

DARPA's Information Awareness Office (IAO) and Total Information Awareness (TIA) Program

Frequently Asked Questions

Question 1: What is the Total Information Awareness (TIA) program?

Answer: TIA is a Defense Advanced Research Projects Agency (DARPA) research effort to create a prototype network that integrates innovative information technologies for detecting and preempting foreign terrorist activities against Americans.

The program is a multiyear, phased, development effort. The information technologies comprising the experimental prototype network are in three areas: advanced collaborative and decision support tools; language translation; and data search, pattern recognition, and privacy protection technologies.

The collaborative reasoning and decision-support technologies will solve existing coordination problems by enabling analysts from one agency to collaborate effectively with analysts in other agencies. A major challenge to terrorist detection today is the inability to quickly search, correlate, and share data from databases maintained legally by our intelligence, counterintelligence, and law enforcement agencies. The collaborative reasoning and decision-support technologies will punch holes in these "stovepipes."

The language translation technologies will enable the rapid translation of foreign language speech and text giving terrorism analysts the ability to quickly search for clues about emerging terrorist acts. Terrorism experts believe evidence of terrorist activities can be found in open-source foreign language publications and broadcasts. The rapid translation technologies will help analysts search a significant amount of material in a much shorter period than is possible today.

The research into data search and pattern recognition technologies is based on the idea that terrorist planning activities or a likely terrorist attack could be uncovered by searching for patterns indicative of terrorist activities in vast quantities of data. Terrorists must engage in certain transactions to coordinate and conduct attacks against Americans; these transactions leave signatures (patterns) that may be detectable. For this research, the TIA project will use only data that is legally obtainable and usable by the U.S. Government. The privacy protection technologies protect the TIA network from internal and external abuses and assure users that their sources and methods cannot be discerned deliberately or accidentally.

Question 2: Why is the TIA program important right now?

Answer: Information about terrorist activity has always been important to protect and defend the United States. After the September 11, 2001, attacks, it was broadly reported that the Federal Bureau of Investigation (FBI) and other agencies had pieces of information on the behavior and activities of the terrorists that, if connected, could have alerted authorities before the plans were carried out. Congress concluded that the failure to identify the threat prior to the attacks had less

DARPA's Information Awareness Office (IAO) and Total Information Awareness (TIA) Program

Frequently Asked Questions

to do with the ability of authorities to gather information than with their inability to analyze, understand, share, and act on that information. TIA will solve existing coordination problems by enabling analysts from one agency to collaborate effectively with analysts in other agencies facilitating their ability to connect the dots—to make the linkages among the indicators of potential terrorist activities before an attack occurs.

Question 3: What is the goal of the TIA program?

Answer: The goal of the TIA program is to research and develop innovative information technology tools that will give the Department of Defense (DoD) intelligence, counter-intelligence, and counterterrorism communities important capabilities to prevent terrorist attacks against the United States. These tools will enable the DoD to preempt terrorist attacks in locations far beyond U.S. borders.

Question 4: What types of technology are being used or developed in the TIA project, and what data are DARPA now collecting and using?

Answer: In the current plan, the TIA network will integrate a number of component technologies. Some technologies under consideration are being developed under existing DARPA programs. Technologies from other R&D and commercial sources also are being considered. Examples of DARPA-developed component technologies are:

- The Genoa II program is developing advanced collaboration and decision support tools that give counter-terrorism analysts, operations, and policy personnel innovative capabilities to share and analyze information on foreign terrorist activities.
- The Translingual Information Detection, Extraction and Summarization (TIDES) Program is developing advanced language-processing technology to enable English-only speakers to find and interpret critical information in foreign language publications and broadcasts.
- The Evidence Extraction and Link Discovery (EELD) Program is developing technology to enable the automated discovery, extraction, and linking of data markers indicative of terrorist activities contained in large amounts of data sources.

DARPA will use two types of data in the TIA research: data in the public domain, such as foreign language newspapers, journals, and broadcasts; and synthetic data, i.e., artificial information generated to resemble real-world data in which we embed simulated data indicative of terrorist activities. Since TIA is a phased, spiral development effort, operational units participating in planned collaboration experiments may choose to share and analyze information on foreign terrorist activities that they are legally authorized to have for the tests.

**DARPA's Information Awareness Office (IAO) and
Total Information Awareness (TIA) Program**

Frequently Asked Questions

Question 5: Is DARPA developing a domestic surveillance capability to create dossiers on each and every American?

