

CSIIR/IOC

Technologies & Capabilities

Presented to

Intrinsically Assurable MANET DARPA Proposers' Day Conference

by

Frederick Sheldon

**Cyberspace Sciences & Information Intelligence Research (CSIIR)
Information Operations Center (IOC)
Computational Sciences and Engineering Division (CSED)**

26 April 2007

FOUO - NOFORN

OAK RIDGE NATIONAL LABORATORY
U. S. DEPARTMENT OF ENERGY

Computational Science & Engineering Division (CSED)



- **Data Systems Sciences & Engineering (DSSE)**

- Systems architecture and design
- Large scale data management

- **Geographic Information Science & Technology (GIST)**

- Population and social dynamics
- Feature and process extraction

- **Applied Software Engineering & Research (ASER)**

- Agent-based methods
- Text analysis

- **Modeling and Simulation (M&S)**

- Predictive simulations
- Discrete event simulations

- **Cyberspace Sciences & Information Intelligence Research**

- Information assurance
- Information Operations

- **Quantum Information Science (QIS)**

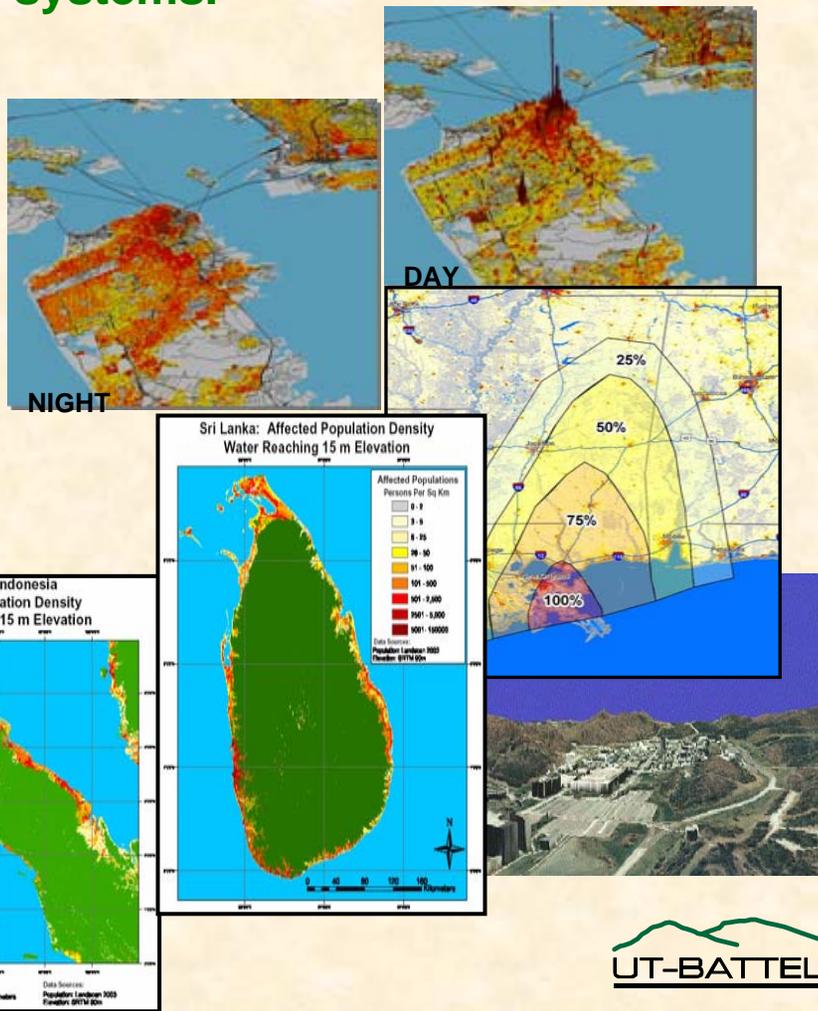
- Quantum Source
- Quantum Theory

Geographic Information Science & Technology (GIST) Group

The mission of GIST is to support national environmental, energy, and defense programs through research, development, and application of geographic information and analysis systems.

