Other types of activities in the organization?
   b. Do they provide funds or services?
2. What other organizations do they interact with?
   a. How do they interact?
   b. Do they attend meetings?
3. Do they Worship?
   a. Where?
   b. How regularly?
   c. Do they go with anyone or meet people there?
   d. Activities before and/or after the service?

WHO (continued)

E. Associations (Continued)

3. Do they Worship? (Continued)

a. What are the profiles of the religious leaders?

- **Who are they?**
- **Where did they come from?**
- **What are their Political orientations?**

F. LIFE FUNCTIONS

1. Residence

a. Where do they live?
b. How long have they lived there?
c. Whom do they live with?
d. Who owns the residence?
e. Why do they live there?

- **Convenience to work or shopping?**
- **Need to be close to others in the terrorists organization?**

f. Who are their neighbors?

WHO (continued)

F. LIFE FUNCTIONS (Continued)

2. Where do they shop? What do they buy?

3. What do they eat? Where do they get it from?

4. Communications Means

   a. Phones - Home, work, cell, etc.
   b. E-mail addresses
   c. P.O. Box

G. TRAVEL

1. Daily Travel - Weekdays, weeknights, weekends

   a. Means
   b. Schedule
   c. Purpose

WHO (continued)

G. TRAVEL (Continued)

2. Type of travel - Non-daily

a. Local
b. Within the U.S.
c. Outside the U.S.

3. General - Non-daily travel

a. Reason for travel?
   - Business or pleasure?
   - Visit family?
   - Education/training
   - Per religious law

b. What transportation means do they use?
c. Who provides the transportation?
d. Public or private? If private, who owns the vehicle? Who operates it?
e. Where do they travel to? How long do they stay? What do they do? With whom do they meet?
f. With whom do they travel?
g. How often do they travel?
h. Do they always make plans to return?

ORGANIZATION

A. WHAT NAME(S) DOES IT GO BY?

B. WHERE DOE IT HOLD ITS MEETINGS? HOW OFTEN? WHO ATTENDS?

C. WHO/WHAT IS ITS SUPERIOR?

1. How are communications carried out between the organization and its superior?
2. How often?
3. Who initiates the communication?

D. WHAT IS ITS COMMAND AND CONTROL STRUCTURE?

1. How does it receive orders?
2. Who sends them and who in the organization receives them?
3. From?
4. Coded or encrypted?
5. How does it report
   a. To whom?
   b. By what means?
   c. According to what schedule?

ORGANIZATION (continued)

E. HOW MANY TERRORISTS ARE IN THE ORGANIZATION?

1. What are their names?
2. How doe it recruit new members?
3. How are they organized? What is each person's function?
   a. Who does the planning?
   b. Who does the management?
   c. Who interfaces with the higher-ups?
   d. Who interfaces with outside groups/contacts?

F. HOW DOES THE ORGANIZATION SUPPORT ITSELF?

1. What is its source of funding?
2. Where does it keep its funds?
3. Whose names are on the accounts?
4. Who is authorized to withdraw funds?
5. What are the organization's funds spent on?
   a. What funds has organization disbursed lately? To whom? For what? By what means?
6. How are the transactions handled?

ORGANIZATION (continued)

G. ARE THEIR FUNDS LIMITED? MIGHT THEY BE INTERESTED IN ADDITIONAL FUNDS?

H. DOES THE ORGANIZATION HAVE ANY DEBTS?

1. **Who provided them and for what purpose?**
2. **When do they have to be repaid?**
3. **Any provisions for forgiveness?**

I. WHAT GROUP(S) IS THIS ORGANIZATION AFFILIATED WITH?

WHY?
(THE PERPETRATOR'S MOTIVATION)

A. WHAT MOTIVATES THE TERRORIST?
   1. Religion?
   2. Ideology?
   3. Power or influence?
   4. Rewards?
      a. Money? For whom—family?
      b. Life in hereafter?
   5. Pressure? Threats? Promises?
      a. Family?
      b. Friends?
      c. Group?

B. WHAT ARE THEIR GOALS? WHAT ARE THEY TRYING TO ACCOMPLISH?

C. WHAT IS THE CONNECTION BETWEEN THEIR MOTIVATION AND THEIR GOALS?

D. WHO DO THEY TAKE ORDERS FROM?

E. HOW DO THEY RECEIVE THEIR ORDERS?

WHAT?
(THE PERPETRATOR'S MISSION)

A. WHAT IS THE ORGANIZATION TRYING TO ACHIEVE?

1. What are its intensions?
2. What are its orders from its parent organization?
3. How does its intensions or orders relate to its motivation or the motivation of its members?

B. HAVE THEY BEEN GIVEN SPECIFIC TARGETS OR TARGET TYPES?

C. HAVE THEY BEEN DIRECTED TO USE SPECIFIC WEAPONS OR WEAPON TYPES?

D. HOW TIGHTLY IS THE ORGANIZATION CONTROLLED BY ITS PARENT?

WHERE?
(The Location of the Target)

A. WHAT ARE THE ORGANIZATION'S TARGETS?

1. How are they chosen?
2. How well are they related to the organization's objectives?
3. How do they relate to one another?

B. WHERE ARE THEY LOCATED?

C. HOW MANY ARE THERE?

D. ARE THEY IN MULTIPLE AREAS?

E. IS TIMING OF PLANNED ATTACKS IMPORTANT FROM A TARGET POINT OF VIEW?

HOW?
(The Means)

A. WHAT WEAPONS/WEAPON MATERIAL ARE/MIGHT BE AVAILABLE TO THEM?

B. WHAT IS THE SOURCE OF THE WEAPONS/WEAPON MATERIAL?

1. From whom or where did/might they acquire them?
   a. Make, buy, steal, supplied, find in trash?
2. Who/what was the original source/manufacture? Location?
3. How are/were they transported?