Answer: No. The goal of the TIA program is to develop information technologies that will provide important capabilities to detect foreign terrorist threats before they attack Americans.

Contrary to some recent media reports, TIA is *not* an attempt to build a “supercomputer” to snoop into the private lives or track the everyday activities of American citizens. TIA is developing and integrating information technology that consists largely of three parts—advanced collaborative and decision support tools; language translation technologies; and data search, pattern recognition, and privacy protection technologies. Together, these components effectively comprise the TIA program.

Question 6: How will privacy issues be resolved?

Answer: Congress will have the major role in resolving any privacy issues that result from TIA research. All TIA research complies with all privacy laws, without exception. In addition, the oversight boards that the Under Secretary of Defense for Acquisition, Technology and Logistics has established will ensure that TIA develops its products and disseminates them in a manner consistent with public policy concerns.

Question 7: Would implementation of TIA require or allow the Government to access or collect personal data on Americans that it does not currently collect?

Answer: The DoD mission to preempt and counter foreign terrorist threats outside the United States would not require the collection of any data currently protected under privacy law.

Question 8: What checks and balances are being designed into TIA to guard against internal abuse and external threats such as computer hacking?

Answer: DARPA recognizes the need to develop effective checks and balances and is developing privacy protections and other advanced security and system-hardening characteristics as part of the TIA program.

DARPA has sponsored studies to create more technology-based privacy safeguards, such as the Information Sciences and Technology (ISAT) Security with Privacy Study. DARPA is evaluating some of the study's technology research recommendations, such as immutable audit and self-reporting data. Immutable audit would track all TIA data search activities and capture data regarding these activities in a strong accounting system that could not be altered or turned off. Such audit control would make it possible to identify abuse of the TIA network as well as

**DARPA's Information Awareness Office (IAO) and
Total Information Awareness (TIA) Program**

Frequently Asked Questions

the identity of the abuser. Self-reporting data would protect the privacy of data even after it is retrieved from a database. For example, if data were passed to an unauthorized individual, self-reporting data would enable auditors to know who accessed it. This is required to protect the sources and methods of different agencies.

Question 9: In a system based on automated examination of personal data, what is required for a person to become identified as a potential or suspected terrorist?

Answer: No efforts are being performed or considered under DARPA's TIA program to identify U.S. citizens as terrorists. TIA research efforts are just beginning to examine processes for identifying individuals as potential or suspected international terrorists.

The automated processing of data still requires a great deal of innovative research, and this is part of the multiyear research effort. Even here, it is doubtful that any automated system will identify terrorists. However, the automated technologies will format data such that analysts from different agencies can collaborate on the outputs and make determinations whether a pattern is suspicious enough to warrant further analysis or data collection.

Question 10: Why is DARPA developing technology with the potential to outpace existing privacy protections?

Answer: TIA is in its first year of an anticipated multiyear research effort, and the full prototype exists only as a vision. Existing privacy protections will not be challenged during the research phase since the only data used to test the technologies will be data that is legally usable by the U.S. Government or is synthetically generated. While the project is underway, there is plenty of time for Congress to review the project's research findings to determine whether changes are necessary.

Given the many opportunities Congress will have to review the program, the concern that the technology will outpace existing privacy protections is totally unfounded.

Question 11: Why is the Department of Defense becoming involved in domestic intelligence issues? Is there precedent for this? What experience does DARPA have in research on law enforcement and domestic intelligence methods?

Answer: The Department of Defense is not involved in domestic intelligence issues.

On the other hand, there is no precedent for the attacks of September 11, 2001. On that date, the United States entered a new era of defense. Terrorist threats that in the past targeted only U.S.

DARPA's Information Awareness Office (IAO) and Total Information Awareness (TIA) Program

Frequently Asked Questions

interests abroad now plan global attacks, and they are not deterred by America's borders. The September 11 attacks highlighted the need for DoD initiatives to preempt terrorists before they reach America's borders.

DARPA has had joint programs with the FBI and the U.S. Customs Service to develop technology that could be used for detecting explosives and drugs at airports and sea ports. DARPA continues this history of collaboration by working on programs such as Project Genoa, which is intended to aid the intelligence, counterintelligence, and counterterrorism communities in sharing to better understand existing data.