Current GIST technologies include:

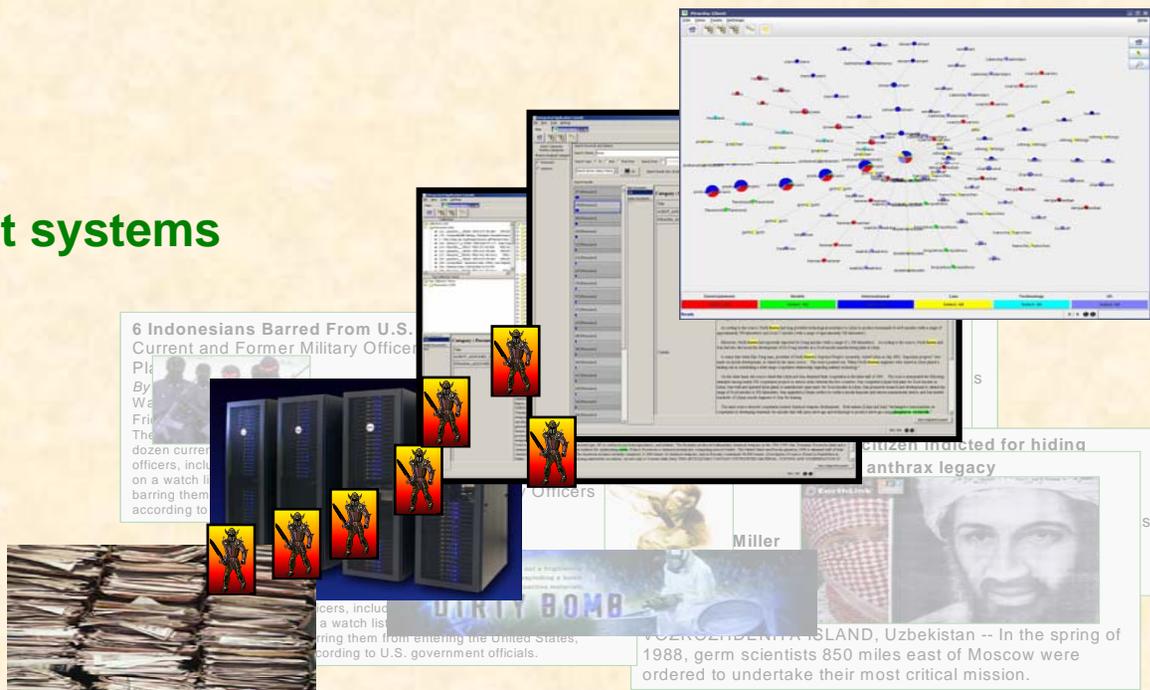
- advanced digital remote sensing
- development of advanced GIS algorithms
- advanced image analysis and interpretation
- automation of imagery processing techniques
- computer cartography and thematic mapping
- 3D visualization and animation
- digital terrain modeling
- demographic modeling
- global positioning systems



Applied Software Engineering Research (ASER) Group

Mission: To pioneer scientific advances and technical innovations in computer science research. We aim to revolutionize the application of computer science research to government, industry, academic, and military issues by:

- Large scale multi-agent systems
- Text analysis
- Text and video fusion



Modeling and Simulation (M&S) Group

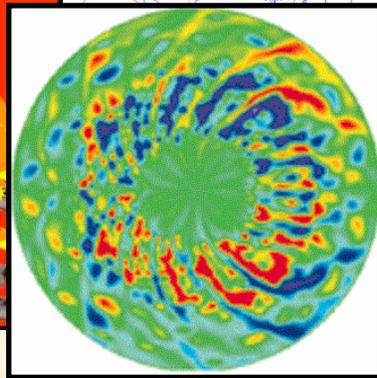
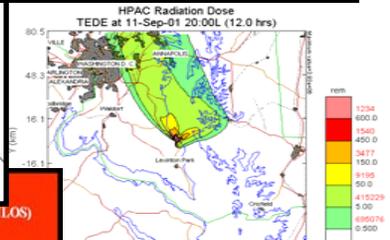
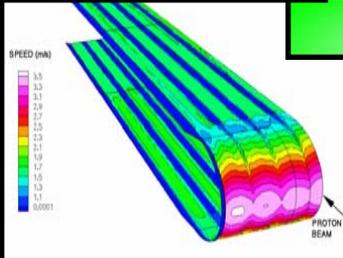
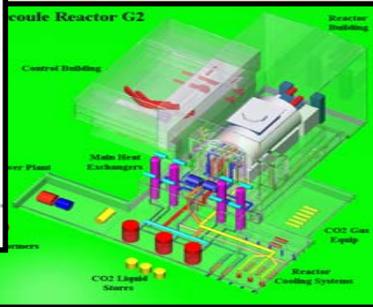
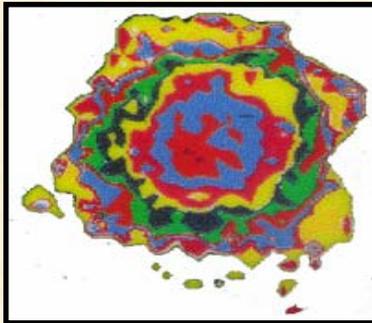
- **Four Focus Areas**

