

18th Annual NDIA SO/LIC Symposium and Exhibition
"Warfare in the Seams:
Defense and Industry Partnering to Win the Long War"

Arlington, VA

26-28 February 2007

Agenda

Monday, 26 February 2007

Military Services' Chief Scientists and Technologists Panel Presentations: ***"Transforming General Purposes Forces for Warfare in the Seams"***
Panel Members:

- Mr. George W. Solhan, Director, Expeditionary Warfare Operations, Office of Naval Research, ***"Warfare in the Seams: Defense and Industry Partnering in the Long War"***
- Mr. Jack McCready, US Coast Guard Research and Development Center, ***"USCG – Deployable Operations"***

National Laboratories Panel Presentations**: *"Technologies from the National Labs to Wage the Long War"***
Panel Members:

- Dr. Mark A. Buckner, Cognitive Radio Program Director RF and Microwave Systems, Oak Ridge National Laboratory, ***"Technologies to Help Wage the Long War"***
  - Dr. Michael V. Fazio, Deputy Program Director for Defense and Homeland Security, Los Alamos National Laboratory, ***"Los Alamos National Laboratory Overview"***
  - Dr. John Garnier, Armor Program Lead/Idaho Survivability Program, Idaho National Laboratory, ***"National and Homeland Security at INL"***
  - Dr. Russell D. Skocypec, Deputy Director Human Systems and Simulation Technologies, Sandia National Laboratory, ***"Technologies from the National Labs to Wage the Long War"***
  - Dr. Peter Vanier, Physicist, Detector Development Division, Nonproliferation and National Security Department, Brookhaven National Laboratory, ***"Stand-Off Nuclear Radiation Detection"***

Tuesday, 27 February 2007

USSOCOM Service Component Panel: ***"Capabilities, Challenges, and Technology Needs for Special Operations in the Long War"***
Panel Member:

- Brigadier General Steven J. Hashem, USA Reserve President, Joint Special Operations University and Center Director, Special Operations Knowledge and Futures, ***"Center for Knowledge and Futures (SOKF) Overview Brief"***
- Brigadier General Steven J. Hashem, USA Reserve President, Joint Special Operations University and Center Director, Special Operations Knowledge and Futures, ***"Joint Special Operations University"***

Reports from the Field Panel: ***"Defense and Industry Vignettes in Waging Warfare in the Seams"*** ***Moderator and Panel Member:*** Colonel Lee An Van Arsdale, USA (Ret), Chief Executive Officer, Triple Canopy, Inc. ***"Warfare in the Seams Industry Vignettes"***

- Major General Benoit Puga, Commander, French Special Operations Command, ***"Waging the Long War on Terrorism"***
- Major General Edward Gruszka, Commander, Polish Special Operations Command, ***"Polish SOF (Report From the Field"***
- Brigadier General Remo Butler, USA (Ret), Vice President: Operations; Operations, Maintenance, and Logistics; Kellogg Brown & Root, ***"Contractors on the Battlefield"***
- Colonel Kenneth Tovo, USA, Commander, 10th Special Forces Group, ***"Combined Joint Special Operations Task Force – Arabian Peninsula (CJSOTF-AP)"***
  1. Video Sadr City Operations July 2006
  2. Video Sadr City Operations August 2006
  3. Video EW Success in Sadr City
- Colonel Norman J. Brozenick, Jr., USAF, Commander, 1st Special Operations Wing, ***"USAF Special Operations in the Seams"***
  1. Video Air Craft Personnel
  2. Video AC 130 H
  3. Video Battlefield Airmen
  4. Video MC 130 H

5. Video MC 130 P
6. Video Medics
7. Video MH 53
8. Video Music
9. Video 6th SOS

Wednesday, 28 February 2007

Keynote Address: ***"Perspectives on Special Operations and Warfare in the Seams"***
Honorable Thomas W. O'Connell, Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict,
Keynote Address: ***"Counter-Network Operations"***
Lieutenant General William G. "Jerry" Boykin, USA, Deputy Undersecretary of Defense for Intelligence and Warfighting Support ***"The Global War on Terrorism or A Global Insurgency"***
Miscellaneous:
Major General Donald Wurster, Vice Commander, Air Force Special Operations Command, ***"Challenges for the Long War"***

1. Video Bad Day
2. Video CV-22
3. Video Die Tired
4. Video Gunship Fire
5. Video Predator Hellfire
6. Video Talon

Major Joe McGraw, NPS, Defense Analysis Department, ***"Limitations of the National Defense Union: Why the DOD-DI relationship is best left at home"***
Captain David B. Moon, USAF, Joint Information Operations Student Department of Defense Analysis***, "Cyber-Herding: Exploiting Islamic Extremists Use of the Internet"***
Lieutenant General John F. Sattler, Director for Strategic Plans and Policy, The Joint Staff, ***"The View from the Joint Staff"***

Theme:

"Warfare in the Seams:
Defense and Industry Partnering to Win the Long War"

Sunday, February 25, 2007

12:00pm-6:00pm **Registration Open**

Monday, February 26, 2007

7:00am-8:45am **Continental Breakfast in Exhibit Hall**

7:00am-7:00pm **Registration**

8:45am **Welcome & Opening Remarks**
Lieutenant General Larry Farrell, USAF (Ret), President, NDIA

Colonel Thomas E. "Tim" Davidson, USAF (Ret), Chairman, NDIA SO/LIC Division and Chairman, 18th Symposium

Major General Kenneth R. Bowra, USA (Ret), Vice Chairman, 18th Symposium

9:00am **Keynote Address: "Challenges to the United States and Coalition Forces in Waging the Long War on Terrorism"**
Brigadier General Mark T. Kimmitt, USA (Ret), Deputy Assistant Secretary of Defense for Near Eastern and South Asian Affairs and Former Deputy Director of Operations and Chief Military Spokesman for Coalition Forces in Iraq during Operation Iraqi Freedom

9:45am **Break**

10:00 am **Military Services' Chief Scientists and Technologists Panel**
"Transforming General Purposes Forces for Warfare in the Seams"
e.g., Training and Technology required to Conduct Military Operations in Cities, Mountainous Regions, Desert Terrain, and to Secure Long Borders from Hostile Incursions
Moderator: J. Frank Wattenbarger, Director Advanced Technologies, Concurrent Technologies Corporation

Panel Members:

- Mr. Richard Chandler, Director of Advanced Technology, US Special Operations Command
- Dr. Mark Ohair, Munitions Directorate, Air Force Research Laboratory

- Mr. George W. Solhan, Director, Expeditionary Warfare Operations, Office of Naval Research
- Mr. Edward J. Doucette, Director, Warfighter Protection and Aerial Delivery, Natick Soldier Research Development and Engineering Center, US Army
- Mr. Jack McCready, US Coast Guard Research and Development Center

11:50am **Lunch (Exhibit Hall B)**

1:40 pm **National Laboratories Panel, Regency Ball Room**
"Technologies from the National Labs to Wage the Long War"
Moderators: Major General Kenneth R. Bowra, USA (Ret), Oak Ridge National Laboratory and Liaison to USJFCOM (J-9)

Panel Members:

- Dr. Mark A. Buckner, Cognitive Radio Program Director RF and Microwave Systems, Oak Ridge National Laboratory
- Dr. Michael V. Fazio, Deputy Program Director for Defense and Homeland Security, Los Alamos National Laboratory
- Dr. John Garnier, Armor Program Lead / Idaho Survivability Program, Idaho National Laboratory
- Dr. Russell D. Skocypec, Deputy Director Human Systems and Simulation Technologies, Sandia National Laboratory
- Dr. Robert G. Spulak, Jr., Manager, Strategic Studies Department, Sandia National Laboratory
- Mr. John Tanke, Department of Energy Liaison to U.S. Special Operations Command
- Dr. Peter Vanier, Physicist, Detector Development Division, Nonproliferation and National Security Department, Brookhaven National Laboratory

3:30 pm **Exhibit Hall Open (See Agenda for Industry Presentations or Demonstrations)**

5:30pm – 7:00pm **Reception in Exhibit Hall**

Tuesday, February 27, 2007

7:00am-8:45am **Continental Breakfast in Exhibit Hall**

7:00am-6:30pm **Registration**

8:45am **Administrative Remarks**

Colonel Thomas E. "Tim" Davidson, USAF (Ret), Chairman, NDIA SO/LIC Division and Chairman, 18th Symposium

9:00am **Keynote Address "Special Operations Forces Capabilities and Requirements to Wage the Long War,"**
General Bryan D. "Doug" Brown, USA
Commander, US Special Operations Command

9:45am **Break**

10:00am **USSOCOM Service Component Panel, Regency Ball Room**
"Capabilities, Challenges, and Technology Needs for Special Operations in the Long War"
Moderator: Lieutenant General William P. Tangney, USA (Ret), Senior Vice President, Future Technologies, Inc.

Panel Members:

- LTG Robert W. Wagner, USA
  Commander, US Army Special Operations Command
- Lt Gen Michael W. Wooley, USAF
  Commander, Air Force Special Operations Command
- Rear Admiral Joseph Maguire, USN
  Commander, Naval Special Warfare Command
- Major General Dennis J. Hejlik, USMC
  Commander, Marine Special Operations Command
- Brigadier General Steven J. Hashem, USA Reserve
  President, Joint Special Operations University and Center Director, Special Operations Knowledge and Futures

12:00 pm **Lunch (Exhibit Hall B)**

1:40 pm **Reports from the Field Panel, Regency Ball Room**
"Defense and Industry Vignettes in Waging Warfare in the Seams"
Moderator and Panel Member: Colonel Lee A. Van Arsdale, USA (Ret), Chief Executive Officer, Triple Canopy, Inc.

Other Panel Members:

- Major General Benoit Puga, Commander, French Special Operations Command
- Major General Edward Gruszka, Commander, Polish Special Operations Command
- Brigadier General Remo Butler., USA (Ret); Vice President; Operations, Maintenance, and Logistics; Kellogg Brown & Root

- Colonel Kenneth Tovo, USA. Commander, 10th Special Forces Group
- Colonel Norman J. Brozenick, Jr., USAF, Commander, 1st Special Operations Wing
- Captain Sean Pybus, USN, NAVSPECWARCOM Representative

4:00 pm **Exhibit Hall Open (See Agenda for Industry Presentations or Demonstrations)**

5:15pm – 6:30pm **Reception in Exhibit Hall**

6:30pm – 9:30pm **Awards Banquet and Dedication to COL Al DeProspero, USA (Ret)**

Wednesday, February 28, 2007

7:00am-8:45am **Continental Breakfast in Exhibit Hall**

7:00am-6:30pm **Registration**

8:45am **Administrative Remarks**
Colonel Thomas E. "Tim" Davidson, USAF (Ret), Chairman, NDIA SO/LIC Division and Chairman, 18th Symposium

9:00am **Keynote Address: "Perspectives on Special Operations and Warfare in the Seams"**
Honorable Thomas W. O'Connell, Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict

9:50am **Keynote Address: "Counter-Network Operations"**
LTG William G. Boykin, USA
Under Secretary of Defense for Intelligence

10:35am **Break in Exhibit Hall (Last opportunity to view Exhibits)**

11:40am **Lunch and Keynote Speaker: "Transforming the Department of Defense for the Long War"**
Admiral Edmund P. Giambastiani, Jr., USN, Vice Chairman, Joint Chiefs of Staff (Invited)

1:30pm **Closing Remarks**
Colonel Thomas E. "Tim" Davidson, USAF (Ret), Chairman, NDIA SO/LIC Division and Chairman, 18th Symposium

UNCLASSIFIED

The Global War on Terrorism
Or
A Global Insurgency

28 February 2007

LTG William G. Boykin, USA
Deputy Undersecretary of Defense for Intelligence for Warfighting Support

What kind of War is this?

- *Terrorism:*
  - "The calculated use of unlawful violence or threat of unlawful violence to inculcate fear; intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological" - JP 1-02

- *Activities:*
  - *Bombings*
  - *Assassinations*
  - *Kidnappings*
  - *Robberies*
  - *Intimidation through violence and threats of violence*
  - *Extortion*
  - *Proliferation of WMD*
  - *Information (IO)*

Insurgency

- *Insurgency:*
  - "An organized movement aimed at the overthrow of a constituted government [or governments] through use of subversion and armed conflict" - JP 1-02

Comparison

- *Terrorism:*
  - "The calculated use of unlawful violence or threat of unlawful violence to inculcate fear; intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological" - JP 1-02
- *Insurgency:*
  - "An organized movement aimed at the overthrow of a constituted government [or governments] through use of subversion and armed conflict" - JP 1-02
- *So which is it?*

How do we fight?

- *Terrorism:*
  - Kill or capture terrorists
- *Insurgency:*
  - Use the 7 elements of National Power

7 Elements of National Power

Diplomacy

Information

Military

Economic

Finance

Intelligence

Law Enforcement

7 Elements of National Power

Diplomacy

Information

Military

Economic

Finance

Intelligence

Law Enforcement

Bottom line

- *Information Operations is a warfighting capability…Strategic Communication is an evolving USG-wide concept and process*
  - *Who directs the USG process day-to-day?*
- *How does the US Government (not just DoD) use Information as an element of National Power?*

Strategic Communication: An Evolving Concept

- Strategic Communication (draft definition): The informational instrument of national power in an era of globalization.
  - Focused US government (USG) processes and efforts to understand and engage key audiences in order to create, strengthen or preserve conditions favorable to advancing national interests and policies
  - Uses coordinated *information, themes, plans, programs and actions in collaboration* with other elements of national power

Strategic Communication

- Policy Statements
- US Military Exercise / Military Presence
- News Releases, Statements
- Leaflets, Broadcasts
- Diplomacy, Demarches, Economic Sanctions
- Military Diplomacy, International Military Education and Training



SC is the process of synchronizing these Lines of Operation

Information Operations: Definition

- **"The integrated employment of the core capabilities of:**

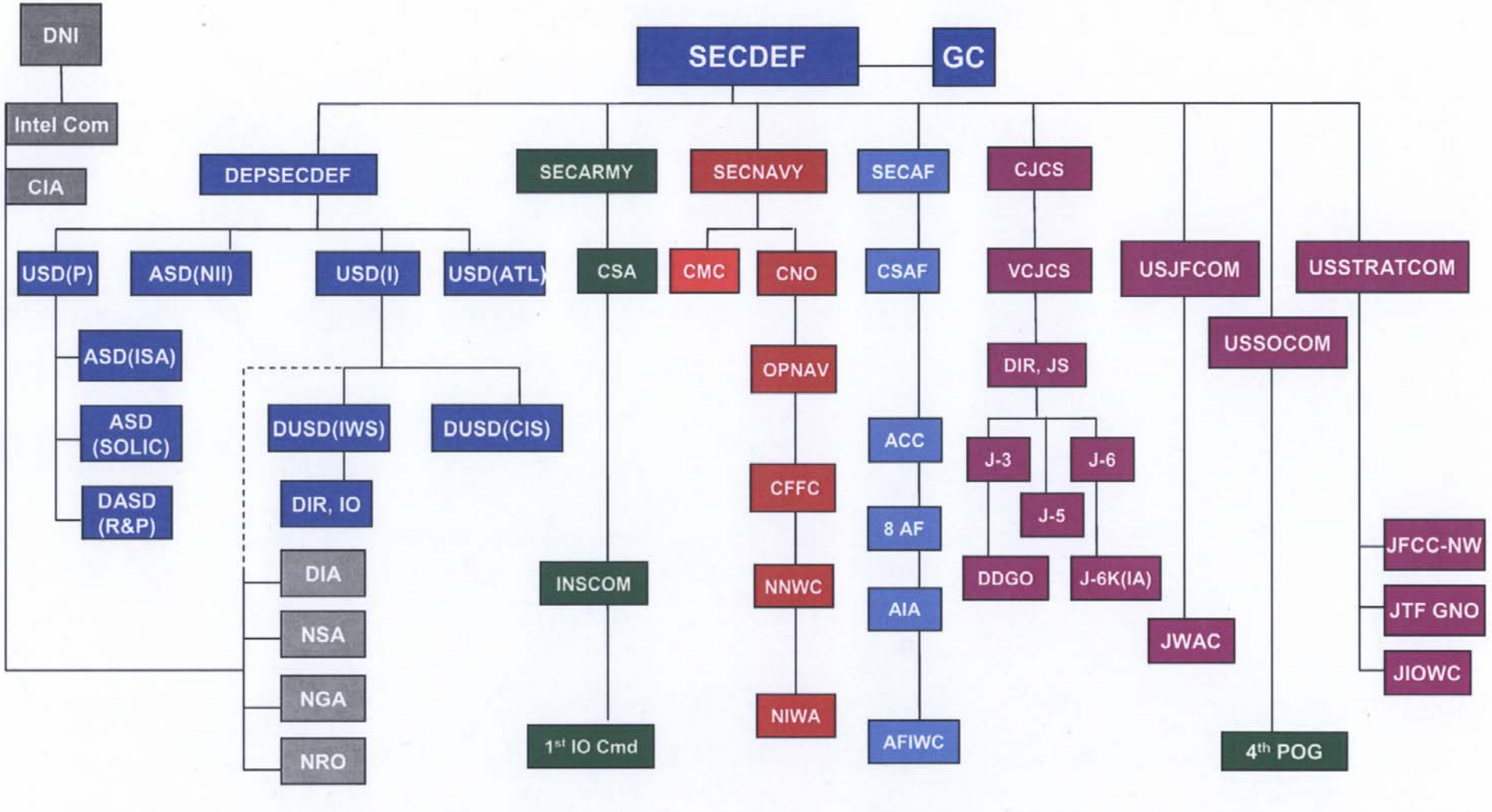
  Electronic Warfare,
  Computer Network Operations,
  Psychological Operations,
  Military Deception, and
  Operations Security,

in concert with specified supporting and related capabilities, to influence, disrupt, corrupt or usurp adversarial human and automated decision-making while protecting our own."

Information Operations: Vision

- **Establish IO as a Core Military Competency for Combatant Commanders to:**
  - **Affect behavior of potential adversaries across the spectrum of conflict**
  - **Exploit, deny, destroy or deceive adversary information during conflict**
  - **Protect friendly information infrastructure and capability**
- **Fully integrate into crisis and deliberate planning**

The DoD IO Community



Information as an Element of National Power

- **Challenges:**
  - Unity of effort and synchronization –no unity of command across USG
  - Lack of commonly understood terms
  - Consensus building, not centralized direction within USG
  - How does the USG convey a consistent message via words and actions?
  - "Psychological Operations"—term can be confusing or intimidating to DoS, others in USG
  - Influencing audiences is not equivalent to deceiving them
  - Potential friction between Public Affairs and Information Operations

7 Elements of National Power

Diplomacy

Information

Military

Economic

Finance

Intelligence

Law Enforcement

National v. Military Intelligence

*"**Title 50** and **Title 10**" Euphemisms for National and Military Intelligence Respectively*

- **National Intelligence** and 'intelligence related to national security'
  - **(A) Pertains to more than one United States Government agency and**
  - **(B) Involves –threats to the United States, the development, proliferation, or use of weapons of mass destruction or any other matter bearing on the United States national or homeland security.**

    (National Intelligence and Reform Act 2004)
- **Military Intelligence**
  - **Intelligence on any foreign military or military-related situation or activity that is significant to military policy making or the planning and conduct of military operations and activities**

    (Glossary of Intelligence Terms and Definitions, Intelligence Community Staff, June 1989)

HUMINT

DoD HUMINT

DoD HUMINT Definition: "A category of intelligence derived from information collected and provided by Human sources" (Joint Pub 1.02)

Types of HUMINT Activities

- Military Source Operations
  - Agent Recruitment
  - Interrogation
  - Debriefing
  - Low Level Source Operations
  - Low Level Contacts
- Attaché
- Recon & Surveillance

Methods of conducting HUMINT Activities

- Clandestine
- Overt (selected tasks)

A Condensed History of HUMINT

- **1917-1941 Attaché critical to intelligence effort (some recruited clan sources)**
  - **Perception of failure at Pearl Harbor**
- **1947 National Security Act (Title 50)**
  - **Established CIA (National Clandestine HUMINT)**
  - **Defined SECDEF authorities**
- **Vietnam – robust capability**
  - **Trained case officers**
  - **HUMINT Detachments are established worldwide**
  - **Conducted clandestine source operations**
- **Post Vietnam/Pre-1993 (Cold War Period) No coherent Defense Program**
  - **Services executed Defense HUMINT Activities**
  - **DIA ran attaché system**
  - **Over time, deferred the Secretary's Authorities**
- **Post-1995 (Perry and White Era)**
  - **Cold War expectations of a peace dividend led to dramatic cuts in Defense-wide HUMINT capability**

*DoD **HUMINT** Key Players*

- **USD(I):** provides policy direction for and oversight of Defense HUMINT activities**…on behalf of SECDEF.**
- **Defense HUMINT Manager (Dir, DIA):** responsible for management of the Defense HUMINT enterprise.
- **COCOMs:** responsible for meeting internal needs in respective AORs
- **Services:** collect military intelligence-
  - In support of COCOMs
  - In support of Service Title 10 related intelligence requirements
- **Directorate for HUMINT (DIA/DH):** collects
  - National Intelligence in support of National Intelligence Requirements
  - Military Intelligence in support of DoD and COCOMs

Military Source Operations (MSO)

- MSO is "… the collection from, by and/or via humans, of foreign military and military-related intelligence, conducted under SECDEF authorities, to satisfy Department of Defense needs."
  - Directly support Defense requirements (E.G., Commanders in the field, operational planners)
  - Not planned, employed, or conducted in response to or for collection of National Intelligence
- Conducted by trained personnel under direction of military commanders
- Encompass full gamut of HUMINT ops (includes LLC and LLSO)
- Require deconfliction
- Report adjunct collection of national intelligence value

Imperatives

- **Coordinate, coordinate, coordinate!**
- **Leverage all HUMINT capability (ES2)**
- **Employ HUMINT capability in all environments**
- **Conduct HUMINT in consonance with other disciplines**
- **Sharing information**
- **Conduct all source intelligence analysis**

Questions







Air Force Special Operations Command

USAF SPECIAL OPERATIONS
IN THE SEAMS

Colonel Norman J. Brozenick, Jr.,
Commander, 1st Special Operations Wing

AIR COMMANDOS

America's Specialized Airpower



AIR COMMANDOS

AFSOC in the Seams

- Special Tactics in Afghanistan
- Foreign Internal Defense in the Trans-Sahara
- Surgical teams in the Philippines
- Global flight operations in hostile or denied airspace

AIR COMMANDOS

Afghanistan

Special Tactics Mission: **Plan, prepare, integrate, synchronize, and control air and space power to achieve assigned objectives**

AIR COMMANDOS

Capability



AIR COMMANDOS

Effect: Disrupt, Deny, Destroy



Combat Controllers

- Controlled 2,086 terminal air strikes = 2.81M lbs of bombs
- Controlled/enabled 8,982 sorties…including air ops at 15 austere airfields



Combat Weathermen

- Provided numerous high fidelity forecasts from forward locations ISO precision strike, CSAR, infil/exfil, refueling, and resupply operations



AIR COMMANDOS

Effect: Rescue and Recover

Pararescuemen

- Rescued/recovered teammates after MH-47 crash
- Conducted mass casualty ops after JDAM mishap Mazar-e-sharif
- Rescued MC-130P crew after crash landing at 10,500'
- Fought on Roberts Ridge… rescued and recovered ISO Operation Anaconda







AIR COMMANDOS

Trans-Sahara Region

Foreign Internal Defense Advisor Mission:
Assess, train, and advise Nigerien airmen in C-130 maintenance and flying operations

AIR COMMANDOS

Capability



AIR COMMANDOS

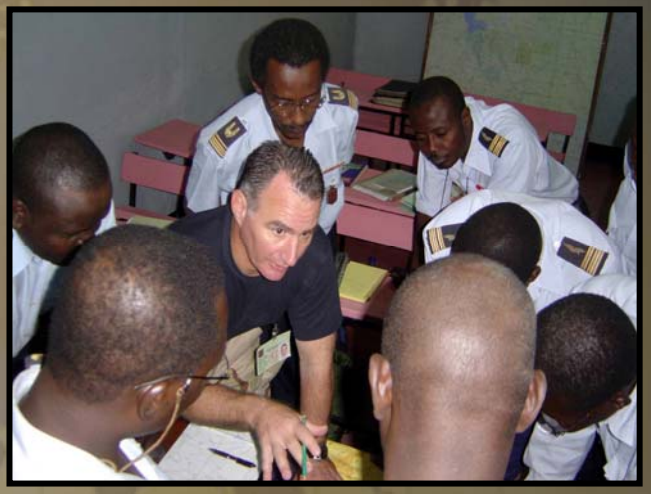
Effect: improve safety, availability, reliability and interoperability

FID Advisors

- Advised Nigerien maintenance refurbish efforts…returned C-130H to flight status

- Trained 46 operations personnel
  - Day tactical flying
  - Aerial re-supply operations
  - Search and Rescue

- Enhanced key relationship ISO EUCOM's Theater Security Cooperation Plan





Republic of the Philippines

Special Operations Surgical Team Mission:
provide trauma care, CASEVAC, and surgical operations for U.S. forces while training Philippine armed forces in same

AIR COMMANDOS

Capability



AIR COMMANDOS

Effect: extend partner nation medical care to forward locations beyond reach

Surgical Teams

- Logged 9K encounters and 3K+ procedures including
  - AFP Clinic: 5,144
  - US Forces: 338
  - CASEVAC: 27
  - Major Surgery: 6
- Supported 30 MEDCAPS







AIR COMMANDOS

Global flight ops in hostile or denied territory

Mission: ISR, infiltration, exfiltration, refuel, resupply, precision fire support, CSAR…*Anytime, Anyplace*

AIR COMMANDOS

Capability



AIR COMMANDOS

Effect: Penetrate, Disrupt, Deny, Destroy

- Found, fixed, finished terrorists & network nodes w/ coalition teammates via
  - Robust C2 network
  - Traditional and “NT” ISR
  - Infiltration/exfiltration
  - Resupply
  - Precision fires
  - Fixed and rotary wing refueling









AIR COMMANDOS

AFSOC Way Ahead…in, above, & beyond the seams

- Fighting and winning the GWOT
- Developing Airmen into highly capable leaders at all levels
- Recapitalizing and modernizing the force

AIR COMMANDOS







Air Force Special Operations Command

USAF SPECIAL OPERATIONS
IN THE SEAMS

Colonel Norman J. Brozenick, Jr.,
Commander, 1st Special Operations Wing

AIR COMMANDOS

UT-BATTELLE

Oak Ridge National Laboratory

"Technologies to Help Wage the Long War"

Presented to the
18th Annual NDIA SO/LIC Symposium

Mark A. Buckner, PhD
Cognitive Radio Program Director
RF & Microwave Systems Group
Oak Ridge National Laboratory
bucknerma@ornl.gov
orbucma@doe.ic.gov

26 February, 2007

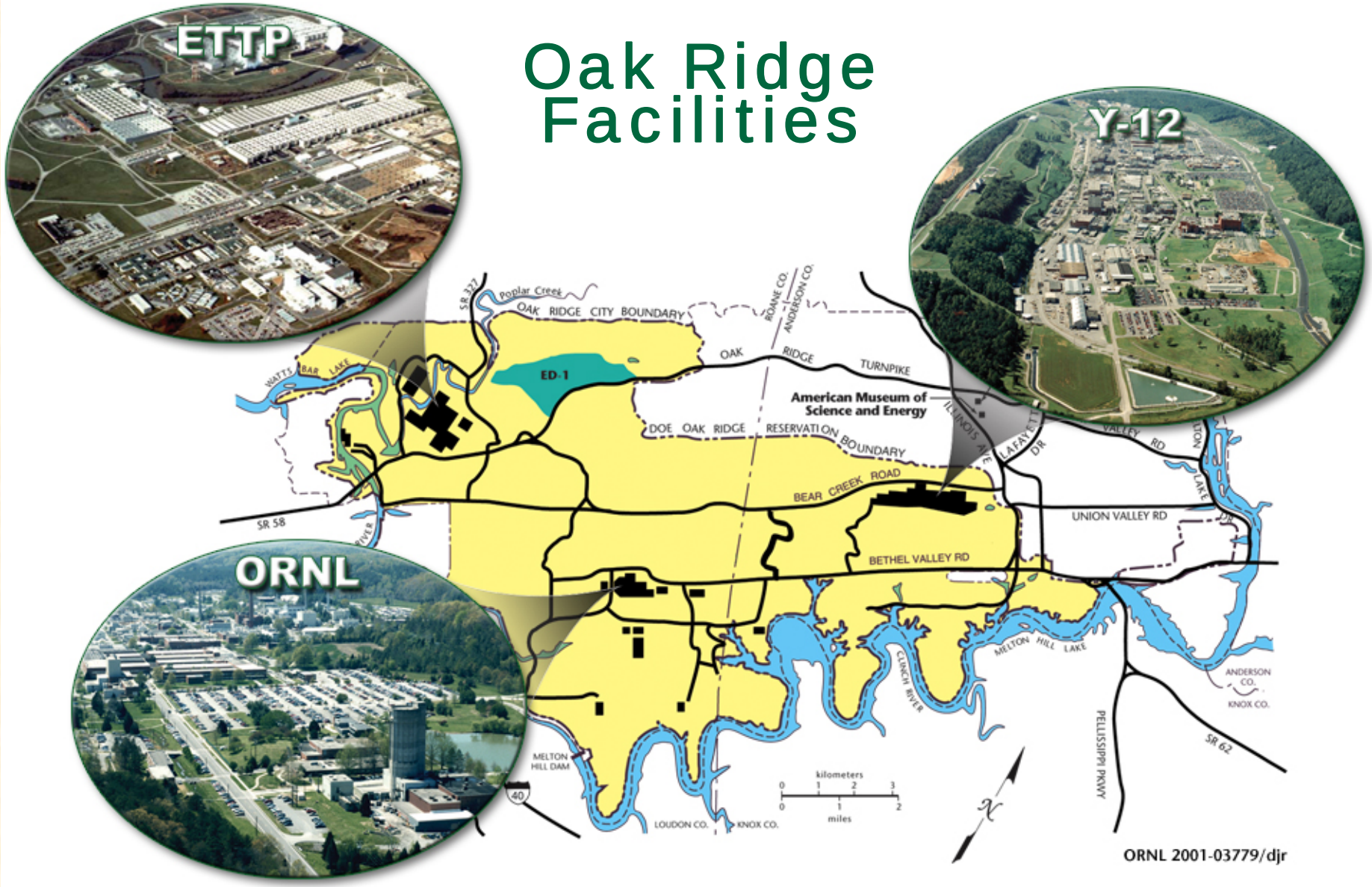


ORNL Cognitive Radio Program Mission:
"to integrate software radio, sensors and computational intelligence capabilities to realize the art-of-the-possible in cognitive computing and communications to address both government and commercial problems, in a manner that enhances US National Security."

Chameleon
...the power of change...

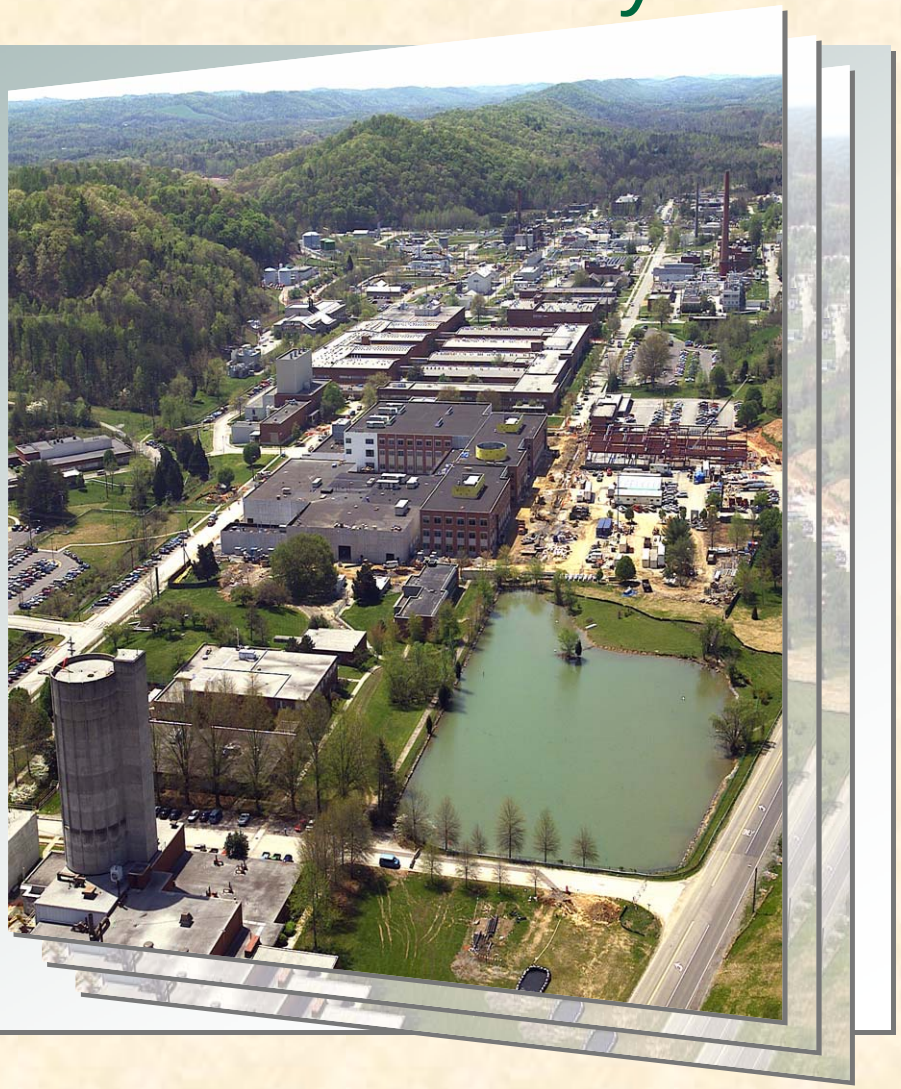
OAK RIDGE NATIONAL LABORATORY
U. S. DEPARTMENT OF ENERGY

Oak Ridge Facilities

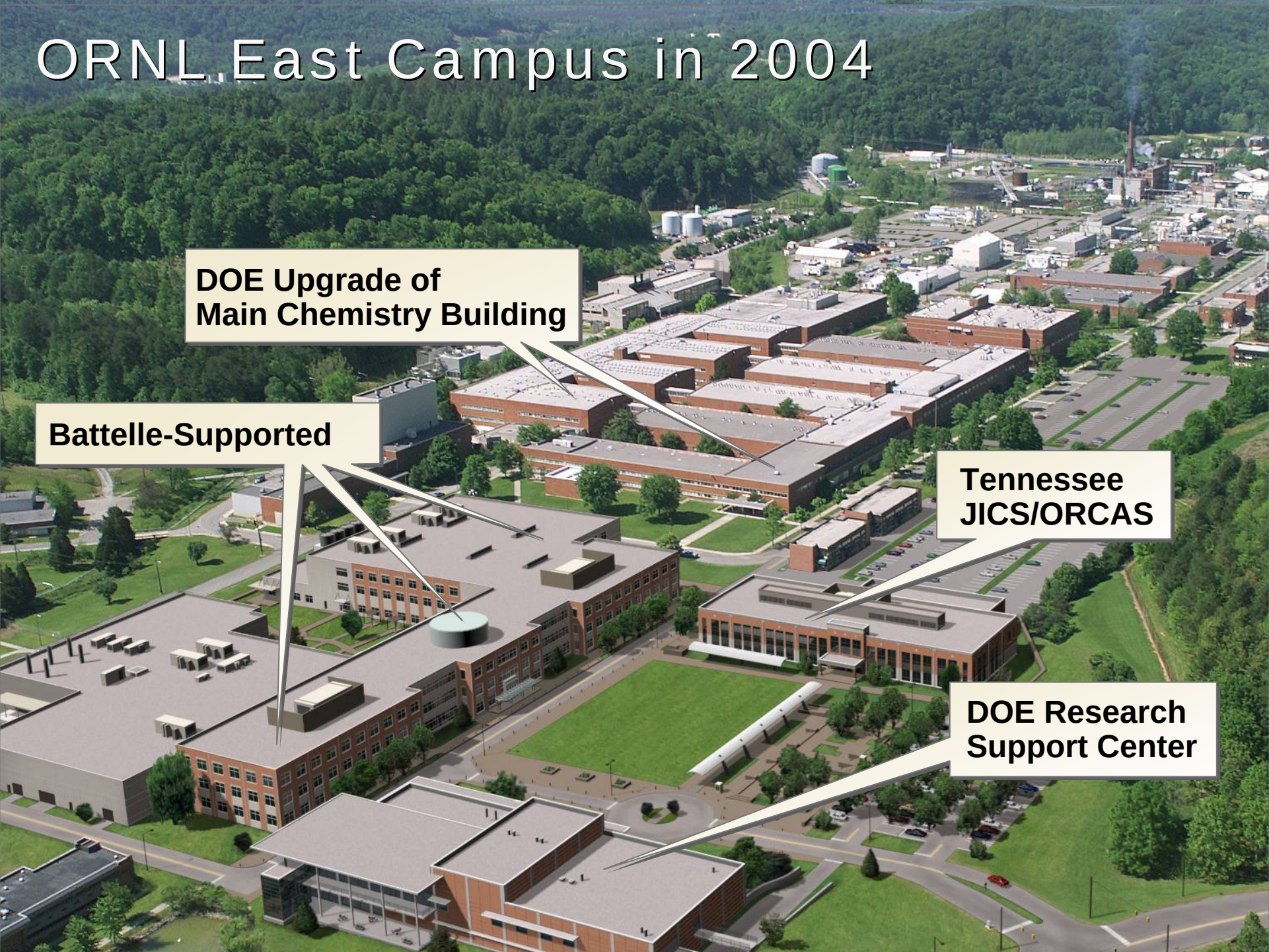


ORNL is DOE's Largest Multi-Purpose Science Laboratory

- **$1 billion budget**
- **3800 employees**
- **3000 research guests annually**
- **Nation's largest energy R&D laboratory**
- **World class computing facilities**
- **Nation's largest concentration of unclassified materials research**
- **$1.4 billion Spallation Neutron Source under construction**
- **$300 million modernization program in progress**



ORNL East Campus in 2004



Multiprogram Research Facility



Capable of handling the full range of national and homeland security work

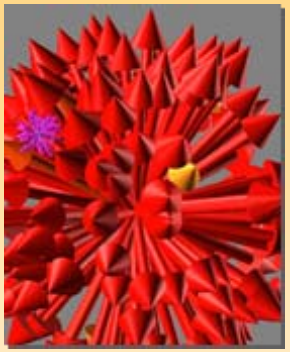
ORNL Science and Technology Agenda Has Six Priorities



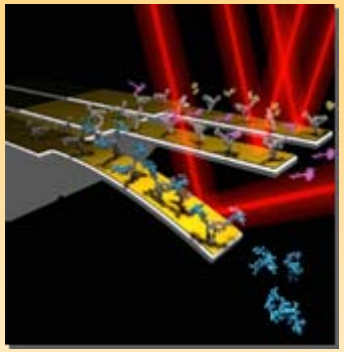
Energy



Homeland/ National Security



Neutron Science



Materials



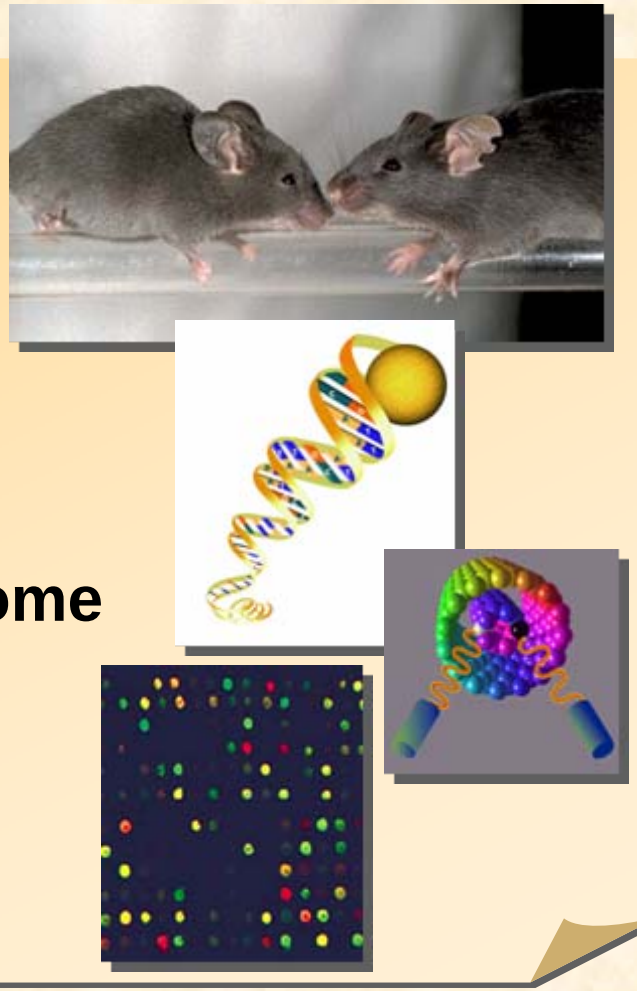
Biology



Computing

A Center Of Excellence For Understanding Complex Biological Systems

- **Moving into a new Laboratory for Comparative and Functional Genomics**
- **Designing a state-funded facility for the Joint Institute for Biological Sciences**
- **Sequencing the hybrid poplar genome**
- **Exploring microbial genomes for bioremediation**
- **Applying life sciences capabilities to needs in homeland security**

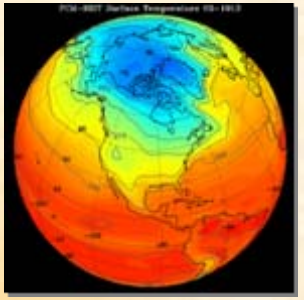


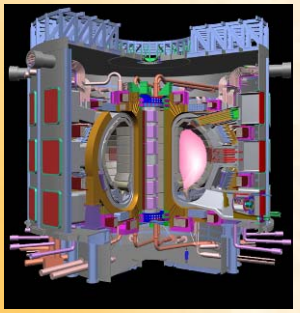
We are at the forefront in computing and simulation

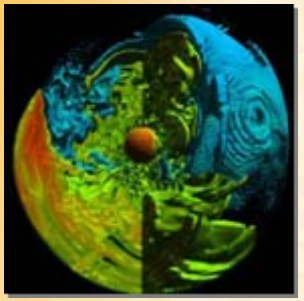
- **Leading the partnership to develop the National Leadership Computing Facility**
  - **World's best scientific computing capability**
  - **100 teraflops in 2006; 250 teraflops by 2007**
- **Attacking key computational challenges**
  - **Climate change**
  - **Fusion**
  - **Nuclear astrophysics**
  - **Materials sciences**
  - **Biology**



- **Providing access to our computational resources through high-speed networking**









We are developing and deploying world-class tools for nanoscale R&D

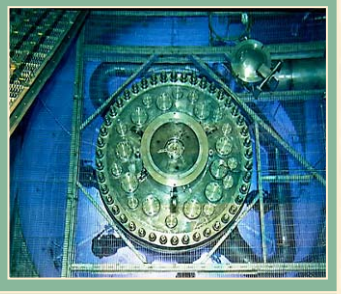
Spallation Neutron Source

- High-intensity neutrons for materials research at the nanoscale
- 1.4 MW of beam power on target
- 16 instruments



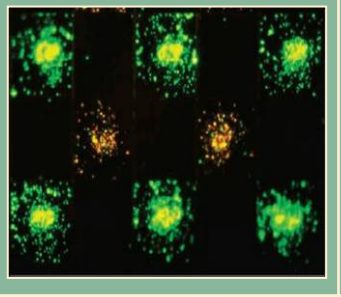
High Flux Isotope Reactor

- The nation's leading research reactor
- World-class for neutron scattering



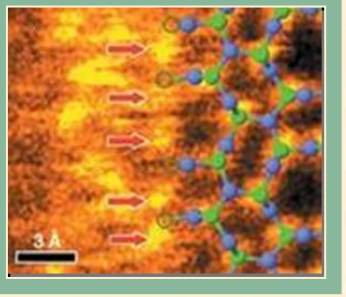
Center for Nanophase Materials Sciences

- $65M facility now in operation
- 75 user projects already under way
- DOE's first nanoscience research center



Ultrahigh-resolution microscopy

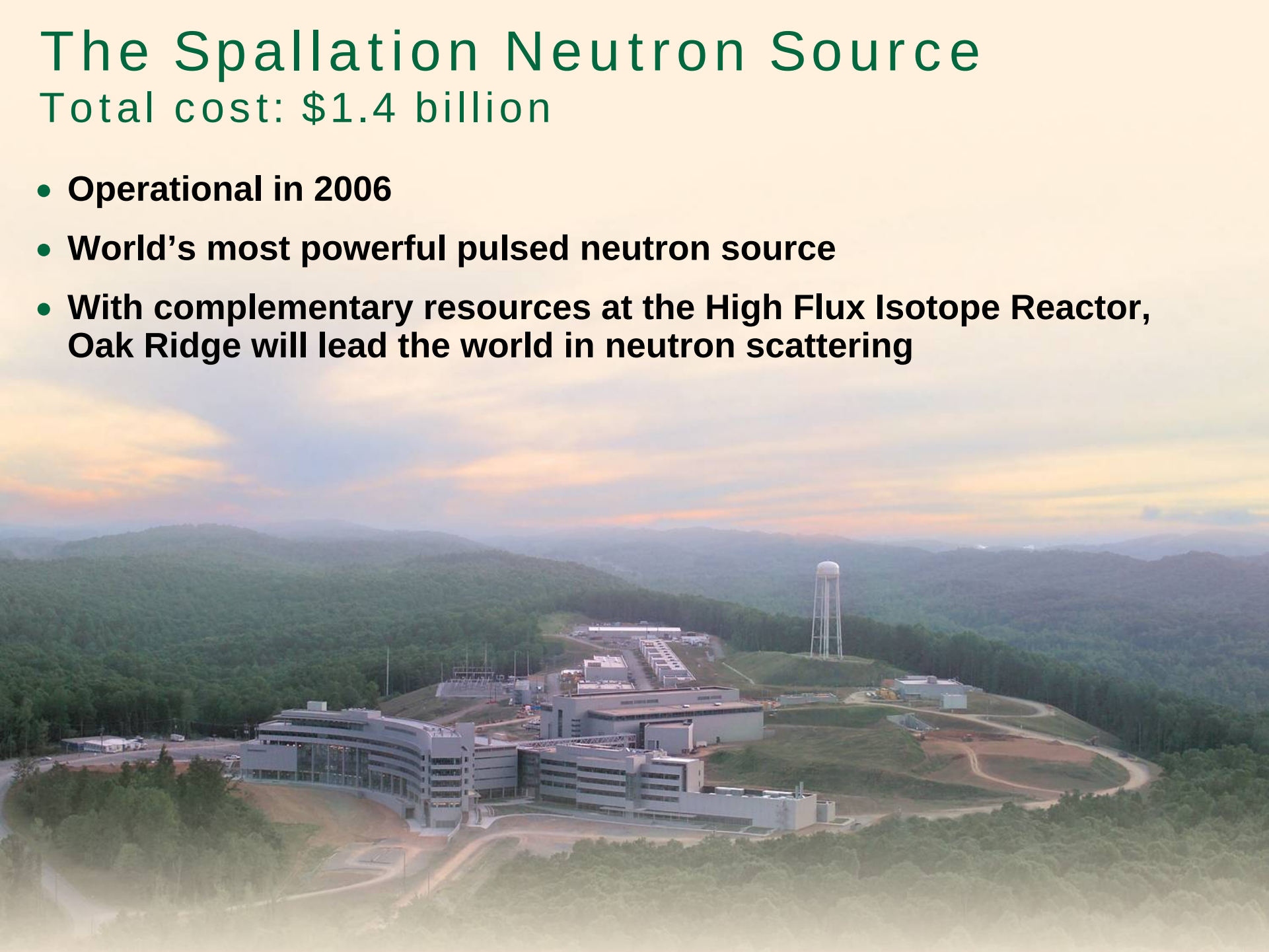
- Advanced Microscopy Laboratory
- Aberration-corrected electron microscope
- World-record resolution: 0.6 Å



The Spallation Neutron Source

Total cost: $1.4 billion

- **Operational in 2006**
- **World's most powerful pulsed neutron source**
- **With complementary resources at the High Flux Isotope Reactor, Oak Ridge will lead the world in neutron scattering**



We have significant strengths in key areas

Radiological and nuclear weapons countermeasures

- **RDD attribution studies, forensics program development, and decontamination of the aftermath**
- **Active interrogation technologies**
- **Radiation detection technologies and new materials**

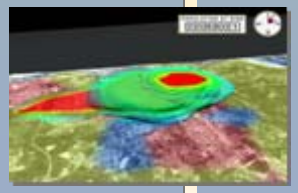
Chemical and biological

- **Mass spectrometry**
- **Bioinformatics**
- **Host-pathogen interactions**



Threat vulnerability testing and assessment

- **Geospatial science**
- **Plume/effect modeling**
- **Cybersecurity technology**



Infrastructure protection

- **Vulnerability assessment and mitigation**

Crosscutting

- **Sensor technologies**
- **Knowledge discovery**



Program areas





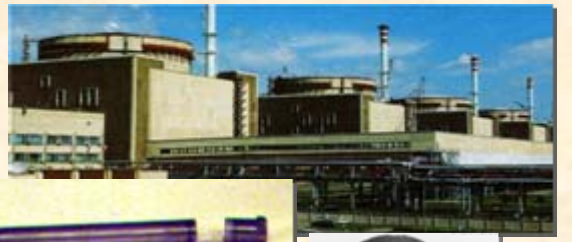


- **Defense Nuclear Nonproliferation**
- **Homeland Security**
- **Department of Defense**
- **Other Government Agencies**

Nuclear Nonproliferation Programs

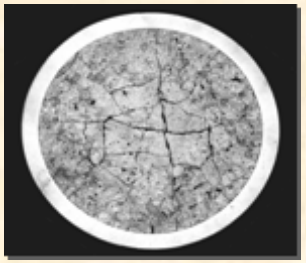
- **Material Protection Control and Accounting**
- **Fissile Materials Disposition**
- **International Safeguards**
- **HEU Transparency**
- **Export Controls**
- **Radiological Dispersal Devices**
- **Nuclear Material Detection & Identification**











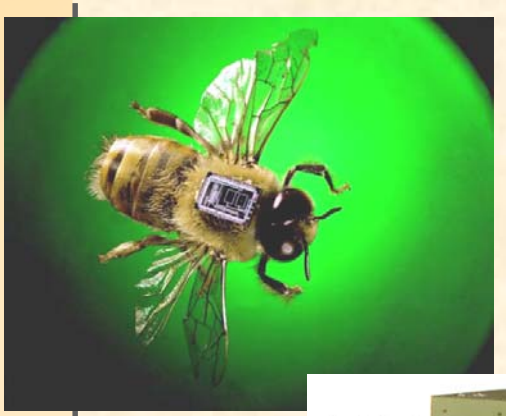
Homeland Security Programs

- **Radiological/nuclear countermeasures**
- **Threat and vulnerability testing and assessment**
- **Biological and chemical countermeasures**
- **Standards development**
- **Countermeasures Testbed**
- **Regional Technology Integration**
- **Protective Security Analysis Center**
- **Transportation analysis**
- **Highway weigh station radiation portal monitors**
- **FEMA support activities**



Department of Defense

- **Military transformation**
- **Chem/Bio defense and early warning**
- **Logistics and transportation management**
- **Defense materials**
- **Sensor miniaturization and communication**
- **Information management, synthesis and analysis**







SensorNet



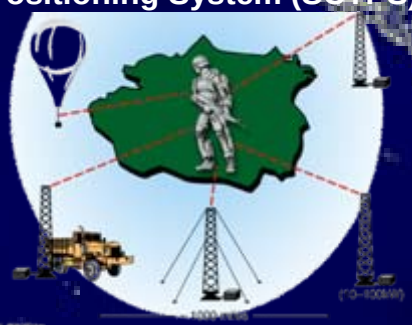
Marine Asset Security & Tracking System (MAST)



MICLOG



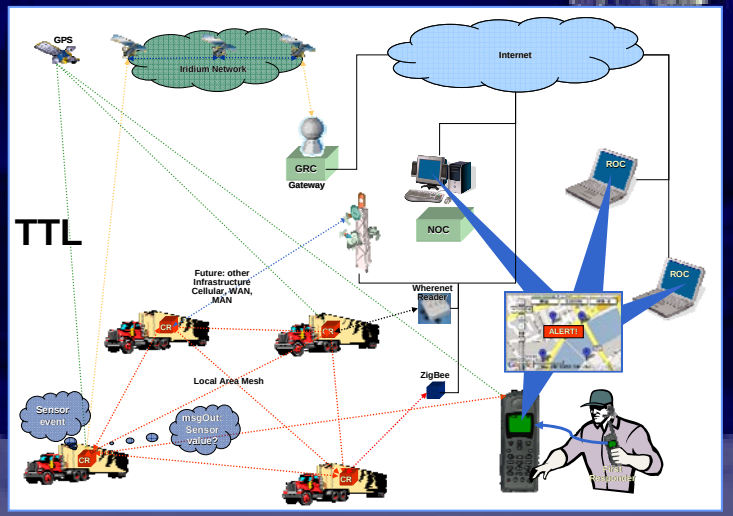
Small Contingency Theater Positioning System (SCTPS)





IC

TTL





NGA Evacuation Management & Accountability System (NEMAS)

ORNL Tracking System

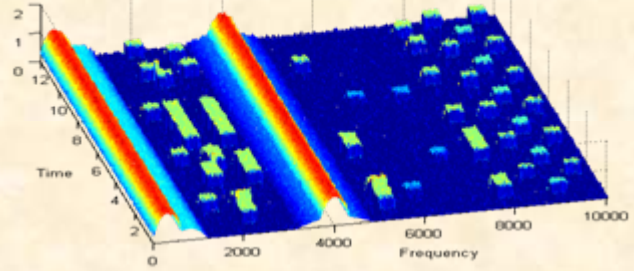


Cognitive Radio: What is it?

