Dr. John Poindexter, Director
Information Awareness Office (IAO)
Information Awareness Office Overview

Good morning. Today I would like to tell you about the new Information Awareness Office and the programs we are developing. To introduce this I have a short video for you.

(Play video - about 6 minutes)

The world has indeed changed dramatically since the Cold War when there existed 2 super powers. During the years I was in the White House it was relatively simple to identify our intelligence collection targets. It was sometimes hard to collect the intelligence, but the targets were clear. Today, we are in a world of asymmetries. The most serious asymmetric threat facing the United States is terrorism, a threat characterized by collections of people loosely organized in shadowy networks that are difficult to identify and define and whose goals are the destruction of our way of life. The intelligence collection targets are thousands of people whose identities and whereabouts we do not always know. It is somewhat analogous to the anti-submarine warfare problem of finding submarines in an ocean of noise—we must find the terrorists in a world of noise, understand what they are planning, and develop options for preventing their attacks. If we are to preserve our national security, we must figure out a way of combating this threat.

I think the solution is largely associated with information technology. We must become much more efficient and more clever in the ways we find new sources of data, mine information from the new and old, generate information, make it available for analysis, convert it to knowledge, and create actionable options. We must also break down the stovepipes—at least punch holes in them. By this, I mean we must share and collaborate between agencies, and create and support high-performance teams operating on the edges of existing organizations. Tools are needed to facilitate these collaborations, and to support these teams that work to ensure our security.

The Information Awareness Office at DARPA is about creating technologies that would permit us to have both security and privacy. More than just making sure that different databases can talk to one another, we need better ways to extract information from those unified databases, and to ensure that the private information on innocent citizens is protected. The main point is that we need a much more systematic approach. A variety of tools, processes and procedures will be required to deal with the problem, but they must be integrated in a systems approach built around a common architecture to be effective.

Total Information Awareness—a prototype system—is our answer. We must be able to detect, classify, identify, and track terrorists so that we may understand their plans and act to prevent them from being executed.

To protect our rights, we must ensure that our systems track the terrorists, and those that mean us harm. IAO programs are focused on making Total Information Awareness—TIA—real. This is a high level, visionary, functional view of the world-wide system—somewhat over simplified.

One of the significant new data sources that needs to be mined to discover and track terrorists is the transaction space. If terrorist organizations are going to plan and execute attacks against the United States, their people must engage in transactions and they will leave signatures in this information space. Currently, terrorists are able to move freely throughout the world, to hide when necessary, to find sponsorship and support, and to operate in small, independent cells, and to strike infrequently, exploiting weapons of mass effects and media response to influence governments. We are painfully aware of some of the tactics that they employ. This low-intensity/low-density form of warfare has an information signature. We must be able to pick this signal out of the noise. Certain agencies and apologists talk about connecting the dots, but one of the problems is to know which dots to connect. The relevant information extracted from this data must be made available in large-scale repositories with enhanced semantic content for easy analysis to accomplish this task. The transactional data will supplement our more conventional intelligence collection.

While our goal is total information awareness, there will always be uncertainty and ambiguity in trying to understand what is being planned. That's why our tools have to build models of competing hypotheses. That is, we need to bring people with diverse points of view together in a collaborative environment where there is access to all source data, discovery tools and model building tools. Collaboration has not been so important in the past when problems were less complex, but now it is essential. And tools have to make the analysis process more efficient, to properly explore the multiple possibilities.

This is the analytical environment. I could have called it the intelligence community, but in the case of counter-terrorism, it is broader to include law enforcement, friendly allies, outside experts etc. A similar environment exists for the policy and operations community, but the functions and tools are different. The mission here is to take the competing hypotheses from the analytical environment and estimate a range of plausible futures. The objective is to identify common nodes, representing situations that could occur, and to explore the probable impact of various actions or interventions that authorities might make in response to these situations.

The Information Awareness Office has a number of ongoing projects to address the functional requirements of this vision, and we will be starting new projects to complete the picture. The program managers who follow will give you the details, but I want to show you how they all fit into this system plan.

Jonathon Phillips is working on Human Identification at Distance, to achieve positive identification of humans using multi-modal biometric technologies. Such a system could be used for security systems, for example, or could be used to track potential terrorists.

