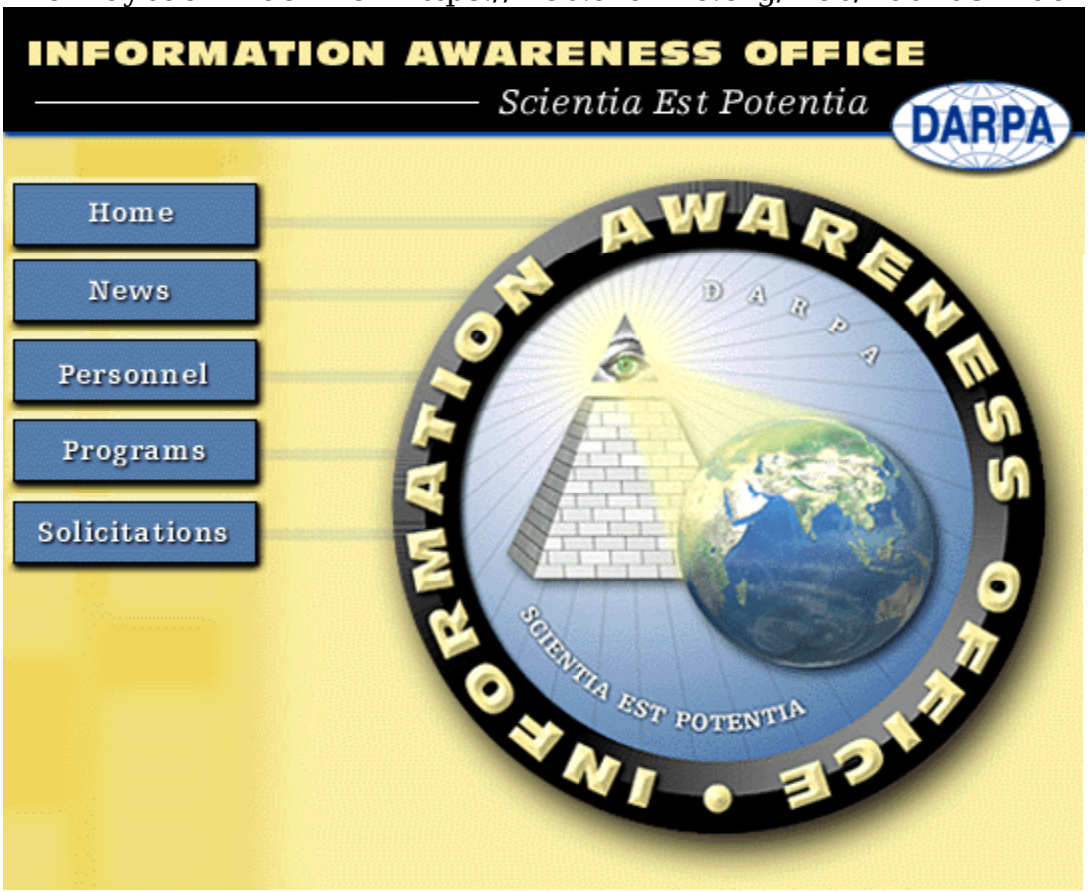

IAO Mission: The DARPA Information Awareness Office (IAO) will imagine, develop, apply, integrate, demonstrate and transition information technologies, components and prototype, closed-loop, information systems that will counter asymmetric threats by achieving total information awareness useful for preemption; national security warning; and national security decision making

IAO Vision: 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. IAO plans to develop technology that will allow understanding of the intent of these networks, their plans, and potentially define opportunities for disrupting or eliminating the threats. To effectively and efficiently carry this out, we must promote sharing, collaborating and reasoning to convert nebulous data to knowledge and actionable options. IAO will accomplish this by pursuing the development of technologies, components, and applications to produce a proto-type system. Example technologies include:

- Collaboration and sharing over TCP/IP networks across agency boundaries
- Large, distributed repositories with dynamic schemas that can be changed interactively by users
- Foreign language machine translation and speech recognition
- Biometric signatures of humans
- Real time learning, pattern matching and anomalous pattern detection
- Entity extraction from natural language text
- Human network analysis and behavior model building engines
- Event prediction and capability development model building engines
- Structured argumentation and evidential reasoning
- Story telling, change detection, and truth maintenance
- Business rules sub-systems for access control and process management
- Biologically inspired algorithms for agent control
- Other aids for human cognition and human reasoning

It is difficult to counter the threat that terrorists pose. Currently, terrorists are able to move freely throughout the world, to hide when necessary, to find unpunished sponsorship and support, to operate in small, independent cells, and to strike infrequently, exploiting weapons of mass effects and media response to influence governments. This low-intensity/low-density form of warfare has an information signature, albeit not one that our intelligence infrastructure and other government agencies are optimized to detect. In all cases, terrorists have left detectable clues that are generally found after an attack. Even if we could find these clues faster and more easily, our counter-terrorism defenses are spread throughout many different agencies and organizations at the national, state, and local level. To fight terrorism, we need to create a new intelligence infrastructure to allow these agencies to share information and collaborate effectively, and new information technology aimed at exposing terrorists and their activities and support systems. This is a tremendously difficult problem, because terrorists understand how vulnerable they are and seek to hide their specific plans and capabilities. The key to fighting terrorism is information. Elements of the solution include gathering a much broader array of data than we do currently, discovering information from elements of the data, creating models of hypotheses, and analyzing these models in a collaborative environment to determine the most probable current or future scenario. DARPA has sponsored research in some of these technology areas, but additional research and development is warranted to accelerate, integrate, broaden, and automate current approaches.