"a disruptive, but unobtrusive technology" [Haykin05]

Cognition/Intelligence?

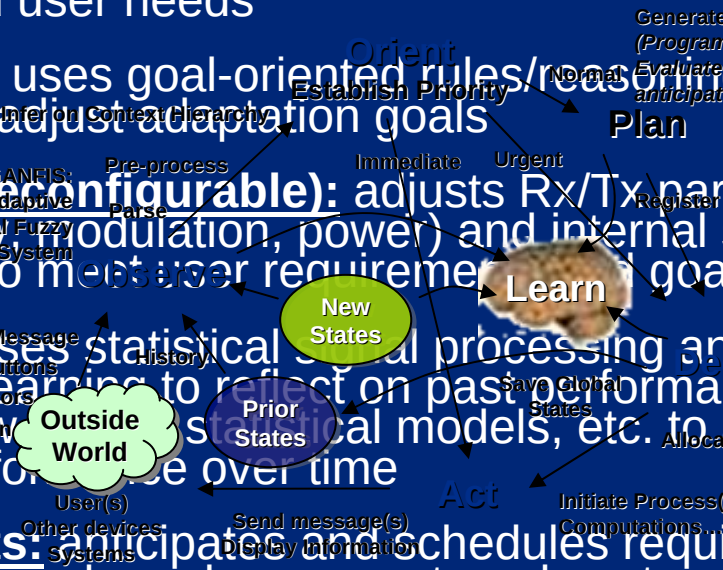
- "**knowing**, **perceiving**, or **conceiving** as an act…" [Oxford English Dictionary]
- "**interdisciplinary study** … concerned with exploring general principles of intelligence through a synthetic methodology termed learning by understanding." [Pfeifer & Scheier99]
- Intelligence: "The capacity to **acquire** and **apply** knowledge, especially toward a purposeful **goal**." [American Heritage_00]



Future Cognitive Systems:
"will converse with the user, anticipate their needs and adapt to meet them … "

Cognitive Radio is an intelligent wireless communication systems that:

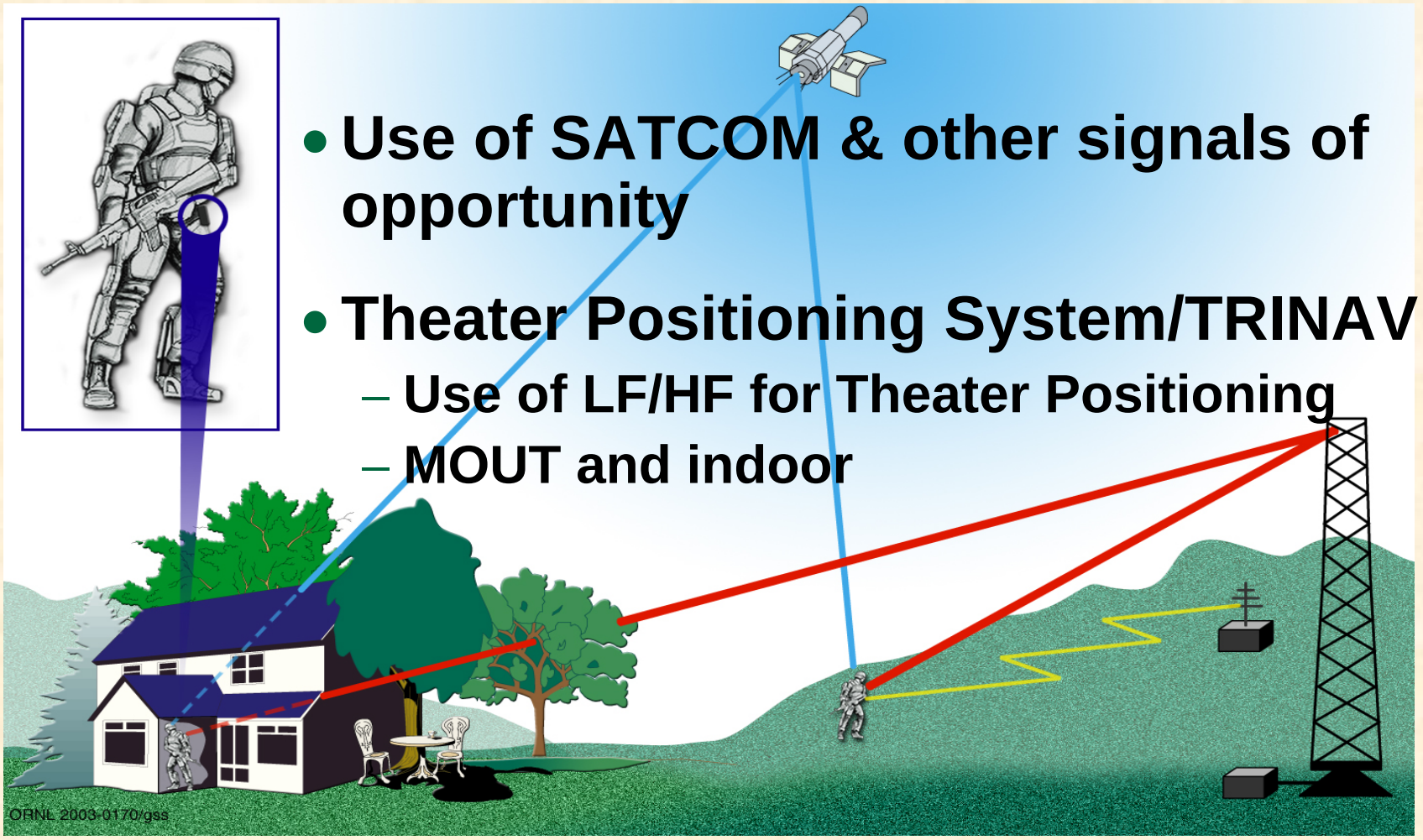
- **Senses (Awareness):** acquires and maintains knowledge of its environment, internal capabilities/ states and user needs
- **Reasons:** uses goal-oriented rules/reasoning (model-based) to adjust adaptation goals
- **Adapts (reconfigurable):** adjusts Rx/Tx parameters (frequency, modulation, power) and internal states in real-time to meet user requirements/goals
- **Learns:** uses statistical signal processing and machine learning to reflect on past performance and create new statistical models, etc. to achieve better performance over time
- **Plans/Acts:** anticipates and schedules required future actions based on current and past conditions
- **Collaborates:** leverage experience/capabilities of other CRs to attain goals
- **For the primary purpose of providing:**
  - Highly reliable communications w/ assured QoS
  - Robust performance
  - Efficient spectrum utilization



Overview of SD/CR-related Capabilities

- **Multi-Waveform Prototypes**
  - **One effort combined wideband RFID waveform (30 Mcps DSSS) with narrow band RFID and Satcom.**
  - **Another effort combined Satcom waveform with sensor signal processing.**
  - **Started an effort to combine Satcom, specialized comms, conventional terrestrial communications, sensor signal processing and cognitive control engine into a single prototype by end of FY08.**
- **Rapid Prototyping**
  - **Use of MATLAB/Simulink/Sys Gen Model-Based Design Approach.**
  - **Prototype SDR system was tested OCONUS within 60 days of receipt of funds.**
- **Reduced SWAP**
  - **Working on rapid method to port SDR designs to ASIC**
  - **Working with DOD to develop improved power source**

Geolocation Gap-Fillers



Waveform Development Progress

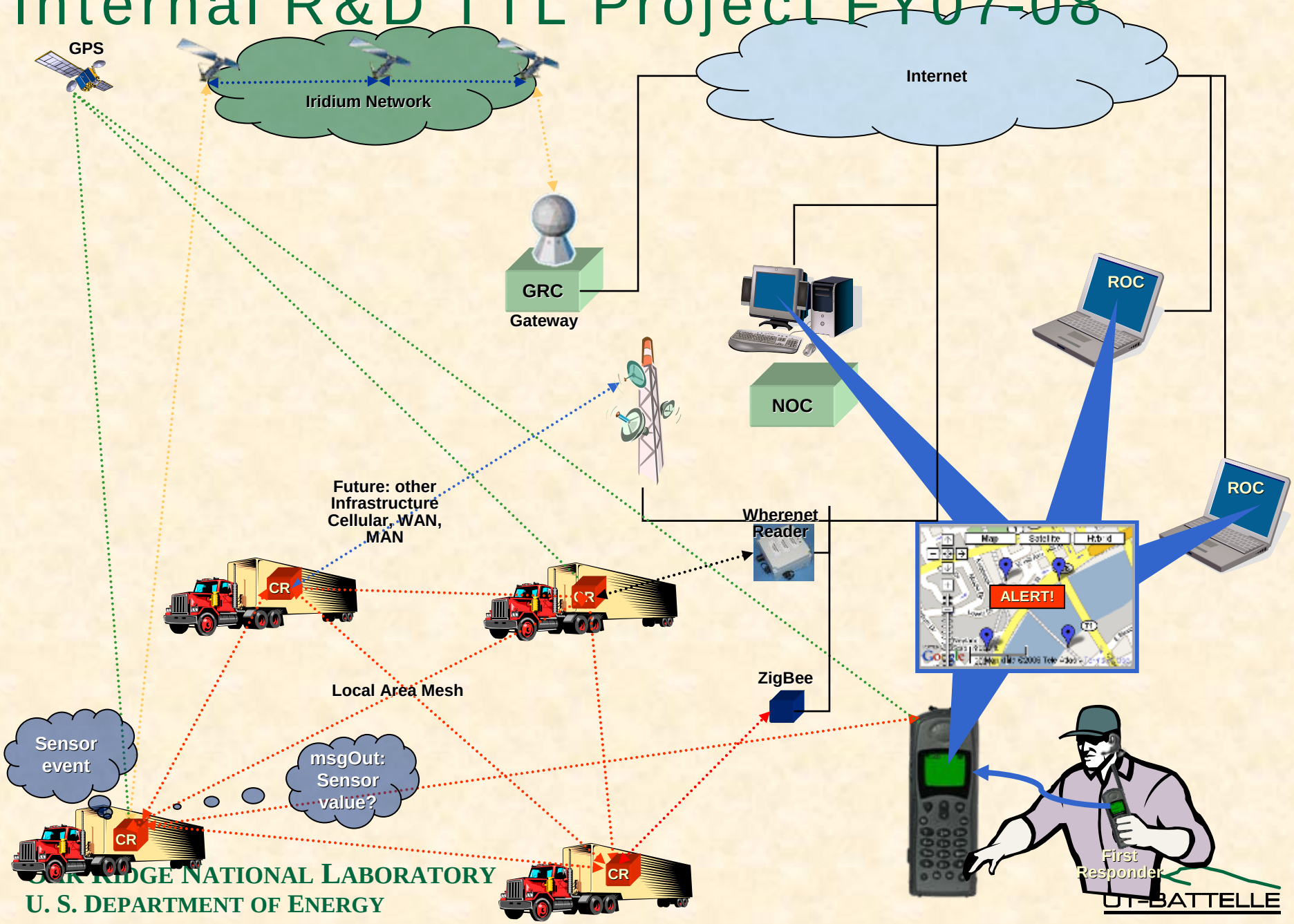
- Zigbee
- IEEE 802.11b
- Bluetooth
- Wi-Max
- UWB
- SATCOM
- FastHSS
- LPI/LPD Waveforms
- LF Navigation (TPS)
- Legacy Sensor

RFID/Tagging Waveforms
- WhereNet
- SAVI

- Channel Sounder Waveforms



Internal R&D TTL Project FY07-08





Contractors on the Battlefield

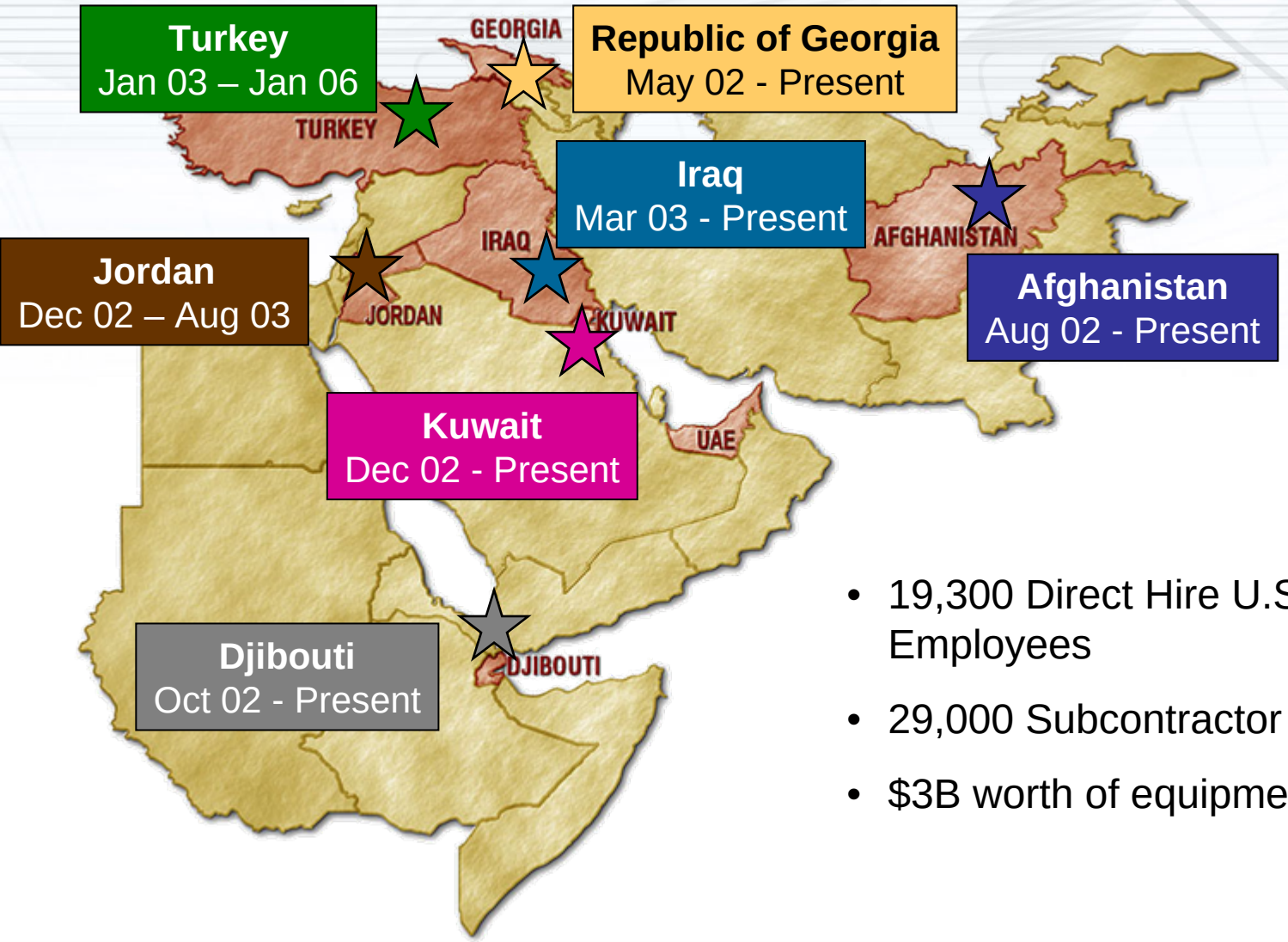
27 February 2007





KBR
Government
and Infrastructure

LOGCAP III in OEF and OIF

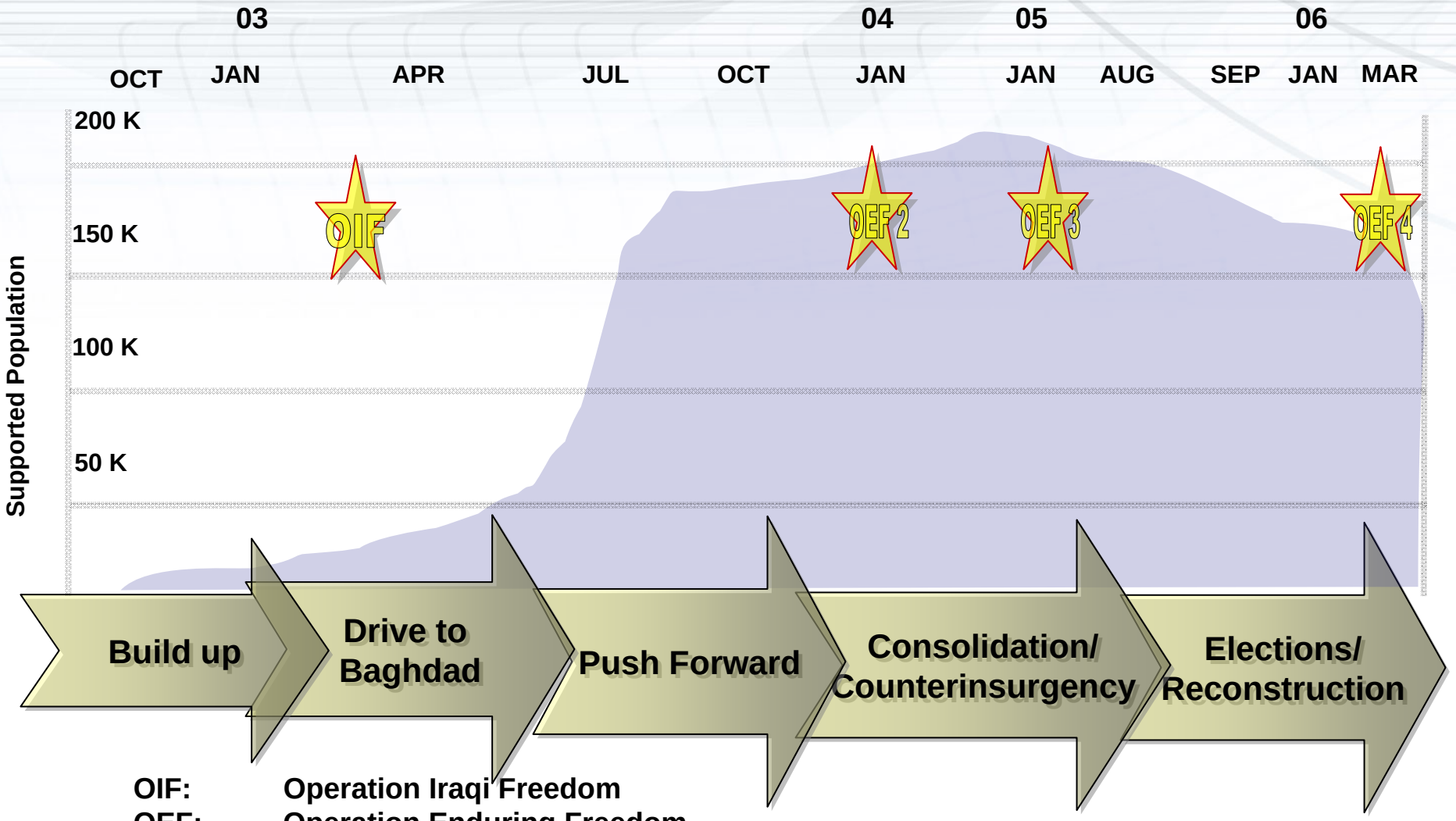


- 19,300 Direct Hire U.S. & International Employees
- 29,000 Subcontractor personnel
- $3B worth of equipment and supplies

KBR
Government and Infrastructure

Iraq – Constant Change . . . . As Expected

Pace and Scope . . . . Unexpected



OIF: Operation Iraqi Freedom
OEF: Operation Enduring Freedom

KBR
Government and Infrastructure

Contractor Mobilization

- Recruiting Qualified Personnel
  - Pool of Experienced Personnel
  - Recruiting Efforts
  - Third Country Nationals (Including Former Balkan HCNs)
  - Host Country National Hires
- Processing & Deploying Personnel
  - Medical screening
  - Background check
  - Job-specific training (defensive/evasive driving course, NBC training, etc.)
- Retaining Qualified Personnel
  - Pay
  - R&R
  - Prospect of Continued Work





LOGCAP III Program Overview – *We Deliver*

DESIGN • CONSTRUCT • OPERATE • MAINTAIN

BASE CAMP SUPPORT

- Ice
- Fuel
- O&M
- MWR
- DFAC
- HVAC
- Water
- Billeting
- Laundry
- Latrines
- Showers
- Fire Fighting
- Vector Control
- Waste Removal
- Power Generation



LOGISTICS SUPPORT

- Class I – Rations & Water
- Class II - Indiv Equip/Tools/Supplies
- Class III – Fuel (Packaged & Bulk)
- Class IV - Construction Material
- Class V - Ammo
- Class IX - Repair Parts
- Joint Distribution Center
- Forward Re-Distribution Point
- Maintenance Organizational/Direct
- Ice Distribution
- Mail Distribution
- Movement Control
- Maintenance/Recovery
- Material Handling Equipment
- Line Haul (Bulk Fuel/HET/Flatbeds)

CLSS

TTM

We Deliver DAILY	Water (Gal)	10 MM	Fuel (Gal)	839,000	Ice (Tons)	429
	Meals	432,000	MWR Patrons	77,000	Laundry (Bags)	33,000
SCOPE	Number of Countries	8	Total KBR Employees	18,000	Boots on Ground	225,000

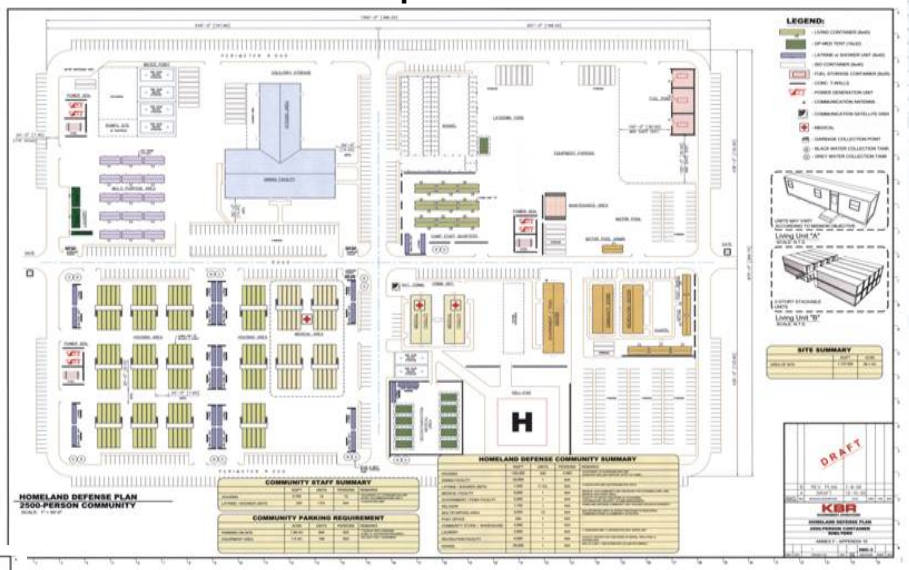
as of 21 Sep 06

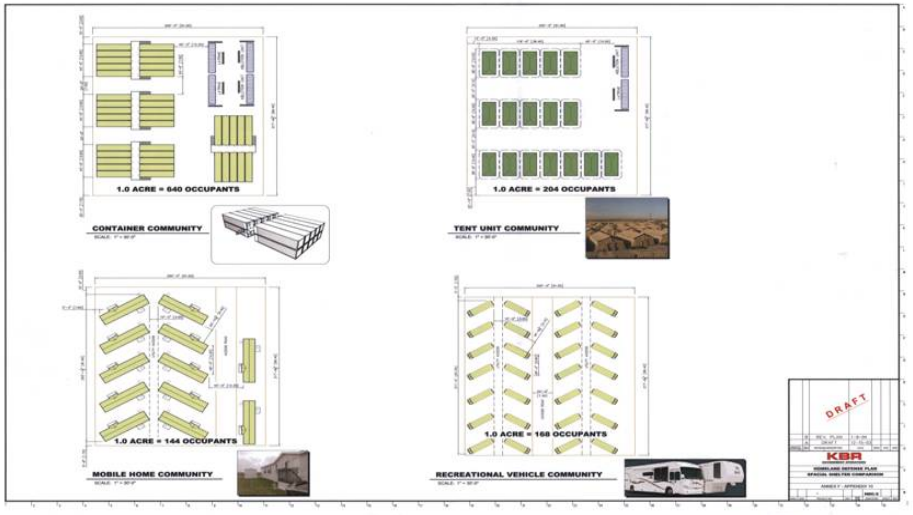
KBR
Government and Infrastructure

Life Support – Village Concept



Sample Site Plan





Available Accommodations



KBR
Government and Infrastructure

Operating Environment

KBR: A Civilian Company in War!

From the beginning of the shooting war on 20 Mar. 2003, Task Order 43 grew from a base of zero through a period of extremely rapid growth to meet the mission





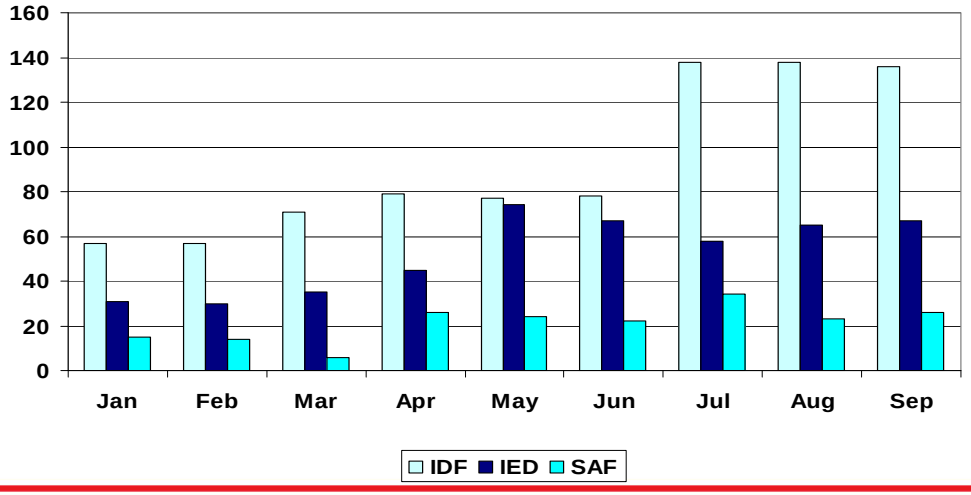


Continually Escalating Environment -- Small Arms Fire, Rocket Attacks, Mortars and Improvised Explosive Devices *and* Extremes of Climate, Brutal Road Conditions & Rock Throwing

Force Protection...Hostile Environment

- The enemy has options to impact our mission
- Since beginning of project
  - **68 Killed in Action**
  - **524 Wounded in action**
- Period from 01 Jan – 30 Sep 06
  - **400+ Improvised Explosive Devices**
  - **800+ Indirect Fire**
  - **200+ Small Arms Fire**

Contractors on the battlefield is not just a phrase … it is a reality!





KBR
Government and Infrastructure

Force Protection – Camp D4 Falcon
Enemy Mortar Rounds Ignite Ammo Storage Dump



- 10 Oct 2006 - 120 KBR Personnel
- Located 10 miles south of Green Zone
- 3 Mortar attacks on camp

No KBR or Military casualties

Multi-national Force – Iraq (Baghdad Sites)

KBR Continues Operations
In A Combat Environment Without A Single Mission Failure



Rocket Attack BIAP Laundry



Hard Car after IED



War Eagle Mortar Attack

How difficult is it to maintain a schedule in Baghdad?

- D1A Hope/War Eagle received 314 mortar and 7 rockets in one month with 103 in one day
- One Expat Subcontractor was kidnapped and 12 HCN subs were killed during the construction of the War Eagle DFAC
- **Every day during the POP an indirect fire attack was directed at one or more of the sites on this project**

Local Nationals and the Iraq Mission – Economic Zones







- Create a ‘safe’ area where the HN labor force is more efficiently utilized
- Build an area which houses an industrial type zone which utilizes local labor in manufacturing, servicing and/or training
- Create a work force that may be later screened for work ‘inside’ the wire
- Keep construction costs low by
  - Allowing the HCNs to build infrastructure
  - Use hasty type structures which use salvage and harvested raw materials as much as possible

Contractors on the Battlefield

Congressional Budget Office Study (October 2005)



Billions of 2005 Dollars	20 Year Total
LOGCAP Contractor Support	$41.4
Total Army Costs	$93.0
Difference in Total Cost	$51.6

The Future -- Integrated Team



Back up

KBR
Government
and Infrastructure

Theater Transportation Mission

Convoy Commander Position – The Backbone of TTM

KBR initiative to improve command and control over each convoy

Convoy Commanders:

- **Capitalize on ‘ATTITUDE’**
- **Increase responsibility**
- **Enhance communications**
- **Provide ‘field’ leadership**
- **Facilitate ‘TEAM’ building**
- **Key element of stability**
- **Many with previous military experience**
- **Trusted by soldiers**
- **After action agents**

Many now serve within other KBR functions







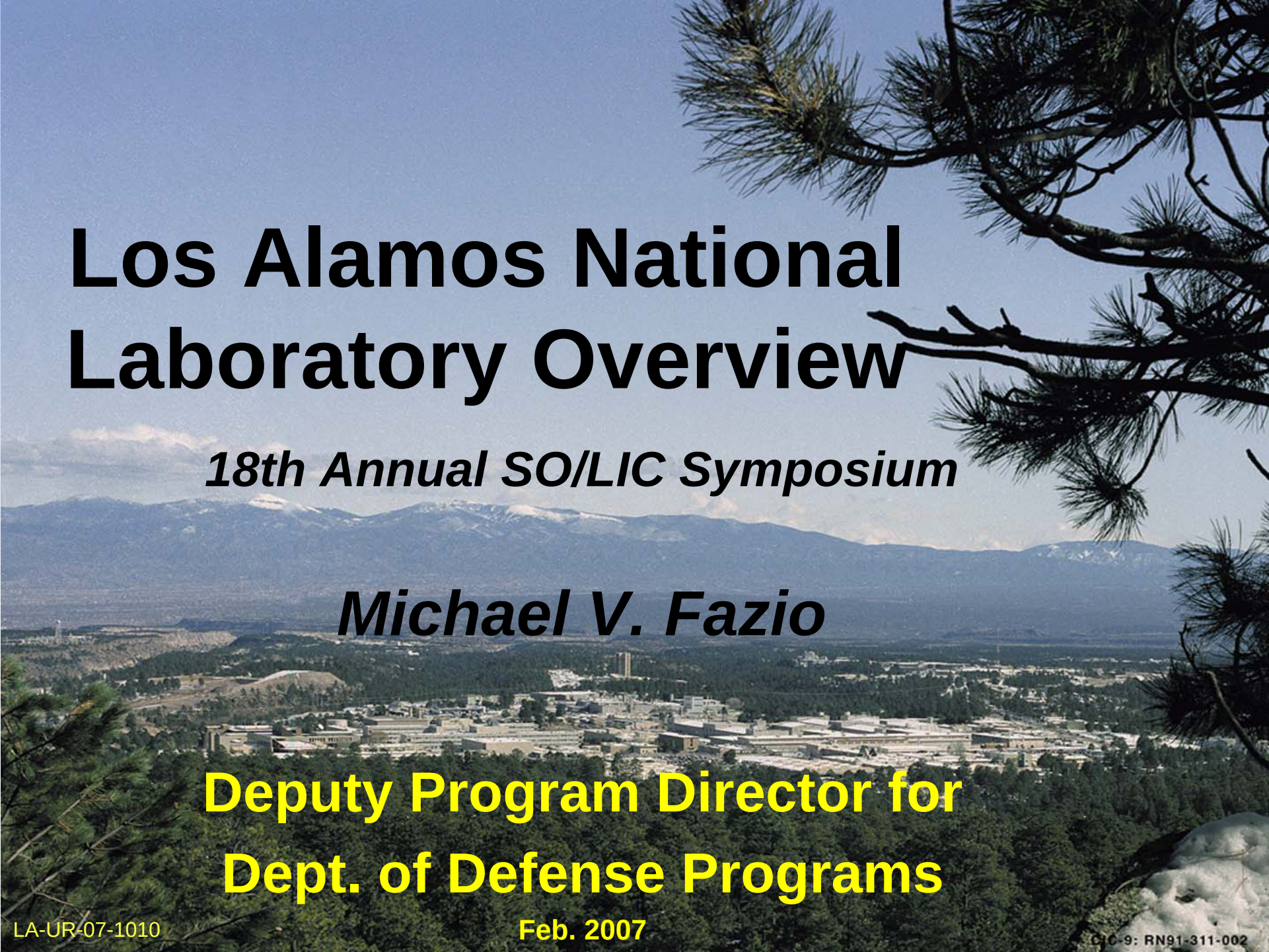
“An Essential Element of Success”!!!

KBR
Government and Infrastructure

Defense of Freedom Medal

- **Support ASC in presentation of Defense of Freedom Medals to wounded KBR employees and families of deceased KBR employees**
- **Provide KBR senior leadership opportunity to thank employees and their families for their service**
- **47 awards presented on 09 February 2007 – Houston**
- **31 awards presented on 17 March 2006 – Houston**
- **8 awards presented in January 2006 – Iraq**
- **1 award presented in May 2006 – Iraq**
- **8 awards presented in July 2006 – Iraq**
- ***38 nominations submitted pending approval***





Los Alamos National Laboratory Overview

18th Annual SO/LIC Symposium

Michael V. Fazio

Deputy Program Director for
Dept. of Defense Programs

LA-UR-07-1010

Feb. 2007

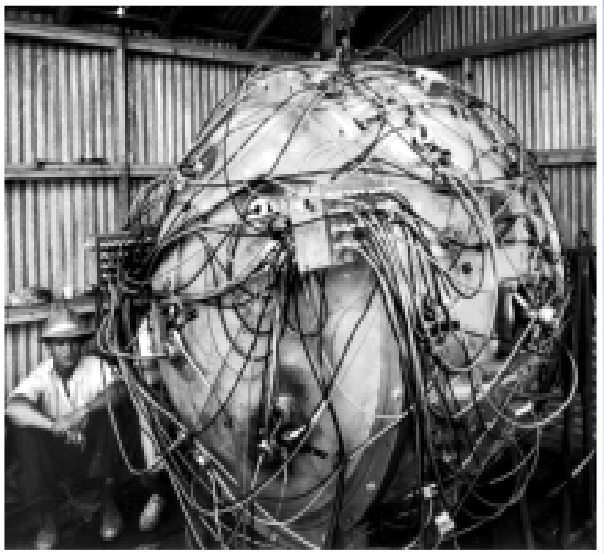
CIC-9: RN91-311-002

Our Mission - 1943: in the span of two years……..

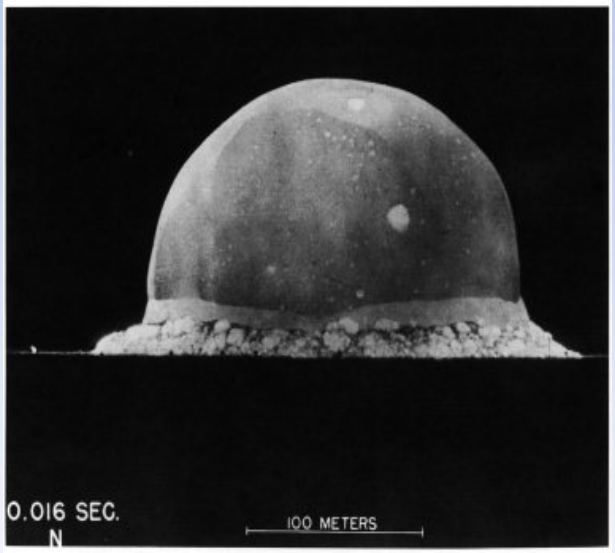
"the physical sciences were turned up-side down."



PAJARITO PLATEAU



THE GADGET



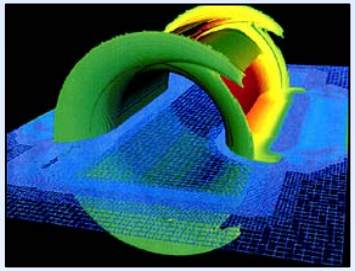
TRINITY SHOT

2007 Mission: Enhance Global Security by

- **Ensuring the safety and reliability of the U.S. nuclear deterrent**
- **Reducing global threats**
- **Solving national problems in defense, energy, environment, infrastructure, and health security**

Los Alamos National Laboratory executes a large and complex set of programs

Weapons Research



Large-Scale Simulation
Stockpile Stewardship



Pit Manufacturing



B61-11



W76, W78, W88
for Trident &
Minuteman III

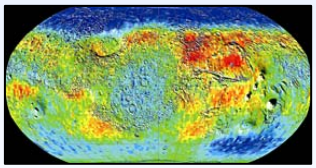


W80 for Advanced
Cruise Missile

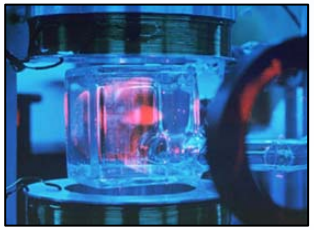
Basic Research



Fuel Cell



Neutron Spectrometer
Map of Mars

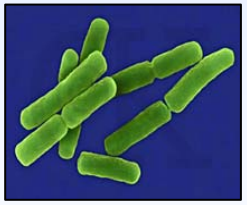


Atom Trapping
and Cooling

Threat Reduction



Nuclear Response



Advanced
Characterization
of Biological Agents

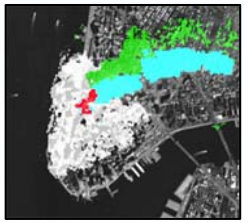


Image Analysis



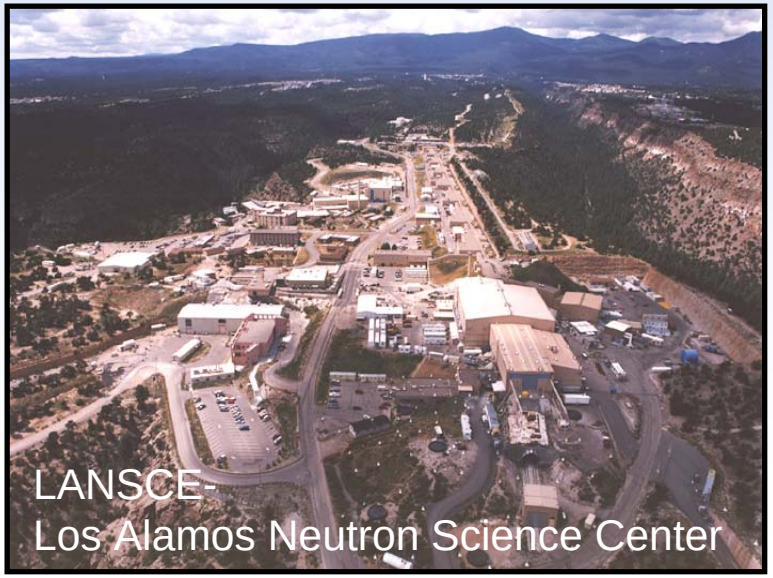
Los Alamos encompasses a large and complex site

- Core Employees 9000
- Technical Staff 4000
- PhD 2000
- Post-docs 400
- Students 1500
- Operating budget ~$2.2 B
- Land area ~40 square miles

Very broad and deep science and engineering capabilities, driven by critical National needs



LANL (green) compared with Washington, D.C.



Strategic Thrust Areas for Threat Reduction



Nuclear Nonproliferation

Defense

Threat Reduction

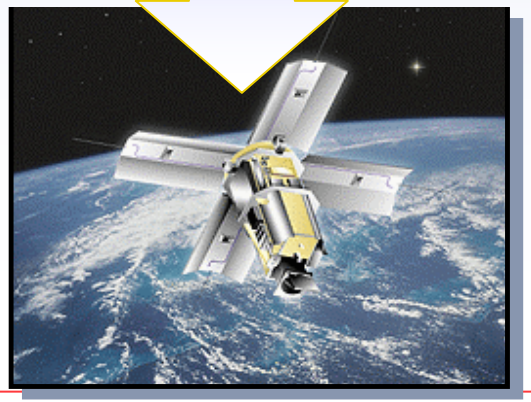
Homeland Security

International Technology



Tunable Metastable Interstitial Composite (MIC) Explosives
Nanoscale High Energy Density Materials

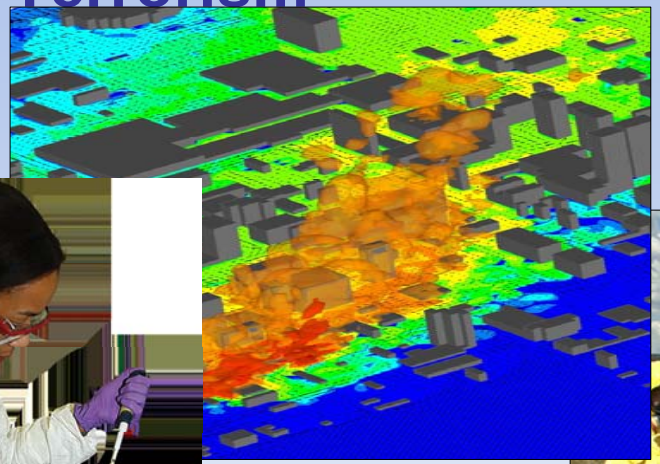




Distributed Satellite Sensor Systems

"Global Situational Awareness Coupled with Response"

Homeland Security - Reducing Threats of WMD and Terrorism



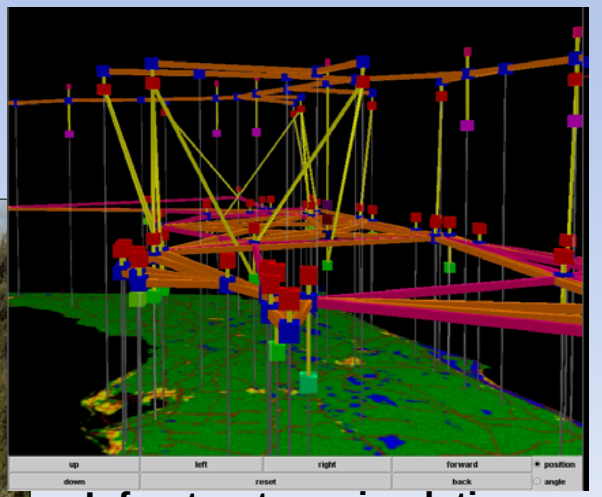


Airborne toxin transport modeling

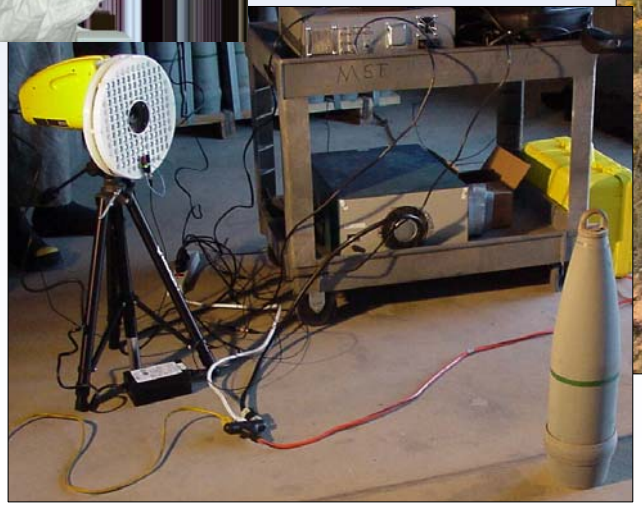
Bioforensics



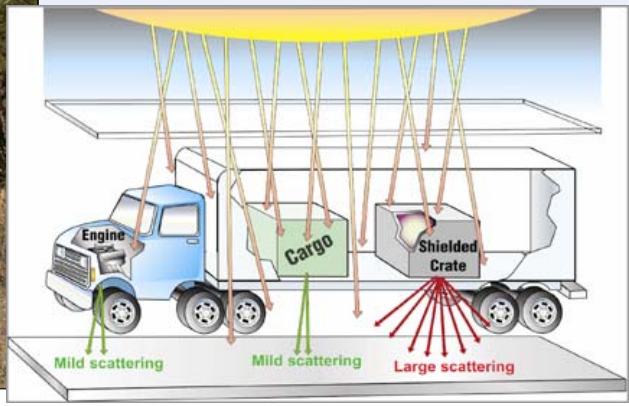
Nuclear emergency aid



Infrastructure simulation & analysis



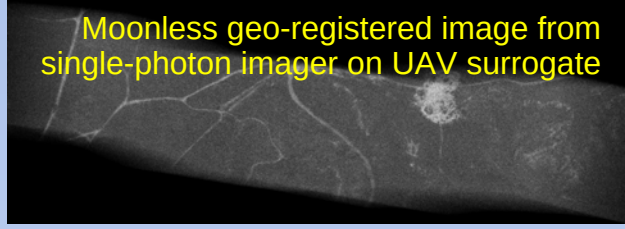
Noninvasive acoustic chemical ID

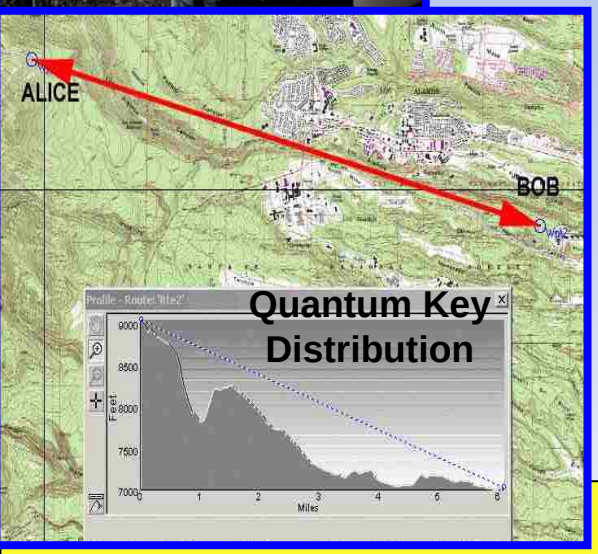


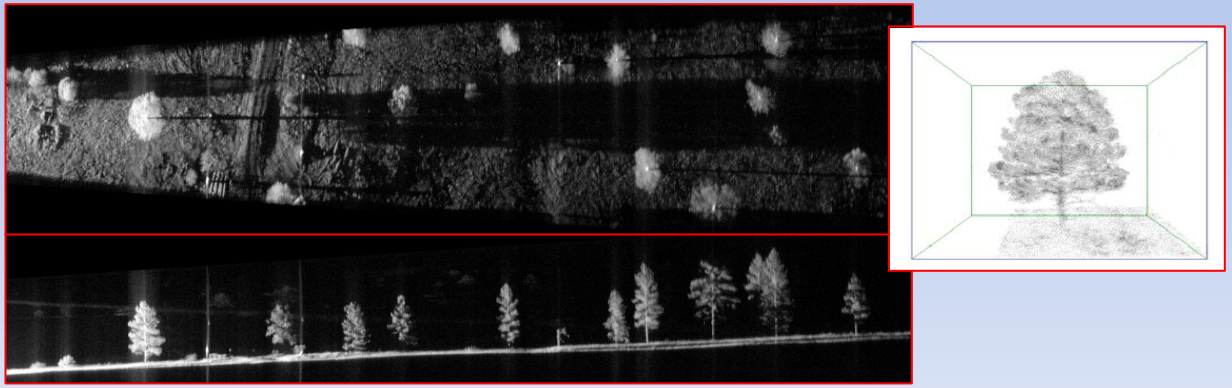
Nuclear detection - passive muon radiography

Defense - *Deter, Detect, Deny, Respond*



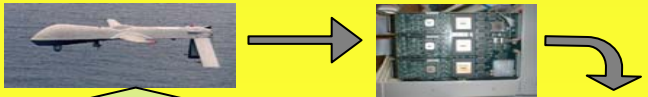






RULLI- Remote Ultra-low light 3D imaging with time tagged single photons

GENIE: GENetic Imagery Exploitation



Automated Scene Classification - translation of expert knowledge into automated knowledge extraction to handle huge data flows



Input Image | Training Image | Test Image | Output of GENIE

Contact: Nancy David, 505-667-8896, ndavid@lanl.gov

Mission Driven Science is a Los Alamos Hallmark - Satellite-Based Nuclear Explosion Monitoring

New solutions from science resulting from national needs

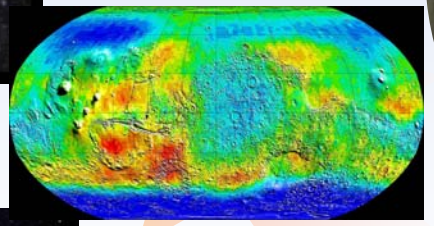
New Science Contributions

Gamma-ray bursts, water on moon/mars, magnetospheres of earth and planets.