- **Parallel Discrete Event Simulations for Large Systems**

- **Multi-disciplined Physics-based Predictive Simulations**

- **Simulation of Complex Highly Coupled Nonlinear Systems & Networks**

- **Inverse Simulations to Determine Unknown Causes from Known Effects**



Cyberspace Sciences & Information Intelligence Research (CSIIR) Group - Mission

- Conduct basic and applied research to develop secure trusted systems
- Understand existing and emerging cyberspace threats to critical assets
- Advance state-of-the-art in insider threat detection, deterrence, and mitigation
- Develop leading-edge end-to-end integrated core capabilities and solutions to:
 - Deny adversaries the opportunity to exploit vulnerabilities
 - Validate advanced technologies to defend, preserve, and mitigate risks
 - Enable continued survival of friendly cyberspace infrastructure
- Ensure continuing security, survivable, and dependability of the national critical cyber infrastructure through rapid proactive scalable prototyped technologies

The collage features several key visual elements:

- Network Diagram:** A network graph with a central node circled in blue, representing a critical asset or hub.
- SCADA Systems & Critical Infrastructure Protection:** A slide showing various industrial systems including electric power generation, transportation systems (a train), and water treatment and distribution.
- IVA Compliance Enabling Technology (ICETECH):** A slide detailing the ICETECH IVA Concept of Operations and the Cyber Situational Awareness Architecture, which includes components like Control Framework, Agent Based, Distributed, Near Real Time Control, and Fusion of Detectors.
- Network Map:** A map showing various nodes and hubs, including 'Internet', 'sumo', 'phido', 'hub', 'valor', 'aztec', 'vigilant', 'puffin', 'zia', 'seahawk', 'maya', 'sandman', 'arawak', 'victor', 'kiowa', 'antigua', and 'pueblo'.
- 3D Visualization:** A 3D rendering of a network cluster with nodes and connections, labeled 'Cluster of nodes sharing the same group key'.

CSIIR - Overview

- **CSIIR is a dedicated research organization**
- **Consists of 22 organic and 4 matrix staff**
- **Manages the Information Operations Center (IOC), a specialized information operations research capability**
- **Classified and unclassified research facilities**
 - **Network labs**
 - **RF isolation chamber**
- **Threat assessment**
- **Red teams and vulnerability assessment**
- **Sponsors the annual Cybersecurity and Information Infrastructure Workshop, hosting participants from academia, industry, and government**

Technology Prototypes & Capabilities

- **AdAASS - Adaptive Analyst Assessment Support System**
 - **CAMIO - Cultural and Media Influences on Opinion**
 - **HIT-IT - Heuristic Identification and Tracking of Insider Threat**
 - **ICETECH - Information Assurance Vulnerability Assessment (IAVA)
Compliance Enabling Technology**
 - **ORCAT – Oak Ridge Content Analysis Tool**
 - **TARA - Threat Assessment Risk Analysis Management Framework**
 - **TEAM – Terrorist Evolutionary Assessment Model**
 - **UNTAME - Ubiquitous Network Transient Autonomous Mission Entities**
 - **Others.....**
-
- **RED Team**
 - **Threat Assessments**
 - **Vulnerability Assessments**
 - **Network Laboratory**
 - **IF Isolation Laboratory**
 - **Information Operations**

Research Interest and Proposals

- *Distributed Zero-Day Attack Detection*
- *Trust-Based Agent Security Services*
- *Virtual Machines for Seamless Security (ViMaSS)*
- *Adaptable, Intelligent, Malfeasance Detection (AIMD)*
- *Anomaly Detection via Nonlinear Analysis (ADNA)*
- *Digital Asset Protection (DAP) mitigating Emerging Hybrid Malware and Other Threatening Activities*
- *Distributed Intrusion Detection and Attack Containment (DIDAC) for Organizational Cyber Security*
- *EEG Biometric*
- *Active Tracking & Archiving Forensic (ATAF) Tool*
- *Insider Threat Detection (ITD) System*
- *New Paradigm for Knowledge Discovery*
- *Software Testing Verification and Validation*
- *Ticketed E-mail*
- *Insider Threat Emulation Model (ITEM)*
- *Waveguide Entangled Photon Source*
- *Quantum Information Theory, Encryption & Computing*

THANK YOU

QUESTIONS ?

FACT SHEETS AVAILABLE

www.ioc.ornl.gov

OAK RIDGE NATIONAL LABORATORY
U. S. DEPARTMENT OF ENERGY

FOUO - NOFORN