DARPA’s Initiative on Countering Terrorism:

Overview of TIA and IAO Programs

Dr. Robert Popp
Acting Director
Information Awareness Office (IAO)
rpopp@darpa.mil
703-248-1520
Background...
Formation of the Information Awareness Office (IAO)

- DARPA developing technology for counter terrorism since 1995
  - Several initiatives attacked significant parts of the problem

- 9/11 drove home need to change
  - Needed an integrated approach

- Army’s Intelligence and Security Command (INSCOM) Information Operations Center (IOC)
  - Offer was made to join forces
  - Use IOC as laboratory to integrate & experiment with R&D technology

- IAO office was formed (Jan 2002) to focus and accelerate DARPA’s counter terrorism thrust

Terrorism: a threat that is characterized by systematic use of actual or threatened physical violence against innocent people in pursuit of political objectives and for the purpose of creating a climate of fear to coerce governments into ceding to those political objectives.
**TIA Technology Assessment**

- Real world operational environment
- Existing intel and counter-intel data
- Three-month experiment cycles
- Incremental transition to TIA nodes

**New Technology Assessment**
- Synthetic unclassified data
  - Ordinary “vanilla” transactions (noise)
  - Suspicious transactions (false alarms)
  - Red team terrorist transactions (signal)
- Avoids privacy / sources & methods issue

**IAO Organization...**
Designed for rapid prototyping and assured transition

**Development**
- Director DARPA
- Director IAO

**Transition Example**
- TIA
- Information Operations Center at INSCOM

**Other DARPA, GOTs/COTs Programs**
- Genoa II
  - WAE
  - RAW
- EARS
- TIDES
- GALE
- Babylon
- Symphony

**Collaboration**
- Decision Support
- Predictive Modeling

**Foreign Language Technologies**
- Genisys
- MinDet
- HumanID
- NGFR
- Bio-ALIRT

**DB Processing**
- EELD
- SSNA
- ARM

**Privacy Protection Biometrics**
- Bio-ALIRT

**TIA Technology Assessment**
- • Real world operational environment
  - • Existing intel and counter-intel data
  - • Three-month experiment cycles
  - • Incremental transition to TIA nodes
Combating Terrorism Through Information Technology

Pattern Analysis

Predictive Modeling

Analysis Tools and Decision Aides

Collaboration Tools

Foreign Languages

Pre-Incident Indicator Vector

A set of numerical weight is derived for each pre-incident indicator

Location

Target

Tactic

Attack

No Attack

Env

New information available

Multidimensional argument summary

Unidimensional argument

Supporting documents

Supporting critical path analysis

Supporting query structure

Environmental

Social

Economic

Military

Cascaded arguments
What is TIA...

Information technology is our weapon against terrorism

- **TIA (Terrorism Information Awareness)**
  - Experimental multi-agency R&D system/network for counter terrorism
  - Core enabling technologies
    - Collaboration, Analysis and Decision Support
    - Foreign Language Technologies
    - Pattern Analysis and Predictive Modeling
    - Database Processing
    - Sources & Methods and Privacy Protection
    - Biometrics
  - Supporting strategic, national focus
    - NSC, IC, NFIP, Unified Commanders
    - Preemption and prevention is what we want to enable

- **TIA is not ...**
  - developing “collections” technology
  - building a “grand database” or “dossiers” to snoop on Americans
  - “mining data” in violation of U.S. laws or policies
Primary TIA Focus...
Developing analytical tools

• **TIA Focus:**
  - A **collaborative R&D network**
  - Providing users with **data analyzing tools** to solve problems together
  - **3 month experiment threads**
    - Structured discovery with security
    - Secure collaborative problem solving
    - Link and group understanding
    - Context aware visualization
    - Decision making with corporate memory

• **Collaboration, Analysis and Decision Support**
• **Foreign Language Technologies**
• **Pattern Recognition and Predictive Modeling**
• **Database Processing**
• **Sources & Methods and Privacy Protection**
TIA Analysis Goal...