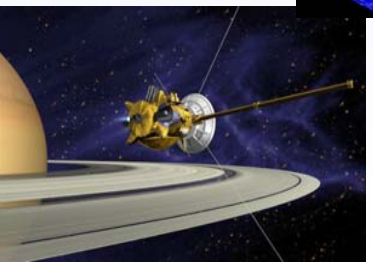


Solutions

Triggering codes, imaging for homeland security, new detectors.



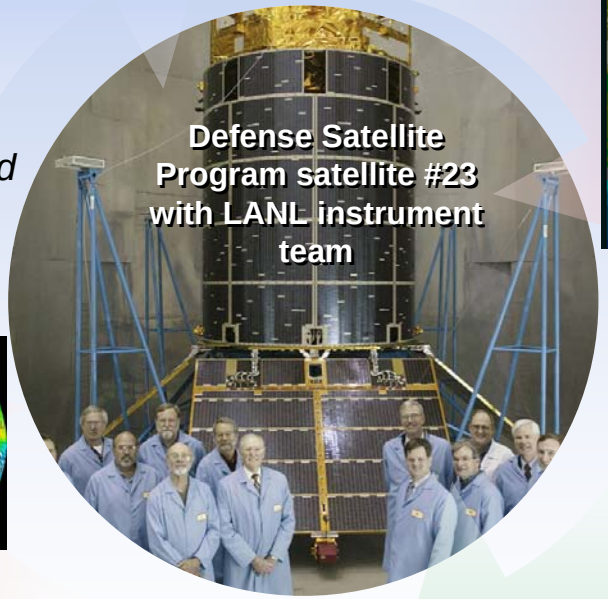
Map of Hydrogen (Water) on Mars



Cassini exploring Saturn's moons and rings 2005

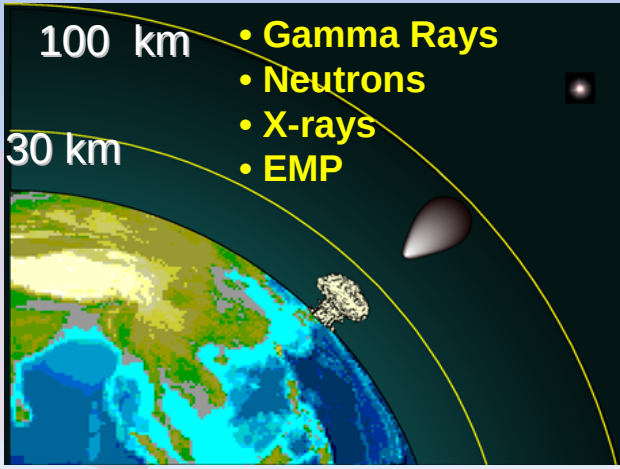
National Need

Detect nuclear explosions in atmosphere and space - everywhere, all the time.



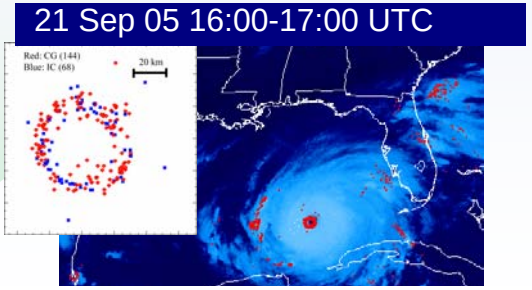
New Capabilities

Coded aperture x-ray imaging, Doppler neutron spectroscopy, neutral-particle imaging.



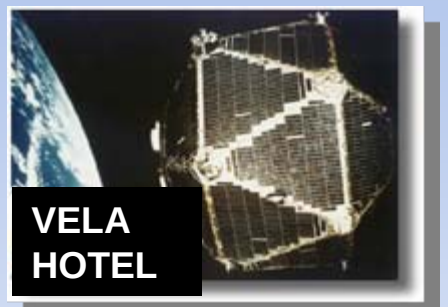
Existing and Emerging S&T

Satellite Instrumentation, x-ray, gamma-ray, neutron, EMP sensors

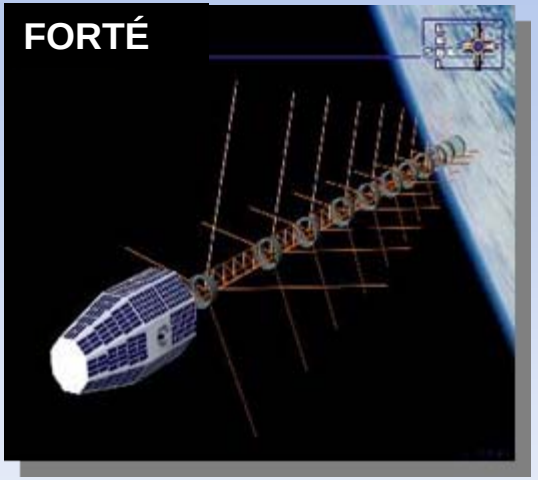


Rita category 5: intense lightning marks boundary of eyewall - EdotX sensors

40 Years of Space Experience - A Headstart on Persistent Surveillance - *1400 sensors, 120 instruments, 60 satellites*



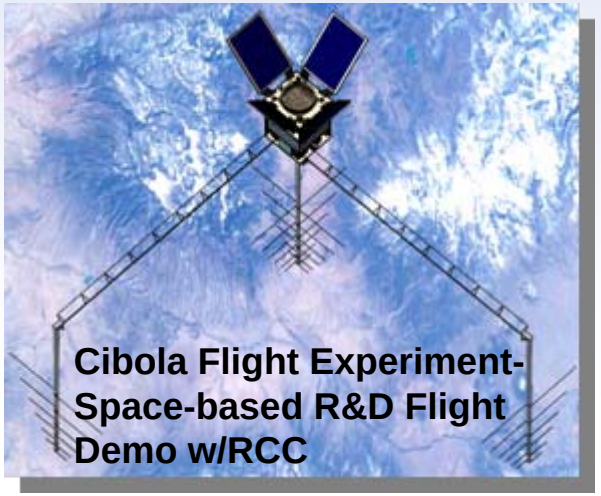








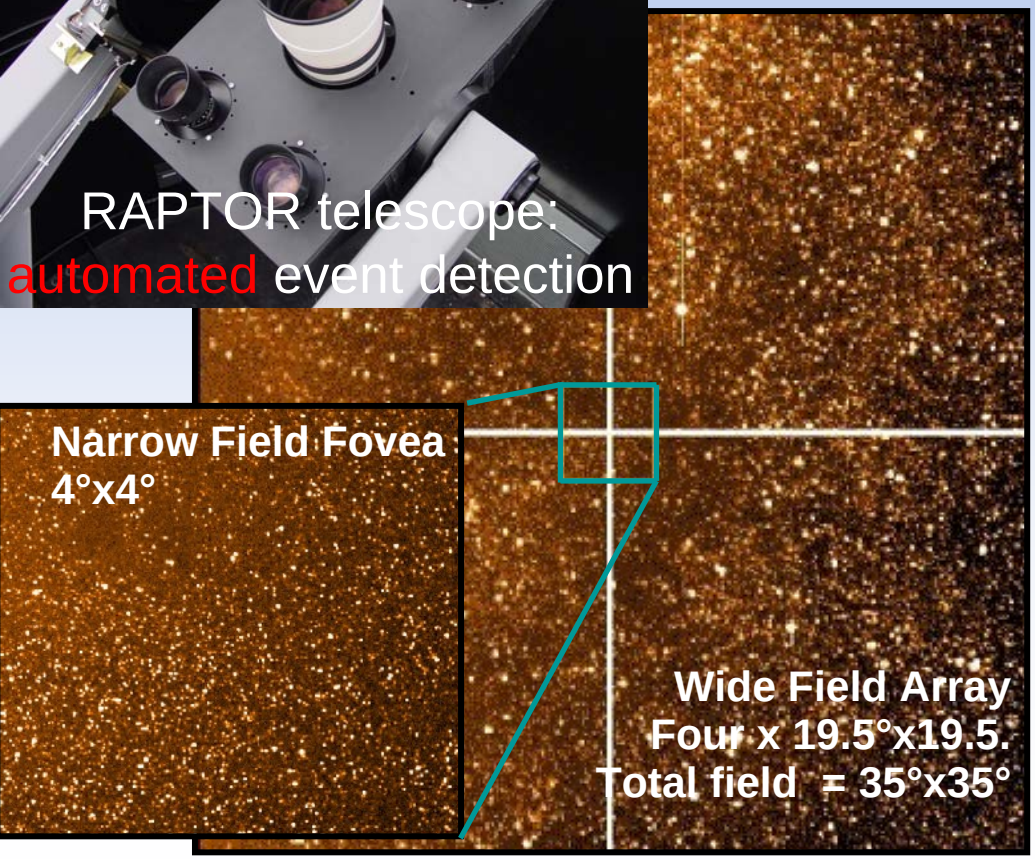




Thinking Telescopes - Find and conduct detailed follow-up observations of transient source anomalies in real time - against a huge background



Nightly variation of the optical sky, even for bright objects, is largely unexplored



Networked Robotic Hardware

- Wide FOV
- Rapid response
- Real time analysis pipeline

Machine Learning

- Automated feature extraction
- --Anomaly detection
- -- Object classifiers

Thinking Telescope

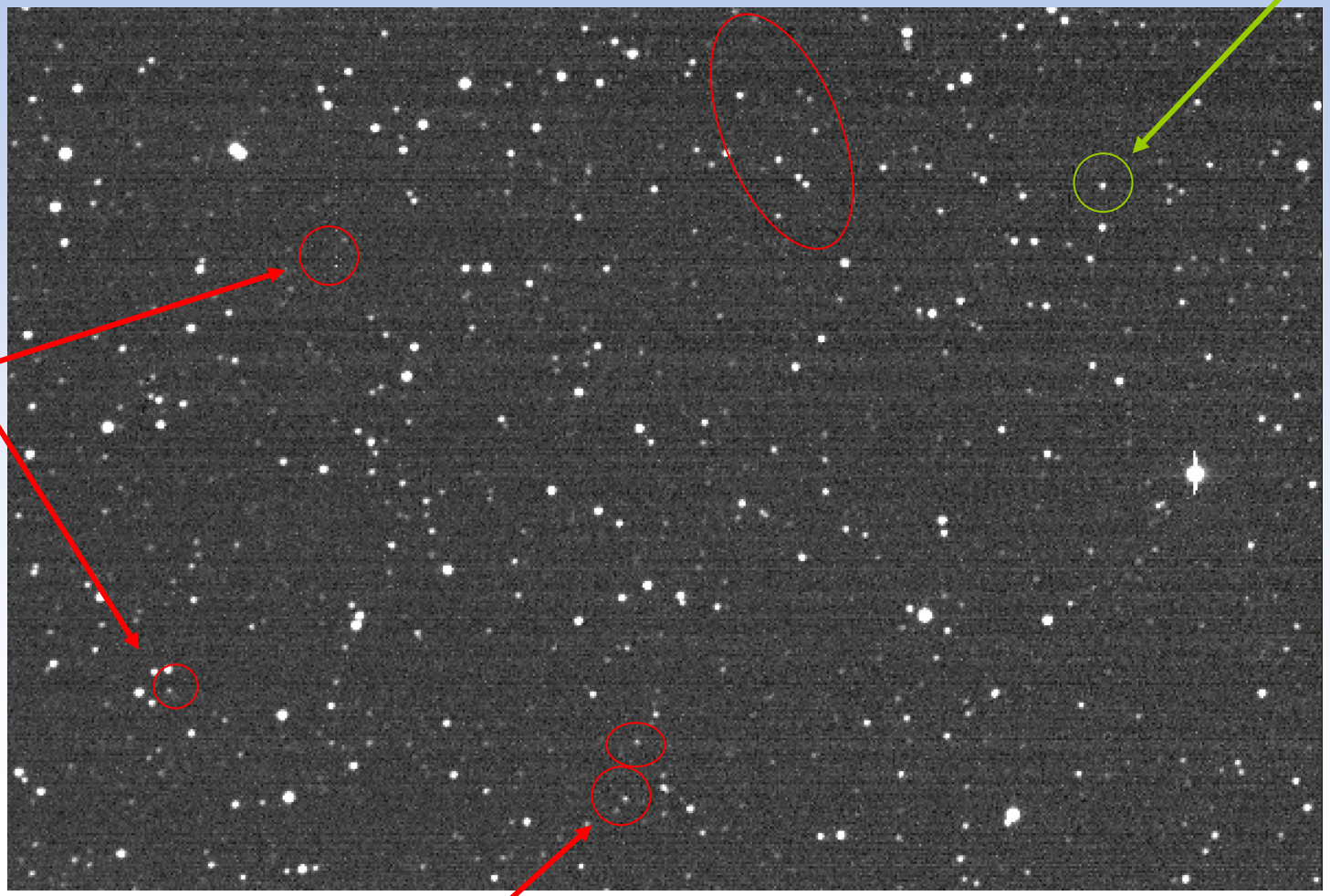
Adv. Database Technology

- Virtual observatories
- -- Distributed disk arrays
- -- Intelligent clients

Change detection tools can be applied to terrestrial applications

Contact: Tom Vestrand, 505-665-9542, vestrand@lanl.gov

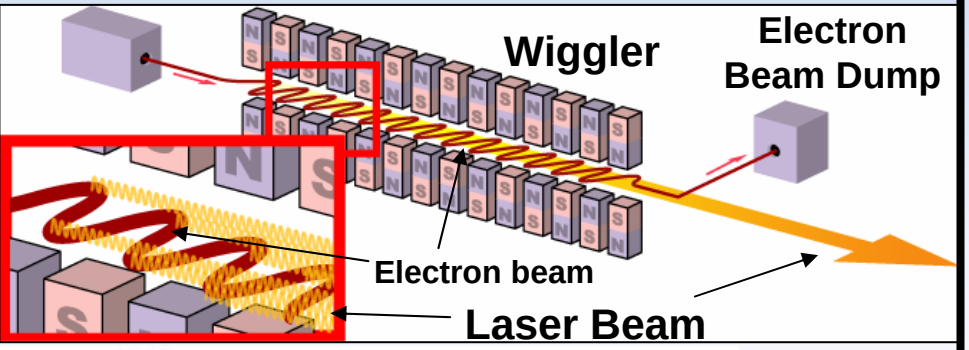
The Problem: 2 Minute Look at 1/50,000 of the Haystack

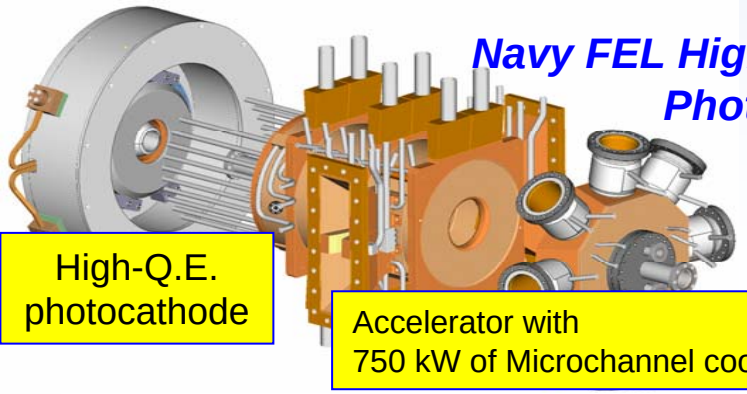




Directed Energy - Response at the Speed of Light

40 Years of High Average Power Accelerator Experience Supporting Navy ***Free Electron Laser*** *Development*





Navy FEL High Current Photoinjector

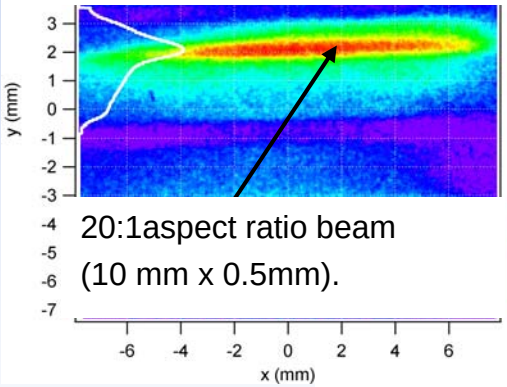
High-Q.E. photocathode

Accelerator with 750 kW of Microchannel cooling

Ultra-Compact High Power (0.5 MW/10kW) 100-300 GHz ***MM-Wave/THz Sources***

Enabling Technology:

- *Sheet beam formation and transport*
- *Planar RF structures*



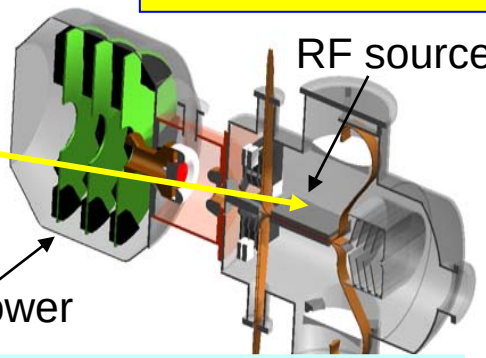
20:1aspect ratio beam (10 mm x 0.5mm).

Enabling technology for:

- Radar
- Hi-Res Imaging
- Covert Comms
- Remote Sensing
- Active denial

Planar RF structure





Ultimate TWT Configuration

Contact: Bruce Carlsten, bcarlsten@lanl.gov

Los Alamos Multi-Disciplinary Capabilities Are Tapped to Look for End to End Solutions

IED - Defeat Chain

INTELLIGENCE **SURVEILLANCE** **DETECTION** **DEFEAT**

Multiple Pathways For Technology Insertion & Deployment

Intel & Analysis

- Intelligence on terrorist threats and emerging capabilities
- Understanding terrorist capabilities in WMD and advanced explosives

Modeling Societies & Intents

- Threat Anticipation Project: simulations of insurgency societies

Sensors & Information Science

- Surveillance and detection of electronics
- Wide area persistent surveillance & real-time data distribution
- Remote Raman-LIBS detection
- Stealthy Insect Sensors of H-E vapor
- High power mm wave deployable sources to detect at-range and/or pre-detonate
- Knowledge engines, decision-making algorithms, data-fusion
- Anomaly, change recognition, identification and tracking algorithms

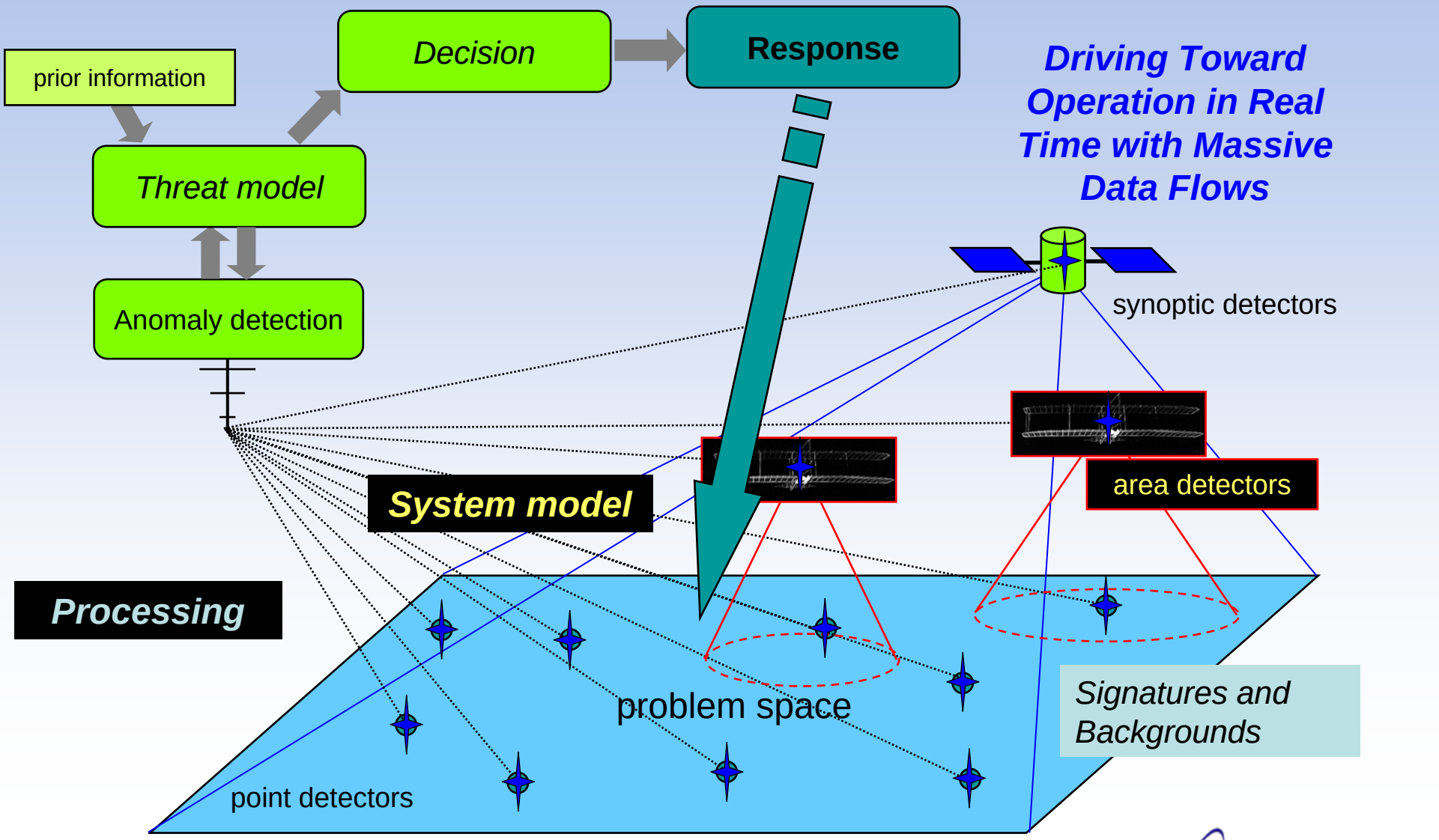
High Explosive Chemistry & Facilities

- Single H-E crystal characterization for detection sensors
- HE signatures

Disable & Defeat Capabilities

- High power microwave defeat of electronics
- Thermite Blanket for IED defeat
- Render Safe Technologies

The Challenge: Event to Knowledge to Action *in Real Time*



Los Alamos Continues a 63 Year History of Paradigm Changing R&D

- Mission-driven science in the National interest
- Underpinned with broad and deep multidisciplinary science and engineering capabilities - *much more than a nuclear weapons laboratory*
- Long history of successfully fielding complex hardware on time scales of days, weeks, & years in harsh environments with autonomous operation
- Portfolio extends across many programs with many sponsors
- Routinely partner and collaborate with other government agencies,industry, and academia

Contact: Michael Fazio, 505-667-3281, mfazio@lanl.gov

National and Homeland Security at INL

- *The United States of America is faced with unprecedented challenges in National and Homeland Security*
- *The Idaho National Laboratories is well positioned to meet many of these challenges and enable sustainability for the long war*

Idaho National Laboratory

- **Multi-Directorate Federal R&D Laboratory**
- **Leverage science and engineering technologies to form international partnerships that address both DOE R&D and National and Homeland needs**
- **Annual budget of ca. $600M**
- **3,400 scientists, engineers, technicians, and other staff**
- **Three S&T Campuses on 890 square mile site**



The INL R&D

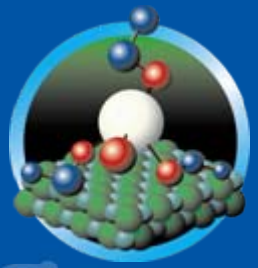
Mission execution is guided by five laboratory divisions



Nuclear Energy



National Security



Energy and Environmental Sciences



Advanced Test Reactor



Specific Manufacturing Capability

Idaho National Laboratory

Our Focus Areas Support *Multiple Missions and Enable Sustainability*

Global Security	National Defense	Homeland Security	Special Programs	Energy Security

Focus Areas



SCADA / Cyber/ Power Grid



Wireless Technology



Unmanned Vehicle Systems



Explosives Detection & Testing



Chemical / Nuclear Detection, and Nonproliferation / Safeguards & Security



Special Mfg Center Emerging Armor-- Vehicle / Barrier/ Structural/ Personnel

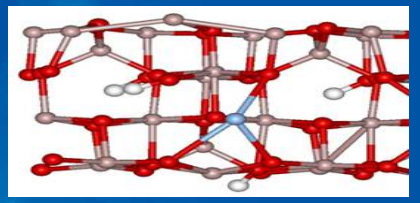
Technology Platforms



Process Controls



Materials



Physics, Molecular Science, Modeling

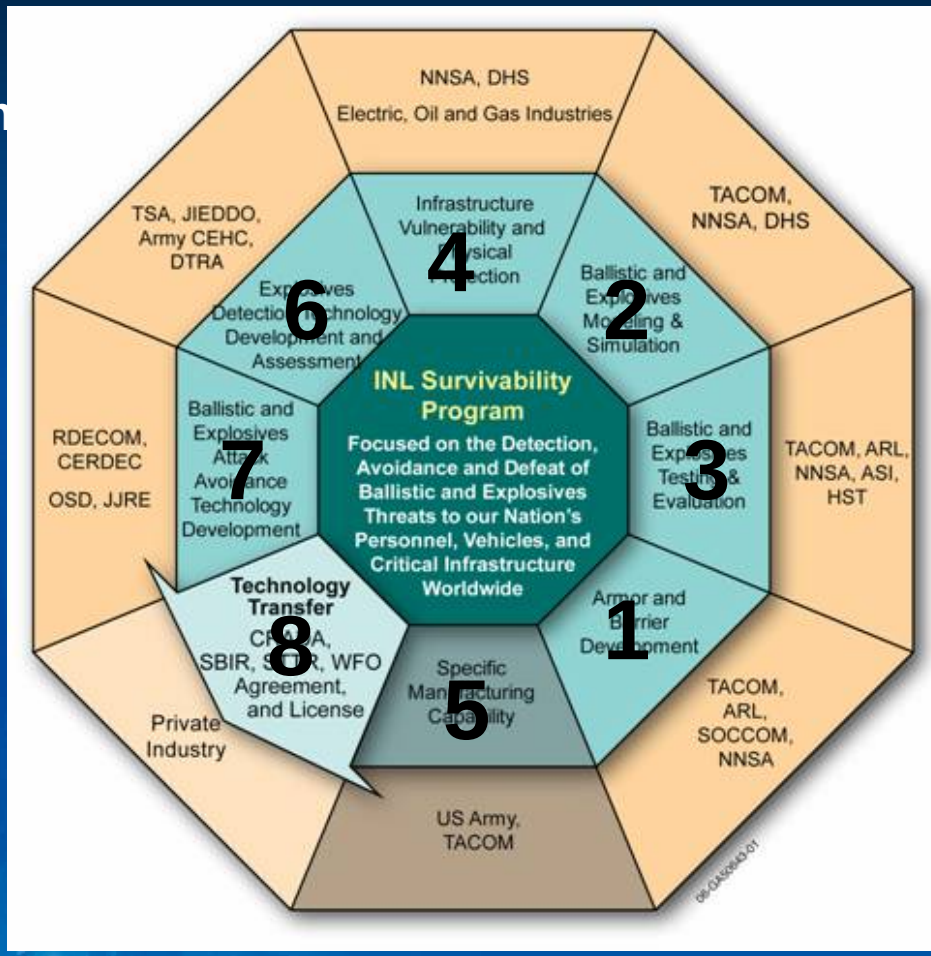
National & Homeland Security
Objectives & Key Customers We Serve

Mission Area	Customer	Strategic Objective
Global Security	NNSA	Reduce global nuclear threats through innovative nonproliferation and counterproliferation technologies
National Defense	DoD	Provide solutions to asymmetric threats and combat WMD
Homeland Security	DHS	Develop science and technology to protect critical infrastructure systems and improve resilience
Special Programs	Various Clients	Provider of choice, in selected areas, for technology based solutions to the U.S. Intelligence Community
Energy Security	DOE-OE	Enhance security and reliability of the nation's energy systems

National and Homeland Security
INL Survivability Program (ISP)

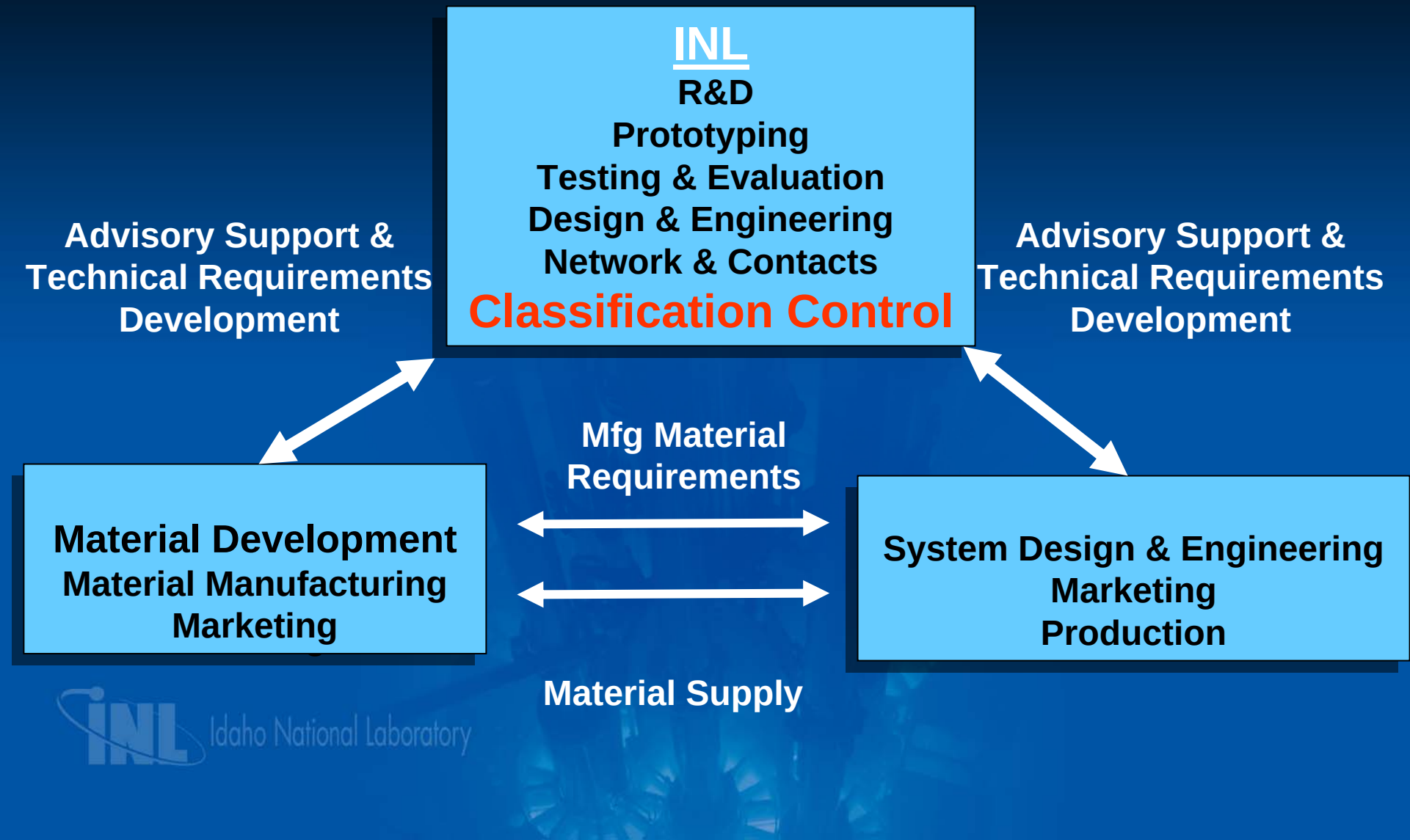
The ISP is an Agile Collaboration of Capabilities at *One* Location

1. **Armor and Barrier Development**
2. **Ballistic and Blast Modeling Simulation**
3. **Ballistic and Blast Test & Evaluation**
4. **Critical Infrastructure Vulnerability Assessments**
5. **Specific Manufacturing Capability**
6. **Explosives Detection and Advanced Technology Development**
7. **Ballistics and Explosives Attack Avoidance & Hardware Development**
8. **Technology Transfer for Scale Up**
   Hardware to the End User



Idaho National Laboratory

Example of INL Commercial Partnership in Survivability Systems Development



National and Homeland Security

INL Survivability Program (ISP) - Leadership

Armor Development



- Leadership in design, development, and testing of high-density, lightweight armor against multiple threats.
- Test range with extensive capability for confidential testing.
- INL armor proven against ballistic, kinetic, blast & frag threats.

Explosives Testing



- Leadership in trace and bulk explosives detection, blast effects, shock and vibration analysis.
- Class Facilities: 20,000 Lb TNT equivalent test range and Class II, Div. I Operations Room for explosives assembly.
- Performance/ Resiliency Testing: Ballistic Penetration, Structural Analysis, Computer Modeling/Simulation,
- Development of Protective Countermeasures.

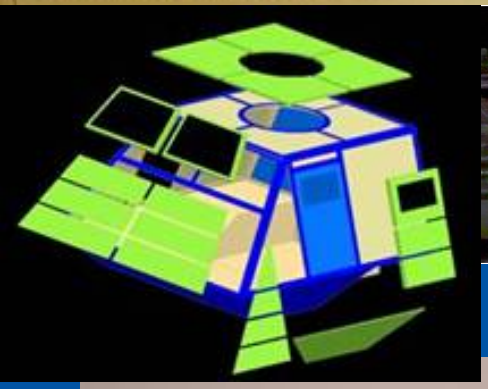
Technology Development

- Leadership through over 3,500 world-class scientists and engineers in technology development and national security solutions.
- Award-winning technologies in Global use: Idaho Explosives Detection System. Breaching Shotgun, Tactical Timed Firing Device, Change Detection System, PINS for Munitions Assessment

Armor and Barrier Development











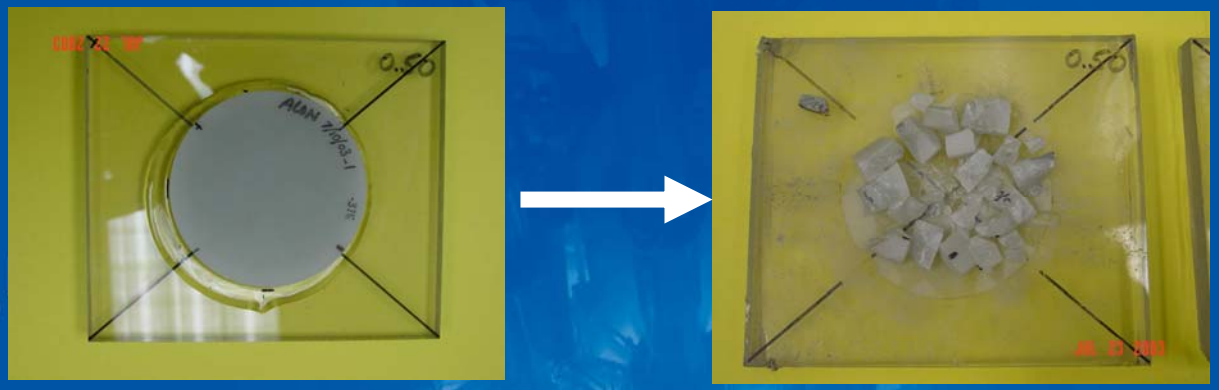
- **Advanced Materials**
  - Ballistic Steels
  - Alloyed Metals
  - Ceramics
  - Transparent Ceramics
  - Polymers
  - Composites
  - Joining
- **Design & Simulation**
  - Ballistic
  - Blast
  - Fragmentation
- **Prototyping & Evaluation**
- **Special Manufacturing Center**
  - Over 9000 Abrams Premier battle tanks in use worldwide

Optical Armor and Ballistic Results



- Aluminum Oxy-Nitride is a “premier” transparent armor material. Today, AlON is not available to in commercial quantities. Presence of residual porosities will prevent full optical transparency
- INL is developing novel approaches to **pressure-less sintering** of ALON.

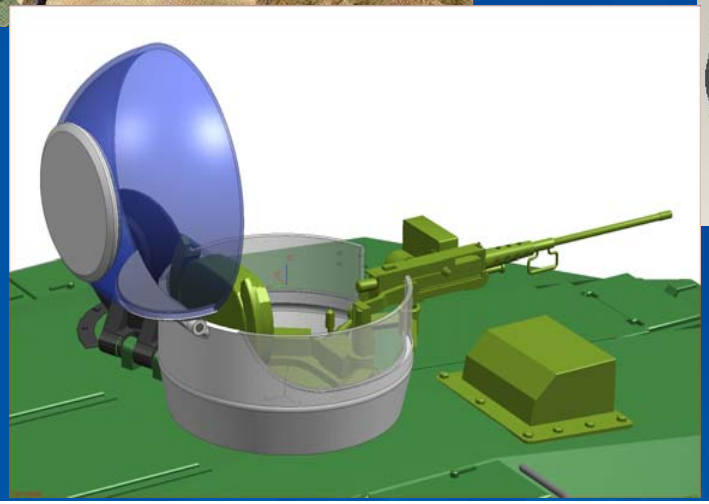
- Successful Target LOS AD = 10.5 lb/sq ft
- Design: ALON + polyurethane + polycarbonate
- Defeat: 30-cal APM2 @ 2810-2828 ft/sec @ 20.5’ standoff

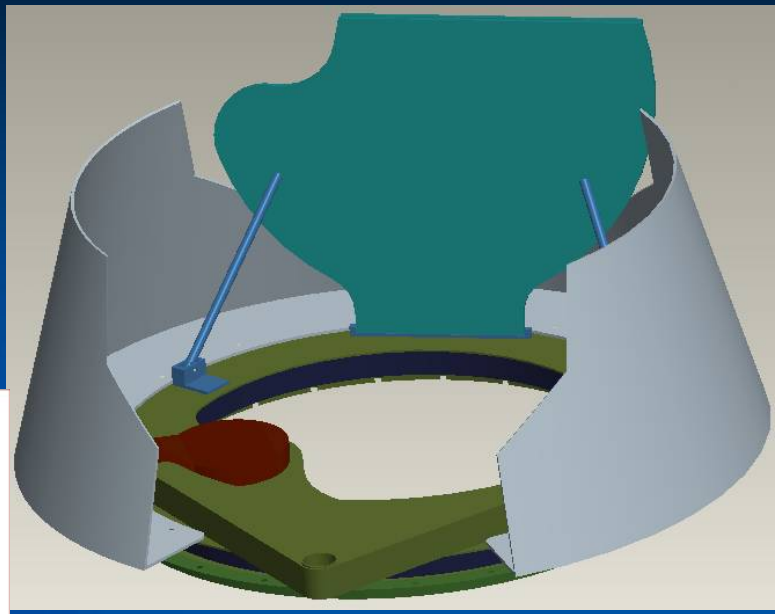


Lightweight, High-performance Gunner Ballistic Cupola

INL CRADA Demonstration Project







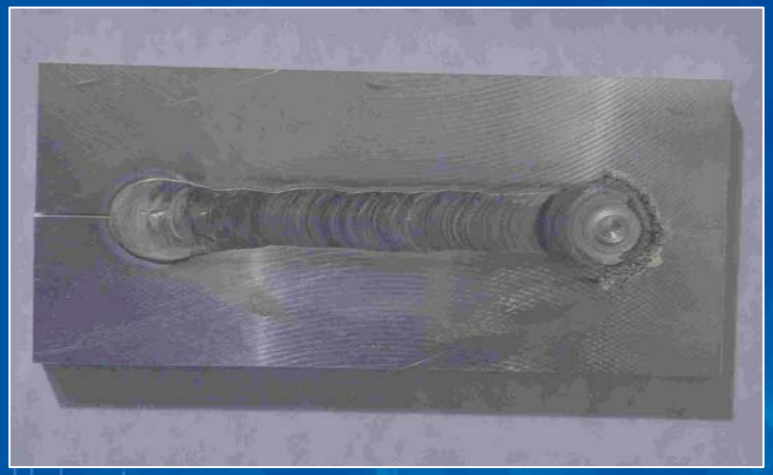
Improved Ballistic / Blast Resistant Conformal Armor Cupola

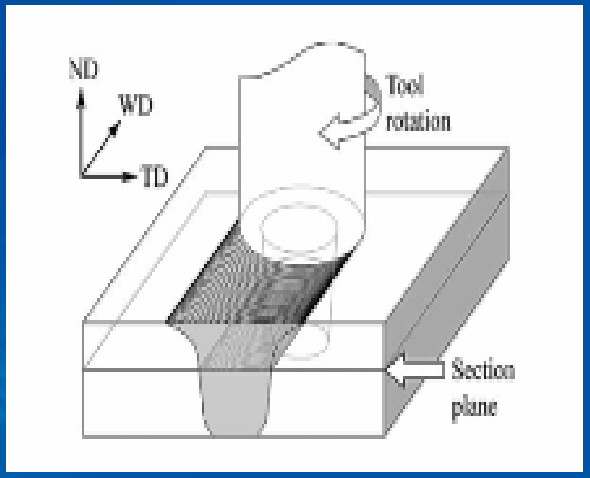
Joining and Welding of Metal Alloys Using Advanced Solid-State Friction Stir Welding





INL's Advanced Tooling Materials

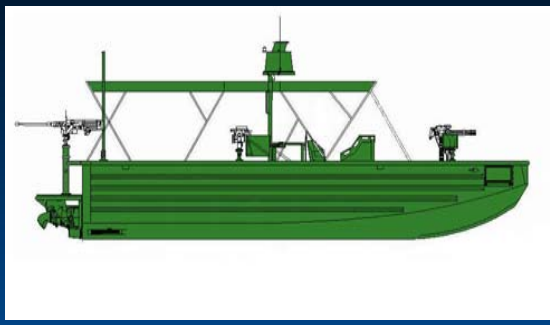




ISP's Full Scope Multi-Services Supports

Up-Armoring Special Operation Combatant Crafts

- **Armor expertise and T&E support to USSOCOM on retrofit armor solutions for the Coastal Assault Craft (CAC) and new Special Operation Craft – Riverine (SOCR)**
- **Consultation and design supports provided to SOCR builder**
- **Development of close-quarter ricochet and shrapnel suppression system**
- **Riverine fleet expanded from initial "x" to "y" units, based in Stannis, MS**
- **Currently deployed at Tigris River, Iraq**







INL Live-fire Range Complex & Capabilities



- 10 ranges
- Live fire training
- Various weapons

- **Surface Danger Zones = 4.7 miles. At the 20,000 lb range = 8 miles**
- **Live Fire Ballistic Test Range**
  - **30 cal, 50 cal APM2**
  - **14.5 mm BS32, BS41**
  - **20 mm FSP and AP**
  - **LAW and RPG**
  - **30 mm FSP and AP**
  - **Other: hypersonic**
- **Explosive R&D range**
  - **500 lbs.**
  - **20,000 lbs.**
- **Fabrication shop support**

INL Idaho National Laboratory

Design and Simulation

- Vehicle Armor
- Personnel Protection
- Barrier Armor
- Ballistic Effects
- Blast Effects
- Combined Ballistic and Blast
- Molecular modeling (explosives)
- Molecular Engineering (novel organics)
- Processing of Ceramics and Polymers

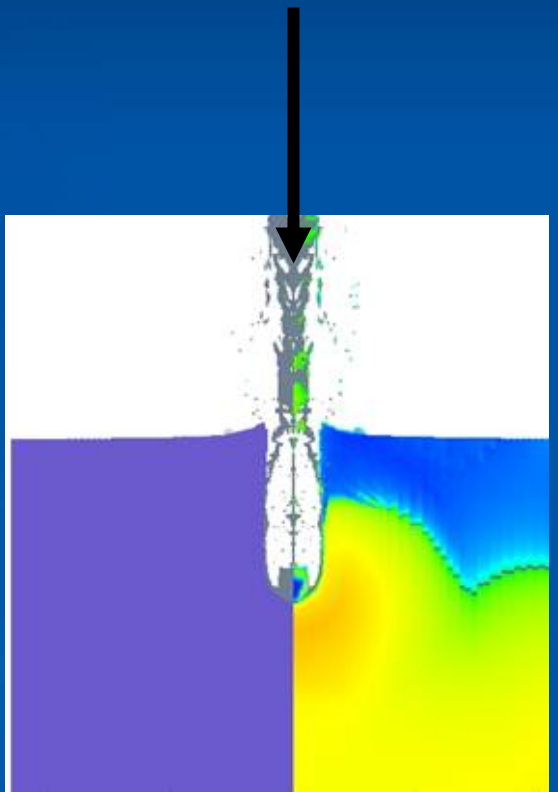
INL Applied Mechanics

INL Center For Advanced Modeling and Simulation (CAMS)

- **Analytical**
  - Nuclear Reactor safety analyses
  - Pressure vessels and piping
  - Flight safety
  - Shock and vibration
  - High-velocity and hyper-velocity impact
  - Blast
- **Experimental**
  - Impact
  - High strain-rate materials
  - High temperature materials
  - Shock and vibration
- **Design**
  - Prototype and One-of-a-kind

Analytical Tools:

- ✓ ABAQUS/ Explicit
- ✓ LS-DYNA
- ✓ CTH
- ✓ ALEGRA
- ✓ ALE3D



INL Idaho National Laboratory

Explosives Detection & Defeat

Bulk Explosives Detection Programs

Trace Explosives Detection Programs

Tactical Timed Firing Devices/Disruptors

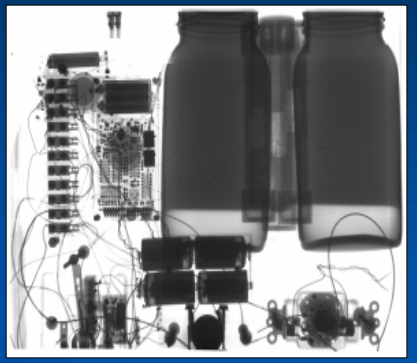
Bulk Explosives Detection Programs

Neutron Interrogation Systems - X-Ray and CT Technologies

1. **Portable Isotopic Neutron Spectroscopy (PINS)**
   --- Identifies chemicals/explosives in munitions









Single Munitions Scanner (SMS) (component of Mobile Munitions Assessment System (MMAS)

2. **Remote/Standoff Explosives Detection System (R/SEDS)**
   --- Detects explosives in medium-sized trucks and vans



INL Idaho National Laboratory

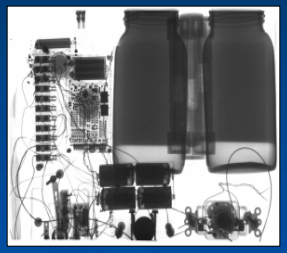
Trace Explosives Detection Programs

I. Trace Detection Systems Testing – FAA and TSL





- Perform Independent Validation and Verification testing for the Transportation Security Administration (TSA)
- Test trace detection systems against actual explosive threats
  - IEDs in Electronic Devices
  - IED Manufacturers
  - IED Couriers
  - IED in Suitcases



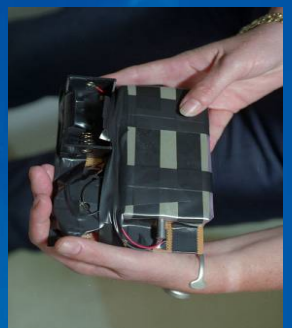




- Ion Mobility (+-) Spectrometer research in trace explosives

II. Trace Detection Systems Development

- Develop and test advanced Ion Mobility Spectrometer (IMS) concepts and prototypes
- TeraHertz Sensors R&D
- Advanced IMS modeling capability



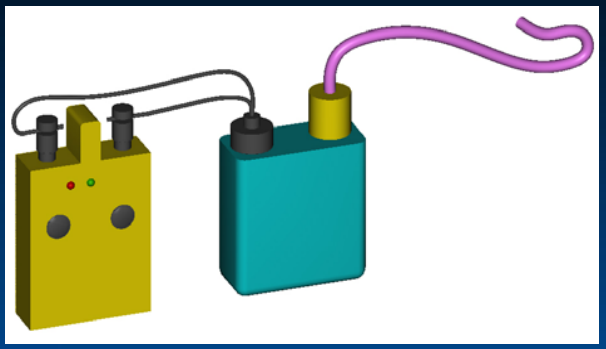


INL Idaho National Laboratory

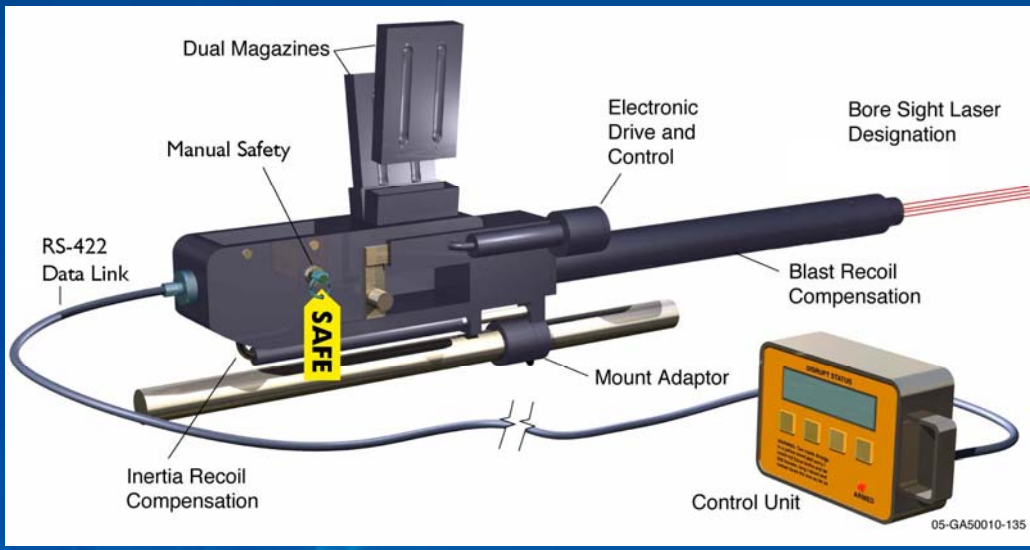
Tactical Timed Firing Devices/Disruptors