C. HOW/WHERE ARE THE WEAPONS/WEAPON MATERIALS STORE?

1. Before weapon construction?
2. During weapon construction?
3. After weapon construction?

HOW? (continued)
(The Means)

D. WHAT ARE THE TERRORIST'S CAPABILITIES AND SKILLS?

1. To construct, employ, utilize these types of weapons?
2. How did they gain these capabilities and skills?
   a. Work experience?
   b. Military?
   c. Terrorist run/supported camps?
   d. Other training?

5. HOW EFFECTIVE WOULD THE WEAPONS BE AGAINST THE INTENDED TARGETS?

1. Would the weapons/targets combinations create the fear/panic the terrorists seek?

6. HOW MIGHT THEY TRANSPORT THE WEAPONS TO THE TARGETS?

HOW? (continued)

(The Means)

G. WHAT MEANS MIGHT THE TERRORISTS USE TO ACTIVATE/SET OFF THE WEAPON?

H. WHAT DETECTABLE SIGNATURE IS ASSOCIATED WITH EACH TYPE OF WEAPON?

1. **As it is being built, while it is stored, & when it is deployed?**
2. **At what distance?**
3. **By what sensor or sensor types?**

WHEN?
(The Timeframe)

A. DO THEY CURRENTLY HAVE WEAPONS MATERIAL?

1. If not, what are they missing for use against their intended targets?

B. DO THEY HAVE THE SKILLS TO USE IT?

1. If not, what skills are they missing?
2. How might they obtain the needed skills?
   a. In what timeframe?
   b. Has anyone with these types of skills applied for a visa or recently entered the country?
      - If they are in the country, are they nearby the terrorist's organization?
      - Do they need to be physically close to the terrorist organization?

C. WHAT EVENTS, WHICH MIGHT BE OF INTEREST TO THE TERRORISTS, ARE PLANNED FOR THE TARGET AREA?

1. What is the timeframe of these events?

D. HAVE FAMILY MEMBERS OR CLOSE RELATIVES OF ANY OF THE MEMBERS OF THE ORGANIZATION LEFT THE UNITED STATES RECENTLY?

(This page is intentionally blank.)

APPENDIX C

DISTRIBUTION LIST FOR IDA DOCUMENT D-2849

Appendix C
DISTRIBUTION LIST FOR IDA DOCUMENT D-2849

Defense Agencies	**No. of copies**
Mr. Paul McHale Asst. Secretary of Defense for Homeland Security 2600 Defense Pentagon Washington, DC 20301-2600	1
Other Organizations	
Mr. Steven I. Cooper Chief Information Officer Department of Homeland Security Washington, DC 20528	1
Ms. Margaret D. Blum Associate Administrator for Port, Intermodal, and Environmental Activities Maritime Administration Department of Transportation 400 7th Street, S.W. Washington, DC 20590	1

Other Organizations (cont.)	No. of copies
Ms. Susan Howland Project Director Delaware River Maritime Enterprise Council Two Neshaminy Interplex, Suite 208 Trevose, PA 19053	1
Institute for Defense Analyses 4850 Mark Center Drive Alexandria, VA 22311-1882	10
Total Distribution	**14**

REPORT DOCUMENTATION PAGE	Form Approved OMB No. 0704-0188

1. REPORT DATE (DD-MM-YY)	2. REPORT TYPE	3. DATES COVERED (FROM – TO)
June 2003	Final	June 2003–June 2003

4. TITLE AND SUBTITLE

Defender's Edge
Utilizing Intelligent Agent Technology To Anticipate Terrorist Acts

5A. CONTRACT NO. DASW01-98-C-0067

5B. GRANT NO.

5C. PROGRAM ELEMENT NO(S).

6. AUTHOR(S)

L. B. Scheiber, J. E. Hartka, R. S. Murch

5D. PROJECT NO.

5E. TASK NO. CRP-1089

5F. WORK UNIT NO.

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Institute for Defense Analyses
4850 Mark Center Drive
Alexandria, VA 22311-1882

8. PERFORMING ORGANIZATION REPORT NO. IDA Document D-2849

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

IDA Contracting Officer's Representative
4850 Mark Center Drive
Alexandria, VA 22311-1882

10. SPONSOR'S / MONITOR'S ACRONYM(S)

11. SPONSOR'S / MONITOR'S REPORT NO(S).

12. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for public release; distribution unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

This report examines the need for, the potential of, and the steps involved in applying intelligent software, called Intelligent Agents, to the problem anticipating terrorist acts.

The examination of the need provides an indication of the fragmented nature of the current flow of intelligence data from the collecting organizations, through the processing of the data into information, to the organizations designated to take action on the resulting information.

The examination further indicates that the multitude of data sources, coupled with the significant amount of data available to be collected can be projected to lead to an overwhelming amount of data. It also noted a lack of a detailed data collection and analyses plan.

The report describes a way forward which includes both an approach to developing a data collection, data analyses and information distribution plan, and a concept for utilizing intelligent agents to process the data collected into actionable information.

15. SUBJECT TERMS

Intelligent Agents, intelligent software, artificial intelligence, terrorists, terrorism, counterterrorism, 9/11, shipping containers, ports, supply chains, security.

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NO. OF PAGES	19A. NAME OF RESPONSIBLE PERSON
A. REPORT	B. ABSTRACT	C. THIS PAGE	Unlimited	111	Mr. David A. Erickson
Unclassified	Unclassified	Unclassified			19B. TELEPHONE NUMBER (INCLUDE AREA CODE) (703) 845-2202