Harness various technologies to invert bathtub curve
**Major TIA Accomplishments...**

- **Collaborative R&D Network**
  - Allows agencies to solve CT problems collaboratively and experiment with prototype information technologies

- **System Integration Framework**
  - Rigorous approach for IT integration analogous to signal processing

- **Technology Experiments & Assessment**
  - Conducting experiments every three months; early results very promising
TIA Provides a Collaborative R&D Network
Facilitating experimentation of CT technology

- Collaborative Environment
  - Classified Network
  - Real Users
  - Real Problems
  - Real Data

- Each Site has Advanced Technologies
  - COTS/GOTS
  - DARPA
  - INSCOM
  - Other IC Members

Network of:
- Agencies
- People
- Tools
- Data
Early Experimental Results...

More and better CT analysis in a shorter period of time

Analytical Results

Analytical Modeling Tools

JFIC, INSCOM, CIFA, JWAC worked a problem

Does al-Qaeda pose CBRNE threat to “top five” cities in US?

Peer-to-Peer Collaboration Tools

Create problem-centric space for data sharing & analysis
Decision Support Tools
- Understand complex situations
- Provide competitive analyses
- Offer more options
- Utilize models for:
  - Context for information
  - Definition of search parameters
  - Method for sharing & reasoning

Collaboration
- Bring diversity to problem solving
- Addresses uncertainty in data
- Punch holes in the stovepipes
- Hybrid center-edge collaboration
  - **Center**: corporate memory, data warehouses, central servers
  - **Edge**: trust, agile, ad-hoc
**TIA Enabling Technologies**

**Foreign Language Translation**

- **TIDES Program**
  - Translation – Arabic & Chinese
  - Detection – discover critical data
  - Extraction – pull out key entities
  - Summarization – reduce amount of material user must read

- **EARS Program**
  - Rich automatic speech-to-text transcriptions (words + metadata)
  - Reduce word error rate to 5-10%

- **Babylon Program**
  - Rapid two-way translation
  - Tactical field environments
  - One-way devices transitioned to Afghanistan and Guantanamo
  - 48 langs: Farsi, Urdu, Pashto, etc

---

**Voice Input**

- Halt! Don’t move!
- Man komk mekham!
- Are you hurt?

**Audio Output**

- Waisa, harkat nakon!
- I need help!
- Aya majroh shodee?
- I am in labor!
Evidence Extraction & Link Discovery (EELD)
- Discover complex patterns indicative of terrorist activity
- Evidence Extraction – people, places, things, events, etc
- Link Discovery – relations between different entity types

Pattern Learning – attack plans, group relationships, etc
**TIA Enabling Technologies**

**Predictive Modeling**

- **Wargaming the Asymmetric Environment (WAE) Program**
  - Predict future terrorist group attacks (target, tactic, time, etc)
  - Based on behavioral sciences
  - Being used by agencies for I&W

- **Bio-ALIRT Program**
  - Early detection and warning of bio-terrorism event
  - Explore value if unconventional data sources: OTC medications, school absenteeism, grocery food sales, etc
**TIA Enabling Technologies**

**Biometrics**

- **Human ID at a Distance (HID)**
  - Develop automated multi-modal biometric techniques for identifying humans at a distance (500 ft)

- **Multi-modal Biometrics**
  - Face Recognition
  - Gait – body dynamics

- **Advanced Sensors**
  - Images, photos, video, infrared, hyper-spectral, radar

- **2D and 3D Techniques**
• **Funded research in privacy technology (part of two IAO programs)**
  – Bio-ALIRT – *k*-anonymity (CMU)
  – Genisys – numerous promising approaches (PARC)
    - privacy appliance
    - selective revelation
    - anonymization
    - expunging filters
    - audit trails
    - encrypted queries
    - self-reporting data
    - SW agents
    - inference control

• **Funded privacy studies:**
  – *Center for Strategic and International Studies (CSIS)*
    - Developing a blueprint of a new privacy protection model, including oversight and structural and legal protections
  – *Potomac Institute*
    - Examining nexus of technology, policy and legal issues associated with counter terrorism and civil liberties
  – *University of Connecticut and MIT*
    - Explore concept of using data transforms (e.g., plain-text to cipher-text) to solve complex analytical problems while simultaneously protecting privacy
• Agencies are experimenting w/ TIA prototypes
  – Using existing, legally obtained data