Remote Firing Devices





Multi – IED Disruptor uses "operator selected" kinetic energy penetrators



Idaho National Laboratory

Sponsor: Technical Support Working Group (TSWG)

Critical Infrastructure Test Range Complex



Idaho National Laboratory

Critical Infrastructure Test Range Complex

- National, comprehensive program where technologies, systems and policies that protect the nation's critical infrastructure are developed, tested and validated under real-world conditions
- INL is the DOE National SCADA Test Bed
- INL separate site power grid. $100M's of isolated infrastructure investments over past 50 yrs.
- Research Test Beds include:
  - Explosives Detection (Bulk and Trace)
  - Explosives/Weapons Effects Testing
  - Unique Communications/Wireless Test bed
  - UAV Research
  - SCADA Vulnerabilities
  - Cyber Security and Physical Security
  - Contraband & Weapons Detection



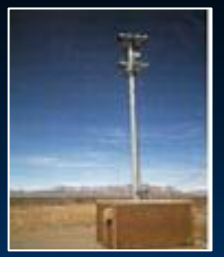




INL's Unique Communications Range Capabilities

1) "Clean" Frequency Spectrum

- Low RF noise: No urban areas or military bases
- NTIA Experimental Radio Station, Local Spectrum Manager
- Can use Next Generation / International frequencies given: a) no harmful interference, b) test / experimental use only





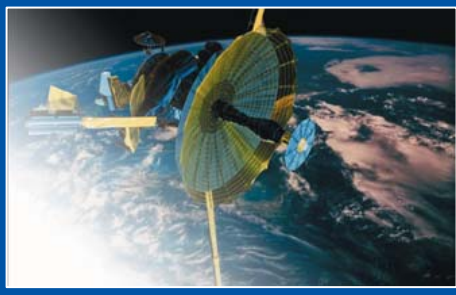
2) Full-Scale, Isolated Communications Networks

- Cell grid is isolated from PSTN, Fiber net isolated via DWDM
- Ability to link with other INL assets or external labs
- Future: Full Telco/ISP test range combined with Cyber R&D



3) "Open" Range that Cooperates with Commercial Vendors

- Commercial infrastructures are complex
- Mix of worldwide (foreign) vendors
- Leverage testing experience with cutting-edge commercial technologies



4) Flexible, Multi-program Lab

- Confluence of a variety of infrastructures (Cyber, SCADA, Comms, Physical)
- Variety of capabilities (R&D, Integration, IV&V Test, QRC, Train, Analysis …)
- Range assets, simulation resources, engineering, and operations staff

Idaho National Laboratory

Robotics

- DOD Unmanned Systems Program Area
- Robotic Autonomous Countermine Development
- Robotic Intelligent NOde (RINO)
- Next-Generation User Interface Development
- UAV Autonomous Flight Operations
- Geospatial Data Collection/Exploitation
- Unmanned Air/Ground Vehicle Collaboration

INL Idaho National Laboratory

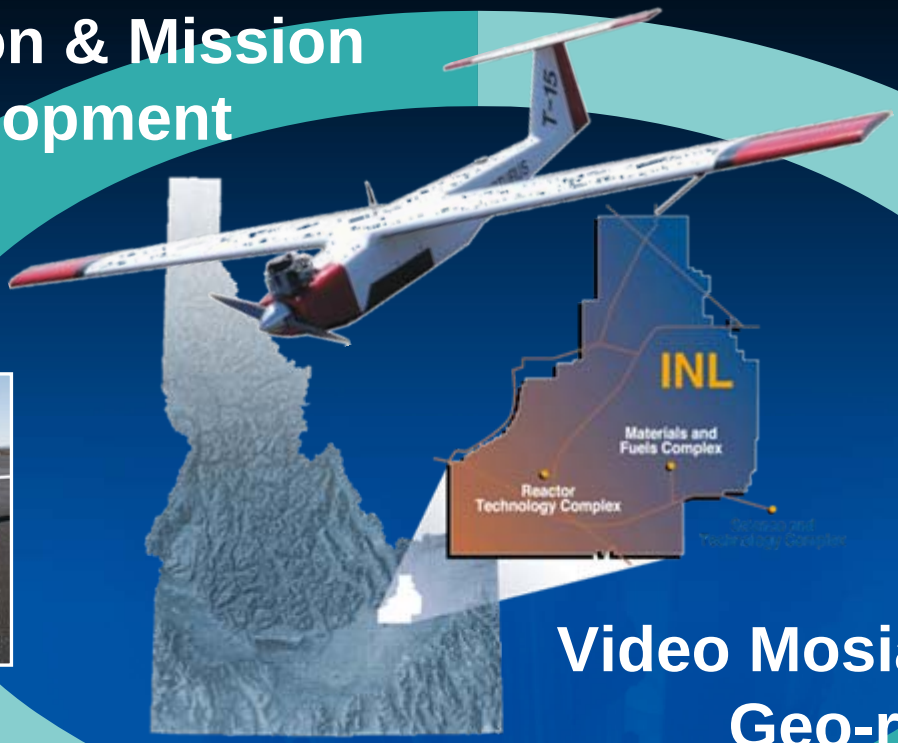
DOD Unmanned Systems Program Area

Application & Mission Development

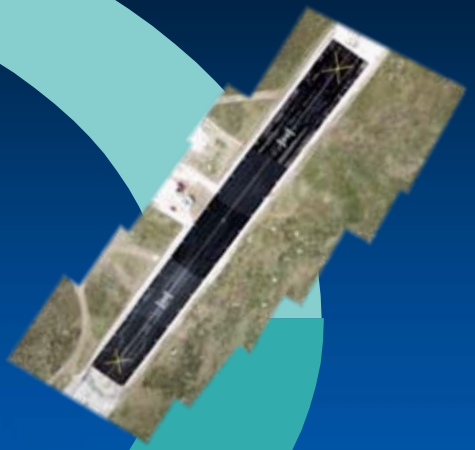




Unmanned Systems R&D



INL Facilities Infrastructure



Video Mosiac, Stabilization, Geo-referencing

Robot Intelligence Kernel





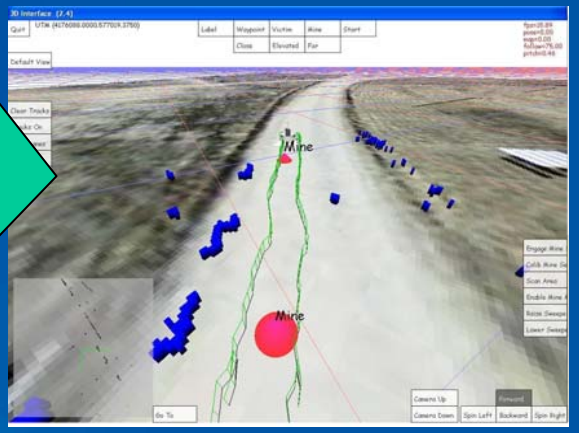
INL Idaho National Laboratory

Robotic Autonomous Countermine Development









- 4 times faster than trained human
- 100% (134 / 134) Detected SLM
- Low Cost

Robotics: Robotic Intelligent NOde (RINO)

- **Capability for 5 mission variants with and *without* human**

Mode of Autonomy	Defines Task Goals	Supervises Vehicle Direction	Motivates Motion	Prevents Collisions
Teleop	*Human*	*Human*	*Human*	*Human*
Safe	*Human*	*Human*	*Human*	*Robot*
Shared	*Human*	*Human*	*Robot*	*Robot*
HLTasking	*Human*	*Robot*	*Robot*	*Robot*
Autonomous	*Robot*	*Robot*	*Robot*	*Robot*

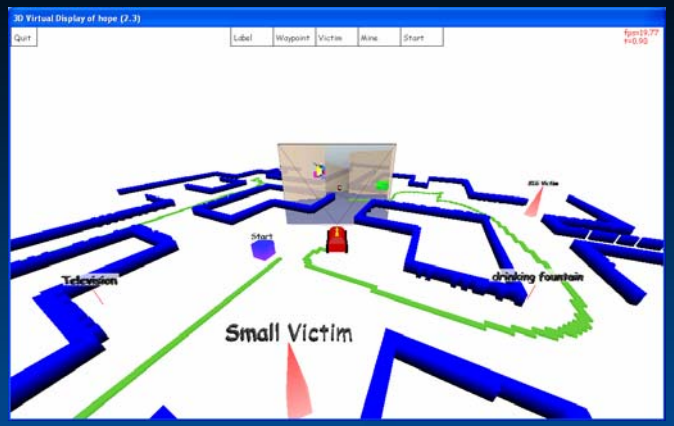
- **Development of an autonomous unmanned system for COTS 4-Wheel ATV for test and demonstration of sensors, behaviors, and payloads for ground based Unmanned Vehicles System Development.**



- **Affordability: commercial ATV Ground Vehicles**

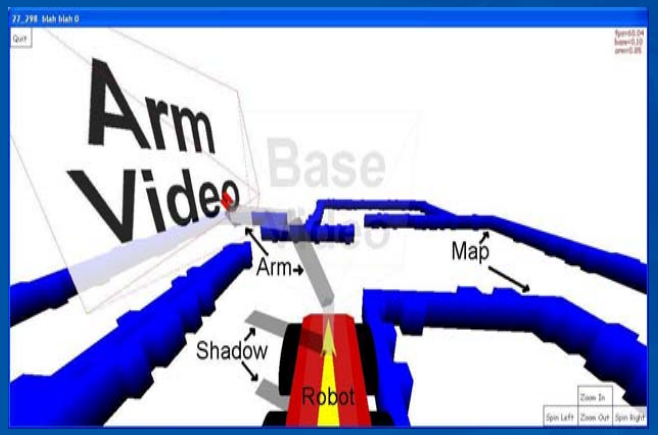
Idaho National Laboratory

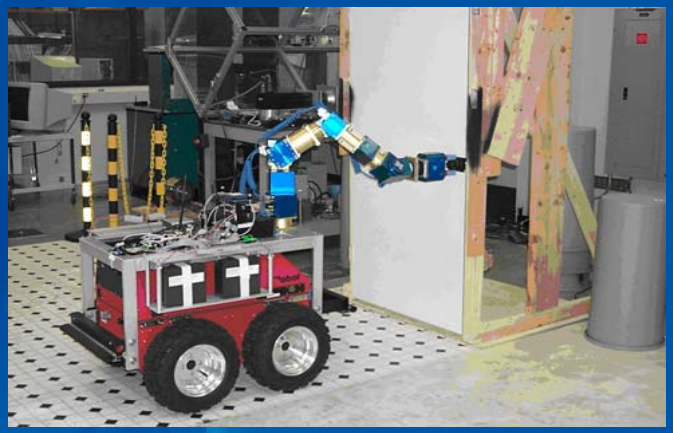
Next-Generation User Interface Development





- **Detection and Recognition → Decision and Action**

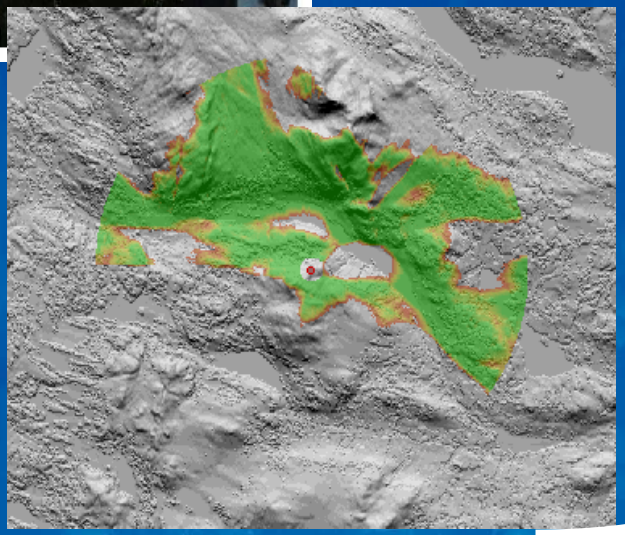




UAV Autonomous Flight Operations
Geospatial Data Collection/Exploitation



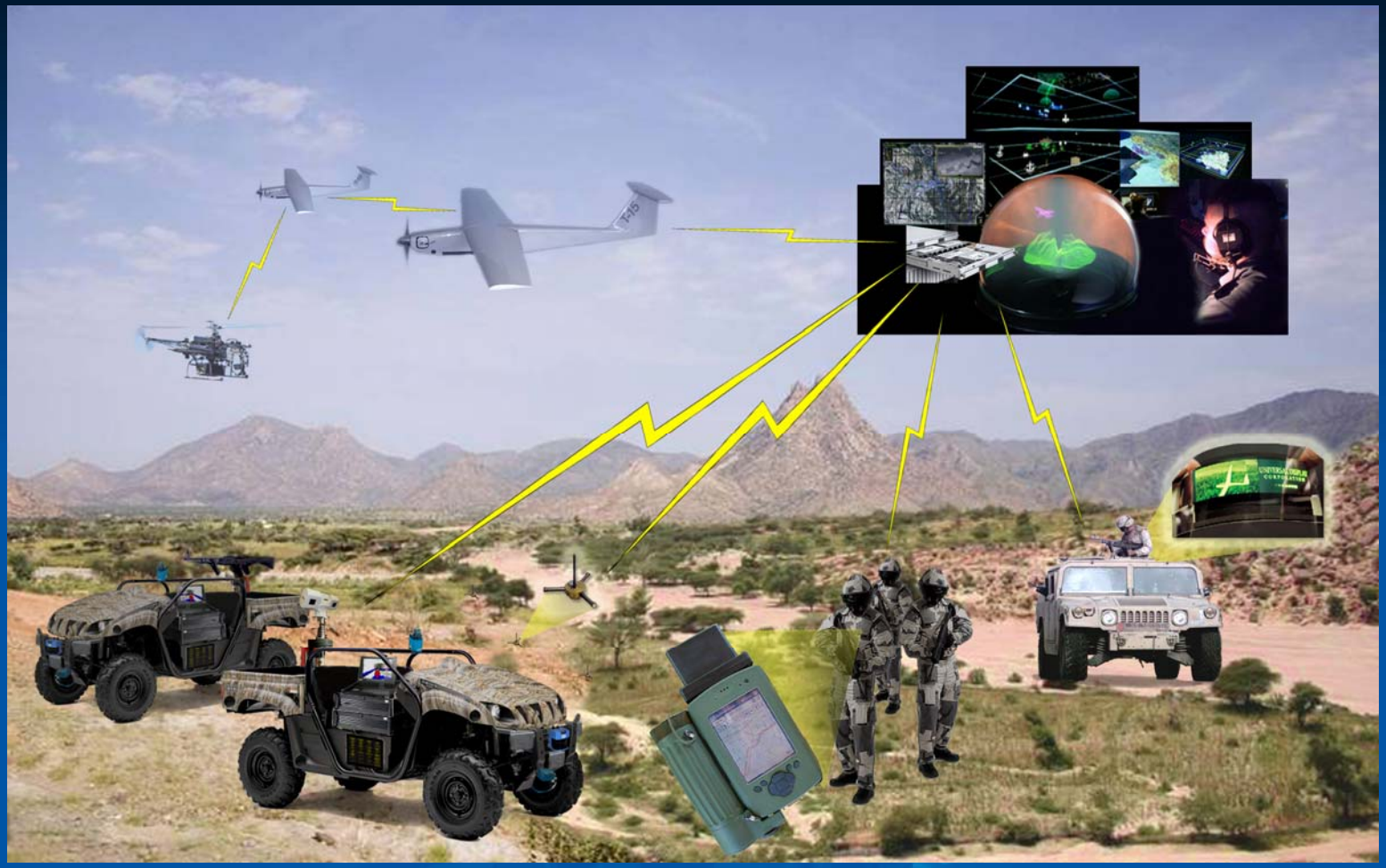






Idaho National Laboratory

Unmanned Air/Ground Vehicle Collaboration



Idaho National Laboratory

Idaho National Laboratory INL

National and Homeland Security at INL

- The United States of America is faced with unprecedented challenges in National and Homeland Security
- The Idaho National Laboratories is well positioned to meet many of these challenges and enable sustainability for the long war



John Garnier
Armor Program Lead
john.garnier@inl.gov



POLISH SOF
(REPORT FROM THE FIELD)









MG Edward GRUSZKA

AGENDA

- CURRENT POLISH SOF STRUCTURE
- SOC MISSION STATEMENT
- SOF MAIN TASKS
- OPERATIONS & COOPERATION
- WAY AHEAD



THREATS

GLOBALIZATION





ASYMMETRIC ACTIVITIES

COLLAPSING REGIMES







DEMOGRAPHIC DIFFERENCES

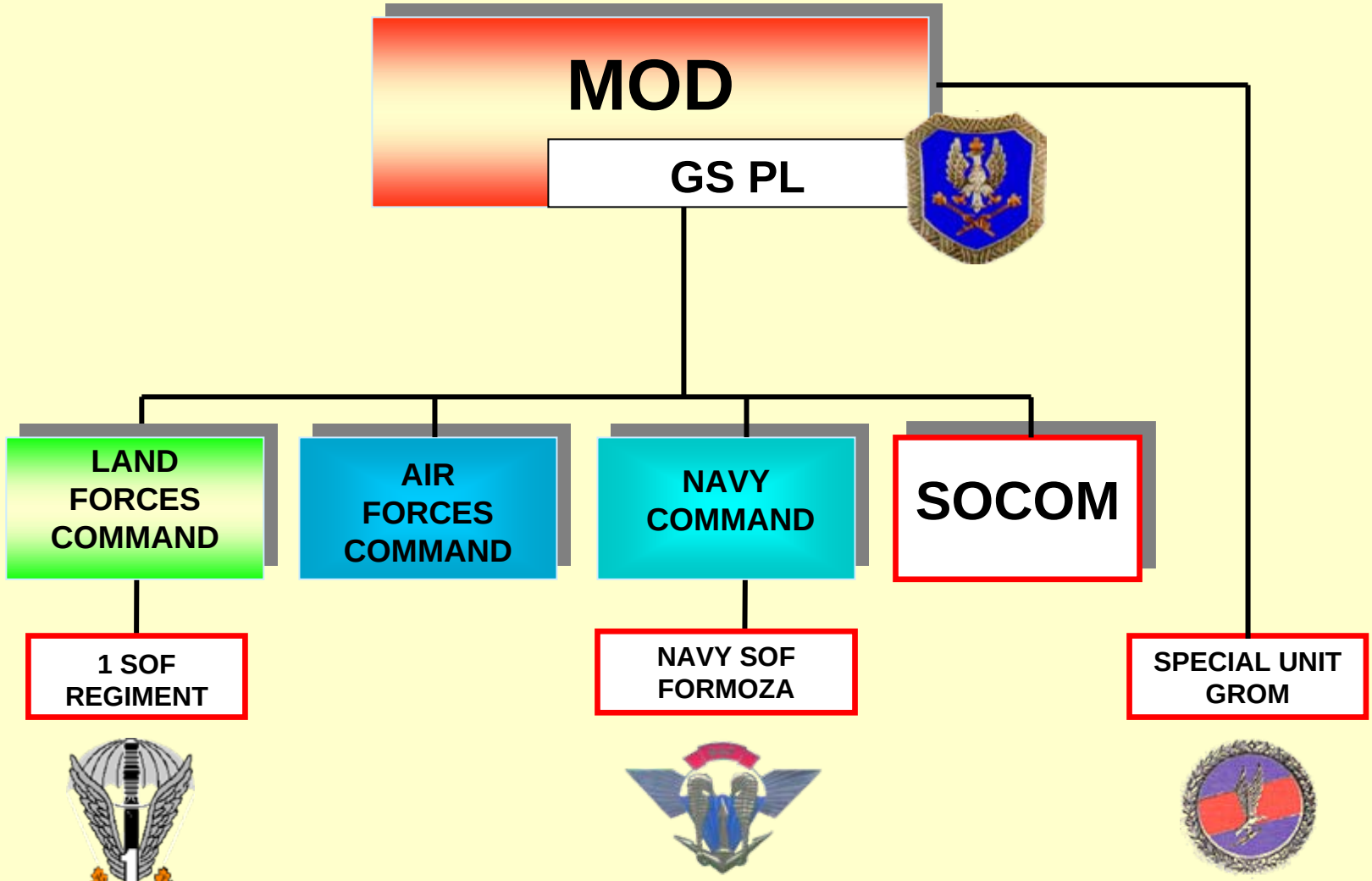
NATURAL RESOURCES VIOLENCE





UNSTABLE MIDDLE EAST

CURRENT SOF STRUCTURE



(PL) SOC MISSION

Enable and support Special Operations across the Poland and Alliance and provide the focal point for Special Operations expertise to MOD by:

- C^2 Polish SOF;
- Providing direct link between SOF and MOD;
- Providing MOD with timely, effective, Special Operations Forces advice in support of the planning and execution of operations;
- Coordinating, synchronizing and supporting of the SOF force generation process;
- Translating SOF strategic estimates into SOF operational tasks;
- Developing and publishing SOF Policies, Doctrine, SOP and SOI;
- Coordinating, synchronizing, and supporting SOF education, training and exercises;
- Coordinating training and development capability of the Polish SOF through a Federation of NATO SOF Training Centers.

SOF MAIN TASKS



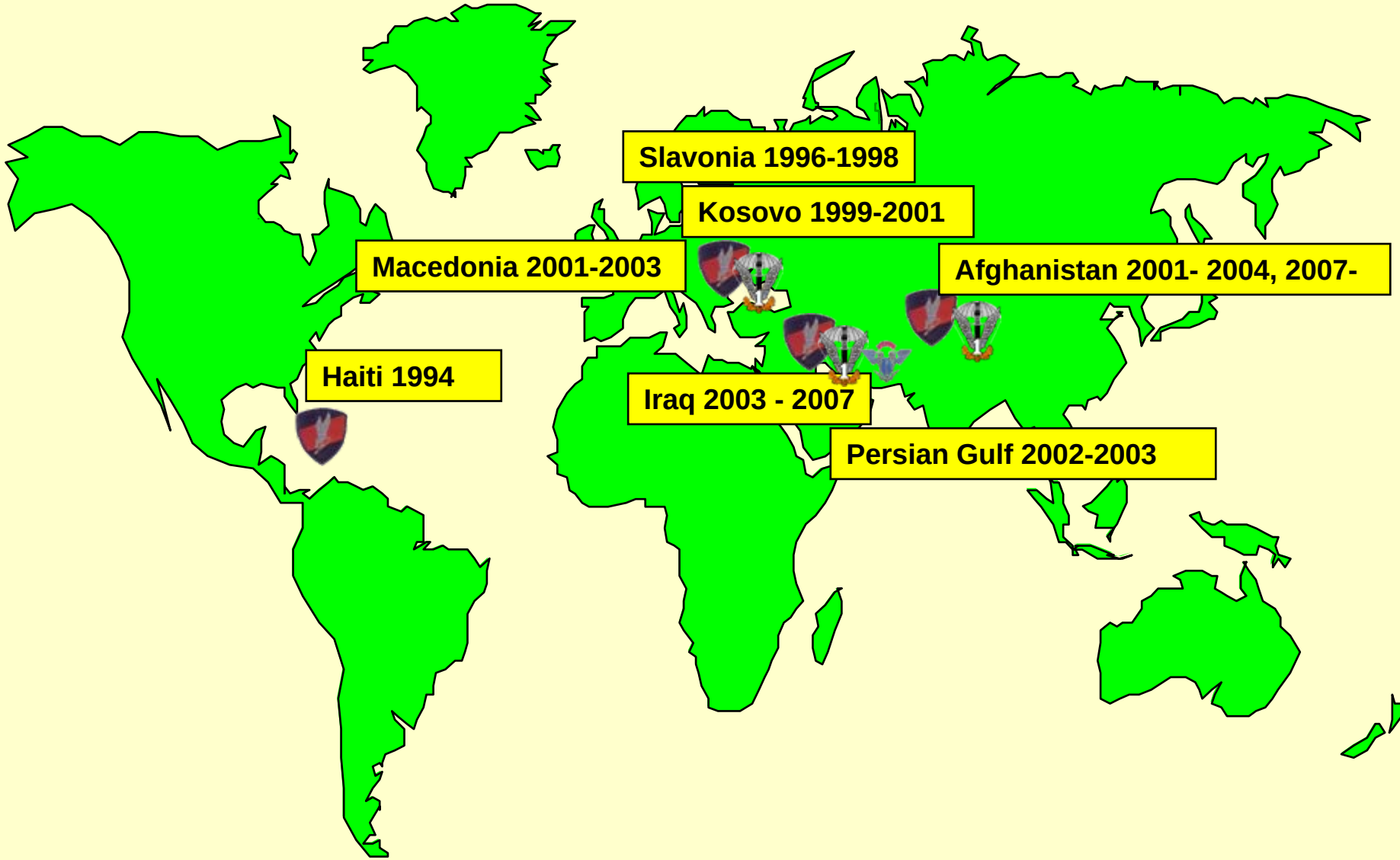
- SPECIAL RECONNAISSANCE
- DIRECT ACTIONS
- COUNTER TERRORISM OPERATIONS
- MILITARY ASSISTANCE
- MISCELLANEOUS







MAIN OPERATIONS



IRAQ







AFGHANISTAN



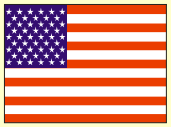


ISAF

کمک او همکاری

MULTIRATERAL COOPERATION

GROM


3,5,10 SFG
Navy Seals


22 SAS Reg
SBS


BBE

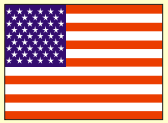

Marine Jagerkommando
Haeren Jagerkommando


URNA


YPT


Israel SF

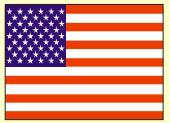
1st SOF Regiment


10 SFG
75 Ranger Reg


21 SAS Reg


200th Deep Recce Coy

FORMOZA


Navy Seals


BBE

TRAINING









THEY SAID …

„ Unit GROM is absolutely parallel with DELTA unit. It is a very big achievement giving Poland an important international asset”

Zbigniew Brzeziński – Former Security Adviser of US President

„ Polish SOF unit GROM is the first class, outstanding people with outstanding morale ... I would be very happy if I could work with this unit during the emergency situation”

Generall Wayne A. Downing

WAY AHEAD

DIRECTIONS

- REORGANIZATION OF C2 STRUCTURE
- UNITS TTPs AND EQUIPEMENT UNIFICATION
- REORGANIZATION CS, CSS
- EQUIPPED WITH HIGH TECHNOLOGY

FUTURE SOF STRUCTURE









- MOD
  - GS PL
    - SOB
- LAND FORCES COMMAND
  - SOB
- NAVY COMMAND
  - SOB
- AIR FORCES COMMAND
  - SOB
  - Air SOF Wing
- SPECIAL OPERATIONS COMMAND
  - SPECIAL UNIT GROM
  - NAVY SOF FORMOZA
  - 1 SOF REGIMENT
  - SOF Training Center
  - CS & CSS UNITS

HIGH TECHNOLOGY

NETWORK-CENTRIC CAPABILITIES





CYBER SPACE



UNMANNED AERIAL VEHICLES





OPTOELECTRONICS, GPS



HIGH TARGETING ASSETS





INTEROPERABILITY

- Interoperability needs to be a community effort.
- We have concentrated on CIS to date, we are moving into Intel Recce Surveillance and Target Acquisition (IRSTA)…what next?
- Joint Special Operations Capabilities Task Force is therefore the primary point of entry.
- Impact to date:
  - CIS experimentation campaign;
  - Precision Airdrop systems in service;
  - Warfare Ops Center connectivity.

QUESTIONS ?

US Special Operations Command

Center for Knowledge and Futures (SOKF)

Overview Brief

Briefer: BG Hashem

Director - SOKF

Date: 27 FEB 07

The overall classification of this briefing is:
UNCLASSIFIED

Derived From: N/A
Declassify On: N/A

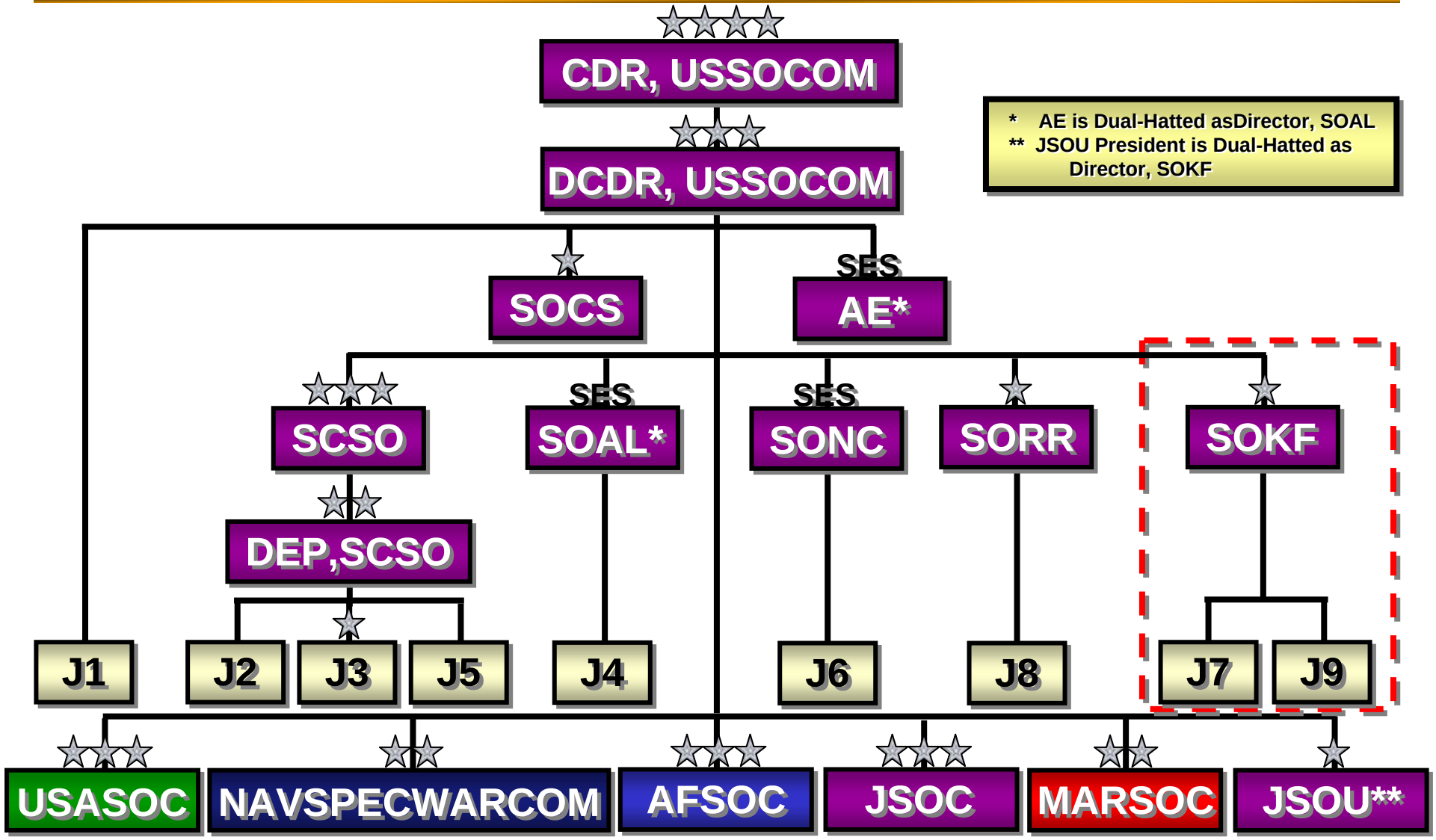
Mission

The Center for Knowledge and Futures develops and integrates warfighting capabilities for the present and future in order to train, organize and equip special operations forces to synchronize and execute global operations against terrorist networks and deploy combat ready forces to combatant commands.

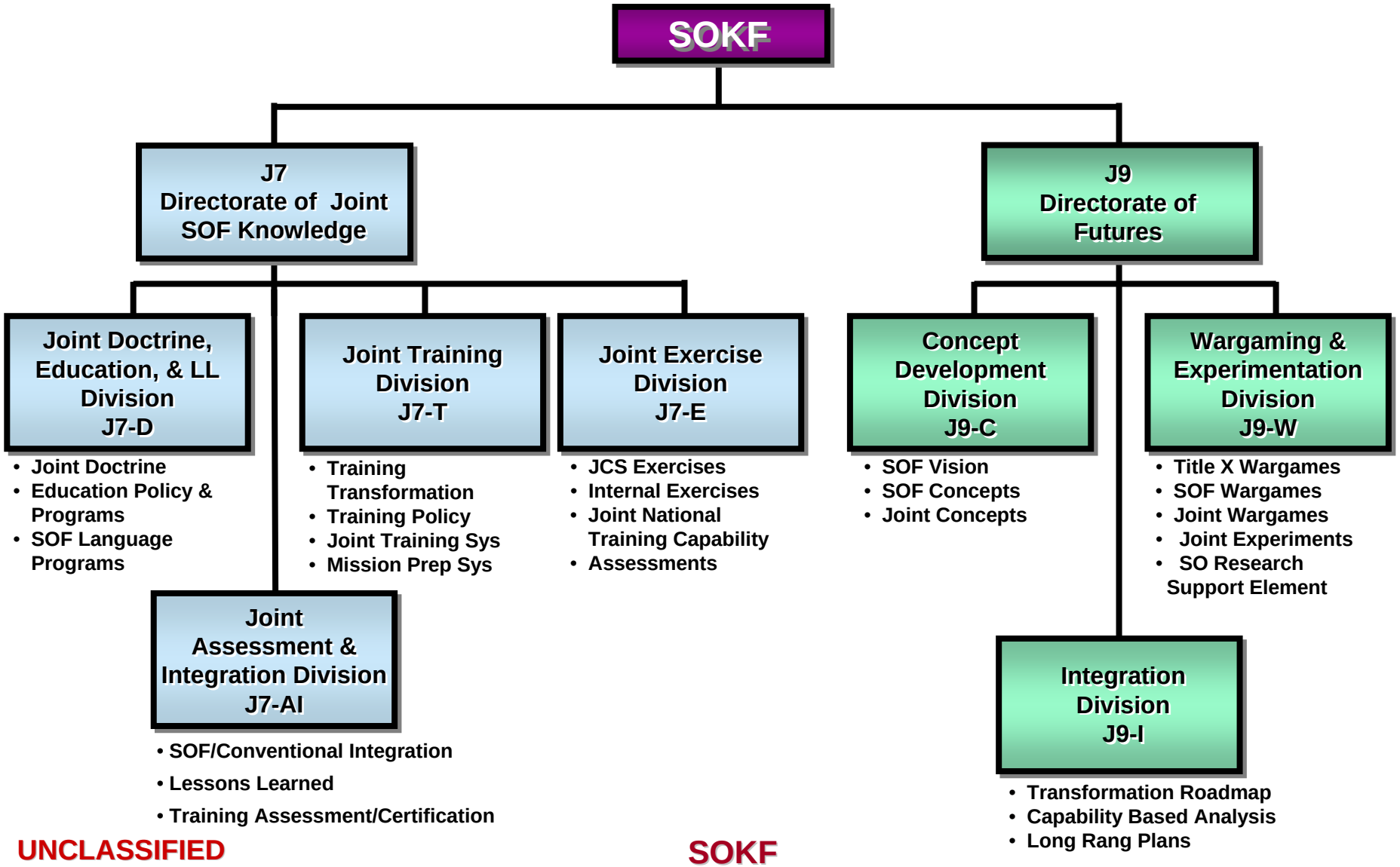
SOKF Title 10 Functions

- Develop Strategy, Doctrine, and Tactics
- Educate and Train SOF
- Conduct Specialized Courses
- Prioritize and Validate Training Requirements
- Ensure Interoperability of Equipment and Forces
- Conduct Joint SOF Concept Development, Wargaming, Experimentation, and Integration
- Ensure Combat Readiness of SOF
- Prepare SOF to carry out assigned missions

USSOCOM Organization



SOKF Organization



Joint SOF Body of Knowledge (J7)

- **Develop Joint special operations doctrine and tactics, techniques, and procedures**
  - **Facilitate integration of SOF doctrine into joint and service institutions**
- **Develop a comprehensive education strategy that complements component, Service, and PME programs**
  - **Provide support to JSOU**
  - **Expand educational opportunities for SOF**
- **Execute USSOCOM's Lessons Learned Program**
  - **Provide recommended solutions to observations**
  - **Integrate Lessons Learned into joint doctrine and education**

Joint SOF Training
(J7)

- **Execute the SOF Language Program**
  - Strategy, prioritization and program management
- **Provide training oversight**
  - Develop training policy, identify and validate training requirements
- **Manage CJCS Joint Training System for USSOCOM**
  - Develop and maintain JMETL
  - Develop joint training plans, policies and publications
- **Develop and conduct specialized courses**
  - Military Liaison Element Seminar
- **Oversee Mission Training & Preparation Systems (MTPS)**
  - Training simulations, planning, preview & mission rehearsal

Warrior Preparation
(J7)

- **Ensure USSOCOM's readiness to perform its warfighter tasks**
  - **Plan, coordinate, and execute a comprehensive internal exercise program designed to enhance the effectiveness of the deployable battlestaff (ABLE WARRIOR and ABLE FOCUS)**
- **Assess command support to GCCs and training events**
  - **Coordinate support to the Joint National Training Capability (JNTC) exercise program**
  - **MRX participation, JSOTF training**
  - **SOF participation, scenario development, exercise management and assessment**

Strategic Visioning & Joint Concept Development (J9)

- **Lead creation of a compelling SOF Vision of the future**
  - **Develop joint SOF-specific and Joint Operating Concepts IAW the "USSOCOM Future Concept Development Campaign Plan" to mature the Vision**
  - **Synchronize concept development with Joint community, DOD, and interagency**
  - **Sponsors concepts and associated capabilities within SOF for Joint experimentation**
  - **Develop future SOF capabilities supporting the War on Terror**
- **Develop USSOCOM Transformation Roadmap**
  - **Design long-range strategy and vision implementation plan**

Wargaming and Experimentation (J9)

- **Lead USSOCOM's Wargame and Experimentation activities IAW approved Wargame and Experimentation Campaign Plan**
  - **Design, develop, and publish detailed external wargame plans to guide, measure, and validate objectives based on SOF concepts**
  - **Ensure data collection/analysis plans are developed for analytically sound wargame results**
  - **Identify SOF capability gaps as candidates for experimentation**
  - **Provide DOTMLPF change recommendations from experiment results**
  - **Manage and prioritize activities of the SORSE**

Capabilities Based Assessment (J9)

- **Develop, Coordinate, and Maintains USSOCOM Long Range Planning Process**
  - **Integrate futures requirements into command resourcing and planning processes**
  - **Manage USSOCOM and Component Joint SOF Future Concept related Joint Capabilities Integration Development System Analysis**
- **Manage USSOCOM Capability Evaluation Process**
  - **Develop and maintain USSOCOM Prioritized Capability List**
  - **Coordinate solutions to capability gaps**
  - **Coordinate S&T and Acquisition proposals**

Summary

- SOKF integrates the *J7* and *J9* to *conduct SOF Combat Development*
- Responsible for SOF *training standards*, *doctrine*, *lessons learned*, *SOF language programs*, *education programs*, *exercises*, *interoperability*, *future concepts*, *experimentation*, *wargames*, and *integration of future requirements* into command resourcing and planning processes

SOKF supports the education and training of the SOF warfighter of today, while shaping and preparing USSOCOM for the warfight of tomorrow

Joint Special Operations University



“Joint SOF Education for the Long War”

BG Steven Hashem

President

USSOCOM Vision

“To be the premier team of special warriors, thoroughly prepared, properly equipped, and highly motivated: at the right place, at the right time, facing the right adversary, leading the Global War on Terrorism, accomplishing the strategic objectives of the United States.”

USSOCOM Vision

“To be the premier team of special warriors, ***thoroughly prepared***, properly equipped, and highly motivated: at the right place, at the right time, facing the right adversary, leading the Global War on Terrorism, accomplishing the strategic objectives of the United States**.”**

JSOU Mission: Provide education for Joint SOF

JOINT SPECIAL OPERATIONS JSOU UNIVERSITY

Agenda

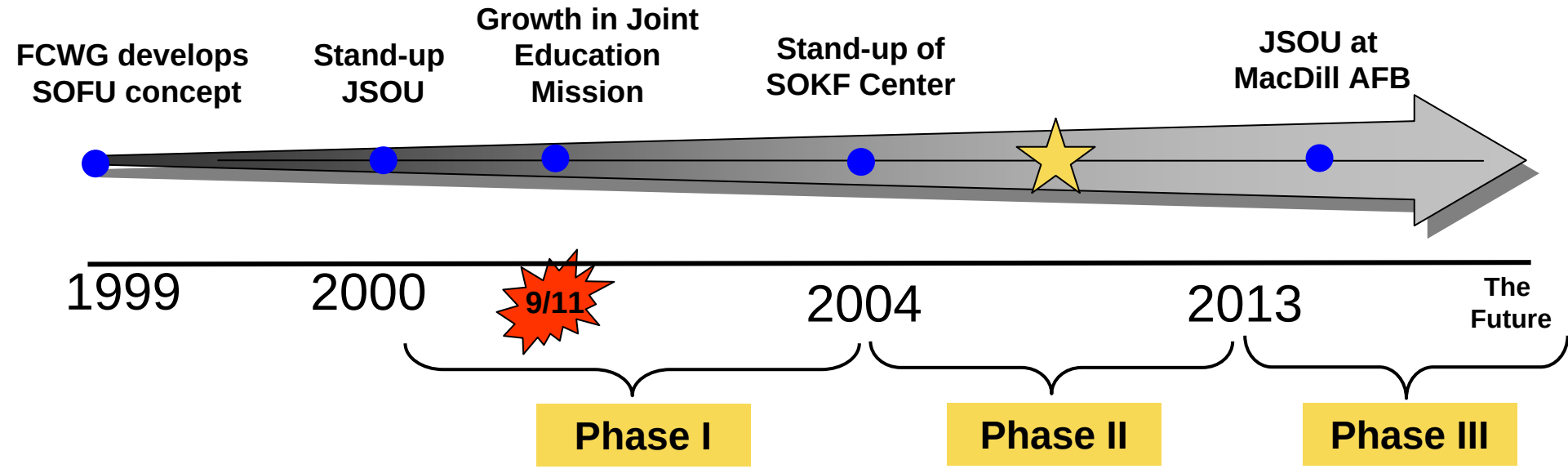
JSOU Mission Overview

Warfighters Certificate Program

Strategic Educational Engagement

JOINT SPECIAL OPERATIONS
JSOU
UNIVERSITY

JSOU's Evolution



- Phase I — Start-up activity (completed)
- Phase II — Implementing a Strategic Plan for SOF Education
- Phase III — Optimization of the organization

JOINT SPECIAL OPERATIONS UNIVERSITY

JSOU Mission

- **Develop SOF and SOF Enablers for strategic and operational leadership**
- **Educate military and civilian professionals on the employment of SOF in a joint, interagency, and multinational environment**
- **Research and publish on national security issues critical to the SOF community**

Agenda

JSOU Mission Overview

Warfighters Certificate Program

Strategic Educational Engagement

JOINT SPECIAL OPERATIONS
JSOU
UNIVERSITY

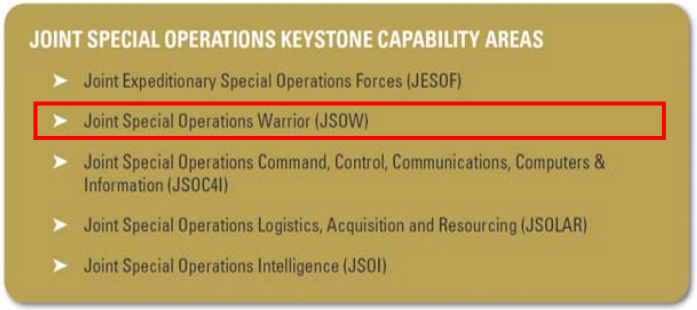
JSOWC Supports the JSOKCA JSOW

JOINT SPECIAL OPERATIONS KEYSTONE CAPABILITY AREAS

- Joint Expeditionary Special Operations Forces (JESOF)
- Joint Special Operations Warrior (JSOW)
- Joint Special Operations Command, Control, Communications, Computers & Information (JSOC4I)
- Joint Special Operations Logistics, Acquisition and Resourcing (JSOLAR)
- Joint Special Operations Intelligence (JSOI)

JSOWC Relates to JSOW

- **Develop an educational process to produce future Joint Special Operations Warrior who will be prepared for global expeditionary employment and with the ability to synchronize operational and strategic activities**
- Develop a prototype of the Joint SOF Warrior System, blending individual skills with the proper equipment, weapons, mobility, support, and communications systems
- Establish a process for Joint SOF human capital development
- Develop a Joint SOF “cradle to grave” career management system emphasizing selected educational, overseas and exchange or liaison assignments



Joint Special Operations Warfighters Certificate

- **JSOWC program consists of 3 modules:**
  - **SOF Force Application and Strategy Course**
  - **Irregular Warfare Course**
  - **SOF Collaborative Planning Course**
- **Nominative course for mid-level officers, warrant officers, and senior NCOs**
- **Goal: Prepare students for Joint Special Operations duty positions**

Critical to developing *Joint* SOF Warriors

JOINT SPECIAL OPERATIONS JSOU UNIVERSITY

JSOWC Curriculum Overview

Joint Special Operations Warfighter Certificate

Module 1 (10 Days)

Joint SO Force Application and Strategy

- National Policy
- Strategy Development
- Employment in Strategic Planning
- Centers of Gravities and Critical Factors
- Special Operations Forces Integration into Planning
- Evolution of Joint Special Operations Doctrine, Structure, and Functions
- Special Operations Forces C2 Structures and Functions
- Special Operations Forces Integration into Joint Targeting

Module 2 (10 Days)

Irregular Warfare

- Introduction to Irregular Warfare
- Counter Insurgency and CT
- IW - The Indirect Approach
- IW - The Direct Approach
- Interagency Collaboration in IW
- Intelligence support to IW
- Civil Military Operations in support of IW
- Information Operations and PSYOP in IW

Module 3 (10 Days)

Joint SO Collaborative Planning

- Doctrinal Basis for SOF Planning
- Operational Level Planning
- Planning Support Agencies and Activities
- Digital Planning and Collaborative Tools
- Instructor Facilitated Exercise
- Student Led Exercise

Prerequisite - ISOF

JOINT SPECIAL OPERATIONS JSOU UNIVERSITY

Future Certificates

- **JSOWC success will provide foundation for additional certificate programs**

- **JSOKCA logical guide to future certificates:**
  - **Intelligence**
  - **Logistics**
  - **Command and Control**

Agenda

JSOU Mission Overview

Warfighters Certificate Program

Strategic Educational Engagement

JOINT SPECIAL OPERATIONS
JSOU
UNIVERSITY

Strategic Educational Engagement

- International engagement via Special Operations Combating Terrorism Course
- Growing interagency educational program provides a domestic “engagement” with key partners in the interagency process
- Research, Publications, and Symposia provide both outreach and engagement on SOF topics

Combating Terrorism Fellowship Program (CTFP)

- **Directly supports USSOCOM's international engagement initiatives**
- **Special Ops Combating Terrorism Course**
  - **Two SOCbT iterations -- Great success!**
  - **Students: 46 International and US SOF**
  - **Top-notch international and US instructors**
- **Strategic Engagement in FY07**
  - **Curriculum support to SOCCENT Annual Symposium in UAE**
  - **Regional programs for SOCPAC and SOCEUR**

Interagency Educational Program

- **Joint SOF Interagency Collaboration Course**
  - **3 iterations per FY in Washington and Tampa**

- **New USSOCOM Interagency Taskings**
  - **SOF Executive Interagency Seminar**
  - **SOF Interagency Support Team Preparation**
  - **IA Partner SOF Orientations**

In Concept Development

JOINT SPECIAL OPERATIONS UNIVERSITY

Last Words



"Our commitment to this nation requires still more of our warriors. It requires a constant force evolution, not in response to our adversaries, but in advance of our adversaries." **General Brown, CCSO 2006**

JOINT SPECIAL OPERATIONS
JSOU
UNIVERSITY

Joint Special Operations University



"Joint SOF Education for the Long War"

BG Steven Hashem

President

Backup Slides

JSOF Leadership Competency Model



Force Application
- Operational Art
- Joint & Combined Warfighting
- SOF Integration
- Joint SOF C4ISR
- Situational Awareness

Vision & Strategy
- Vision Creation & Execution
- Strategic Art
- Strategic Awareness
- Opportunity Development

Force Management
- Asset Management
- Technology Management
- Resource Management

Developing Partnerships
- Communication
- Collaboration
- Influencing/Negotiating
- Cultural Awareness

Interpersonal Orientation
- Team Building
- People Development
- Conflict Resolution

Action Orientation
- Problem Solving
- Decisiveness
- Initiative
- Adaptability
- Risk Management

JSOU UNIVERSITY

Strategic Studies Division

- **Research and Publication**
  - Core Staff + Editor
  - Annual Research Plan
  - PME Students Papers
  - Essay Contest





- **Education Engagement**
  - Annual Strategic Symposium
  - Periodic Seminars & Workshops
  - Senior Courses + War College Support
  - Ties to Think Tanks, Academia, DoD's Regional Centers
- **Courses**
  - Joint SOF Pre-Command
  - Terrorism Response Seminar
  - SO Combating Terrorism
  - SOF-Interagency Collaboration
  - IA Course Cadre (in development)



- **Senior & Associate Fellows**
  - Focused intellectual research & support across the spectrum

JOINT SPECIAL OPERATIONS
JSOU
UNIVERSITY

UNITED STATES COAST GUARD
RESEARCH & DEVELOPMENT CENTER





USCG - DEPLOYABLE OPERATIONS

Presentation to 18th Annual NDIA SO/LIC Conference
26 February 2007



Providing the Coast Guard with technology expertise and support for operational analysis and development.