DARPA is now working with the U.S. Army Intelligence and Security Command (INSCOM) and a DoD counterintelligence organization to test TIA technology using data that is legally usable by the U.S. Government. TIA is being developed to fulfill a DoD mission requirement (i.e., countering the international terrorist threat). DARPA plans more experiments using collaboration nodes at U.S. Special Operations Command (USSOCOM), another combatant command and additional members of the foreign intelligence community. Other intelligence, counter-intelligence and law enforcement organizations are considering joining as collaboration nodes in future experiments. These organizations support the development of innovative collaboration and data-sharing technologies to preempt foreign terrorist attacks. They want to participate in the TIA research effort.

Question 12: What is the budget for DARPA's Information Awareness Office (IAO) and the TIA program?

Answer: The fiscal year (FY) 2004 budget for IAO is \$169 million, of which TIA development funding is \$20 million. The remainder of the budget funds component software technology development. The budget supports development efforts only. The goal of these efforts is a prototype that will serve as a model for transition to a future operational network, if Congress determines that an operational network should be funded.

Question 13: How much will it cost to implement TIA?

Answer: The cost will depend on the component technologies deployed in the DoD operational community. If all component technologies prove successful, the deployment options include collaborative reasoning and decision support and information visualization technologies; language translation technologies; and data search, pattern recognition, and privacy protection technologies. However, a great deal of the infrastructure to implement TIA exists in the form of secure networks, computer, and displays. The development cost is for advanced collaborative and decision support tools directed toward improving or developing software techniques. The recurring cost for copying software is extraordinarily small.

**DARPA's Information Awareness Office (IAO) and
Total Information Awareness (TIA) Program**

Frequently Asked Questions

Question 14: When is it anticipated that TIA will be ready for use?

Answer: Research under the TIA program is planned for several years. An operational prototype TIA network is the goal of this multiyear effort. During the first 36 months, a range of ideas will be developed via limited demonstrations and preliminary prototypes. During the final 24 months, the most promising research avenues will be extended to support transition of a scalable, leave-behind network prototype. At the end of the multiyear program, Congress will have decided if and how the TIA network will be deployed or further matured.

Question 15: What does the IAO logo mean? Why has it disappeared from the web site?

Answer: DARPA offices have traditionally designed and adopted logos. However, because the IAO logo has become a lightning rod and is needlessly diverting time and attention from the critical tasks of executing that office's mission effectively and openly, we have decided to discontinue the use of the original logo.

For the record, the IAO logo was designed to convey the mission of that office; i.e., to imagine, develop, apply, integrate, demonstrate, and transition information technologies, components, and prototype, closed-loop information systems that will counter asymmetric threats by achieving total information awareness useful for preemption, national security warning, and national security decision making. On an elemental level, the logo is the representation of the office acronym (IAO); the eye above the pyramid represents "I," the pyramid represents "A," and the globe represents "O." In the detail, the eye scans the globe for evidence of terrorist planning and is focused on the part of the world that was the source of the attacks on the World Trade Center and the Pentagon. *Scientia est potentia* means "Knowledge is power." With the enabling technologies being developed by the office, the United States will be empowered to implement operational systems to thwart terrorist attacks like those of September 11, 2001.

The unfinished pyramid and the eye depicted in the logo were taken directly from the reverse side of the Great Seal of the United States of America (for a history of the seal, see <http://www.heraldica.org/topics/usa/usheroff.htm>). Both sides of the seal also appear on the back of the U.S. \$1 bill.

Question 16: How was John Poindexter selected as the Director of DARPA's Information Awareness Office?

Answer: Dr. Poindexter was selected as the Information Awareness Office Director based on a number of factors: his prior experience with DARPA's Project Genoa and the national security

DARPA's Information Awareness Office (IAO) and Total Information Awareness (TIA) Program

Frequently Asked Questions

decision-making process, his technical training and understanding of relevant technologies and their collective application, and his vision and passion for the TIA program.

Prior to September 11, 2001, Dr. Poindexter assisted DARPA's Project Genoa. This 4-year research program was near completion at the time of the September 11 terrorist attacks. The program focused on serving the Intelligence Community by developing information technology aimed at rapidly and systematically organizing data, facilitating collaboration while protecting critical information and testing hypotheses to support decision-making at the national level.

Advanced collaboration technologies are the critical missing centerpiece to innovative new counter-terrorism capabilities. The concepts developed under Project Genoa represent a logical starting point for an expanded and accelerated effort to use information technology to prevent future terrorist attacks.