• Researching technology to extract & fuse sparse terrorist threat-indicative events out of a sea of information clutter
  – Pull threat signal out of the noise
  – Connect the dots
  – Protect sources & methods, privacy

• Ultimate success requires a co-evolution
  – Technology
  – Process/Operations
  – Policy
  – Culture
### Joint Inquiry Systemic Finding

#### #4: While technology remains one of this nation’s greatest advantages, it has not been fully and most effectively applied in support of U.S. counterterrorism efforts. Persistent problems in this area included a lack of collaboration between Intelligence Community agencies, a reluctance to develop and implement new technical capabilities aggressively, the FBI’s reliance on outdated and insufficient technical systems, and the absence of a central counterterrorism database.

#### #5: Prior to September 11, the Intelligence Community’s understanding of al-Qa’ida was hampered by insufficient analytic focus and quality... Analysis and analysts were not always used effectively... (There was) a persistent inability to comprehend the collective significance of individual pieces of intelligence. These analytic deficiencies seriously undercut the ability of U.S. policymakers to understand the full nature of the threat, and to make fully informed decisions.

#### #6: Prior to September 11, the Intelligence Community was not prepared to handle the challenge it faced in translating the volumes of foreign language counterterrorism intelligence it collected...

#### #9: The U.S. Government does not presently bring together in one place all terrorism-related information from all sources... Within the Intelligence Community, agencies did not adequately share relevant counterterrorism information... (even within agencies)...

#### #10: Serious problems in information sharing also persisted, prior to September 11, between the Intelligence Community and relevant non-Intelligence Community agencies...

### On-Going Information Awareness Programs

- **TIA Experimental Multi-Agency Network**
- **Genoa II**
- **Evidence Extraction and Link Discovery**
- **Genisys**
- **Genisys Privacy Protection**

- **Genoa II**
- **Evidence Extraction and Link Discovery**
- **Genisys**
- **Genisys Privacy Protection**
- **Wargaming the Asymmetric Environment**
- **Bio-Event Advanced Leading Indicator Recognition Technology**

- **Effective, Affordable, Reusable Speech-to-Text**
- **Translingual Information Detection, Extraction, and Summarization**

- **TIA Experimental Multi-Agency Network**
- **Genoa II**
- **Evidence Extraction and Link Discovery**
- **Genisys**
- **Genisys Privacy Protection**

- **TIA Experimental Multi-Agency Network**
- **Genoa II**
- **Evidence Extraction and Link Discovery**
- **Genisys**
- **Genisys Privacy Protection**
<table>
<thead>
<tr>
<th>Joint Inquiry Recommendation</th>
<th>On-Going Information Awareness Programs</th>
</tr>
</thead>
</table>
| 3:  ...improve and expand the use of data-mining and other cutting edge analytical tools… | • Genoa II  
• Evidence Extraction and Link Discovery  
• Genisys  
• Genisys Privacy Protection  
• Wargaming the Asymmetric Environment  
• Bio-Event Advanced Leading Indicator Recognition Technology |
| 5:  ...(develop)... an effective all-source terrorism information fusion center that will dramatically improve... counterterrorism analysis… (The center should) have full and timely access to all counterterrorism-related intelligence information, including raw supporting data... (and) implement and fully utilize data mining and other advanced analytical tools… | • TIA Experimental Multi-Agency Network  
• Genoa II  
• Evidence Extraction and Link Discovery  
• Genisys  
• Genisys Privacy Protection  
• Wargaming the Asymmetric Environment  
• Bio-Event Advanced Leading Indicator Recognition Technology |
| 6:  ... implement mechanisms to maximize the exchange of counterterrorism-related information between the FBI and other federal, state and local agencies… | • Genoa II  
• Evidence Extraction and Link Discovery  
• Genisys  
• Genisys Privacy Protection |
| 18:  ...(develop) a national watchlist center… for coordinating and integrating all terrorist-related watchlist systems… | • TIA Experimental Multi-Agency Network  
• Genoa II  
• Evidence Extraction and Link Discovery  
• Genisys  
• Genisys Privacy Protection |