SCIENTIFIC PRINCIPLES

$$E = mc^2$$

$$E = \mu\chi 2$$

Conference Theme

- *Warfare in the Seams: Defense and Industry Partnering to Win the Long War*

- Transforming General Purpose Forces for Warfare in the Seams
  - *e.g., Training and Technology required to Conduct Military Operations in Cities, Mountainous Regions, Desert Terrain, and to Secure Long Borders from Hostile Incursions*

CG Mission

- Safeguard lives, property and the environment from intentional and accidental maritime threats
- Protect maritime mobility by eliminating interruptions and impediments to the economical movement of goods and people while maximizing the recreational use of the Nation's waterways.
- Secure maritime routes by halting the flow of illegal drugs, aliens and other harmful/toxic contraband while preventing illegal incursions of our Economic Exclusion Zone thereby enforcing federal law.
- Defend the nation as one of the five US Armed Services and enhance regional stability in support of the National Security Strategy.

Threats & Challenges

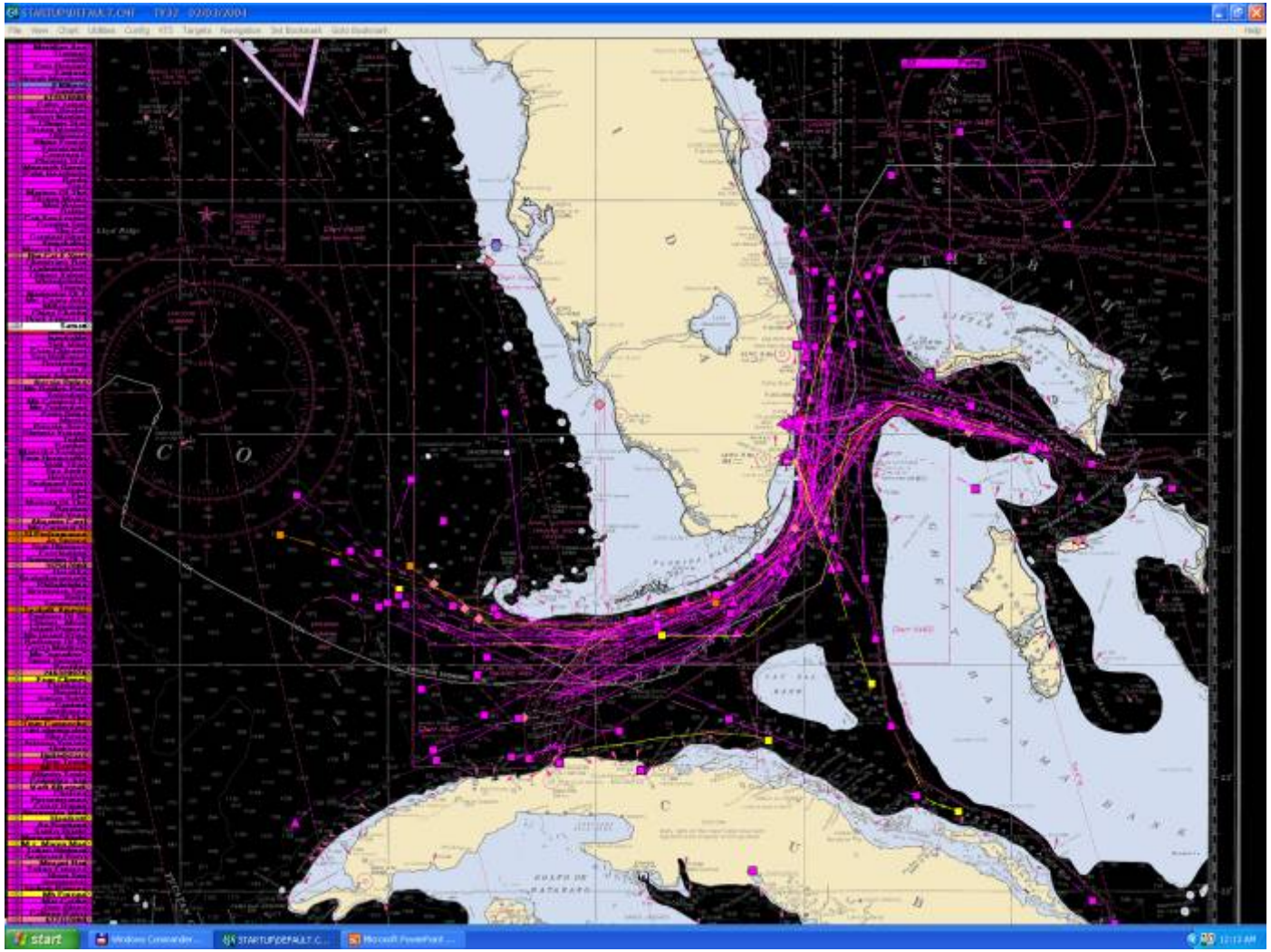


Threats & Challenges (cont.)

- Vessels carrying contraband
  - *WMDs, Explosives, Weapons, Drugs*
- Vessels as weapons
  - *Threat to other vessels and infrastructure*
- Vessels used to smuggle illegal aliens
  - *Go-fast boats, "put-puts" and containers*
- Vessel crews and passengers contain terrorists
  - *Ship jumpers*
- Underwater threats
  - *Swimmers, mines, explosives*



Traffic Density



Thousands of vessel “trips” in the AOR per week

Systems Approach

OPERATIONAL SEQUENCE

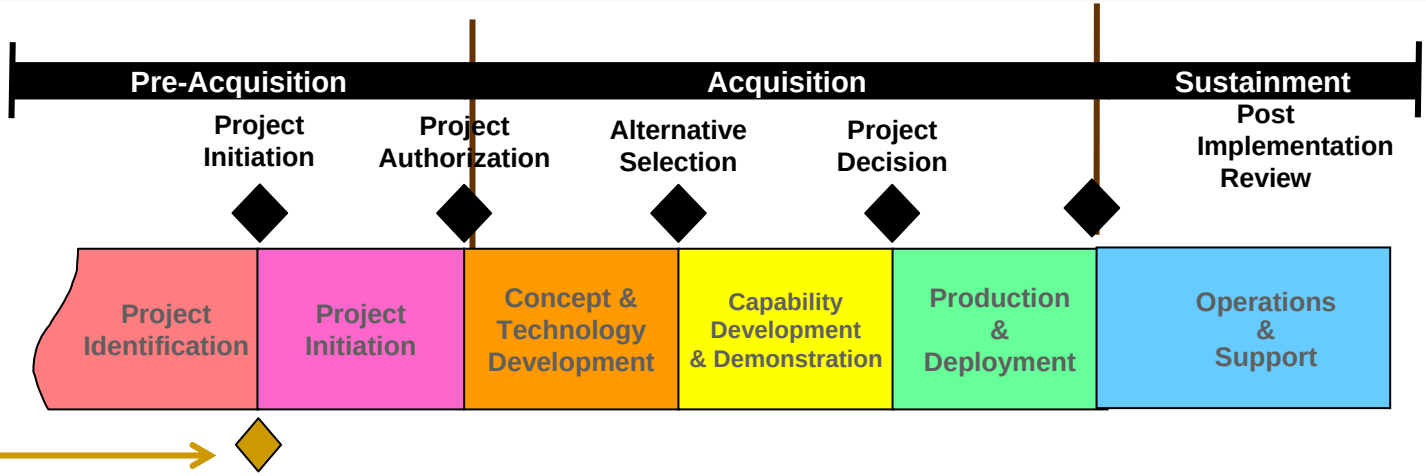
	ASSESS	DETECT	IDENTIFY	DECIDE	ENGAGE
MATERIAL	* Intelligence	* Location	* Vessel ID	* Anomaly	* Intercept
PEOPLE	* Vulnerability	* Track	* Cargo	* Threat	* Inspect
VESSELS	* Threat	* Classify	* Crew	* Action	* Detain
	COMMON OPERATIONAL PICTURE				
	INFORMATION AND COMMUNICATIONS				

- CG COP

Intel Systems	Sensors	ID Systems	Scene & TDA	Field Equip
• MIFC • TVIS	• Coastal Radars • Cameras • OTH Radar Nets • UAVs	• AIS • Blue Force Tracking • Visual Understand	• Auto Scene Understand • Decision Aids • Collaboration	• Sensors • PDAs • Detectors • Weapons

- *System of systems approach to sensors, processing, correlation, analysis, decision and reaction systems*
  - *Open architecture*
  - *Interoperable*

Technology Opportunities



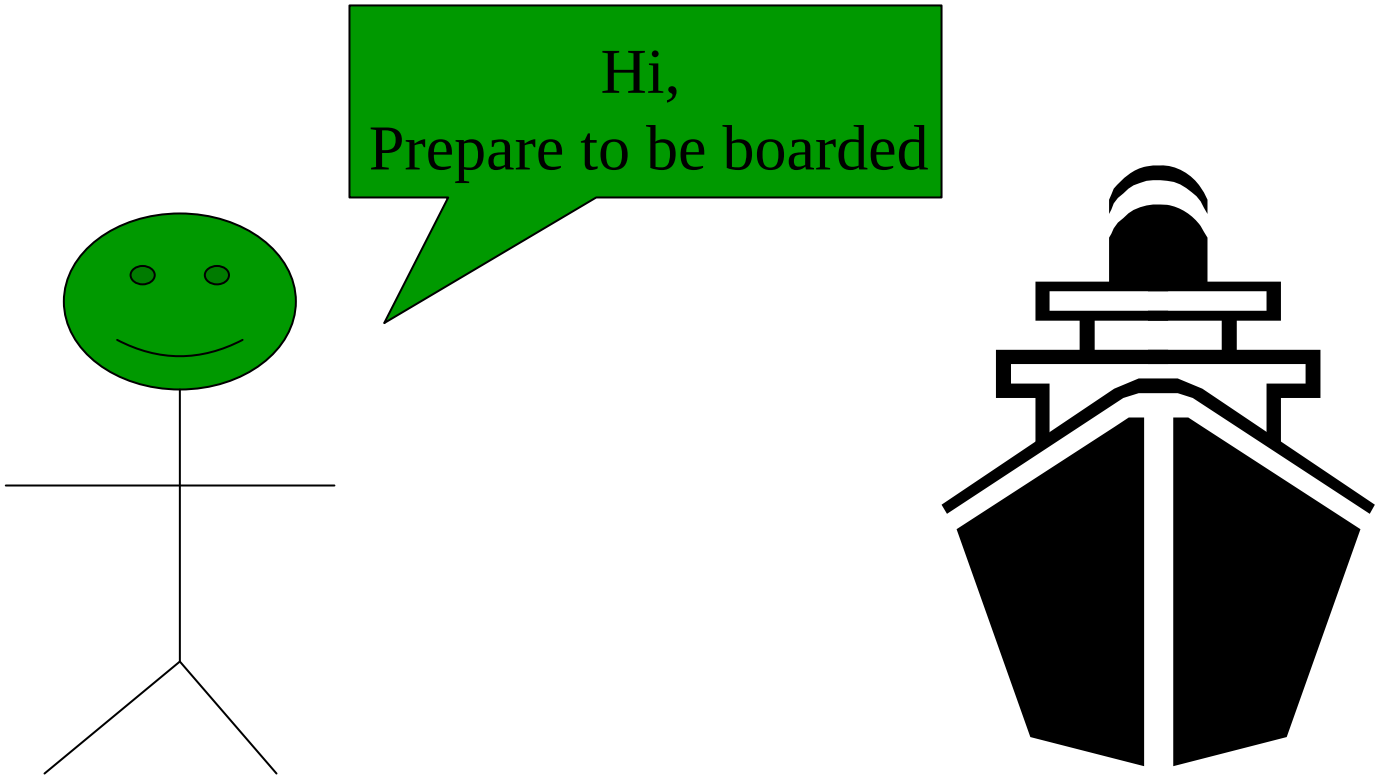
Mission Analysis
Operational Effectiveness

Technology Assessment
Technology Demo
Cost Assessment
Human Systems Study
ORD Development
MNS Development

Market Research
Alternative Analysis
Proof-of-Concept Tests
Modeling & Simulation
Human Sys Integration
Technical Advisor

DT&E
OT&E
Technical Advisor

Boardings – CG Bread & Butter



Boarding Officer Bill/Betty

Attain accurate accounts of material, personnel, etc. for vessel control issues and concerns

Deployable Specialized Forces

- Port Security Units (PSU)
- National Strike Force/Strike Teams
- Tactical Law Enforcement Teams (TACLET)
- Maritime Safety & Security Teams (MSST)
- Maritime Security Response Team (MSRT)

Deployable Specialized Forces

Areas of Interest & Need

- Protective Equipment/Components
- Detection of Agents & Compounds of Interest
- Audio/Visual Tactical Sensing
- Lethal & Non Lethal Technologies
- Tactical Intelligence
- Biometrics
- Enhanced Strategic/Tactical Platform & Sensor Performance

Deployable Specialized Forces

Related Needs

- Weapons Proficiency
- Weapon Retention
- Close Quarters Battle
- Crowd Control
- Fire and Movement
- Site Security
- Moving Targets
- Assistance to other Emergency Responders
- Weapons Transition
- CBRNE Sampling, Monitoring
- CBRNE Evidence Collection
- Night / Low Light Engagement
- Self-Defense
- Vessel Operations
- Suspect Control
- Decontamination
- Communications
- Rescue
- CB Perimeter Characterization
- Unassisted Equipment Donning

Deployable Specialized Forces

Task/Skill

- Weapons Proficiency
- Weapon Retention
- Operating Equipment
- Close Quarters Battle
- Ground Fighting
- Fire & Movement
- Moving Targets
- Weapons Transition
- Night / Low-Light Engagement
- Self-Defense
- Suspect Detaining
- Site Security

Integration Issue

- Dexterity / Tactility
- Weapon Aiming / Sighting
- Weapon Access
- Weapon Clearing / Reloading
- Durability
- Sustainability
- Ability to Communicate
- Visual Acuity
- Hearing Acuity
- Unassisted Equipment Donning
- Sustainability
- Monitoring of Individuals

Deployable Specialized Forces

Task/Skill

- Evacuation of Victims
- Decontamination of Self
- Decontamination of Equipment

Integration Issue

- Limited Capability

Prioritization of Integration Issues

- Sustainability of Wearer
- Communications & Interoperability
- Dexterity Issues
- Donning & Doffing of Equipment & Clothing
- Respirator interoperability/interchangeability
- Integration of equipment in CB ensembles
- Inability to characterize threats – real time
- “Frequency of Use” Analysis for load carriage
- Overall load carrying expectations
- Weapon sights/facemask compatibility

Mission Profile Duration

Mission Profile	Duration for CB Protection
First Responder Perimeter Control	8 - 12 hours (min)
Tactical Operations	4 - 6 hours
HAZMAT	TBD
Emergent SAR	1 – 2 hours

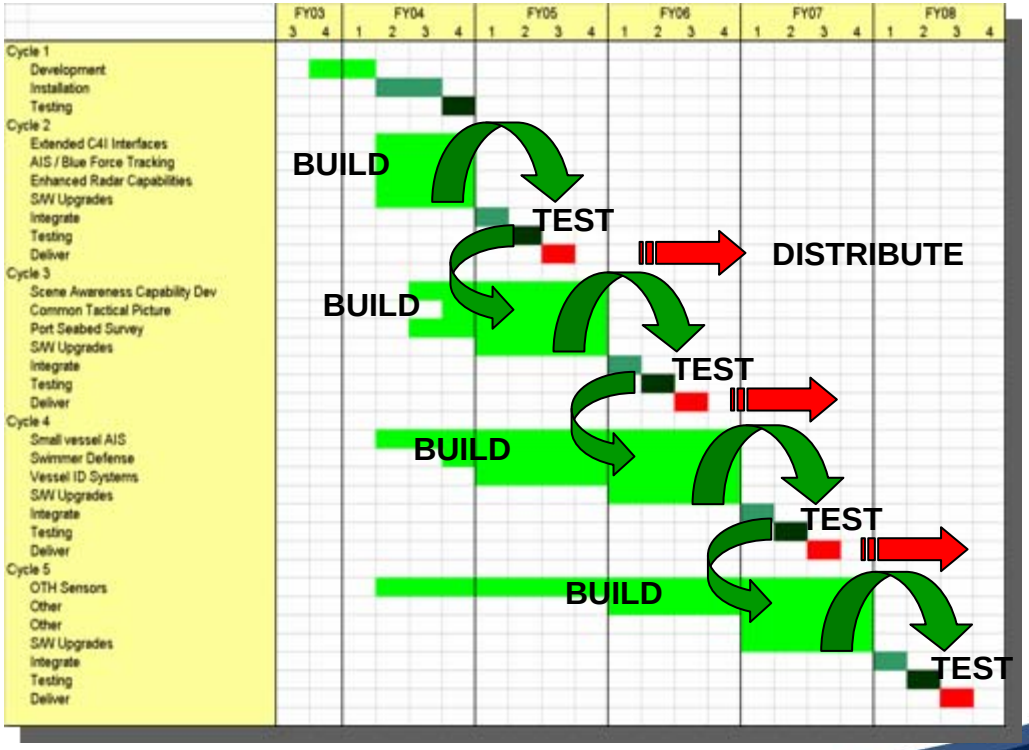
Technology Insertion Goals

- *Invest in products that address priority needs*
- *Develop "best" products as quickly as possible (triage/spiral approach)*
- *Help CG implement products*

Program Evolution

- Spiral Development
  - *Build – Test – Build evolution over multiple years*
  - *Incorporate new sensors, technology and improvements*
  - *Conduct operationally assessments (Test beds)*

- First Spiral
  - *Sensors at three ports*
  - *Sector Command Center*
  - *Web-Based Information Client*
- Second Spiral
  - *Additional Long Range Radars*
  - *Scene awareness*
  - *Common operating picture integration*
- Follow-On Spirals
  - *Wideband local communications*
  - *OTH coastal area surveillance sensors*
  - *Underwater object awareness*
  - *Swimmer and vessel defense*



Technology Community of Interest - Government



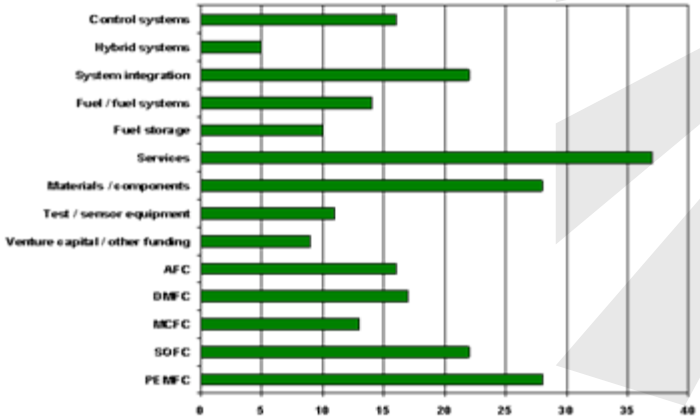
Technology Community of Interest – Academia & Industry



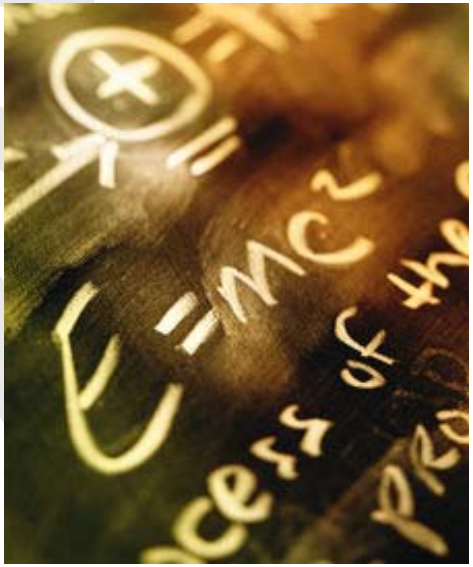
?



USCG R&D



?







Jack McCready

Manager, Deployable Ops & INTEL Pgms
USCG - R&D Center
1082 Shennecossett Rd.
Groton, CT 06340-6096
voice: (860-441-2738)
fax: (860-441-2792)
email: Jack.W.McCready@uscg.mil

LIMITATIONS OF THE NATIONAL DEFENSE UNION:
Why the DOD-DI relationship is best left at home

Opening

The historical relationship between the United States Department of Defense (DOD) and the American Defense Industry (DI) has been an extremely positive one. Images of the great material production of WWII spring immediately to mind. More recently, the great technological innovations made possible by the relationship between the DOD and DI have led to super offensive weapons, and life-saving defensive armament that have no global equivalent. Historically this has been a relationship limited to the physical boundaries of the United States; the direct projection of that material into combat has always been the strict province of the United States Government. Then came 9-11, the Global War on Terror, and a greater demand for personnel than our government agencies could provide.

Unfortunately, our national experiment to project the DI directly into combat zones has proven not nearly as effective as the historical relationship. Forced out of a sense of national security that demanded emergent action, the United States has attempted to extend the DOD-DI relationship into areas where it does not work effectively. In fact, the extension of the DI directly into contested areas of battle space has been at times counter-productive. The images of the DOD-DI today do not conjure up images of B-17s on assemblage lines, but rather, those of American civilians killed or captured while going to work.

The conclusion of this paper—that American citizen contractors should not be permitted in US designated combat areas—is not new; however, the lines of reasoning are unique. Other arguments decry the nation's use of private contractors in order to support a wider anti-war agenda, to loft criticism on the current administration, or as a rejection of our national strategic aims. This discussion is different; it is a proposal to end the use of contractors because their combat zone presence is eminently harmful to the projection of U.S. power. In other words, our ability to reach national strategic ends is hampered by the deployment of American citizen-contractors. To support that claim, this paper investigates the three areas which are most severely affected by the forward presence of the DOD-DI relationship: strategic objectives, ethical means, and Constitutional considerations.

Part I: OBJECTIVE DIFFERENCES

The strategic objectives of the Department of Defense and those of the Defense Industry are radically different. The DOD is charged with fighting and winning the nation's wars to ensure the security of the country and its citizens. The various companies that make up the Defense Industry are charged with increasing the wealth of their shareholders. This is not a slight or a criticism of the Defense Industry; it is simply reality, and normally a very positive attribute of the American free market system. Arguably, it was the American free-market system and its ability to *produce* that was chiefly responsible for U.S. victories in the two global conflicts of the 20th century. Clearly the differences in strategic objectives did not harm the nation's ability to pursue national objectives in

the past, so why the problem now? In the past, American companies and employees did not venture into active combat zones. It is precisely there, beyond the acceptable limitations of DOD and DI union, that the differences in objective create friction.

Even with strategic differences, the connection between DOD and DI in a peacetime environment is symbiotic; the growth and success of one supports the same in the other. When the relationship is extended spatially into an environment of sustained active combat—war by any label—it is more correctly termed syncretism. That is, the attempted union or fusion of two radically different philosophies. Beyond the Forward Edge of the Battle Area (FEBA) or within the designated Area of Operations (AO) the DOD is focused on pursuing lines of operations to ensure strategic victory. The DOD is not primarily concerned with the monetary cost; profit, market share, and quarterly earning do not figure into the decision making of military commanders. For those companies of the DI that deploy shoulder to shoulder with the military, such things do matter. In terms of national blood and treasure, if a DOD operation suddenly turns out to be more costly than expected, a change in operational objectives might be in order to reach the strategic ends. Perhaps more resources are required to overcome a tougher than expected adversary. The point is, the strategic ends remain the same—fight and win the nation's wars. When an American company finds the expenses greater than expected, the result is quite different: they leave. They can leave because *their success* is not tied to American foreign policy pursuits, and because it is not their duty or responsibility to ensure national security. Again, this characterization is not intended to color the DI as unpatriotic or greedy, but simply to explain the natural tension created when the free market enters a combat zone.

The different strategic objective between DOD and the DI leads directly to problems in sustaining a unity of effort. The reasons are quite apparent. The DOD can undertake a civic project, a military objective, or a governmental activity and see it through to completion regardless of the costs. So long as the national leadership is willing to pursue policy aims and national interests, the DOD can continue to dedicate resources to the effort. The DI simply can't work along similar lines. Regardless of the national interests at stake, at some point the danger to company employees becomes too great. At some point the lack of future profits becomes too debilitating. At some point the company shareholders become too disgusted at the loss in share price. In short, when the country pursues national interests through military force, the DOD can withstand changes in environment, military setbacks, and increasing monetary costs. Companies within the DI can't. When the DOD relies on such companies to fulfill supporting roles inside the contested battle space, and those companies can not sustain the effort and choose to exit the arena, the efforts of the DOD and the entire United States Government are undermined.

Foreign populations aren't concerned with the differences in strategic objective. Point of fact: when the United States Government promises to provide security, clean the water, turn on the power, or repair the communications grid, foreign audiences don't differentiate between American government officials and American citizens working for DI companies. In the eyes of affected citizenry, both are efforts under the auspice of the

USG. When a project fails or a promise goes undelivered, the blame falls on the country not the company. Unity of effort is substantially more important than the potential efficiency of the free market in counterinsurgency and nation-building environments.

Part II: ETHICAL MEANS

The United State's use of private contractors in the battle space of the current conflict undermines America's strategic requirement to gain ethical dominance. To effectively engage the enemies confronting the United States in the Global War on Terror (GWOT), in the environments where they exist, requires a national and international debate on the ethical, military means allowable. The United States finds itself fighting an enemy that is not only comprised of trans-national networks, but that also surrounds and embeds itself into local communities. These are organizations that wear no uniforms or distinctive markings, avoid direct confrontation with military forces, and openly advertise collateral damage as a propaganda tool against their adversaries. In short, these are enemy organizations that are using the very concepts of western, Just War discourse as strategic advantage. By wrapping a community of supporters around their organizations, they effectively create safe areas that can not be engaged. Or at least they couldn't be engaged in the past.

Current events make it increasingly apparent that the United States and her allies will, at some point, be forced to take the fight directly to the communities that support our adversaries. Recent campaigns and conflicts have demonstrated the strength of such community-based organizations. The failed Israeli attack on Hezbollah positions in the summer of 2006, the repeated failure of the Pakistani government to control North Waziristan, and the growing threat of the Sadr militia in Baghdad are all examples of what doesn't work to thwart this new type of threat organization. Something else is in order; a new means for attacking the threat where it lives, and the ethical clarity that it is they--the terrorists--who are responsible for collateral damage and death, not us. Such clarity is not possible when we, too, have non-uniformed civilians pursuing political objectives in the battle space.

To ensure national security, the United States will be forced to attack terrorist organizations in their community defenses. The only way this can be done successfully is to make the ethical case that such action is defensive, that the terrorists who seek refuge in those areas are illegal combatants, and that the unavoidable death to innocents is the responsibility of the terrorists, not the United States. American leaders can only make this case by invoking the Hague and Geneva Conventions and the Geneva protocols, and by citing the illegality in the actions of the terrorists themselves. Specifically, illegal acts concerning the lack of uniforms and markings, the intentional endangerment of non-combatants and innocents, and the militarization of sites that are protected from military retaliation. Before the nation can do this; however, requires that we first clean our own house. We can no longer allow American companies and their American citizen employees to move about the battlefield, armed or unarmed, in the pursuit of political objectives. We can no longer rely on private security companies to

protect logistical trains or supply depots. We can no longer accept that the DOD must be supplemented with private industry within contested battle space. This goes beyond the relevant issues of how to protect and punish individual DI employees. The argument here is that the use of American private citizens in this manner necessarily restricts the means available to the DOD. The United States can not make an effective ethical case for engaging illegal combatants when our own nation employs civilian contractors to support the physical acts of war.

The ethical realm makes for a very stark national decision. If the nation continues current practice, and continues to employ DI private companies and American citizens, then we as a nation either restrict the available options to the DOD or we face the certain charges of hypocrisy and tyranny by the international community. However, by ending the practice; by limiting the cooperation of DOD and DI to sovereign areas of stability, the nation is freed from our self-imposed restraints so that we might effectively take the fight to the enemy--where he lives. It is possible to both remain true to our ethical standards for prosecuting war and to also decisively engage terrorist communities, but the nation must first remove our own citizens from the battlefield.

Part III: CONSTITUTIONAL CONCERNS

The use of DI companies and contractors in the current battle space is not the result of an evil conspiracy between national leaders and private industry. It is the result of pragmatic decisions made with an eye on short-term efficiencies. The DOD simply did not have the personnel, numbers or expertise, to immediately launch into a conflict spread across the globe, and one which required multiple campaigns featuring nation-building efforts. While the current situation is understandable—a nation does go to war with the team it has—the Constitutional concerns that the DOD-DI relationship raises must be reflected on. The very way in which we have supplemented the DOD to pursue political objectives is Constitutionally questionable.

The founding fathers considered war to be a serious issue, but one that would have to be pursued from time to time. As such, the framers built checks on the power of the branches to pursue war. The Constitution is very clear on the subject; it provides exceptional executive powers to the President during times of war, and it provides legislative checks on the executive's power to pursue policy aims through war. Specifically, the legislature is given the responsibility to raise, fund and maintain the separate military services. Inherent in this responsibility, is the power to limit or grow the size of the services through funding.

The use of private companies and citizens to supplement the DOD is a Constitutional issue because it erodes the power of the legislature to "raise and support" the services. While the Congress still approves the budget, the services can use discretionary funds, and purchase capabilities through DI contracts. Supplemental bills provide additional funds for contracting at the discretion of the DOD. This all adds up to a DOD that remains strategically unequipped to prosecute the conflict at hand, while the missing ingredients are continuously provided by the DI directly into the battle space. In so

doing, the services themselves assume the responsibility to "raise and support". The DOD is an agency of the executive, and, therefore, does not have the Constitutional authority to raise and support itself. The executive branch, through the use of DI contracts, has obtained power not granted to it. Furthermore, the continued erosion of the legislative 'check' on the executive's power to pursue war is unhealthy for the nation. The DOD projection of DI companies and employees into combat zones is uncomfortably close to becoming, in a word, unconstitutional.

To be clear, this is not a rebuke of the President or a free-pass for the Congress. It is the legislature's responsibility to uphold their Constitutional duties, not the other branches of government. Constitutionally, the legislature does not have the option of allowing the services to grow themselves or to supplement their own capabilities through the DI. They, the United States Congress, are fully responsible for such decisions, and it is they who must fulfill that role.

THE REASONS WHY

In light of the current political climate, it is critical to point out what this argument is not. It is not a rebuke or a critique of those American citizens who are working as private industry contractors. Too often these people are portrayed as nothing short of mercenaries; not true. Many are decorated military veterans, and almost all personally support the national objectives that they help pursue. Nor is this an argument against the Defense Industry or the companies that comprise it. The United States simply couldn't pursue its many national interests without the American defense industry and the free market that it operates in. When the DI is limited physically to operating exclusively outside of U.S. combat areas, the relationship between the DI and the DOD is an incredibly useful instrument of national power. Finally, this is not a criticism of the U.S. government for allowing the DOD-DI relationship to blow past its functional limitations into the physically contested areas of the GWOT. National leaders did what they thought had to be done in order to execute the national strategy. The limited resources and capabilities to execute the GWOT required emergency action. What is important now is to recognize the limitations of the DOD-DI relationship, and to take the necessary corrective actions.

CLOSING RECOMMENDATIONS

Clearly, it is time to move the DI back into a more positive relationship with the DOD. To do this, the DI must be restricted to the physical space outside of all U.S. declared combat areas. This includes not only companies and citizens working with the DOD, but those contractors working with any agency of the United States Government (USG). In short, all Americans working in combat areas should work for, and be employed by, the USG. This would ensure a unity of effort, at least within agencies, that we do not currently posses. Similarly, by restricting the DI from combat zones, the nation is more able to employ the necessary military means to engage an enemy that employs human camouflage. To destroy terrorist organizations, the United States is going to require the moral courage and standing to declare such terrorists 'illegal combatants', and to raid the

communities that they hide within. Finally, it has been over five years since the USG required emergency action to engage the immediate threat. The Constitutional concerns raised by employing private companies and contractors should be put to rest. The sustainability of our national strategy demands this.

The need for corrective action is not completely unnoticed or unrecognized. One of the most underreported elements within the President's State of the Union Address in January 2007, is also the most germane to this argument. The President briefly mentioned a State Department initiative called the Civilian Reserve Corps (CRC). This initiative would provide on-demand experts that could supplement national efforts as *working representatives of the USG*. While the initiative is limited in scope, similar initiatives spread across the wealth of governmental agencies could provide the enhanced capabilities that we currently seek out through the DI. This is a project worthy of national attention and resources. In fact, it is precisely through the DI that the nation can expect to find the valuable personnel, as well as the responsible companies, that would provide the bodies for the CRC.

What is most required at this time is a national recognition of the problem. The DI-DOD relationship has historical significance, and is one of the primary reasons the United States emerged from the 20th century as the world's sole superpower. The American free market, and the defense industry it created, is a positive for American power and national security. However, the leap of this relationship into the physical battle space of the GWOT has come with a cost. Instead of the efficiency that we normally think inherent of free market systems, the spatial transition of the DI into active war zones has led to strategic inefficiency. By limiting the physical presence of the DI, and by increasing the capabilities of USG agencies including the DOD, the U.S. can better pursue the necessary national objectives that we have laid out before us.

Joe McGraw
MAJ, NPS
Defense Analysis Department



NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

Cyber-Herding:

Exploiting Islamic Extremists Use of the Internet

by

David B. Moon, Capt, USAF
Joint Information Operations Student
Department of Defense Analysis

The views expressed in this paper are those of the author and do not necessarily reflect the official policy, position, or endorsement of the Naval Postgraduate School, the United States Special Operations Command, the Department of the Air Force, the Department of the Navy, the Department of Defense, or the United States Government.

Additionally, the author of this paper has no knowledge of any public or private agencies, organizations, groups, or individuals engaged in cyber-herding as described in this paper or any similar activities. It is entirely possible that some entity is engaged in cyber-herding or similar activities, but this author could not find any evidence in the public record to indicate anyone is practicing cyber-herding.

Introduction:

On November 28, 2006, the Al-Fajr Information Center released the first issue of the *Technical Mujahid Magazine.*[1] The purpose of the online magazine is to help prevent aggressive acts against Muslims in cyberspace and to assist the mujahid in their efforts.[2] A mujahid is a Muslim fighting in a war or involved in any other struggle.[3] The magazine proclaims that the Internet provides a golden opportunity for the mujahid to break the Western media control over information. The magazine also recognizes that the internet could represent a vulnerability to the mujahid and suggests security measures for the mujahid to follow. The magazine is correct when they say this is a golden opportunity for the mujahid. The internet provides Islamic extremists an excellent medium to spread their ideas to billions of people, and over the years, the extremists have steadily made a greater presence on the information superhighway. As an example, Gabriel Weimann states that from 1998 to the present, “the number of terrorists’ websites has grown from less than 30 to more

[1] http://memri.org/bin/latestnews.cgi?ID=SD137506

[2] Ibid

[3] http://en.wikipedia.org/wiki/Mujahideen

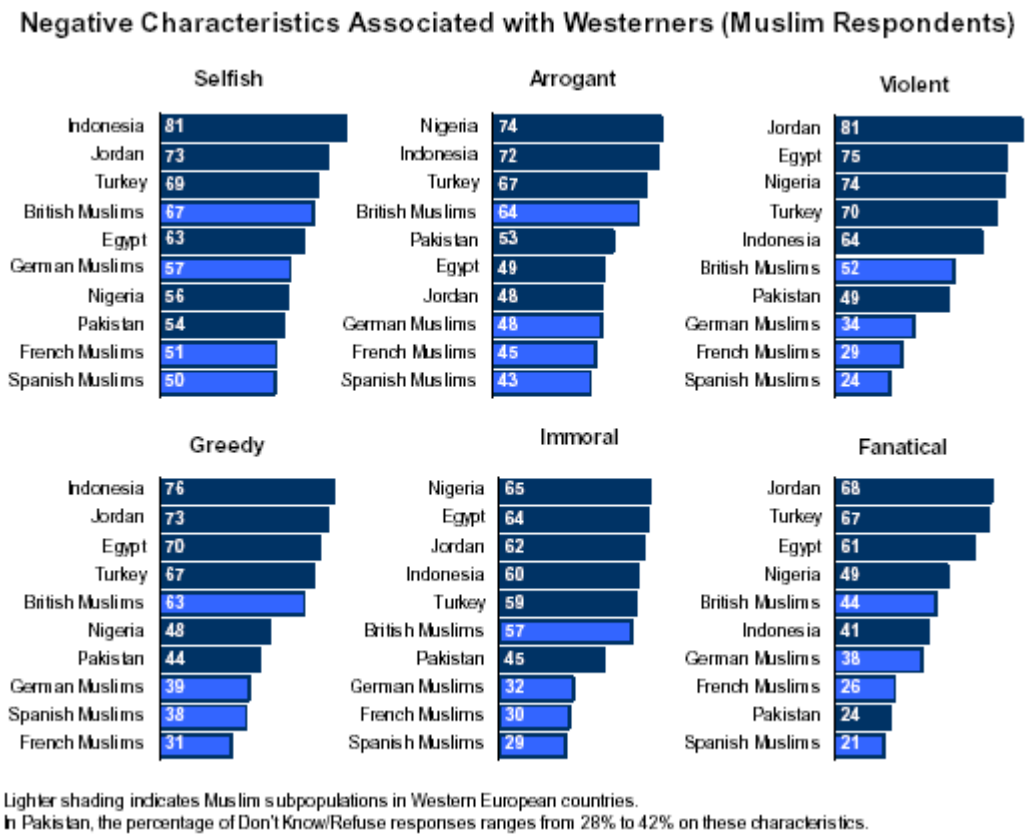
than 4,300."[4] Islamic extremists have used these websites for recruitment, fundraising, coordination, training, propaganda, and a whole host of different activities.

While all of these activities service Islamic extremists' multiple interest, the spreading of their propaganda is perhaps the most dangerous. Over the years, these extremists have learned to shape their messages to appeal to Muslim audiences. Muslims receive messages from the extremists pointing out the unfair policies of the West against Muslim countries, how the West blindly supports Israel against the "poor" Palestinian people, and the West's' attempts to control the Muslim world. The recent wars in Afghanistan and Iraq have only added fuel to this message. The extremists have used these conflicts to reshape their messages by showing the West attacking and occupying two Muslim countries. There is fertile ground in the Muslim world for messages of this nature, as evidenced by the following selections from the Pew Global Attitudes Project's report on The Great Divide: How Westerners and Muslims View Each Other.[5]

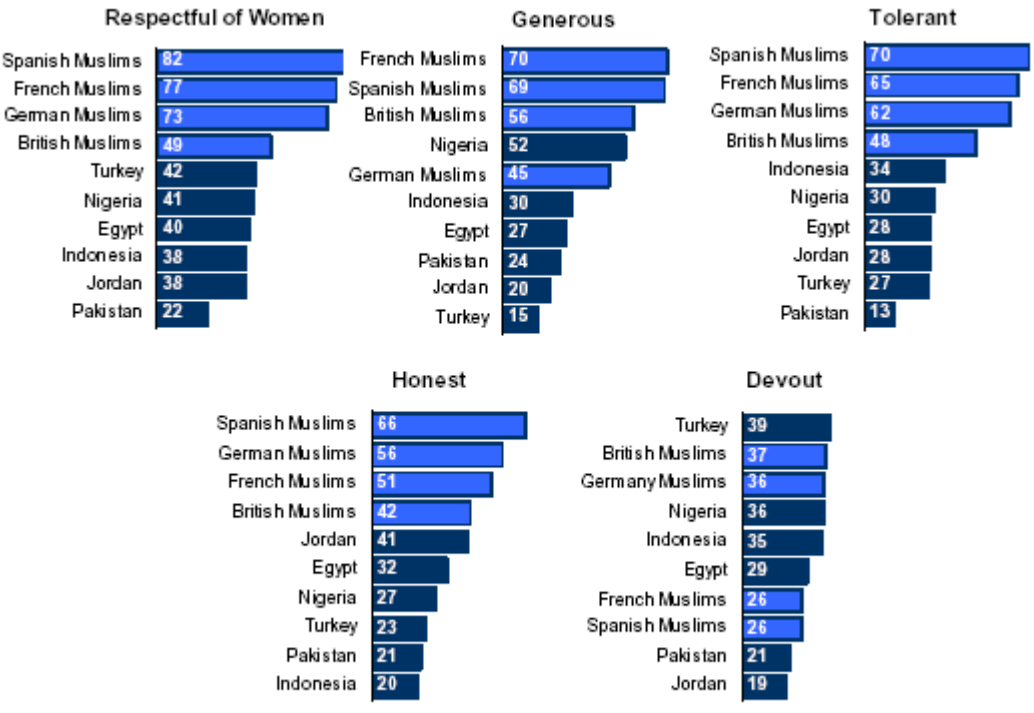
---

[4] Weimann, G. (2006). *Terror on the Internet: The New Arena, the New Challenges*. Pg 15, Dulles, VA: Potomac Books.

[5] http://pewglobal.org/reports/display.php?PageID=831



Lighter shading indicates Muslim subpopulations in Western European countries.
In Pakistan, the percentage of Don't Know/Refuse responses ranges from 28% to 42% on these characteristics.



Lighter shading indicates Muslim subpopulations in Western European countries.
In Pakistan, the percentage of Don't Know/Refuse responses ranges from 26% to 36% on these characteristics.

Figure 1

The results from the Muslims interviewed reveal a very negative image of the West. Islamic extremists shape their messages to reinforce this negative view. What can be done to counter these messages? The first step is to understand the medium that the extremists are using.

The internet has many characteristics that support extremists' information operations, such as being able to reach large audiences. Yet the internet also has inherent weaknesses that can be exploited. One of these weaknesses is the ambiguous nature of the net. You trust that when you go to a website that it is legitimate. If it looks professional, you tend to believe that the site is real. However, criminals or terrorists could just as easily be running that website. The same is true when you chat with someone online. They could be who they say they are, but they could just as easily be someone else pretending to be the person you want them to be. A group called "Perverted Justice," as featured on Dateline NBC, has made great success in catching child predators by using the internet's ambiguous nature.[6] Terrorist organizations also have an inherent weakness that can be exploited using the internet. This weakness is the decentralized nature of terrorist

[6] http://www.perverted-justice.com/

organizations. Many terrorist organizations that do not have state sponsorship organize and accomplish work utilizing social networks versus a hierarchy command structure. This only makes sense. Individuals engaged in criminal activities need to work with people they trust so they can accomplish their mission. In the physical world, social networks are very reliable. However, in the virtual world social networks can be exploited because personalities in the virtual world can be real or fictitious. In order to exploit these weaknesses, a cyber system that invisibly drives Islamic extremists from terrorist websites to covertly controlled websites can be developed. I will generically refer to this system as cyber-herding.[7]

Defining Cyber-herding:

Cyber-herding is the action by which an individual, group, or organization drives individuals, groups, or organizations to a desired location within the electronic realm. Why implement cyber-herding versus engaging in an all out war on extremist websites? The answer to that

[7] Author's note: While discussing this idea with Prof John Arquilla from the Naval Postgraduate School, he applied the term cyber-herding to this concept. The term stuck and this author has been applying it to this concept ever since. Cyber-herding can also be found on the internet in reference to cattle herding, which has nothing to do with the ideas in this paper.

question lies in the realm of intelligence gathering and in the freedom of the internet. While the threat from Islamic extremists' use of the internet is high, intelligence agencies have successfully harvested information from these sites. Thus, an all-out denial-of service attack on extremists' websites would limit intelligence agencies capability to gather information. Indeed, some extremists' websites have been actively targeted and shut down. However, the problem that emerges from this tactic is the freedom of the internet allows extremists to restore or relocate their websites in a matter of hours to days. Thus, these attacks could embolden the extremists by reinforcing the fact that they can set up a new site within a short period. Simply stated, the attacks and subsequent re-emergence could provide them with a simple affirmation: *The powerful United States tries to keep us off the internet but they cannot!* On the other hand, cyber-herding has the potential to covertly neutralize undesirable websites, mine data from controlled websites, map virtual social networks, manipulate extremist messages, and modify the extremists' story. To implement a cyber-herding program effectively, a minimum of four nodes are required.

Objectives of the Cyber-herding Nodes:

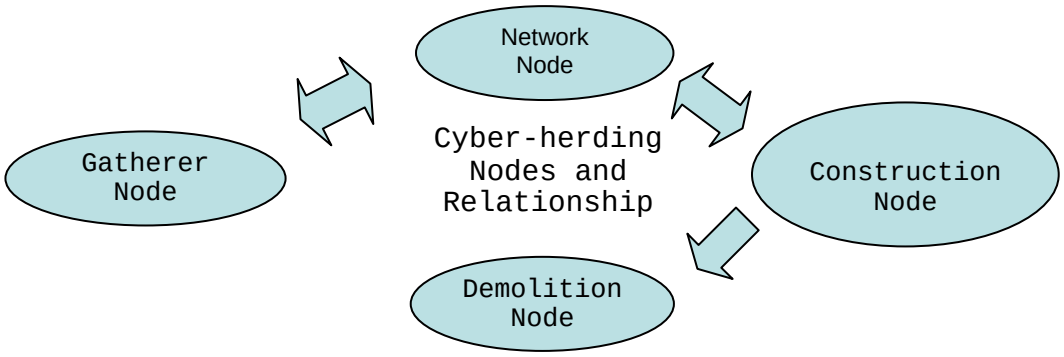


Figure 2

The Gatherer Node:

The gatherer node's objective is to compile and maintain an up to date list for all extremists related uses of the internet.

The Network Node:

The members of the network node have two objectives. The first objective is to insert themselves into the extremists' virtual social network. The second objective is to identify major "hubs" and "links" within the extremists' virtual social network.

The Construction Node:

The members of the construction node have two objectives. The first objective is to create realistic doppelganger extremists websites and chat rooms. A doppelganger refers

to a ghostly double or a look alike. In some traditions, it is an omen of death to see your own doppelganger. The second objective is to create several content rich Darknet environments that offer e-mail, file sharing, chat, instant messenger, and streaming video services. A Darknet is a private virtual network where users connect only to people they trust.[8]

The Demolition Node:

The demolition node's objective is to remotely destroy or disable all extremists' websites, chat rooms, Darknets, etc.

The Cyber-herding Process:

Phase One:

The gatherer node begins the cyber-herding process by tracking down extremists' websites and chat rooms. To facilitate this process, the node seeks public help by placing web-based advertisements asking people to submit Uniform Resource Locators (URL) for any suspected extremist website.[9] The node seeks out help from private groups such as the Rand Corporation, the Search for International Terrorist (SITE) Institute, and the Middle East Media Research Institute (MEMRI) and academic terrorism research

[8] http://en.wikipedia.org/wiki/Darknet
[9] http://en.wikipedia.org/wiki/URL

groups.[10,11,12] The node compiles a list of extremist website URLs. This list becomes a living document that the node constantly updates with identified extremists' sites. In addition, a program constantly checks identified URLs to verify the sites are still active and automatically deletes dead sites. During this process, the network node makes a copy of the list, and begin phase two.

Phase Two:

Upon accessing a site on the list, the members of the network node pose as Islamic extremist sympathizers and/or supporters and begin interacting with members of the site. In chat rooms, the node members start or join conversations supporting extremists themes. The objective is to develop trust relationships with Islamic extremists. Node members contact extremists' websites to see what they can do to support the cause. If needed, the network node would have the authority to make small donations to extremists websites to help build trust. During this phase, the network node maps the extremists' chat rooms. Mapping a chat room involves creating a social network diagram of who is talking to whom within the chat room. The members of the network node are looking for "hubs"

[10] http://www.rand.org/about/
[11] http://www.siteinstitute.org/index.html
[12] http://www.memri.org/

using the sites. These hubs are people who have more connections then anyone else. Malcolm Gladwell in his book, "*The Tipping Point,*" refers to these people as "connectors."[13]

The members of the network node develop virtual fictitious identities. They keep detailed records of their conversations for each identity. This way any member of the network node can be that virtual person. All they have to do is pick a character, and read up on his or her history before chatting.

If the network node discovers any websites not identified on the list, they will update the master list with the new URLs and forward these sites to the gatherer node. The members of network node mark the list to identify sites they are currently working, this ensures the demolition node does not destroy a site the network node is currently operating in. Subsequently, the network node forwards the list to the construction node.

Phase Three:

After the members of construction node receive the list from the network node, they start accessing the sites.

[13] Gladwell, M. (2002). *The Tipping Point: How Little Things Can Make a Big Difference*. Boston, MA: Little, Brown.

They copy the websites content, format, graphics, files, and links. Using this information, the construction node builds doppelganger extremists' websites. All website created should be independent sites, with only passing similarities with other existing websites. At no time will the construction node hijack an existing extremist website as this could cause distrust in the target audience.[14] The construction node forwarded all created sites to the network node. The members of the network node endorse these new websites with their contacts. The members of construction node remove all websites the network node marked and any sites they created from the list. Afterwards, the construction node forwards the list to the demolition node.

Phase Four:

After receiving the list from the construction node, the demolition node systematically begins a process of attacking every site on the list. These attacks can be simple such as contacting the sites service provider to protest the site to try to get the site removed. They can also use more sophisticated attacks such as denial of service attacks, hijacking a website, Structured Query Language (SQL) injections, Cross Site Scripting cookie

[14] http://en.wikipedia.org/wiki/Page_hijacking

stealing, JavaScript injections, and other hacking methods.[15,16] Depending on where the host server is located, it may not be politically feasible to attack some sites directly. In these cases, the demolition node could post the extremists' URLs on internet chat rooms and blogs in the hope that private citizens and/or groups can bring down the sites.

Using the sparse numbers on extremists' websites in Gabriel Weimann's book, *Terror on the Internet,* I have created a mathematic model; see attachment 1, to determine the growth rate of extremists' websites.[17] Utilizing math modeling, I estimated the rate of growth for extremists' websites on the internet is, at least, 2.33 websites a day. At this rate of growth, I have estimated that the total number of extremists' websites ending in 2006 is approximately 6,850 websites. Using this knowledge, the construction node needs to take down at least 2.33 websites a day just to maintain the status quo. But, maintaining the status quo is not the objective.

Going back to math modeling, I estimated parity is achievable in 711 days if the demolition node can take down

---

[15] http://www.loriswebs.com/hijacking_web_pages.html

[16] http://72.14.203.104/search?q=cache:uXBMKQ2TURkJ:milw0rm.com/papers/111+attacking+websites +methods&hl=en&gl=us&ct=clnk&cd=9

[17] Weimann, G. (2006). *Terror on the Internet: The New Arena, the New Challenges*. Pg 15, Dulles, VA: Potomac Books.

an average of nine websites a day and the construction node can build websites at an average of 2.33 websites a day. This is illustrated in figure 3 below. Once parity is achieved, phase five begins.