Doug Dyer is starting a new program called Genisys, which addresses our database needs. This project will imagine and develop ultra-large-scale, semantically rich, easily implementable database technologies. One goal is to develop ways of treating the world-wide, distributed, legacy data bases as if they were one centralized data base, and another is to develop privacy protection technologies.

Next, Charles Wayne leads the programs called TIDES and EARS. These projects address our needs in natural language processing, to provide discovery tools for finding information in foreign languages and converting speech to text. Automated tools are essential in order to reduce our need for expert foreign language translators and listeners in the thousands of existing human languages.

Ted Senator is the program manger for EELD, which stands for Evidence Extraction and Link Discovery. This is a key program in the area of tools for discovery of information. I will let Ted tell you the details on how this goes beyond traditional data mining techniques.

War Gaming the Asymmetric Environment is led by Larry Willis. This is an essential component of our modeling efforts. Bio-Surveillance is another of Ted Senator's programs looking at novel data sources for early warning of the release of biological agents.

Tom Armour is back on the DARPA team to extend the work on the Genoa project with a new program that we have creatively named Genoa II. I told him he had to come back to finish his work.

As some of you know I've been working on Genoa for the past 6 years. We have transitioned some of the Genoa tools and will build on the past work primarily to address tools for collaborative reasoning, estimating plausible futures and creating actionable options for the decision maker. While the original Genoa project was aimed primarily at supporting intelligence analysis, under Genoa II we plan to focus on supporting policy and decision-making at strategic levels.

The overarching program that binds IAO's efforts together is Total Information Awareness or TIA System. The primary goal of TIA is the integration and assured transition of components developed in the programs Genoa, Genoa II, GENISYS, EELD, WAE, TIDES, HumanID and Bio-Surveillance. TIA will develop a modular system architecture using open standards that will enable a spiral development effort that will allow the insertion of new components when they are available. We will produce a complete, end-to-end, closed-loop prototype system in a realistic environment.

To accomplish this we have established an organization whose structure is as diagramed here. We will supplement the programs in IAO with commercial and other government components to rapidly implement early versions of TIA system at our R&D laboratory. We have already begun a spiral development and experiment program in conjunction with Army partners.

Over the next few years we will continuously add functionality to the system as components become available. Where will IAO's projects get data in order to develop their algorithms? To proceed with development, without intruding on domestic or foreign concerns, we are creating a data base of synthetic transactions using a simulation model. This will generate billions of transactions constituting realistic background noise. We will insert into this noise simulated transactions by a red team acting as a terrorist organization to see if we can detect and understand this activity. In the Genisys program we will be investigating the DARPA-hard problem of developing technologies that can give us the capability to detect foreign terrorist activities in this transaction space and achieve enhanced privacy for the innocents.

There are significant information policy issues related when considering data mining in actual transaction spaces. The U.S., and other countries as well, have just begun to consider some of the issues and consequences. There are ways in which technology can help preserve rights and protect people's privacy while helping to make us all safer. We are taking a number of steps to begin a reasoned discussion of the policy issues, imbued with knowledge of technology capabilities. DARPA's Information Systems Advanced Technology panel (ISAT) has been tasked with a summer study on how we can achieve the necessary security we need and still have privacy. Discussions have been started with the National Academy of Sciences to do a longer range study on Information Policy for the InfoSpace of the Future.

We believe that total information awareness is a very difficult problem and in the tradition of the very hard problems that DARPA has addressed in the past. We think we have some very good ideas about how to solve the problem. IAO has an open BAA that was issued last March, and will be open for a year. We will be funding some of the good ideas that we have already received, but if you have good ideas that we haven't seen yet, please tell us about them. The BAA is on the DARPA web site.

I believe the ultimate solution to countering terrorism requires a co-evolution in four areas: technology, process/operations, policy and culture. Our focus is on developing the technology, the first area, and making sure that decisions in the other areas, such as policy, are knowledgeable about what is possible and what isn't. It's an exciting area, and I am proud of the contributions that we will all be collectively making to National security.

Thank you.
Now you will hear from the program managers.