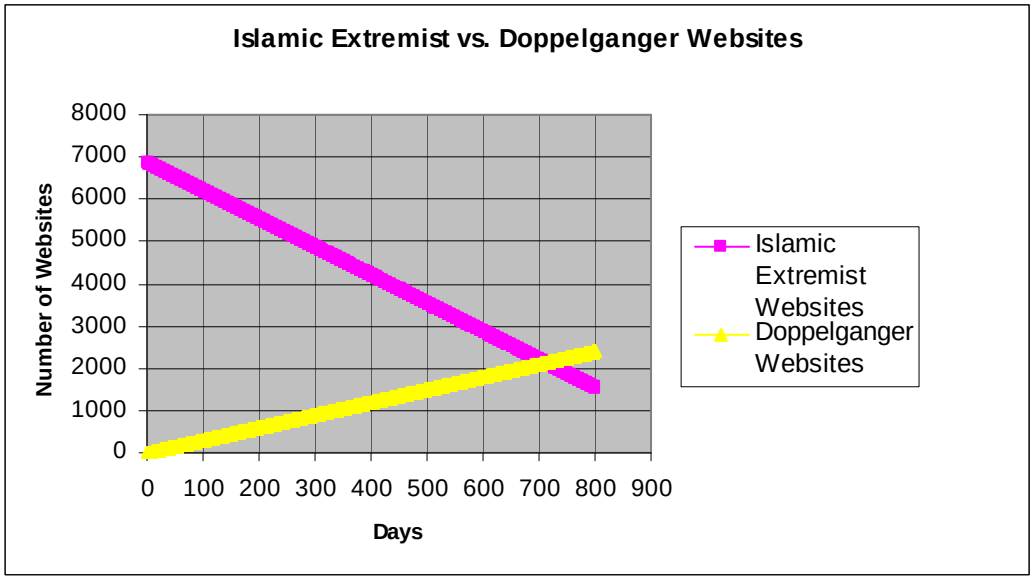


Figure 3

Phase Five:

The purpose of phase five is to change the message. Think of the Islamic extremists' as salesmen. They are selling their ideology to the world. As good salesmen, they highlight the positive qualities of their movement, and suppress negative qualities of their movement. The two main items Islamic extremists suppress is the violence they commit, and their desire to impose their harsh version of an Islamic state upon people, states, and nations. Virtually all internet Islamic extremists expound about the

need for an Islamic state. For them, an Islamic state would solve all of the world's problems. However, none of them actually describes what an Islamic state would look like or how it would function. Extremists' violence and desire for an Islamic state are weaknesses that phase five exploits. During phase five, the construction node will make subtle changes to the websites under their control to highlight violent acts committed by extremists. In the view of most Muslims, Islam is the religion of peace. To them, the association of violence and Islam is a contradiction. By focusing on the violent acts committed by Islamic extremists in the name of Allah, support for the extremists should wane within the Muslim community. The construction node will also start to describe what an Islamic state will look like and how it will function. However, each site will have a different version of what an Islamic state will look like. Some sites will focus on installing an Islamic Caliphate, while others will focus on national Islamic states.[18] The Caliphate is an Islamic federal government that represents both political leadership and unities of the Muslim world applying Islamic

[18] http://en.wikipedia.org/wiki/Caliphate#Reestablishment_of_a_modern_Caliphate

law know as Shariah law.[19] As there is no set Shariah law recognized by all Muslims, each site would have its own version of Shariah law that will be enforced under the Islamic state.[20] The sites will also highlight the role of women in an Islamic state, rights of non-Muslims, and punishments for violating Shariah law. The purpose of all of this is to let potential supporters of the sites know what they are getting into. An Islamic state may sound like a good idea to many Muslims. However, once these Muslims come to understand the details of an Islamic state, they may start questioning if it really is a good idea after all. In addition, by attaching different versions of an Islamic state to different extremist groups should foster hostilities between these groups. This should help keep the different factions from uniting to achieve their goals.

Phase Six:

Going back to math modeling, by day 1,032 virtually all of the extremists' websites could potentially be eliminated. At this time, the construction node would stop making new websites. The demolition node will continue to attack any identified Islamic extremists' sites.

---

[19] Ibid
[20] http://en.wikipedia.org/wiki/Shariah

Additionally, the demolition node will start to shut down construction node sites at the same rate they were attacking the extremists websites. At this pace, all websites will be eliminated by day 1375. I recommend that on day 1369, the demolition node stop shutting down sites created by the construction node. This will leave approximately 50 sites in operation for monitoring, and message control. This is illustrated in figure 4 below. The demolition node will continue to attack any extremists' website that makes it on the list.

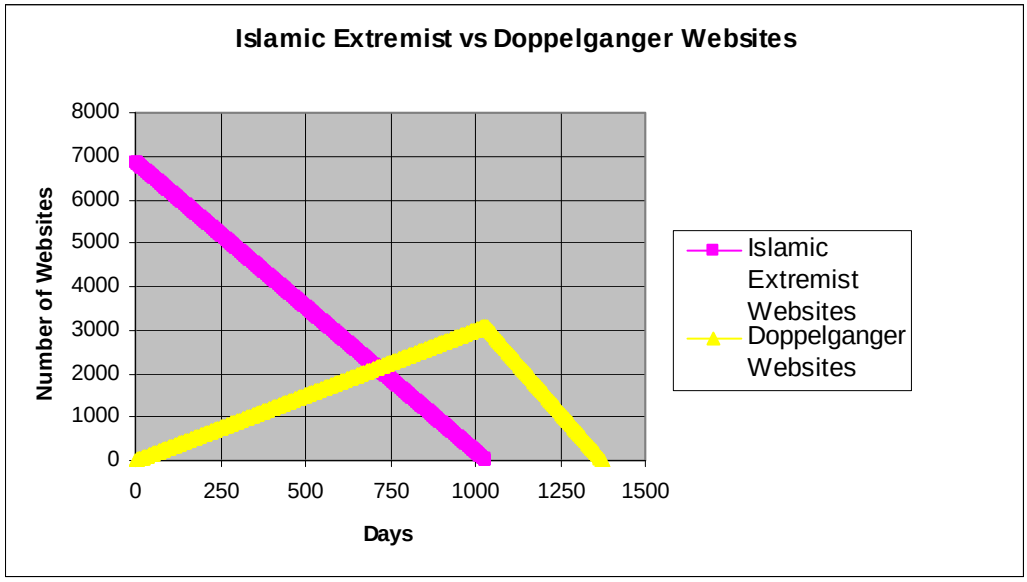


Figure 4

Phase Seven:

During this phase, the construction node will develop content rich Darknet environments. As stated earlier, a Darknet is a virtual private network where users connect

only to people they trust.[21] These Darknet environments will offers e-mail, file sharing, chat, instant messenger, and streaming video services. Once a Darknet is created, the construction node will send the URL to the network node.

The members of network node will pick a connector with which they have developed a strong trust relationship, and invite that connector to become a member of the Darknet. This invitation will come in the form of three emails: one containing the URL of the site, one containing a temporary username, and one containing a temporary password. When the connecter clicks on the URL, a website will open. The only thing on this website is two fields for a username and a password and a submit button. When the connector fills in the fields and clicks the submit button, a prompt will appear requesting the user to establish a new username and password. Once the connector establishes a new username and password, a welcome message will appear. The welcome message informs the user that he is entering a secure website developed to promote the Islamic extremists' causes, and he was chosen to have access to the site because of his faith and dedication. The message will also tell the connector that he can invite

[21] http://en.wikipedia.org/wiki/Darknet

up to 10 people to join the website, but he must only invite people he trusts 100 percent. The purpose of this message is to make the subject feel special for being chosen, and to make the subject feel secure.

If the connector likes the website, then he may chose to invite others. On the other hand, if he does not like the website, then the network node will have to start over with a new connector. Anyone invited to join the network will go through the same process as the connector. Using small-world theory, the network node can have extremists build a detailed map of their virtual social network.[22] Psychologist Stanley Milgram illustrates this theory in his 1967 study in which he showed that no less than six people separate people from each other.[23] The Six degrees of Kevin Bacon game also illustrates this theory, in which the game's objective is to connect any Hollywood actor with Kevin Bacon within six associations.[24]

As people join the Darknet, a computer program constructs a social network map showing the connections between the individuals and people that invited them to join the network. The program also updates the map whenever users send e-mails from their Darknet e-mail

[22] http://en.wikipedia.org/wiki/Small_world_phenomenon
[23] Ibid
[24] http://en.wikipedia.org/wiki/Six_Degrees_of_Kevin_Bacon

account, and chat with other Darknet users. Additionally, the Darknet runs IP and e-mail tracking software against all users. This software provides geographical locations for the users IP addresses and e-mail. In addition, the software provides contact information on the person that owns the IP address, and contact information on the person's host service provider. The social network map incorporates all of this information. The map can be used to identify geographical clusters within the network, links between clusters, and vital network hubs that can be targeted for human intelligence surveillance. If multiple users are accessing the Darknet using the same computer, this may show a possible headquarters for extremists groups that can be targeted for human intelligence. Another benefit of the Darknet is the ability to mine data from Darknet e-mail accounts, file sharing, and chat room conversations.[25]

[25] http://en.wikipedia.org/wiki/Data_mining

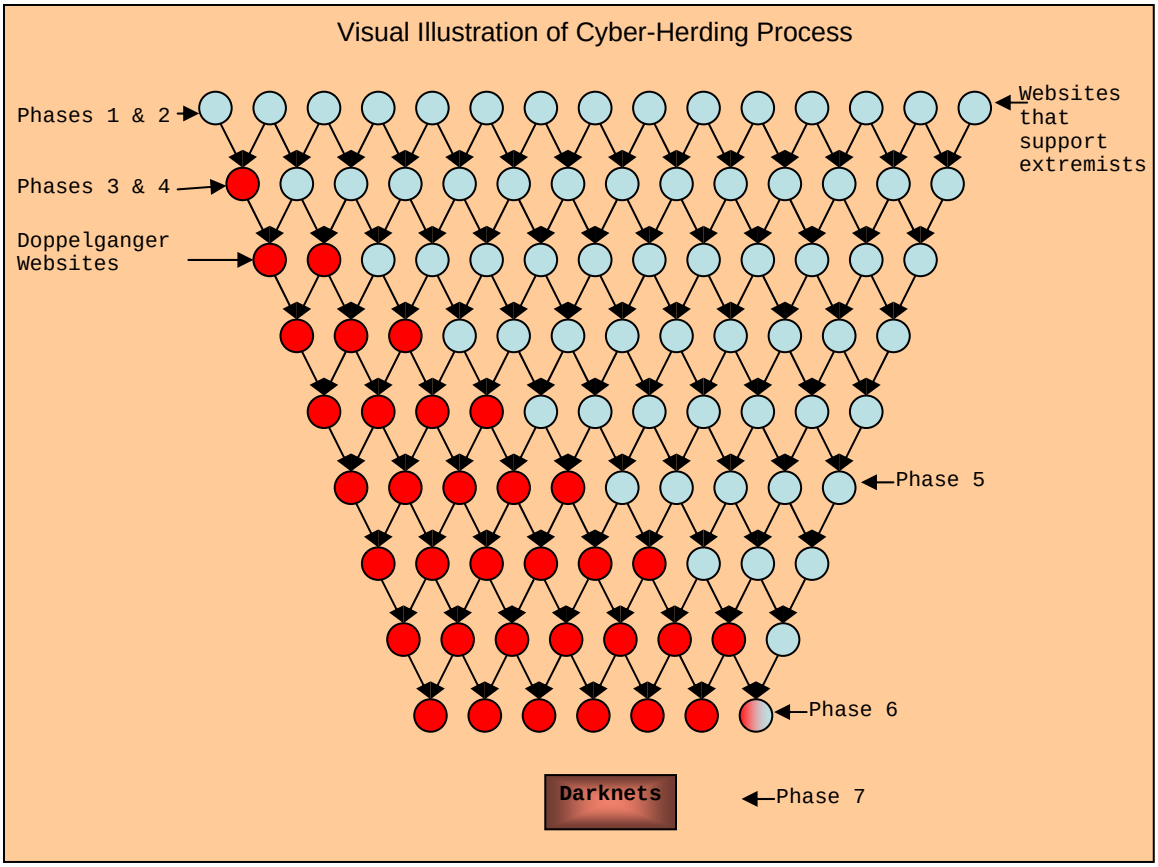


Figure 5

Limits of Cyber-Herding:

The major limitation of cyber-herding is language fluency. Every node involved in this process will need to be multilingual, with a focus on Arabic. Before the process can begin, an investment must be made into recruiting people fluent in Arabic and training people in the Arabic language. The other limitation is time. Cyber-herding is not a quick easy fix. It will take time to develop trust relationships and attack offensive websites. The last limitation is in changing the message. The construction node can make subtle changes to the extremists

message by highlighting weakness in Islamic extremists themes, however cyber-herding cannot be used to try to change people's beliefs about America or the West. Any attempt to go down that path will lead to failure.

Conclusion:

The internet provides Islamic extremists a golden opportunity to bypass normal media outlets, and take their message directly to the people. This allows them to spread their ideas to an ever-growing audience. Utilizing the cyber-herding process, extremists' information operations can be taken over and their messages and ideas can be modified to make them less appealing to their target audiences. Cyber-herding also increases monitoring and data collection of Islamic extremist information operations. Those willing to make cyber-herding a reality can seize the golden opportunity away from the Islamic extremists and make it their own.

References

Gladwell, M. (2002). *The Tipping Point: How Little Things Can Make a Big Difference*. Boston, MA: Little, Brown.

Weimann, G. (2006). *Terror on the Internet: The New Arena, the New Challenges*. Dulles, VA: Potomac Books.

http://en.wikipedia.org/wiki/Caliphate#Reestablishment_of_a_modern_Caliphate

http://en.wikipedia.org/wiki/Darknet

http://en.wikipedia.org/wiki/Data_mining

http://en.wikipedia.org/wiki/Mujahideen

http://en.wikipedia.org/wiki/Page_hijacking

http://en.wikipedia.org/wiki/Shariah

http://en.wikipedia.org/wiki/Six_Degrees_of_Kevin_Bacon

http://en.wikipedia.org/wiki/Small_world_phenomenon

http://en.wikipedia.org/wiki/URL

http://www.memri.org/

http://memri.org/bin/latestnews.cgi?ID=SD137506

http://pewglobal.org/reports/display.php?PageID=831

http://www.rand.org/about/

http://www.siteinstitute.org/index.html

http://www.loriswebs.com/hijacking_web_pages.html

http://www.perverted-justice.com/

http://72.14.203.104/search?q=cache:uXBMKQ2TURkJ:milw0rm.com/papers/111+attacking+websitesmethods&hl=en&gl=us&ct=clnk&cd=9

“Perspectives on Special Operations and Warfare in the Seams”

Tom O’Connell
Assistant Secretary of Defense
NDIA SO/LIC Symposium
28 Feb, 2007

Thank-yous are in order…….

- Thanks to the NDIA SO/LIC Board
- Thanks to Industry/Government Exhibitors for their investment in the Symposium
- Thanks to the superb members of SOF
- Thanks to the Industry innovators
- Special thanks to TSWG/CTTSO (More Later)

US Special Operations Command





US Army Special Operations Command

Special Forces
Rangers
160th SOAR
Psychological Operations
Civil Affairs Operations



Air Force Special Operations Command

Fixed Wing Special Opns Aviation
Rotary Wing Special Opns Aviation
Special Tactics units



Naval Special Warfare Command

SEALs
SEAL Delivery Vehicle Teams
Special Boat Units



Joint Special Operations Command

Ensures SOF Interoperability; Conducts Joint Studies, Training, and Operations



Marine Special Operations Command

MSOBS
FMTU
MSOSG
MSOS

MARSOC Mission Statement

U.S. Marine Corps Forces, Special Operations Command (MARSOC), as the U.S. Marine Corps component of U.S. Special Operations Command (USSOCOM), trains, organizes, equips; and when directed by CDRUSSOCOM, deploys task organized, scaleable, and responsive U.S. Marine Corps special operations forces worldwide in support of combatant commanders and other agencies.

Issues-SOF

- SOCOM –Great Success in QDR-QDR Falls Short of Required Defense Capacity. Forces ARE Stressed.
- Industry Partnership-Support for the SOF Community has been superb.
- ISR, TT&L, Sensors-Persistent Surveillance is Critical.
- Exploitation-Remote Interrogation, Rapid DOCEX, Lightweight Power
- Recapitalization of Fixed Wing Fleet-Complex Issue
- Foreign SOF Interface and Surrogates-Counter/Network
- New Models of Success-JTF HOA, JIATF-S, W, JTF-P

Issues for SOF

- We cannot be victims of Interagency Turf Struggles. Suggest reading Title 10 of the US Code. Results in Delay of Critical Authorities.
- Personal Conduct of SOF is Explosive Issue (Front Page/Back Page)
- SOF Stations-Key Countries-Should be a standing, funded organization
- Global SOF Posture-European Stability

A Nation at War ?

- **Election Approaching -18 Months of Potential “Silly Season”**





- **Resources constrained??- Heritage 4% Solution (GDP)**

- **Public Opinion – Less Certain**



A Nation at War

- **Fighting two COINS/ Shooting Wars**
- **Trying to transform force**
- **Cold War Authorities and Mindset**







A Nation at War

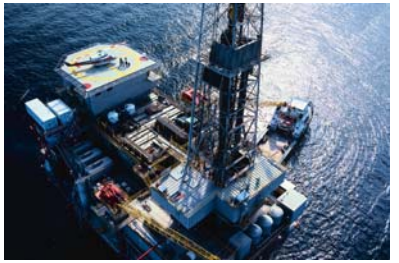
- **Ever Increasingly Hostile Media (Domestic)**



- **Openly Hostile Foreign Media**



- **Energy Uncertainty**



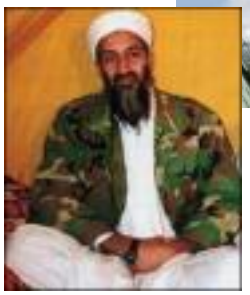
A Nation at War

- **Pandemic uncertainty, Border Demands**
- **Growing Islamic population growing in frustration**
- **WMD within constant reach of the enemy**





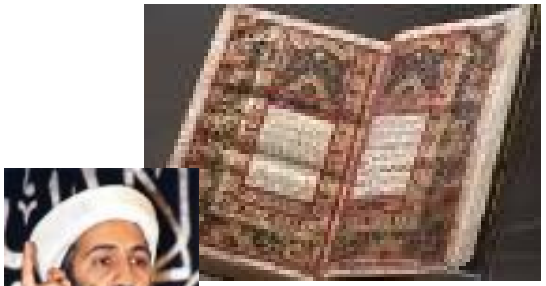




A Nation at War

- **An enemy adept at information technology tools**
- **War in Iraq and Afghanistan will continue to foster view that USA is anti-Islamic**
- **Enemy's perspective of a circa 1500 Caliphate is real**







A Nation at War





- **Al Qa'ida has stated their four major objectives (all are clear and resonate within the Islamic World)**
- **Moderate voices not calling out**
- **New Intel Laws – New Organizations**
  - **SOCOM'S CSO– NCTC**
  - **JIOCs-JIATFs-DNI**

Global War on Terrorism: A War Unlike Any Other

- **In the war on terrorism, our enemies operate globally from:**
  - **States in which we have active military operations.**
  - **States that are not at war with us.**
  - **Ungoverned areas such as failed and failing states.**
- **While the U.S. has the finest military forces in the world, many GWOT tasks can be accomplished better by and with partner nations because they know the local geography, language, and culture.**
- **Building partnership security capacity enables our partners to:**
  - **Disrupt terrorist and criminal activity.**
  - **Meet common threats.**
  - **Fight alongside of us or instead of us.**

Building Partnership Capacity: Cold War Constructs-Outdated and Inflexible

- Existing Cold War tools for building partnership capacity were primarily designed for:
  - Increasing U.S. influence in countries, rather than building their capacity to contribute to the defeat of a common enemy.
  - Building forces to defend against a conventional threat.
  - Measuring quantities of equipment sold and men trained, rather than tangible contributions to U.S. national security.
- This is 2007, not 1947. Interagency needs restructuring
- NSC Staff could benefit from Goldwater-Nichols approach.
- SOCOM has been a model for interagency efficiency.
- What about a Deputy Secretary for Interagency Affairs? Present at EEOB and National Security Advisor with an IT reach-back capability.

Why the QDR Falls Short-

- **We are driven by budget rather than military considerations**
- **Few realize the true impact of inattention in the 1990's**
- **Operational Tempo way up, yet total force is half the size of 1992**
- **Average aircraft age now 24 years…..in 1973, it was 9. Older platforms strain readiness, increase inventory costs**
- **DoD's rush to meet budget targets causes us to cut back and therefore increase production costs in the long run.**
- **Years of uncertainty have shrunken the defense industry...more mergers, more sole source contracts, less research and therefore higher costs.**

Sen. Jim Talent-Heritage

Section 1206 Authority: What It Does and Does Not Do

- **Section 1206 *does*:**
  - **Give DoD a 2-year $200M (per year) train and equip authority.**
  - **Require that DoD jointly formulate programs and coordinate implementation with State.**
  - **Allow DoD to build the capacity of a foreign country's military forces to conduct time-sensitive:**
    - **A. Counter-terrorism or counter-terrorism WMD-proliferation operations; or**
    - **B. Stability operations in which US forces are a participant.**
  - **Require a Presidential review of the Foreign Assistance Act and Arms Export Control Act, due at the end of FY06 (SEP 06).**
  - **Expire on 30 September 2007 -- though could be renewed and even expanded if the Executive Branch demonstrates to Congress that it has been well used.**
- **Section 1206 *does not:***
  - **Create a slush fund for State and DoD operations that are unlikely to build *enduring* security capacity.**
  - **Provide resources for Iraq or Afghanistan, whose training and equipping are provided by separate appropriations.**
  - **Provide appropriated funds – 1206 funds are drawn from DoD O&M accounts.**

Special Operations and Combating Terrorism-New Thrusts



“You Can’t Get to Where You Want to Be by Stayin’ Where You Are”

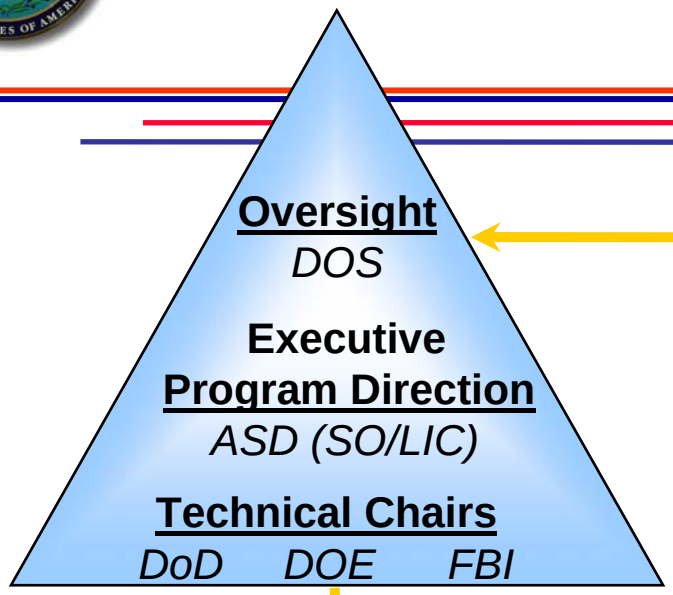

DEPARTMENT OF DEFENSE
UNITED STATES OF AMERICA
DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
FIDELITY
BRAVERY
INTEGRITY
INTERAGENCY
INTERNATIONAL
TSWG
DEPARTMENT OF STATE
UNITED STATES OF AMERICA
DEPARTMENT OF ENERGY
UNITED STATES OF AMERICA
U.S. DEPARTMENT OF HOMELAND SECURITY

TSWG Mission and Objectives

- **Mission: Conduct the U.S. national interagency research and development program for Combating Terrorism.**

- **Objectives:**
  - **Provide interagency forum to coordinate R&D requirements for combating terrorism**
  - **Sponsor R&D for interagency advanced technology development**
  - **Promulgate technology information transfer**
  - **Influence basic and applied research**

TSWG Structure



COORDINATOR FOR COUNTERTERRORISM

PROGRAM MANAGEMENT

National International

DoD-Combating Terrorism Technology Support Office

MULTI-AGENCY MEMBER SUBGROUPS

Blasts Effect and Mitigation — **ATF**	**Explosives Detection** — **TSA**	**Infrastructure Protection** — **FBI / DoD**	**Physical Security** — **DoD / DOE**	**Surveillance, Collection, & Operations Support** — **IC**	**Training Technology Development** — **DoD / DHS**
Chemical, Biological, Radiological, Nuclear Countermeasures — **DoD / FDA**	**Improvised Device Defeat** — **FBI**	**Investigative Support & Forensics** — **USSS**	**Tactical Operations Support** — **DOE**	**V.I.P. Protection** — **USSS**	

TSWG Membership

Department of Defense

- OASD(SO/LIC)
- OATSD(NCB)CP/CBD
- OUSD(A&T) DDR&E and S&TS/LW
- Armed Forces Institute of Pathology
- Defense Advanced Research Projects Agency
- Defense Computer Forensics Laboratory
- Defense Intelligence Agency
- Defense Threat Reduction Agency
- Joint IED Defeat Task Force
- National Security Agency
- Pentagon Force Protection Agency
- Polygraph Institute
- The Joint Staff
- Unified Commands
- US Special Operations Command
- US Air Force
  - Air Combat Command
  - Air Force Research Lab
  - Electronic Systems Center
  - AFOSI
- US Army
  - 52nd ORD
  - SBCCOM / ECBC
  - Corps of Engineers / ERDC / PMDC
  - Criminal Investigations Command
  - Natick RDE Center
  - 22nd Chemical Battalion (Tech Escort)
  - Training and Doctrine Command
  - National Guard Bureau
- US Navy
  - Naval Criminal Investigative Service
  - Naval Facilities Engineering Service Center
  - Naval Special Warfare
  - NEODTD / DTRG
- US Marine Corps
  - Chemical Biological Incident Response Force
  - Network Operations & Security Command

Department of State

- Bureau of Diplomatic Security
- Office of the Coordinator for Counterterrorism
- Overseas Building Operations

Department of Agriculture

- Agricultural Research Service
- Animal and Plant Health Inspection Service
- Food Safety and Inspection Service
- Office of the Inspector General

Department of Energy

- National Nuclear Security Administration
- Office of Energy Assurance
- Office of Security

Department of Health and Human Services/USPHS

- Centers for Disease Control & Prevention
- Food & Drug Administration
- National Institute for Occupational Safety and Health

Department of Homeland Security

- Border and Transportation Security
- Immigration and Customs Enforcement
- Office for Domestic Preparedness
- Emergency Preparedness & Response
- Transportation Security Agency
- Science and Technology
- US Coast Guard
- US Secret Service

Department of Commerce

- National Institute of Standards and Technology
  - Office of Law Enforcement Standards

Department of Justice

- Bureau of Alcohol, Tobacco, Firearms and Explosives
- Drug Enforcement Administration
- Federal Bureau of Investigation
- Federal Bureau of Prisons
- National Institute of Justice
  - Office of Justice Programs
- US Marshals Service

Department of Transportation

- Federal Aviation Administration
- Federal Railroad Administration
- Federal Transit Administration
- National Highway Traffic Safety Administration
- Volpe National Transportation Systems Center

Department of the Treasury

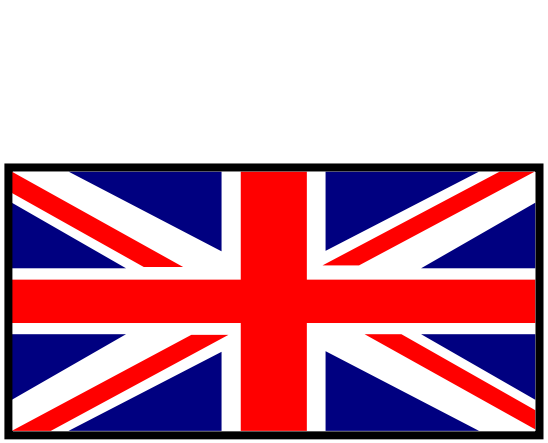
- Federal Reserve Board

Independent Agencies

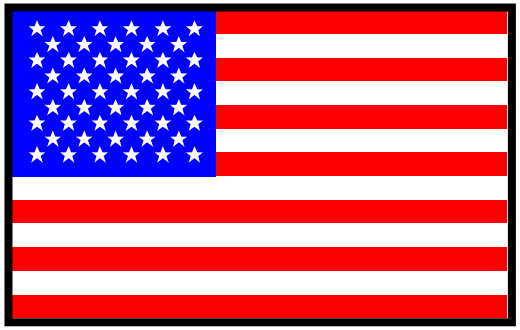
- Environmental Protection Agency
- General Services Administration
- Intelligence Community
- Interagency Board
- National Virtual Translation Center
- Nuclear Regulatory Commission
- State and Local Agencies
- Supreme Court of the United States
- US Capital Police
- US Postal Inspection Service
- US Senate Sergeant at Arms
- US Supreme Court Police

International Partners

Bilateral Combating Terrorism R&D Agreements



United Kingdom





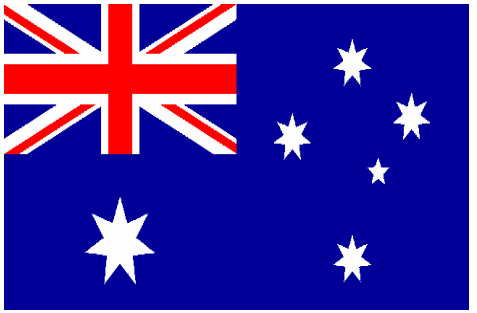
Israel



Singapore



Canada



Australia

Summary

- **Forum to Rapidly Identify, Prioritize, Resolve, and Fund Needs/Requirements**
- **User Driven**
- **Interagency and International**
- **Support Transition to Acquisition and Commercial Production**
- **Fast Track and Flexible Program Forum**


If the Surge Fails • Obama's Plan to Win
U.S.News & WORLD REPORT
FEBRUARY 19, 2007
EXCLUSIVE
Terror's Next Target?
The scary truth about why America remains so vulnerable
$4.50 U.S. / $5.50 CANADA
www.usnews.com

The Breath of the Beast

- “I recognized this arbitrary nature of terror immediately. I have seen its footprints in visits to Babi Yar and the Sbarro restaurant in Jerusalem. I watched it crash into the North Tower and slaughter Daniel Pearl on the internet. All of these events have their own unspeakable individual character but they all share the lunatic devaluation of human life that is born of a totalitarian belief system.” YB Moshe.



Questions/Discussion

MAJOR GENERAL BENOIT PUGA

SPECIAL OPERATIONS COMMANDER, FRANCE



Waging the long War on Terrorism

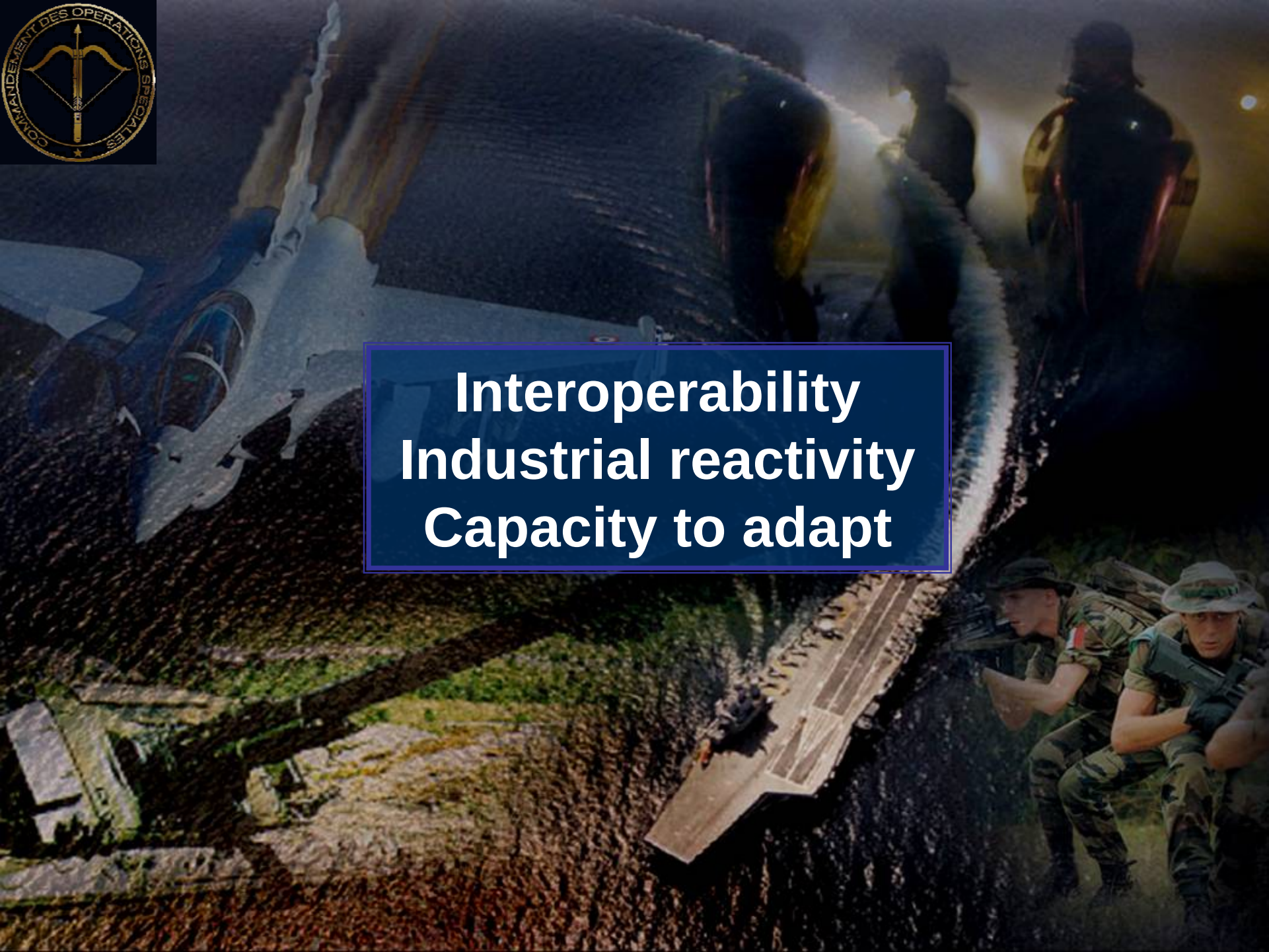
18th NDIA SO/LIC SYMPOSIUM, WASHINGTON – FEBRUARY 2007



Undetectable enemy
Using conventional and non conventional means
Combining classical and non classical actions

Fire power, advanced technology and traditional courses of actions are no longer sufficient.

An enemy that often has the initiative


COMMANDEMENT DES OPERATIONS SPECIALES
Interoperability
Industrial reactivity
Capacity to adapt


COMMANDEMENT DES OPERATIONS SPECIALES
Unpredictable and unstable environment

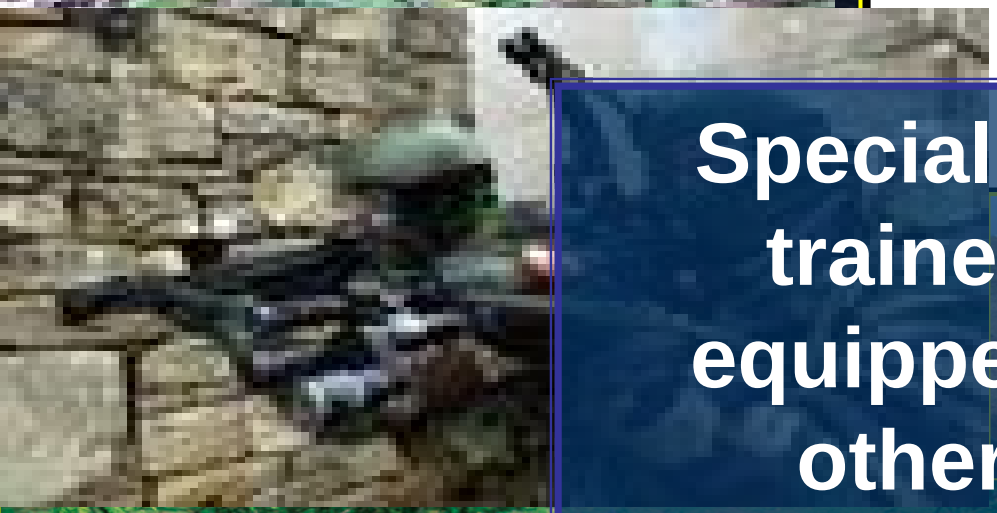

COMMANDEMENT DES OPERATIONS SPECIALES
The political success is now reached during the consolidation phase

New data to be considered

- Interoperability
- security concern
- force protection
- population a major stake
- monitor local security forces
- win the peace
- destabilize the enemy
- confidentiality


COMMANDEMENT DES OPERATIONS SPECIALES
Thinking war and the way to do it differently



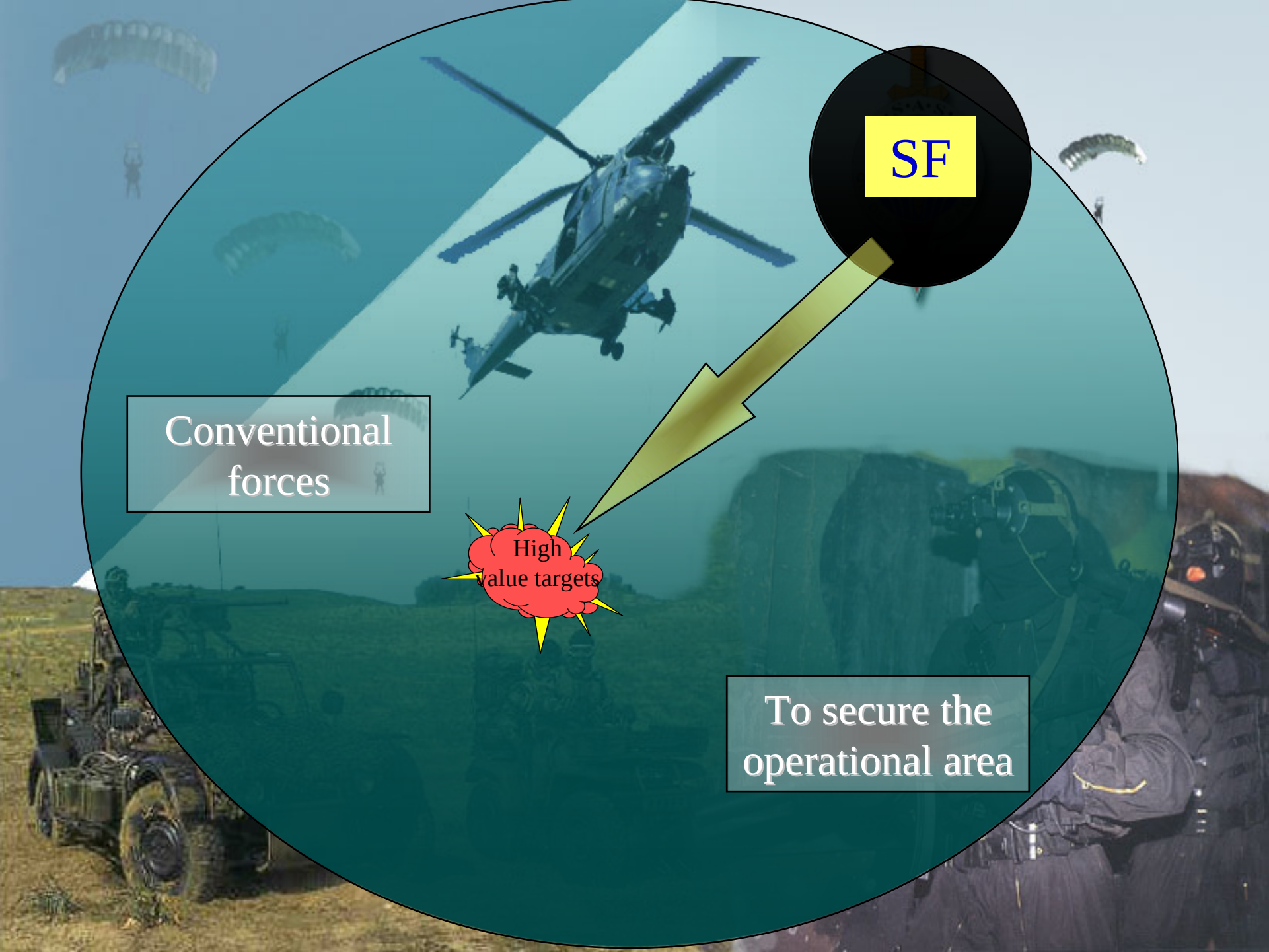


Special Forces trained and equipped to do otherwise








SF
Conventional forces
High value targets
To secure the operational area



- High sensitive targets
- seeking for more interoperability
- mastering capabilities / adapted technology
- intelligence / man in the loop / reliable sensors
- capability to upgrade both procedures and equipment as quickly as possible
- special human intell assets
- sharing information



Conclusion

“The View from the Joint Staff”



Lieutenant General John F. Sattler

Director for Strategic Plans & Policy

The Joint Staff

Purpose

- Brief primer on National and Military GWOT Strategies
- Why Building Partnership Capacity (BPC) is important
- 1206 and 1208 authorities, a success story
- BPC Efforts

UNCLAS

THE THREAT











National Strategy for the GWOT

Ends

Strategic Aims:
- *Defeat violent extremism as a threat to our way of life as a free and open society, and*
- *Create a global environment inhospitable to violent extremists and all who support them*

Ways

Protect *and defend* the Homeland	***Attack terrorists*** *and their capacity to operate effectively at home and abroad*	***Support*** *mainstream Muslim efforts to reject violent extremism*

Expand foreign partnerships and partnership capacity

Strengthen our capacity to prevent terrorist acquisition and use of WMD

Institutionalize, domestically and internationally, the strategy against violent extremists

Means

All Instruments of National Power

Military Strategic Framework for the GWOT

Ends

***Strategic Goal**: Preserve and promote the way of life of free and open societies based on the rule of law, defeat terrorist extremism as a threat to our way of life, and create a global environment inhospitable to terrorist extremists.*

Leadership	*Safe Havens*	**Enemy**	*Finance*	*Communication*
Movement	*Intelligence*	*Weapons*	*Personnel*	*Ideology*

Ways

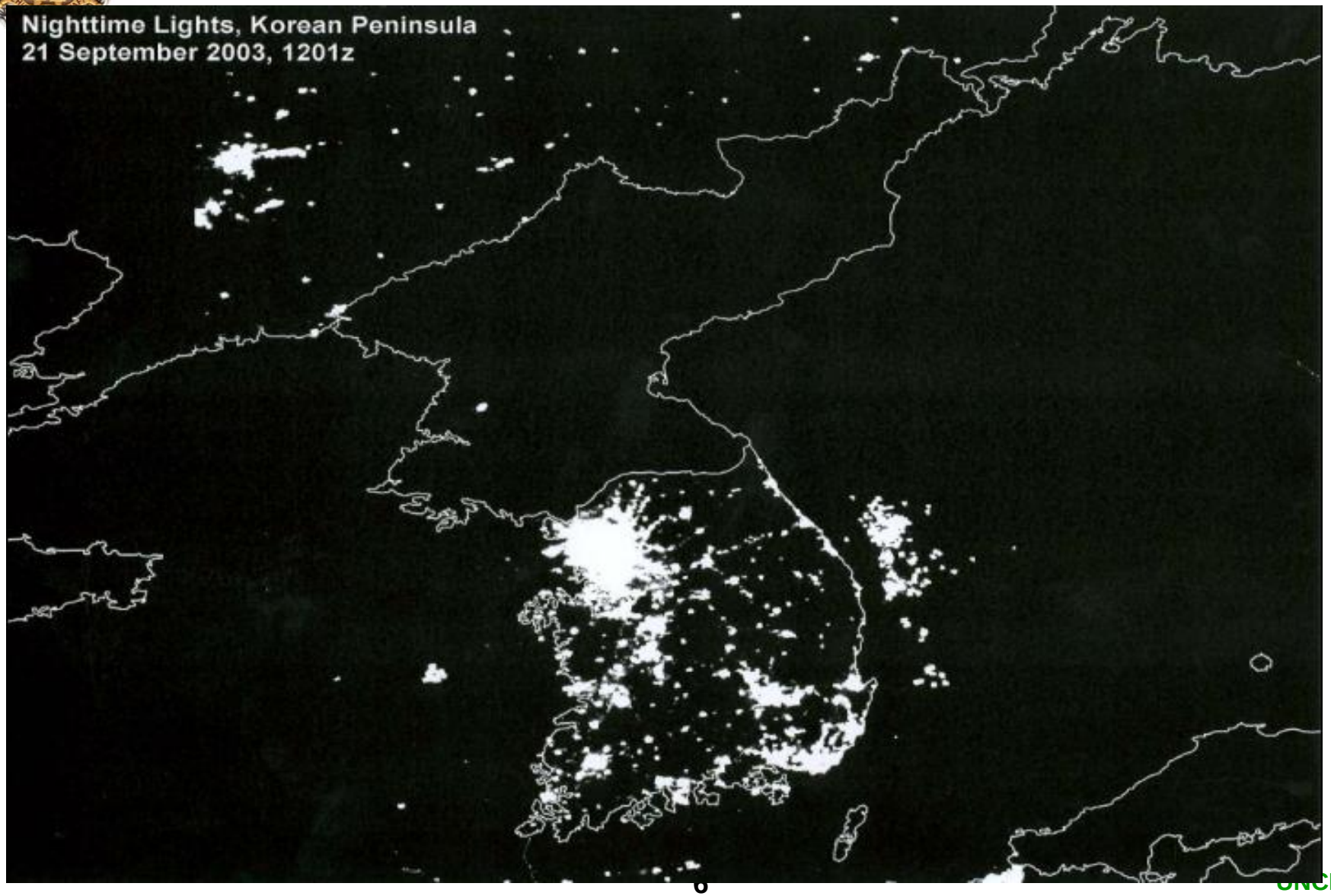
Military Strategic Objectives

Protect the Homeland	Disrupt and Attack Terrorist Networks	Counter Ideological Support for Terrorism
Deny terrorists the resources they need to operate and survive.		
Enable partner nations to counter terrorism.		
Deny WMD/E proliferation, recover and eliminate uncontrolled materials, and maintain capacity for consequence mgmt.		
Defeat terrorists and their organizations.		
Counter state and non-state support for terrorism in coordination with other U.S. Government agencies and partner nations.		
Contribute to the establishment of conditions that counter ideological support for terrorism.		

Means

Combatant Commands, Services, and Combat Support Agencies

KOREAN PENINSULA AT NIGHT



FY 06 Section 1206

- **POTUS authority to direct SECDEF to conduct or support a program to build the capacity of a foreign country's national military forces to:**
  - Conduct counterterrorist operations *or*
  - Participate in or support military and stability operations in which US Armed Forces are a participant
- **Limited to $200M/year from Defense-wide O&M**
- **Would have expired 30 Sep 07**

Combatant Commanders consistently rank 1206 as one of their highest priorities in conducting operations in their AORs.

FY 07 Section 1206

- **Increases authority to $300M/year**
- **Gives SECDEF approval authority with concurrence of SECSTATE**
- **Extends authority through FY08**
- **Removes the "Defense-wide" O&M restriction**

Section 1206 Process

1. Combatant Command/ Chief of Mission initiate request; complete proposal template
2. Coordinate with DOD/DOS counterpart
3. Submit through chain-of-command
4. JS/DOD/DOS review proposals and prioritize
5. DSCA will assess executability and verify cost estimates; OSD Comptroller begin to identify funding
6. Obtain SecDef/SecState approval
7. Submit to President
8. Notify Congress within 15 days of execution

Section 1208: Special Ops Train & Equip Authority

- **FY05 Nat'l Defense Authorization Act, Section 1208:**
  - **Allows SecDef to provide support to foreign forces, irregular forces, groups or individuals engaged in supporting ongoing CT ops by US special ops forces**
  - **Limited to $25M annually (USSOCOM-executed)**
  - **Expires 30 Sep 07**
- **Process:**
  - **SecDef *and* SecState approve EXORDS**
  - **Prior to exercising authority:**
    - **SecDef coordinates with SecState**
    - **SecDef notifies Congress**
  - **SecDef annually reports recipients and amounts**
- **Way Ahead: Seeking Congressional support to make authority permanent**

Building Global Partnerships Act

- **DoD is routinely and legitimately called upon to perform certain activities for which DoD lacks proper authorities**
- **Prepared a bill, *The Building Global Partnerships Act***
  - **Improves our ability to get many of these things done**
  - **COCOMs suggested many elements**
  - **Still in coordination with State**
- **The effort will not succeed without a concerted effort by senior defense leaders and our State counterparts**

Key to prosecution of the war on terrorism

The National Security Initiative Fund

- **Beyond Iraq and Afghanistan, the U.S. is underinvested in preventative strategies that build the capacity of foreign partners**
- **An interagency national security account, administered by DoD and DoS**
  - **dedicated to whole-of-government solutions**
- **Still in coordination with State**

DOS Civilian Reserve Corps

- **DOS expeditionary capabilities currently fall far short**
- **DOS recently proposed creation of a Civilian Reserve Corps**
  - **Would address some shortfalls (≈$25M) while a program (≈$1B/year) is developed**
- **POTUS addressed in State of the Union**
- **DOD can greatly assist DOS in advocating for this proposal to Congress**

Key to executing both post-conflict stabilization and reconstruction and preventative strategies

"Goldwater-Nichols" for the Interagency

- **Focus on reforming our National Security System**
  - **Organization, roles, and missions of the interagency**
  - **'07 NDAA tasks POTUS and SecDef with interagency studies**

US Government exploring the best approach to develop a national security reform agenda

QUESTIONS?

BACKUP

Building Capacity: Takes Time – South Korea

In 1953 – at the end of the Korean War,

- Was devastated by Japanese occupation and the war with the north
- Natural, human, and manmade resources were destroyed
- Had a 95% illiteracy rate and no record of national governance
- Gross Domestic Product was equivalent to the poorest Asian and African Countries

In 2007 – 54 years later,

- Is known as one of the "Asian Tigers" – one of the top four Asian economies
- GDP has grown to match those within the European Union
- A stable and legitimate democratic government with a free market economy
- No longer requires large amounts of American support for survival
- US forces still present

Other Long Term Examples of Success,

- Germany, Japan

"For … the global community, the withering away of the state is not a prelude to utopia but to disaster … These weak states have posed threats to international order because they are the source of conflict and … because they have become the potential breeding grounds for a new kind of terrorism that can reach into the developed world."

Francis Fukuyama, State Building, Cornell University Press, 2004.

Building Capacity in the Cold War

- **Long Term Examples of Success (Decades of Support)**
  - Germany, Japan, South Korea
- **Commonalities**
  - Sustained American Presence – still today (over 50 years)
  - Significant American Investment
  - Democratic societies with free market economies
- **Payoff**
  - Partner nations stood up to Communist threats
  - All are significant allies and trading partners
  - Each is a stabilizing force within their region

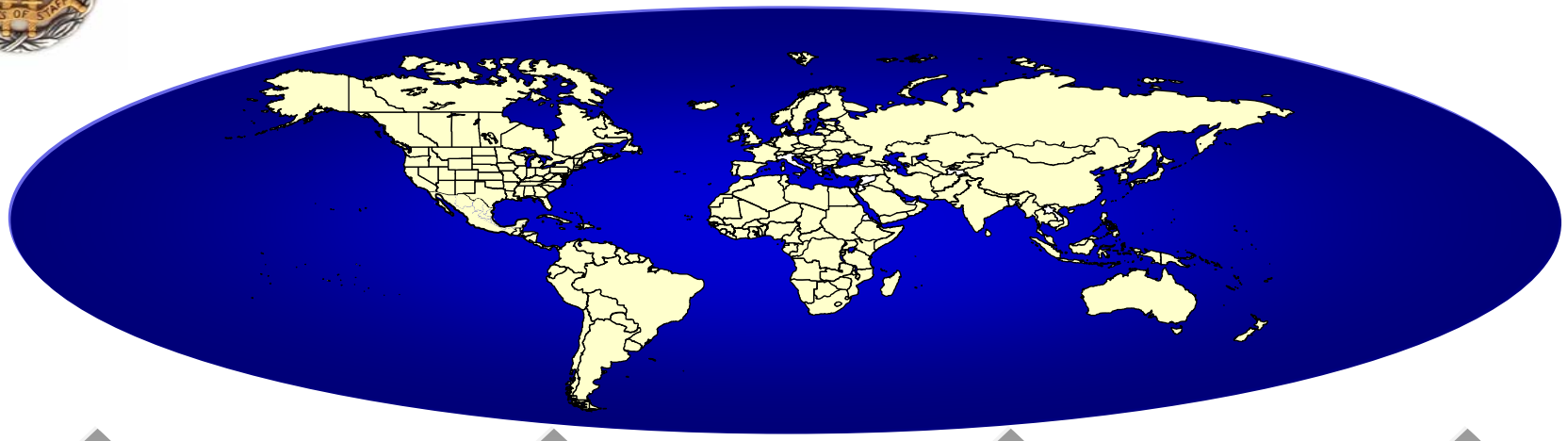
Key Lesson: Capacity building takes decades…but it is what allows the United States to win this war in the long term.

What 1206 Does and Does Not Do

- Section 1206 *does*:
  - Give DoD a 2-year $200M (per year) train and equip authority.
  - Require DoD to formulate programs and coordinate implementation with State.
  - Allow DoD to build the capacity of a foreign country's military forces to conduct time-sensitive:
    A. Counterterrorism or
    B. Stability operations in which US forces are a participant.
  - Require a Presidential review of the Foreign Assistance Act and Arms Export Control Act, due at the end of FY06 (SEP 06).
  - Expire on 30 September 2007 – although it could be renewed and even expanded if the Executive Branch demonstrates to Congress that it has been well used.

- Section 1206 *does not:*
  - Create a fund for State and DoD operations that are unlikely to build *enduring* security capacity.
  - Provide resources for Iraq or Afghanistan, whose training and equipping are provided by separate appropriations.
  - Avoid existing Foreign Assistance and Arms Export Control Act prohibitions on this type of assistance.
  - Provide appropriated funds: 1206 funds are drawn from "defense-wide operation and maintenance" – a narrow slice of overall operation and maintenance funds.
  - Allow DoD to build the capacity of a foreign country's non-military security forces.

Building Global Partnerships Act



Capability

TRAINING

EQUIPPING

EXERCISING

ADVISING

Capacity

LOGISTIC & MATERIEL SUPPORT

TECHNICAL SUPPORT

Compatibility

INTER-OPERABILITY

COMMON LEARNING

INFORMATION & INTEL SHARING

Conditions

SUPPORTING LOCAL POPULATIONS

Four Lines of Approach – 16 New Authorities

(DELIBERATIVE DOCUMENT: For discussion purposes only. Draft working papers. Not subject to FOIA release)

FY 06 Section 1206

- **FY 06 Section 1206 gave the President authority to direct the Secretary of Defense to conduct or support a program to build the capacity of a foreign country's national military forces in order for that country to**
  - Conduct counterterrorist operations *or*
  - Participate in or support military and stability operations in which US Armed Forces are a participant

Combatant Commanders consistently rank 1206 as one of their highest priorities in conducting operations in their AORs.

FY 06 Section 1206

- **Section 1206 was limited to $200 million per year from Defense-wide O&M; no corresponding appropriation**
  - Required:
    - Presidential approval
    - SecState/SecDef concurrence
- **Would expire 30 Sep 07**

Combatant Commands and State prepared proposals for implementation under the authority in FY06

Section 1206

- **1206 *<u>does</u>***
  - Provide an option for Combatant Commands to execute *<u>time-sensitive efforts</u>* in Building Partner Capacity.
- **1206 *<u>does not:</u>***
  - Provide resources for Iraq/Afghanistan. This is done under separate appropriation.

Technologies from the National Labs to Wage the Long War

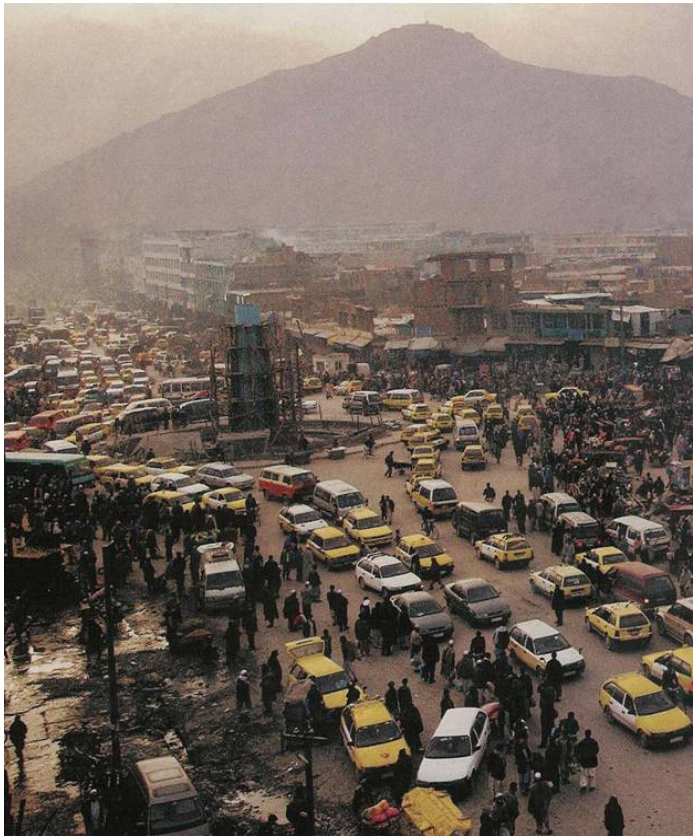
Russell D Skocypec, PhD
Deputy Director
Human, Systems and Simulation Technologies
Sandia National Labs
rdskocy@sandia.gov
(505) 845-8838

February 26, 2007
National Laboratories Panel
18th Annual NDIA SO/LIC Symposium and Exhibition
"Warfare in the Seams: Defense and Industry Partnering to Win the Long War"

Sandia National Laboratories

Characteristics of the threat

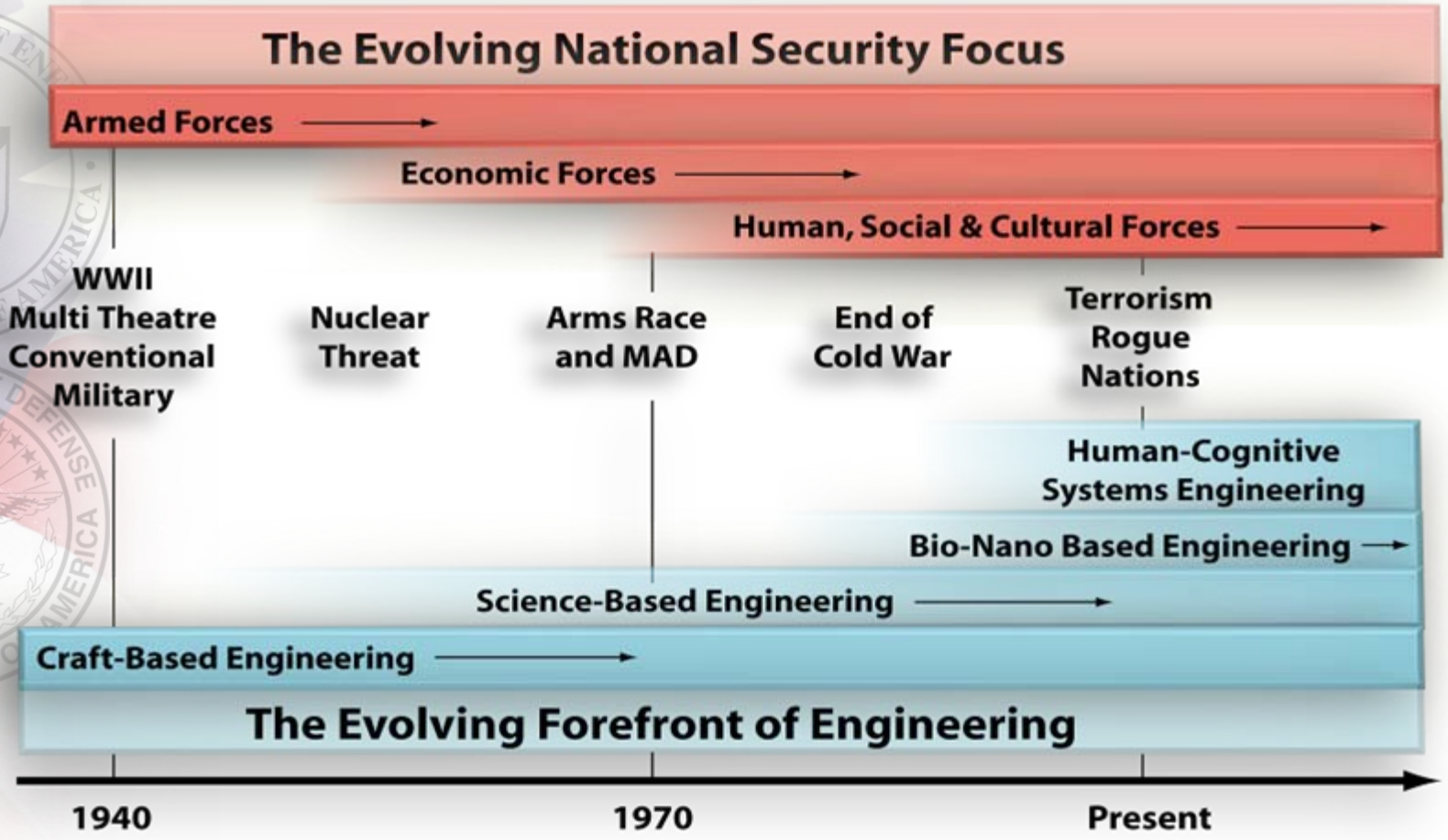
- **Emerging from societies and people who remain *disconnected physically* but who share a *common philosophy***
- **Philosophy enabled by ability to *communicate***
- **Locus of violence has shifted to the *individual actor***
- **Nuanced threat – vague, inconsistent, irrational, difficult to measure, *not well understood***
- **Threats can *adapt and evolve* faster than we are transforming**



Impacts ALL national security agencies/departments
DoD, IC, DHS, … and DOE!

Sandia National Laboratories

Sandia is evolving to meet these challenges



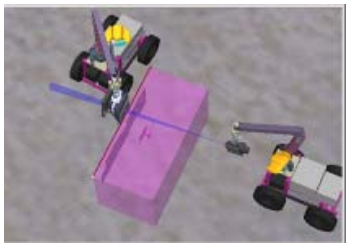
Creating <u>unique</u> national security systems solutions based on solid science for the Long War

Sandia National Laboratories

Key competencies to meet our mission challenges



Modeling & Simulation



Design & Analysis



Fabrication

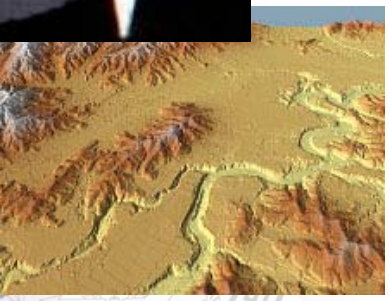


Environmental Testing



Test & Evaluation

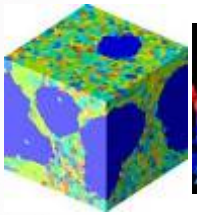




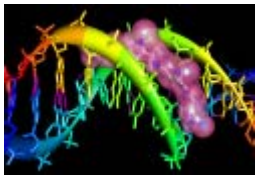
Sensing

8,500+ employees
1,500+ PhDs; 2,500+ MS
~$2.3B operating budget

Foundational S&T:



Materials



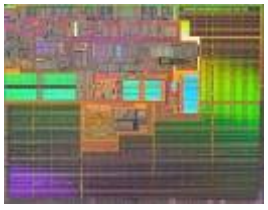
Computing, Information



Engineering



Pulsed Power



Microelectronics, Photonics



Cognition

Often partnering with DoD and industry

Sandia National Laboratories

A DOE Labs team (FIST) has been part of the FCS program for over 6 years

Army - DARPA | LSI - Industry
FIST
Future Force Integrated Support Team
DOE Labs - DoD FFRDC's

DARPA

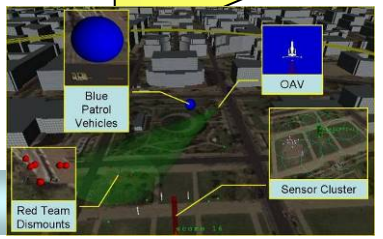
PROGRAM MANAGER FCS
BRIGADE COMBAT TEAM
One Team-The Army/Defense/Industry

U.S.ARMY

FY01 | **FY02** | **FY03** | **FY04** | **FY05** | **FY06** | **FY07**

Govt Tech Resource Analysis Team

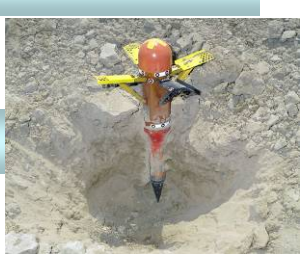
- Architecture
- Combat ID
- Network Vulnerability



- System of Systems Engineering and Integration
- Adv Decision Support System
- Log & Supportability



- Countermine
- Critical Technology Evaluations



- M&S for SoS
- MOUT Analytics, Mobile Network/Comms, UAVs, Humans
- Future Spiral-In Concepts, Sensor Dart, EM Gun Tech Seedlings

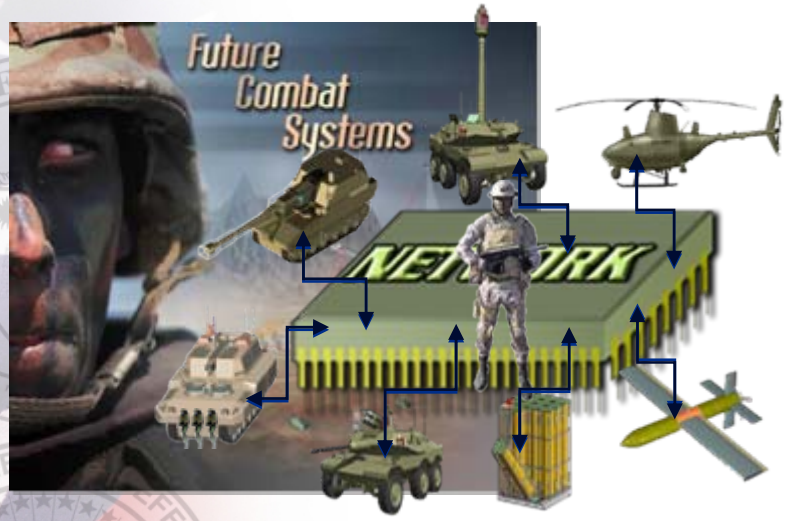


Providing objective technical advice using complementary DOE capabilities

Sandia National Laboratories

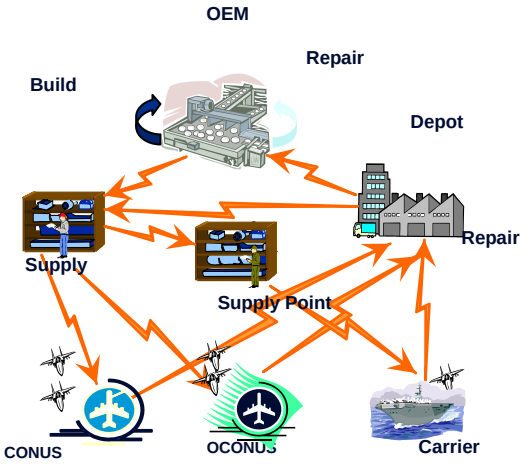
Sandia is partnering with industry to help address system sustainment & readiness challenges

System-of-Systems

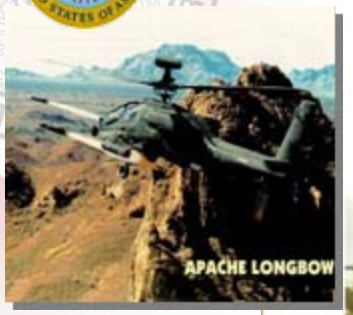


Enterprise & PBL





RECAP/RESET





Manpower & Readiness









Sandia National Laboratories

A DOE Labs team is supporting the Joint IED Defeat Organization (JIEDDO)

Anticipating the Threat

- Continued emphasis on the network, adaptivity, systems solutions

Innovating Solutions

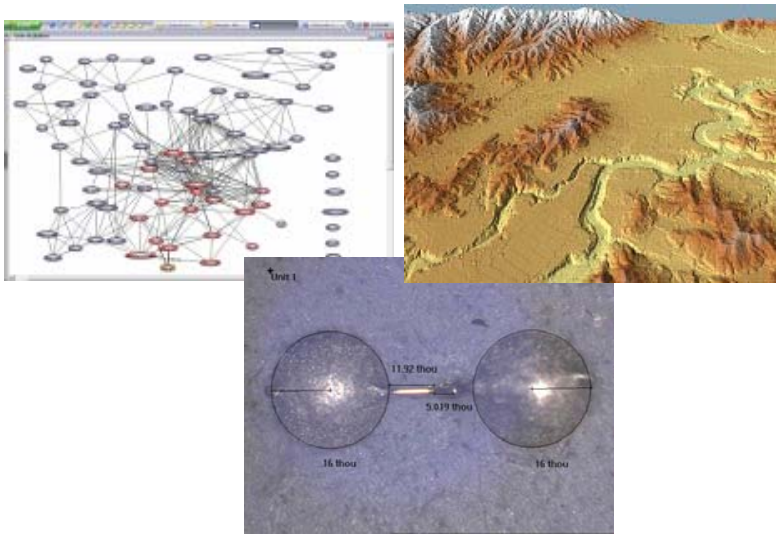
- Embedded staff at JIEDDO
- Reachback to our experts
- Technology contributions
- Systems assessment & recommendations

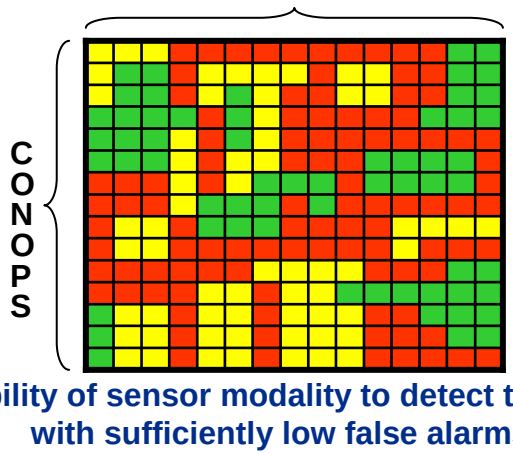
Creating Value

- NNSA/DOE lab team; industry partners

Informing the Debate

- Defense Science Board C-IED Task Force
- National Academy of Sciences Committee
- JIEDDO S&T Plan



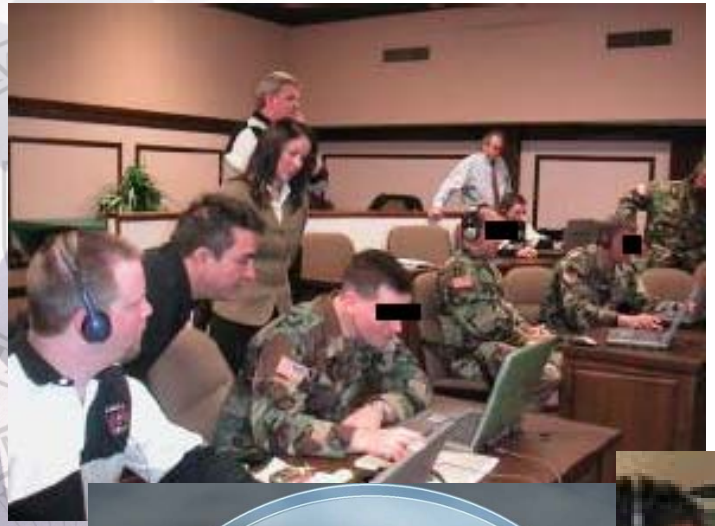


Ability of sensor modality to detect threat with sufficiently low false alarms

Leveraging complementary capabilities at DOE

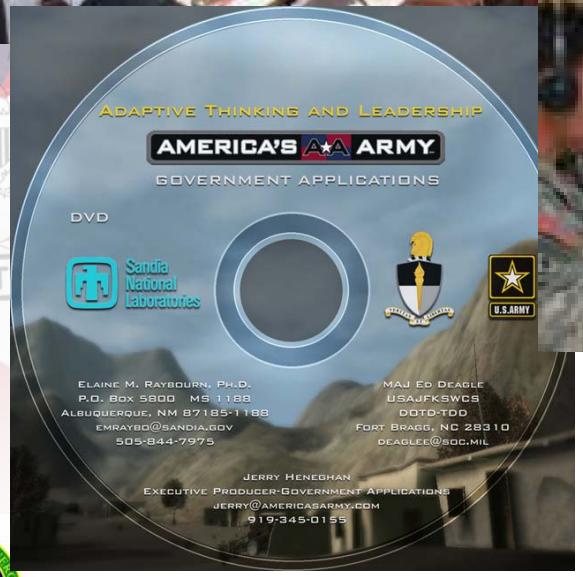
Sandia National Laboratories

Sandia-led team developed non-kinetic training for Special Forces JFK Special Warfare Center and School



Adaptive Thinking and Leadership

Game-based training to augment warfighter situation awareness and negotiation skills through culturally relevant scenarios for future special forces officers and NCO's





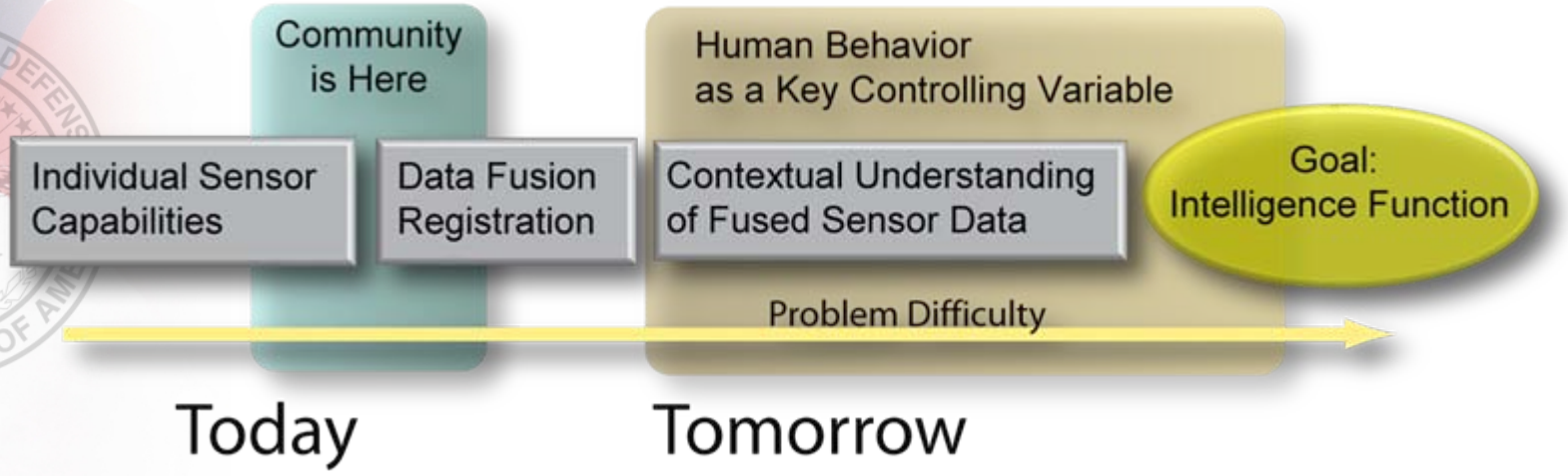


U.S.ARMY

Sandia National Laboratories

The S&T base for the Long War must enable us to discern meaning from great complexity

- **Model processes**
- **Identify potential signatures or create new observables**
- **Develop sensor systems to measure the observables**
- **Fuse data to identify patterns of activities**



We must focus on understanding <u>why</u> (vs only what)

Sandia National Laboratories

Summary

- **The Long War cuts across ALL national security agencies/departments**
- **Sandia is evolving to meet these challenges**
- **The DOE Labs are actively engaged with the services to meet requirements, often partnering with industry**
- **The challenges of the Long War are so great that it is in the national interest to work together**

Sandia National Laboratories

18th Annual SO/LIC Symposium
"Warfare in the Seams: Defense and Industry Partnering in the Long War"



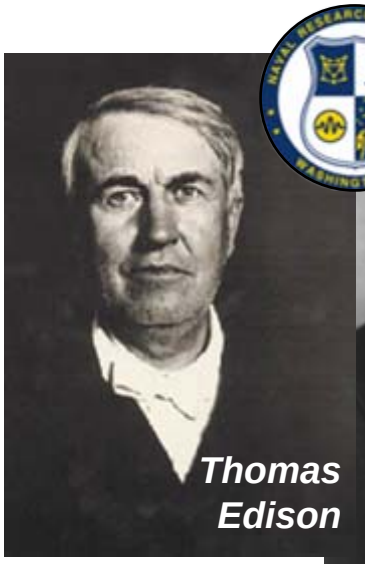
Presented by
George W. Solhan
Deputy Chief of Naval Research for
Expeditionary Maneuver Warfare and
Combating Terrorism S&T Department (ONR 30)

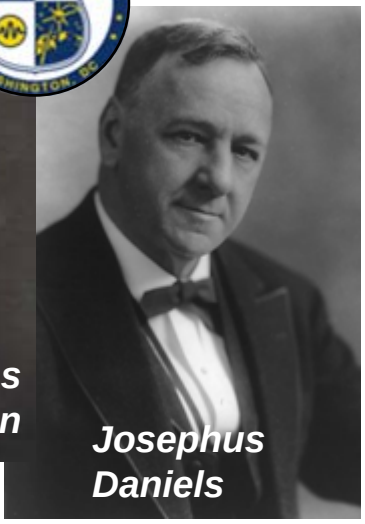
26 February 2007

Naval Research: A Statutory Mission

Naval Research Laboratory *(Appropriations Act, 1916)*:
"[Conduct] exploratory and research work…necessary… for the benefit of Government service, including the construction, equipment, and operation of a laboratory…."

Office of Naval Research *(Public Law 588, 1946)*:
"… plan, foster, and encourage scientific research in recognition of its paramount importance as related to the maintenance of future naval power, and the reservation of national security…. "







Transitioning S&T *(Defense Authorization Act, 2001)*:
"…manage the Navy's basic, applied, and advanced research to foster transition from science and technology to higher levels of research, development, test, and evaluation."

Office of Naval Research (ONR) Science and Technology Program

- $2.2 billion budget (of which $600-800M are pre-assigned congressional plus-ups)
- ONR has three primary investment thrusts:
  - Discovery and Invention (Basic and applied research) (6.1 & 6.2)
  - Future Naval Capabilities (Advanced Technology Demonstrations that are near term programs close to transition to an acquisition program of record) (6.2 & 6.3)
  - Innovative Naval Prototypes (high risk, high profile programs that potentially would be ready to transition in 4-8 years) (6.2 & 6.3)

ONR 30 Mission: Expeditionary Maneuver Warfare and Combating Terrorism

Office of Naval Research *(Public Law 588, 1946)*:
*"… **plan, foster, and encourage scientific research** in recognition of its paramount importance as related to the maintenance of **future naval power**, and the **preservation of national security**…. "*

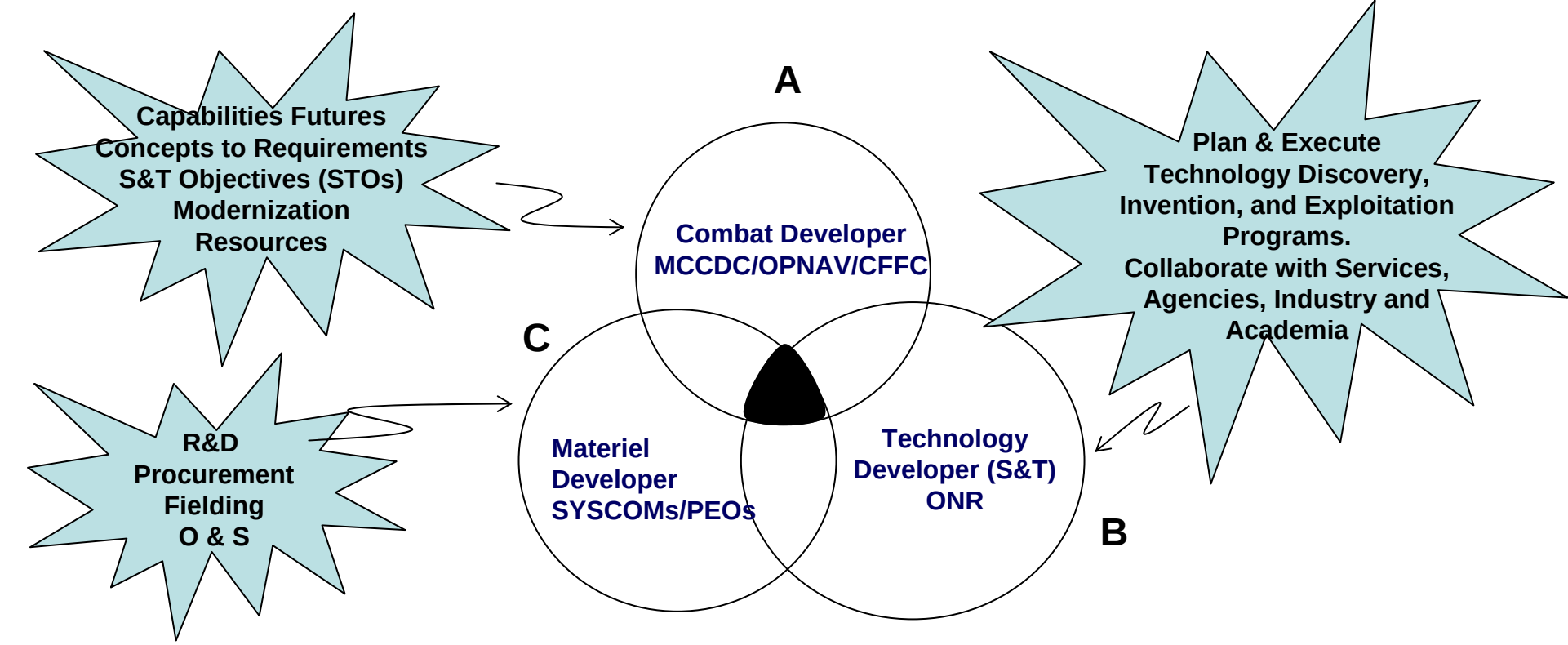
Expeditionary Maneuver Warfare and Combating Terrorism (Code 30)
*To lead the Department of the Navy's Science and Technology efforts that develop future **combat capabilities for Naval Expeditionary Maneuver Warfare and the Department's role in Combating Terrorism**:*

*…the exploitation and subsequent application of Science and Technology in order to enhance the ability of the **Navy-Marine Corps team to achieve assured access and conduct decisive operations as the naval portion of a joint campaign.***



Investment Thrust Areas:

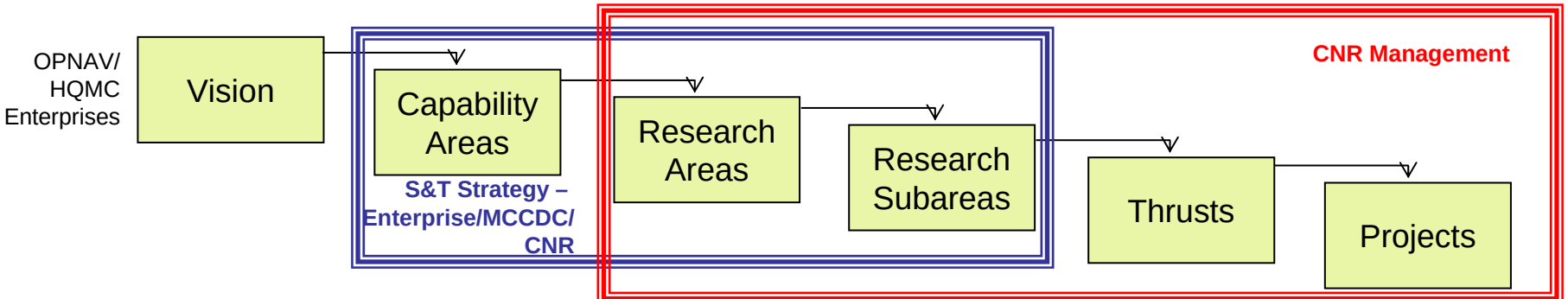
- **C4**
- **Fires**
- **Force Protection**
- **Human Performance**
- **Operational Adaptation**
- **Logistics**
- **Manuever**
- **Mine Countermeasures**
- **Maritime Irregular Warfare**



A Concept → Capability Futures → Gaps → Requirements

B Capability Futures → Gaps → Requirements → Technology

C Requirements → Technology → R&D/ Production → Capability



Background

- ***11 Sep 2001: US engaged in Global War on Terror***
- ***Sep 2005: ONR Code 30 created, and assigned CbT mission***
  - *Initiated an Executive Leadership Team (ELT) (Department Heads and Directors) and Working Group (Deputies) to review, analyze, and develop recommendations for a coordinated and integrated ONR-wide CbT S&T program*
  - *Conducted coordination meetings with DHS, NECC, USCG, and USMC Distributed Operations representatives to develop appropriate reliance, relevance and ultimately transition*
- ***April 2006: ONR CbT Taxonomy approved and CbT portfolio analysis completed***
- ***August 2006: Began development of a coordinated and integrated ONR CbT S&T investment strategy***

National & Naval GWOT Strategy/Analysis

Revolutionary Research . . . Relevant Results

Strategic Guidance

National Security Strategy (2002)

Key Goals

- Strengthen Alliances to Defeat Global Terrorism and Work to Prevent Attacks Against Us and Our Friends
- Work with others to Defuse Regional Conflicts
- Prevent Our Enemies from Threatening Us, Our Allies, and Our Friends with Weapons of Mass Destruction
- Transform America's National Security Institutions to Meet the Challenges and Opportunities of the 21st Century

- National Defense Strategy *(2005)*
- National Strategy for Combating Terrorism (2003)
- National Strategy for Maritime Security (2005)
- National Strategy for Homeland Security (2002)

Naval Guidance

NSP | NOC | USMC OpCon

Other Guidance

QDR | FM 3-24 COIN

External Coordination

ONR CbT Capability Areas

- Global Maritime Domain Awareness
- Operational Adaptation
- Maritime Irregular Warfare

Revolutionary Research . . . Relevant Results

CbT Capability Areas & Enabling Capabilities

Global Maritime Domain Awareness

- *All Source Collection*
- *Intelligence & Information Analysis & Fusion*
- *Netcentric Dissemination*
- *Persistent, Pervasive, Affordable Surveillance*
- *Tag, Track, and Locate*

Operational Adaptation

- *Warfighting Decision Superiority*
- *Commander's Preparation of the Environment*
- *Information Operations and Related Capabilities*
- *Battlespace Shaping*
- *Operational Culture Understanding & Communication*
- *Mission Gaming and Rehearsal*
- *Adaptive Thinking and Leader Development*

Maritime Irregular Warfare

- *Ship Disabling Non-Lethal Systems*
- *Enhanced Maritime Interception Operations*
- *Expeditionary Security*
- *Biometrics*
- *Real-time Forensic Site Exploitation*
- *Logistics for Distributed Forces*
- *Extended Small-unit ISR*
- *Extended Small-unit Engagement*
- *Enhanced Individual and Small-unit Mobility*
- *CBRN Defense*
- *Tactical Comm in Complex Environments*

Counter IED

- *IED Prediction*
- *IED Prevention*
- *IED and Mine Detection*
- *IED and Mine Neutralization*
- *IED and Mine Effects Mitigation*
- *Technical and Forensic Exploitation*

Asymmetric and Irregular Warfare (Combating Terrorism)

Revolutionary Research . . . Relevant Results

Vision: **Enable Naval forces to preempt and defeat adaptive non-conventional threats operating within complex physical and social terrain.**

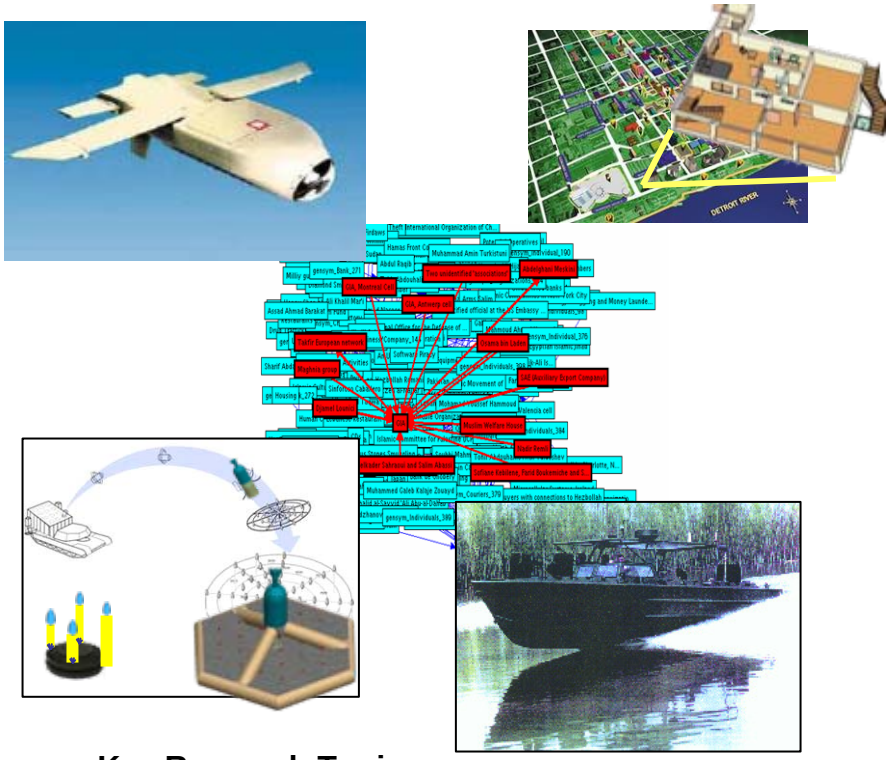
Objectives

ISR:
- **Unmanned Vehicles**: Intelligent autonomous unmanned vehicles, sensors, and communications
- **Interior/Exterior Imaging**: Rapidly reconstruct and fuse multi-aspect sensor data into 3-D tactical models of building interiors and exteriors
- **Riverine Surveillance**: Common and persistent maritime picture on and below the surface/shore

Intelligence Analysis:
- Image and Pattern recognition tools
- Societal, cultural, and behavioral modeling
- Biometrics

Active and Passive Forensics Tools:
- Field-portable forensic tools, sensors, and sensor networks; as well as spectrally-coded particulate markers and probes

Advanced Countermeasures:
- Dominate EM spectrum
- Predict, detect and neutralize IED's and P-IED's
- Deny adversaries the ability to hide among civilian population
- Phase 0 S&T



Key Research Topics

Unmanned Undersea Vehicle Technologies
Unmanned Air and Ground Vehicles
Intelligent and Autonomous Systems
Automated Image Understanding
Information Processing & Presentation
Social, Cultural & Behavioral Modeling
Biometrics
Nanoscale Electronic Devices and Sensors
EW Attack
Counter IED
Non-Lethal weapons

Irregular Warfare--Defined

"Irregular warfare is a form of warfare that has as its objective the credibility and/or legitimacy of the relevant political authority with the goal of undermining or supporting that authority. Irregular warfare factors indirect approaches, though it may employ the full range of military and other capabilities to seek asymmetric advantages, in order to erode an adversary's power, influence and will." (Irregular Warfare Roadmap - QDR)

Detecting and Effecting anonymous irregular threats dispersed throughout the human landscape…"irregular"

versus

Finding and Destroying distinctive conventional formations concentrated on the physical landscape…"traditional"

Revolutionary Research . . . Relevant Results

Traditional Warfare vs. Irregular Warfare

	Traditional Warfare	Irregular Warfare
1	The center of gravity is often the adversary's ***military forces and political leadership***	The center of gravity is usually the ***indigenous population***
2	Influencing the ***physical terrain*** is key.	Influencing the ***social & cultural terrain*** is key
3	Conducted by ***regular forces*** of ***nation states*** that are ***separate and distinct*** from the civilian population	Often conducted by ***irregular forces*** of ***state or non-state networks*** that are ***embedded*** (not distinct) from the civilian population
4	***Focused kinetic effects -- Physical***	***Distributed non-kinetic effects -- Psychological***
5	**Symmetrical –** less opportunity to adapt forces and material	**Asymmetrical** – more opportunity to adapt forces and material
6	Focus on the **kinetic destruction** of the adversaries warfighting material from ***stand-off*** distances	Focus on the ***non-kinetic influence*** of local and regional populations requiring ***face-to-face*** interaction.
7	***Tactical competence*** is critical	***Cultural and tactical competence*** is critical
8	Threat forces and relationships ***easily templated***	Threat forces and relationships ***difficult to template***
9	***d i M e*** ***(Diplomatic, Information, Military, & Economic with emphasis on the Military)***	***D I m E – High interagency*** ***(Emphasis on Diplomatic, Information, and Economic)***
10	***Metrics of success are easily defined***	***Metrics of success are not easily defined***
11	**Proven technological advantage**	**Advanced technology advantage remains unproven as benefactor to irregular warfare**

Revolutionary Research . . . Relevant Results

Operational Adaptation (OA):
"The Information Warfare Game Changer"

Revolutionary Research . . . Relevant Results

Operational Adaptation

***Definition*:** (OA) The development and sustainment of a tempo of operations and a rhythm of adaptation and decision superiority that is beyond an adversary's ability.

****

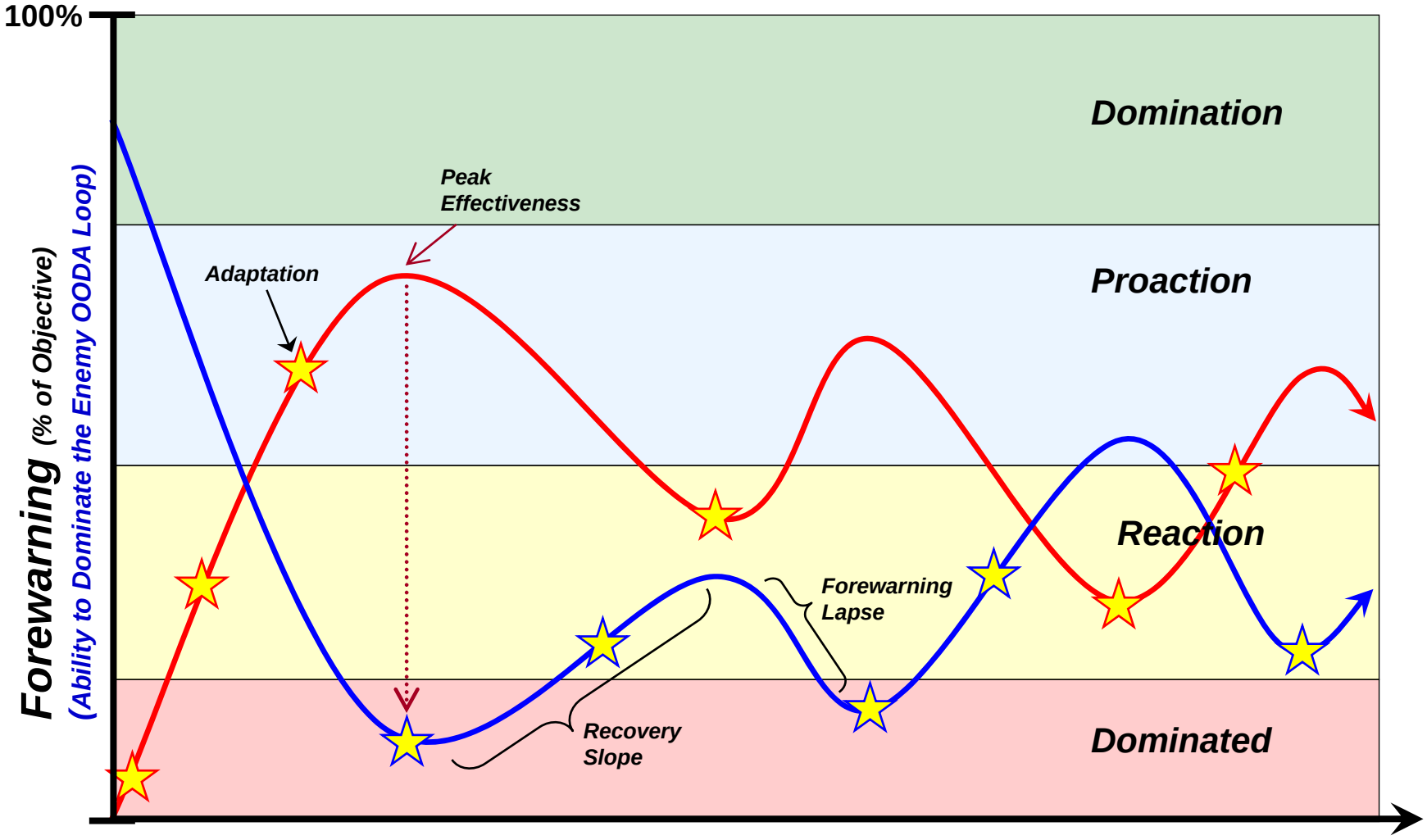
Revolutionary Research . . . Relevant Results

Previous Studies Have Pointed Toward The Need For "Operational Adaptation"

- **June 2001 Institute for Defense Analysis study:**
  "New Perspectives on Effects-Based Operations"
- Key attributes of Effects Based Operations:
  - Focus on decision superiority (not just precision engagement or targeting)
  - Applicable in peace and war
  - Look beyond the direct, immediate first-order effects
  - Adaptation at the operational level occurs in a disciplined process
  - Include all elements of national power (economic, political, etc)
- **Game Changer**
  - "Victory is gained through a tempo or rhythm of adaptation that is beyond the other side's ability to achieve or sustain." FM 3-24

Revolutionary Research . . . Relevant Results

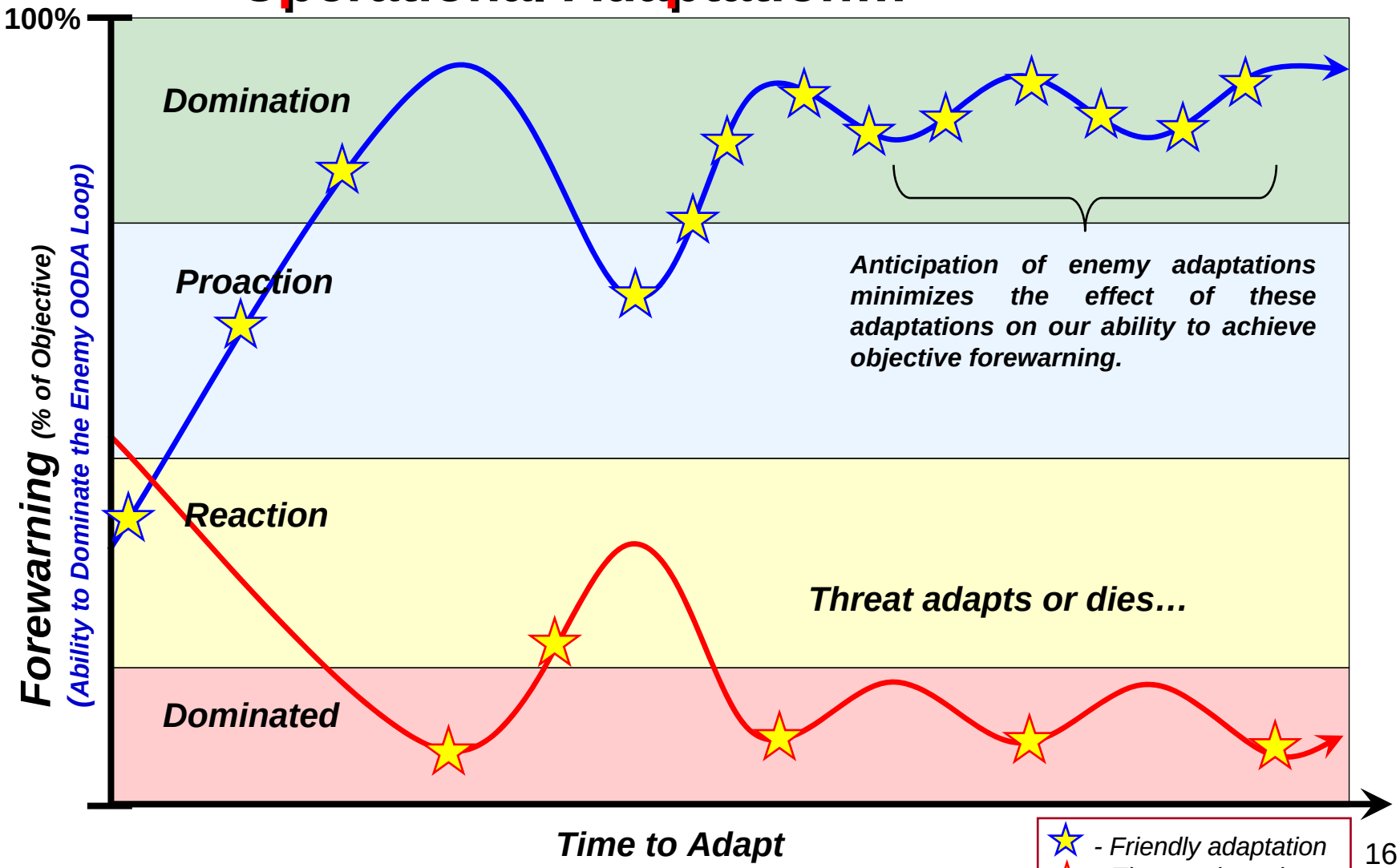
Current Situation…The Adaptation Dance



Revolutionary Research . . . Relevant Results

Objective Effects of Operational Adaptation…

Forewarning Objectives:
Tactical – *Hours*
Operational – *Days*
Strategic – *Weeks*



The OODA Loop (Boyd Cycle)
(The Key to Solving Operational Adaptation)



The Observe, Orient, Decide, Act (OODA) Loop provides a standard description of decision making cycles that is widely understood and accepted throughout the U.S. military. It was developed by Colonel John (Richard) Boyd (January 23, 1927–March 9, 1997) who was a United States Air Force fighter pilot and military strategist of the late 20th century whose theories have been highly influential in the military and in business.

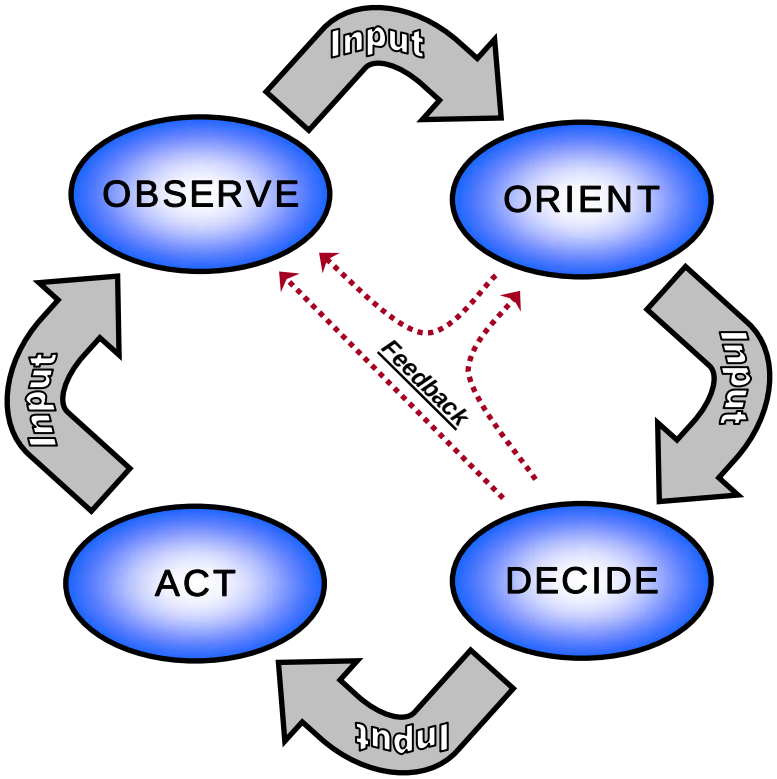
Four Activity Components

1. ***Observe*** *– collect, store, and access raw (but relevant) data and information related to one's environment, situation, objective, opposition, etc. This activity includes observation of the effects of one's own actions or inactions.*
2. ***Orient*** *– analyze the results of one's observation activities in order to achieve understanding of the situation or in order to uncover gaps in one's observations.*
3. ***Decide*** *– incorporate one's understanding of the situation to develop appropriate courses of action (COAs), analyze competing COAs, predict 2nd- and 3rd-order effects, and select the combination of actions (and inactions) that will achieve the most favorable effect(s). This activity may uncover additional gaps in one's observation and orientation activities.*
4. ***Act*** *– execute the actions selected during the previous activity.*

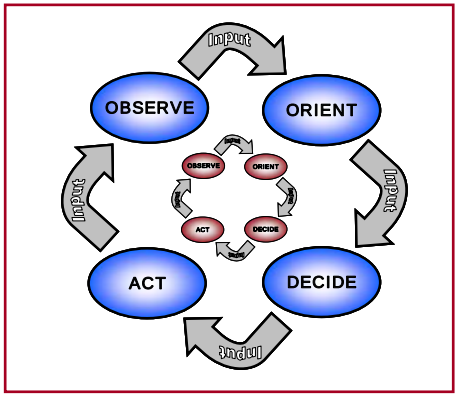
The OODA Loop (Boyd Cycle)

Revolutionary Research . . . Relevant Results

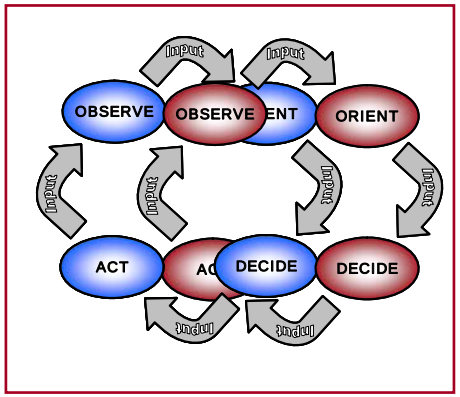
The Observe, Orient, Decide, Act (OODA) Loop provides a standard description of decision making cycles that is widely understood and accepted throughout the U.S. military.



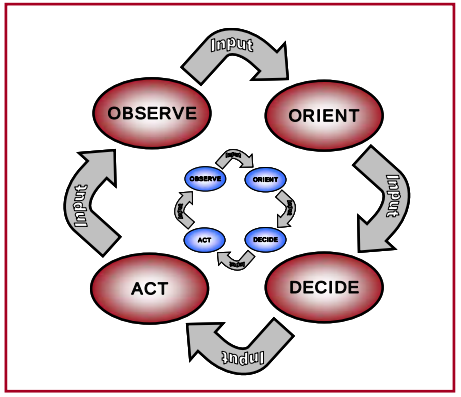
Dominated



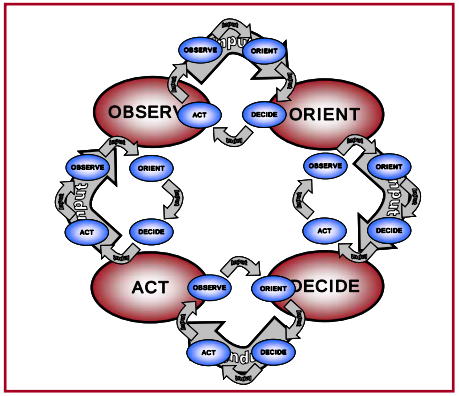
Reactive



Proactive

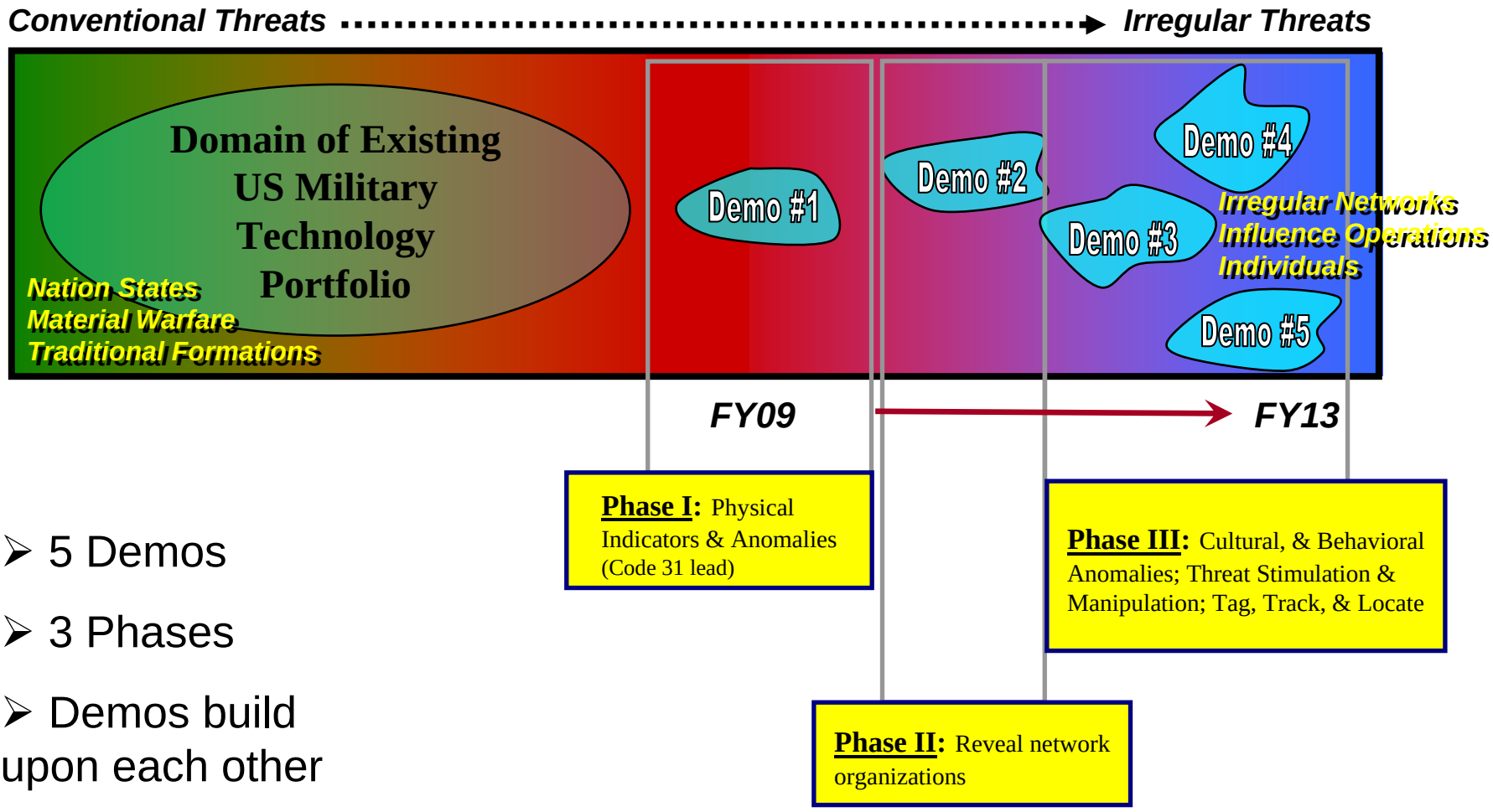


Domination *of all domains*



Proposed S&T Plan:
Road to Operational Adaptation

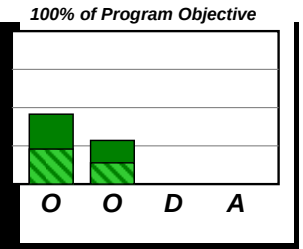
Technology Effectiveness Spectrum



- 5 Demos
- 3 Phases
- Demos build upon each other

Demo 1 – Phase 2: Affordable Persistent Pervasive Surveillance

(Wide Areas up to 200 nm² - Open Ocean, Littoral, Rivers & Urban)



Commercially Available SatCom

10 – 30 Kbps

10 – 30 Kbps

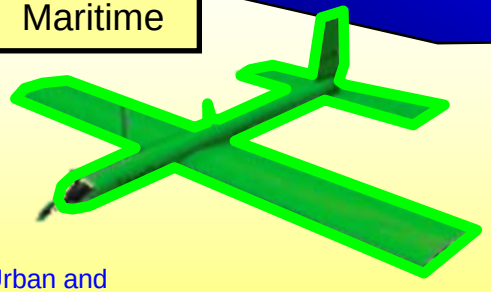
10 – 30 Kbps

10 – 30 Kbps

Maritime

Riverine

Urban/ Asymmetric



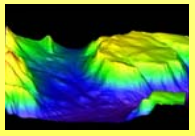
Urban and Terrain Imaging



GPS



GIS Geodata

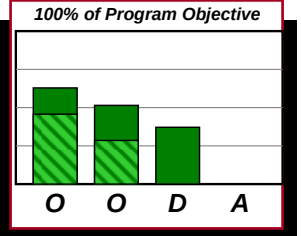


Methodology:

- Stealthy, long range, and high endurance UAVs for “eyes in the sky” - deployable from ocean and remote locations
- Inexpensive, low power consumption surveillance payloads
- Panoramic, wide-aperture optical sensors with 3-D imaging
- Data processing for minimization of transmitted data using physical indicators and anomalies
- Low bandwidth, over the horizon datalinks

Demo 2: Near Real-Time Forensics and Social Network Mapping

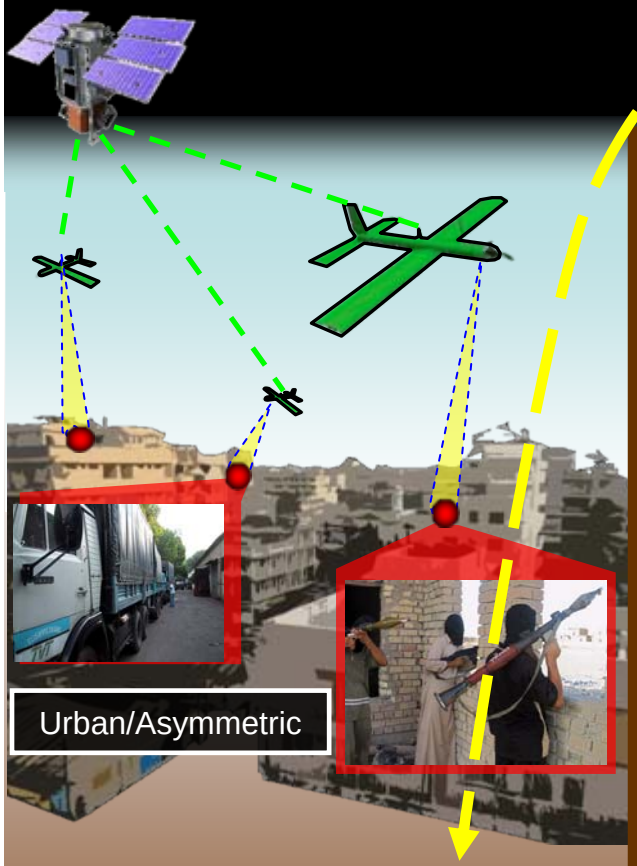
(Attack forensics and potential forewarning of seconds prior to attack)



Global Intel Sources

- Timeline +

Attack Occurs



Surveillance & Global Intelligence Info Databased

Attack Analyzed Using Database Info

Methodology:

- All-source intelligence fusion;
- social network mapping; persistent, pervasive surveillance; multi-spectral collection and analysis; and automated tracking of entities

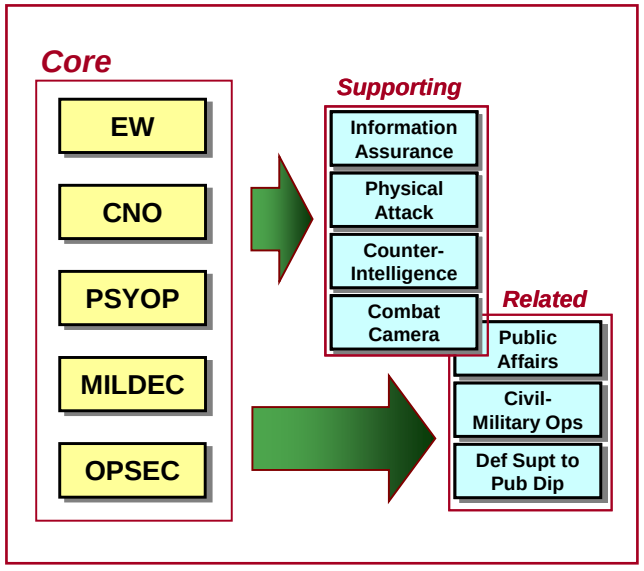


- Analysis Algorithms Define Network(s) in Near Real-Time Using Surveillance, Intel & Attack Info
- Enemy Network Rapidly Identified

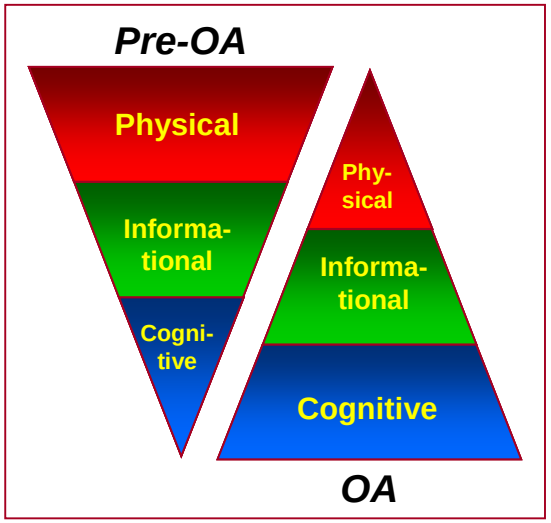
Revolutionary Research . . . Relevant Results

Information Operations Evolution (Demo 5)

Information Operations are the integrated employment of electronic warfare (EW), computer network operations (CNO), psychological operations (PSYOP), military deception (MILDEC), and operations security (OPSEC), in concert with specified supporting and related capabilities, to influence, disrupt, corrupt or usurp adversarial human and automated decision making while protecting our own.



Technology Focus on the Information Environment



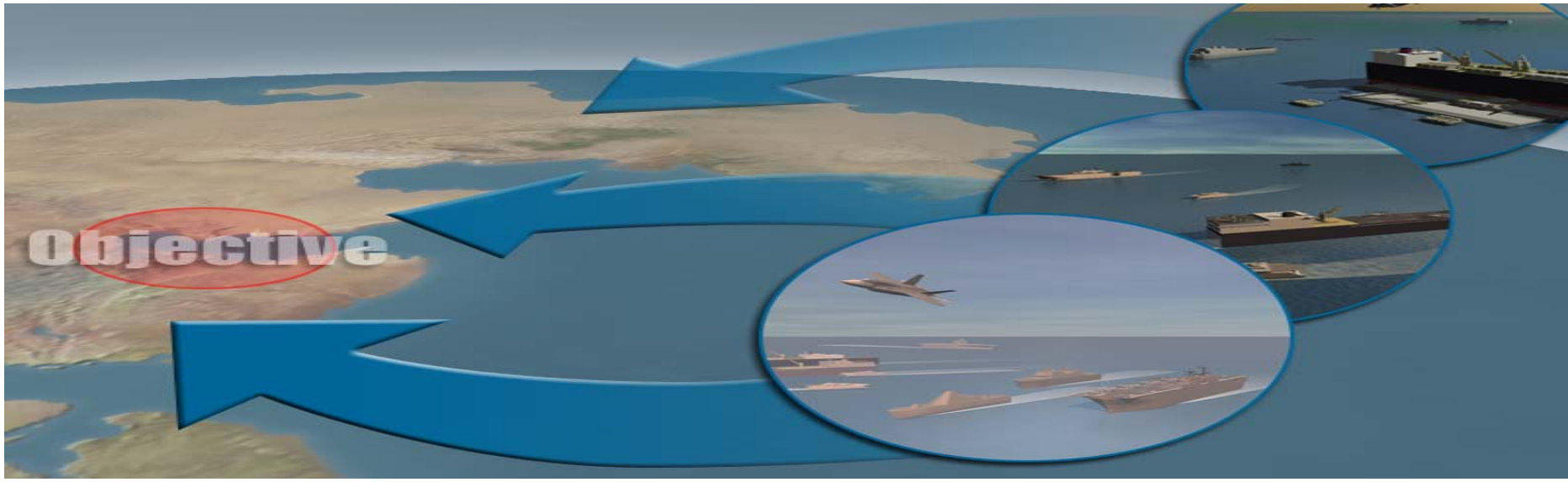
Disrupt → Stimulate → Influence → Manipulate

Pre-OA

OA

Distributed Operations (DO)

"***Maneuver Warfare** is the shift from quantitative characteristics of warfare – mass and volume – to qualitative factors of speed, stealth, precision, and sustainability*"



"***Distributed Operations** constitutes a form of Maneuver Warfare. The essence of this concept lies in the capacity for coordinated action by highly capable units, dispersed throughout the breadth and depth of the battlespace, ordered and **connected** within an operational design focused on a common aim."*

Distributed Operations

Revolutionary Research . . . Relevant Results

Vision: **Enable dispersed small units to dominate extended battlespace through advanced warfighter training, unambiguous situational awareness, robust communications and sense and respond logistics.**

Objectives

Training
- Enhancement of Physical and Cognitive Performance
- Simulation – based scenarios for enhanced training
- Rapid assimilation of cultural environments

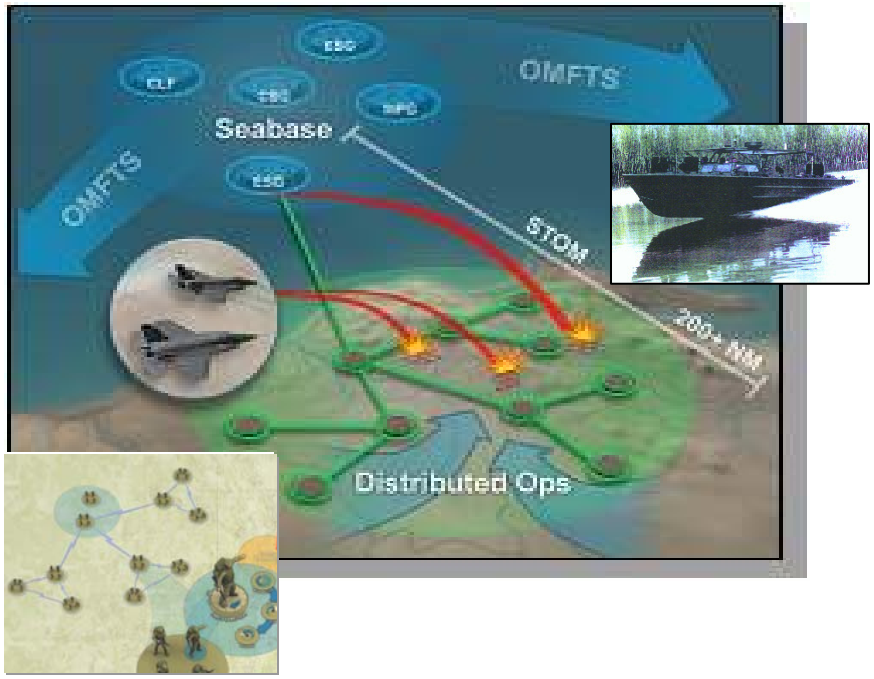
Communications
- Robust Command and Control networks
- Airborne relays on manned and unmanned platforms

Logistics
- Rapid re-supply and medical evacuation whenever possible
- Real–time automatic supply sensors and network
- Optimize medical self-sufficiency

Fires
- Integrate firepower of distributed ground, offshore, and air assets
- Blue Force Tracking down to the individual

Survivability
- Warfighter stealth technology
- Warfighter exoskeleton technology

Maneuver
- Adaptable and survivable tactical mobility systems to enhance operational tempo and extend range of vehicles and soldiers
- Advanced materials to reduce combat load



Key Research Topics

Training, Education & Human Performance
Expeditionary C4
Communications and Networks
Expeditionary Logistics
Expeditionary Firepower
Precision Strike
Expeditionary ISR
Unmanned Air and Ground Vehicles
Special Warfare / EOD
Land Mine Countermeasures
Expeditionary Maneuver/ Individual Mobility

Revolutionary Research . . . Relevant Results

Decreasing the Marine's Load

Yesterday's & Today's Marine – Overloaded!

1960s



Today



No Change

Treat the Marine as a system – Focus on the entire individual

~Make smart tradeoffs between performance & weight~

Improvements in:

- Combat Load
- Ergonomics
- Nutrition
- Physiologic Performance (Endurance, Strength)
- Fatigue Management
- Protection

Tomorrow's Marine: Optimized for Combat Endurance

Equals improvements in a Marine's load-bearing capability

Human Performance, Training & Education (HPT&E) 6.2 Investment

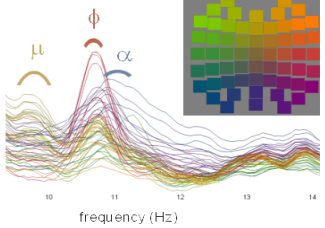
Revolutionary Research . . . Relevant Results











OBJECTIVE:

- Optimize individual & team performance using a range of solutions, scaleable across all leadership levels & echelons in complex combat environments (e.g., DO).
- Provide fundamental KSAs for a complete Warfighter in any combat situation via methods that generate & maintain combat effectiveness (e.g., basic skills acquisition, consolidation in scenario-based training, situation-targeted education)
- Continual assessment and diagnosis of individual and team capabilities and potentials
- Develop physically realistic models for combat performance simulation & evaluation
- Delineate neural mechanisms differentiating transition of learner from novice to expert

TECHNICAL APPROACH:

- Operational metric assessment, ID baseline performance level, scenario design & validation study
- Develop foundational learning theories extended to complex tasks for a range of expertise levels, training mitigation strategies triggered by neurophysiological markers of learning, cognition & expertise, & principles of expertise development on a continuum of novice to expert
- Develop training mitigation strategies triggered by behavioral and neurophysiological markers of learning, cognition and expertise
- Design and develop principles of expertise development on a continuum of novice to expert learning framework for both individual and team training
- Build task-specific models of expertise development in dismounted and mounted task environments; Develop simulation based automated diagnostic assessment of Knowledge, Skills, Abilities & Potentials (KSA&Ps) to drive HPT&E systems

PAYOFF:

- Enhanced combat capabilities at individual and small unit level
- Significant increases in training efficiency, completion, and effectiveness rates per unit time for individuals and small unit leaders in both real and virtual/augmented environments
- Enhanced training via tailored and real-time closed-loop training systems that are based on neuro-cognitive and psychologically-driven instructional strategies developed
- Ensure a small, yet potent fighting force by realizing the full potential of each Marine via efficient, targeted assessment and selection methods
- Enhanced team cognition and combat effectiveness capability
- Enhanced Warfighter capability to effectively/efficiently Observe, Orient, Decide, and Act during complex, stressful combat conditions
- Support USMC S&T Master Plan and STOs

The Ultimate Customer – The Warfighter!

Caveat: Real Customer: SYSCOMs, PEOs, DRPMs

HOT Buttons:

1. **Survivability**
2. **Reduce Combat Load**
3. **Small Unit Excellence**
4. **Fuel Efficiency**
5. **Light weight portable power sources**
6. **“Transparent” Urban Structures**
7. **Modular, Scaleable Weapons**
8. **CIED, MCM, CRAM**
9. **Operational Adaptation**
10. **Infantry combat load reduction**



Revolutionary Research . . . Relevant Results

QUESTIONS?



Combined Joint Special Operations Task Force – Arabian Peninsula (CJSOTF-AP)

Purpose: Provide an Operational Overview

COL Kenneth Tovo

27 February 2007

The overall classification is:
Unclassified

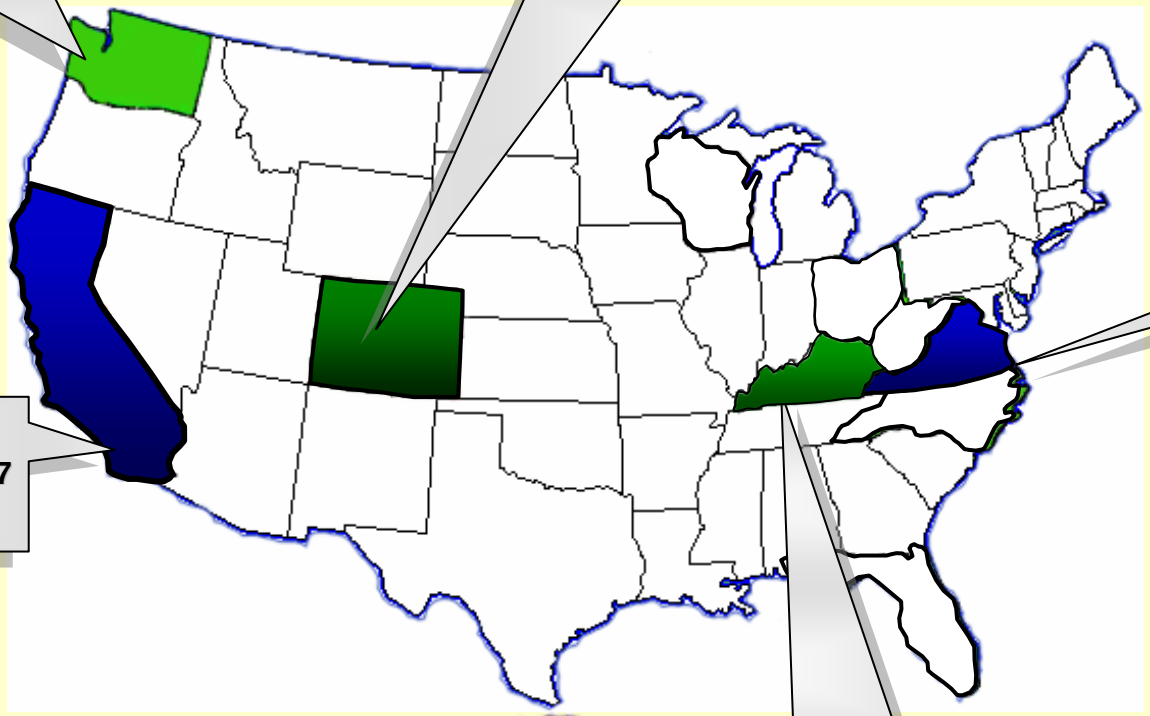
Agenda

- Who We Are (1 slide)
- Photos (3 slides)
- CJSOTF-AP Operational Reach (1 slide)
- Foreign Internal Defense (1 slide)
- Operational Vignette (4 slides)
- Non-Kinetic Vignette (2 slides)
- Summary (1 slide)

Who We Are

Green Berets
1st SFG (A)
FT Lewis, WA

CJSOTF-AP HQ
Green Berets
10th SFG (A) HQ
FT Carson, CO



SEALS
SEAL Tm 4, 8, and 10
Little Creek, VA

SEALS
SEAL Tm 3, 5, and 7
Coronado, CA

CJSOTF-AP HQ
Green Berets
5TH SFG(A)
FT Bragg, NC

Goal: Self-Reliant and Self-Sustaining





Strength: Tactical Confidence







Focus: Inculcating Values –

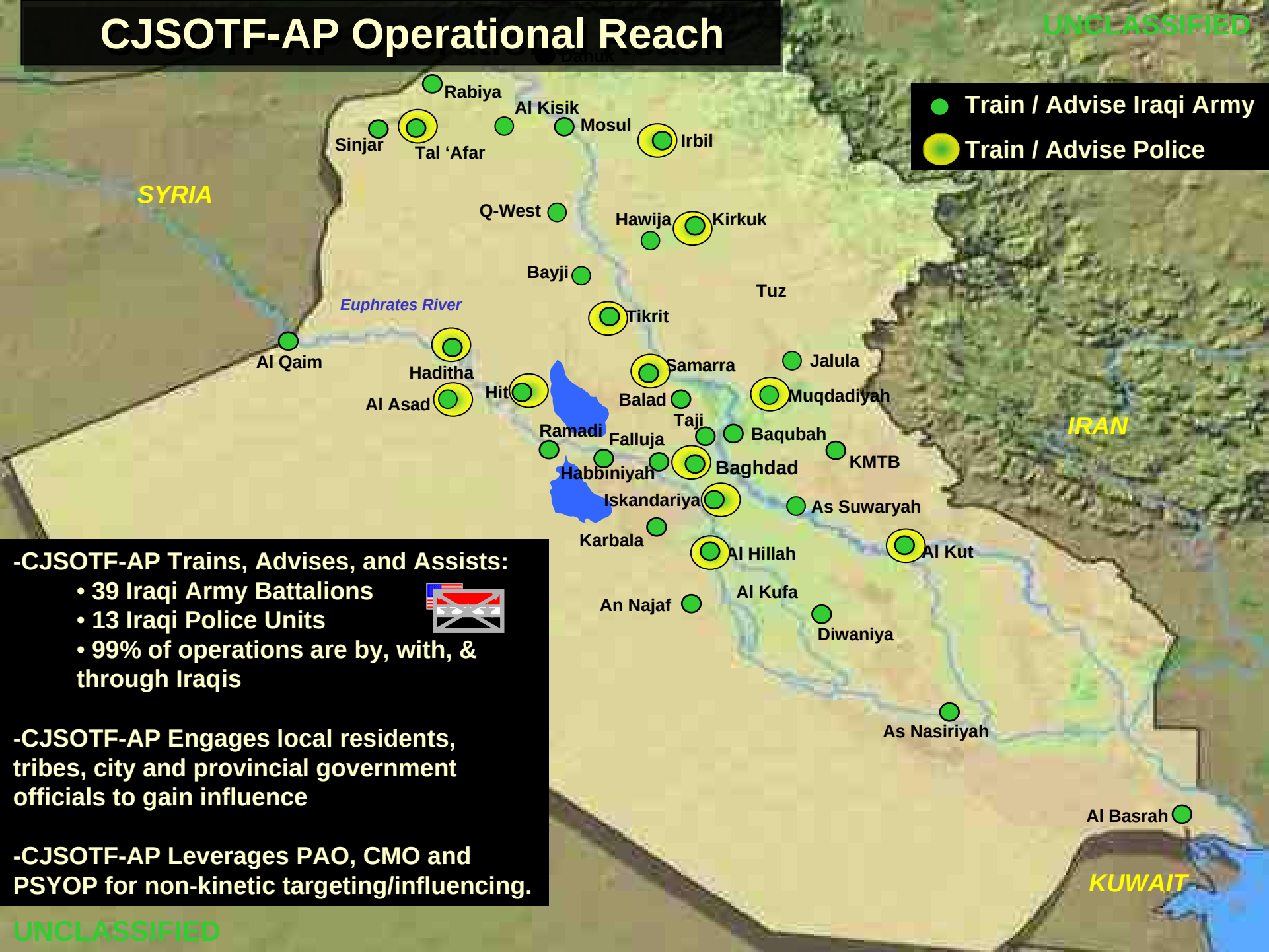
Nation over Self, Tribe, or Religious Interests





CJSOTF-AP Operational Reach

UNCLASSIFIED



-CJSOTF-AP Trains, Advises, and Assists:

- 39 Iraqi Army Battalions
- 13 Iraqi Police Units
- 99% of operations are by, with, & through Iraqis

-CJSOTF-AP Engages local residents, tribes, city and provincial government officials to gain influence

-CJSOTF-AP Leverages PAO, CMO and PSYOP for non-kinetic targeting/influencing.

UNCLASSIFIED

How the CJSOTF Fights

Foreign Internal Defense in combat

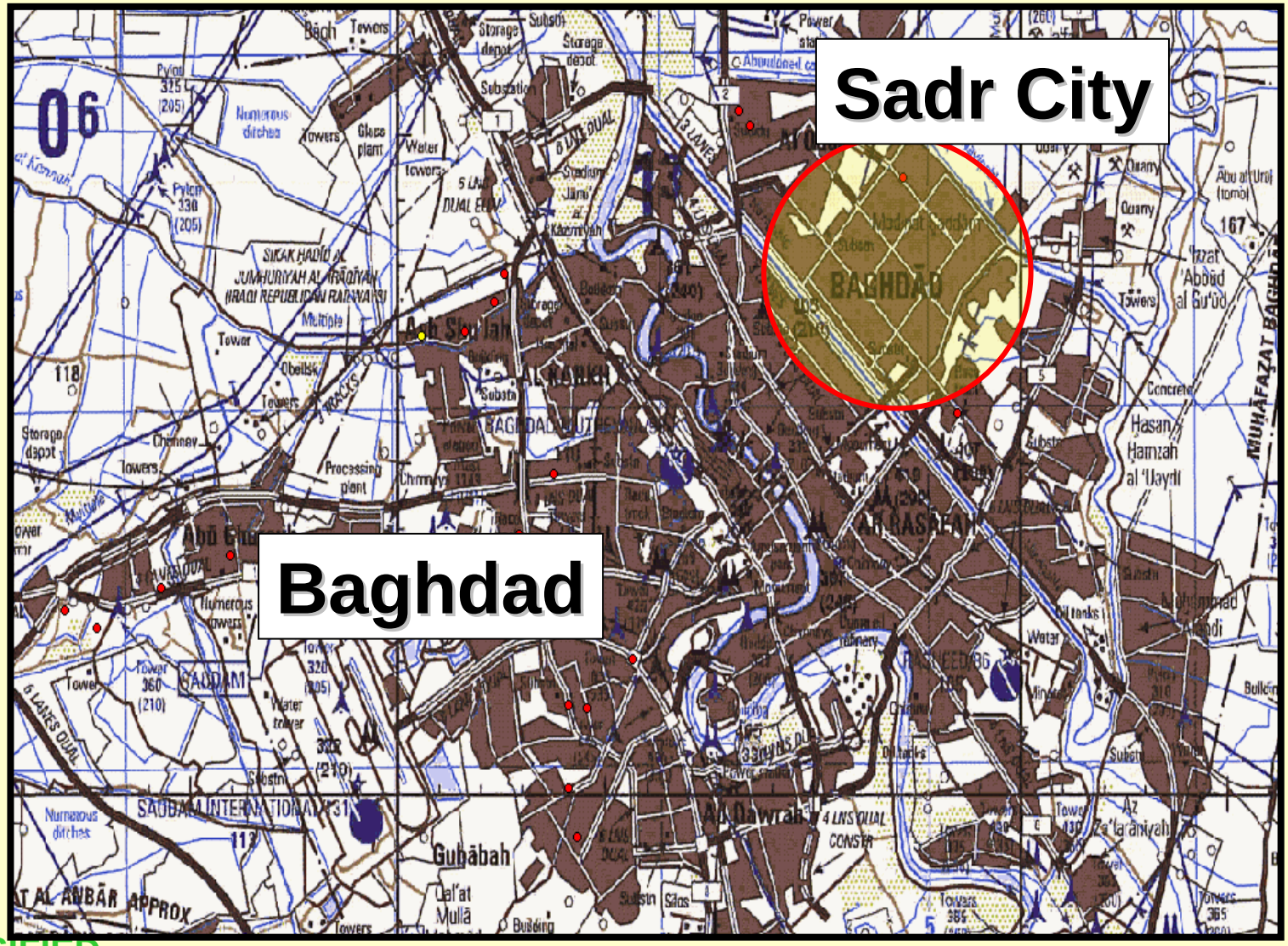
FID activity	Physical output	Effects output: messages to target audiences
Training ISF	 *Capable ISF*	Effective Cohesive Values Based
Targeting	 *Precision collection* *Find the enemy*	Vigilant Precise Culturally attuned
Combined Ops	 *Precision operations* *Fix & finish the enemy*	Competent Evenhanded ISF in the lead

+ *Accentuate Positives*

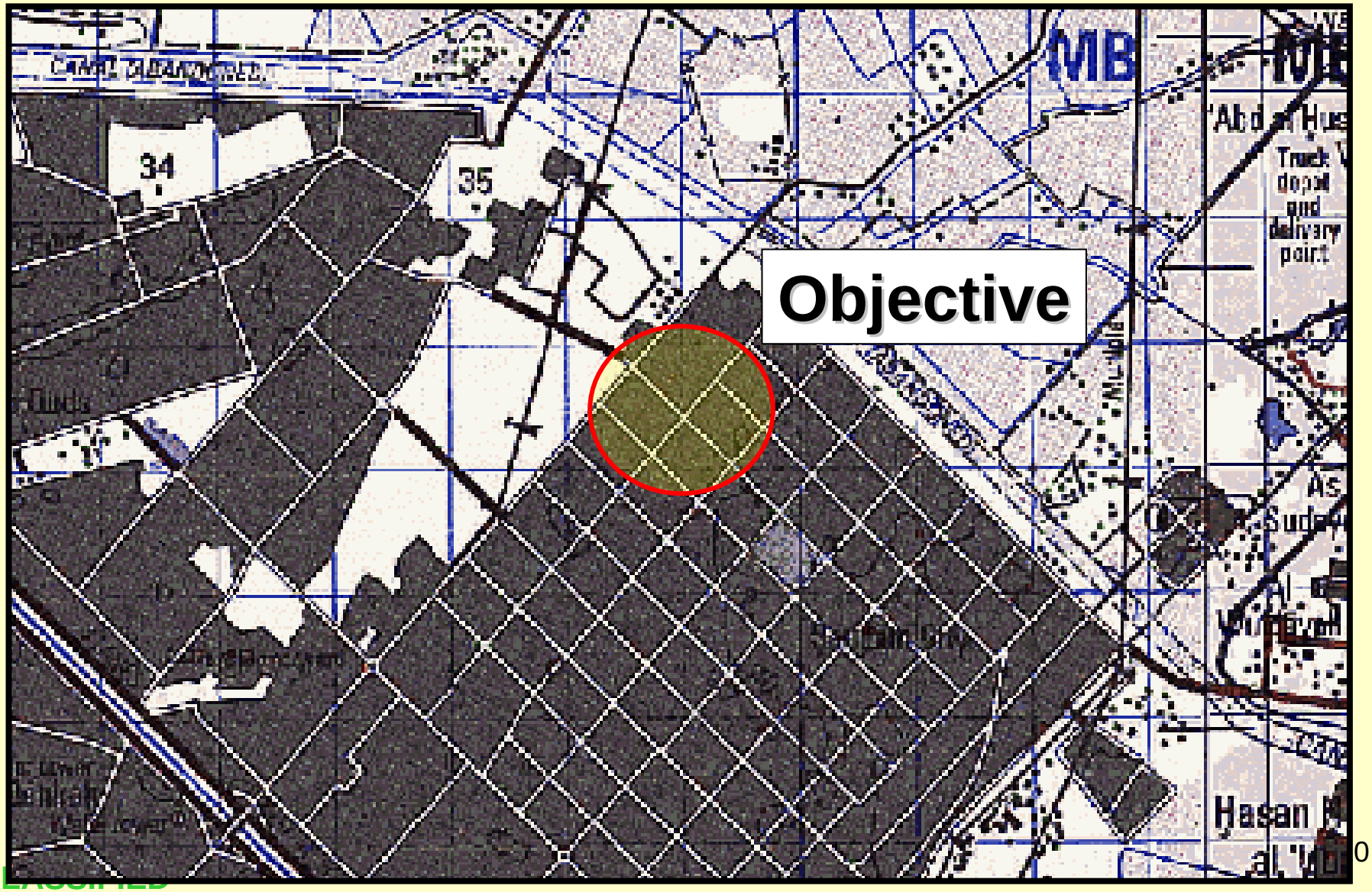
Information Operations

Mitigate Negatives −

Operational Vignette



Operational Vignette

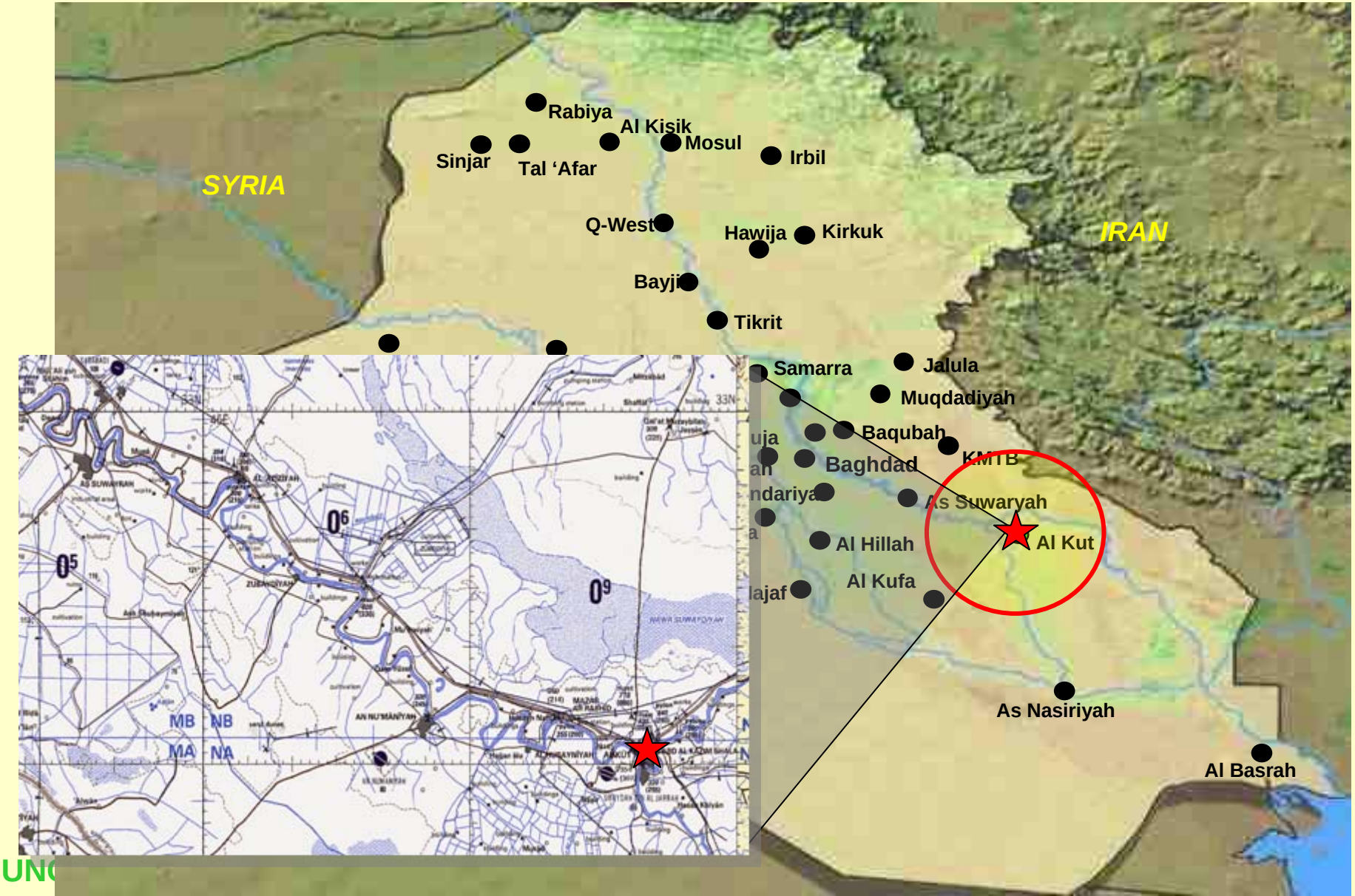


Operational Vignette

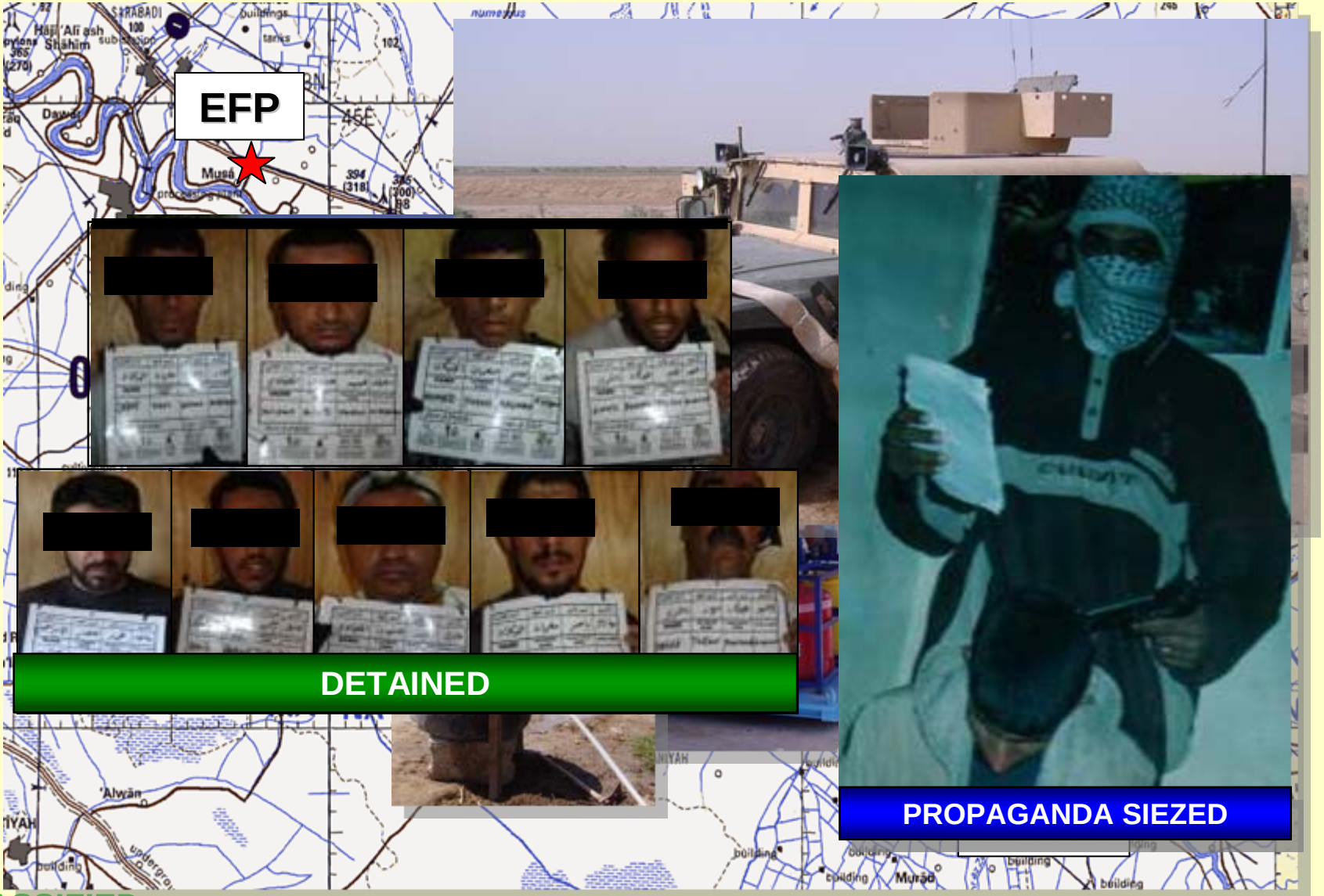


Operational Vignette

Non-Kinetic Vignette



Non-Kinetic Vignette



Summary

CJSOTF-AP's role in Iraq is three-fold:

- **Develop ISF capability to conduct COIN**
- **Neutralize insurgent capability through intelligence-driven, precision operations**
- **Employ non-kinetic enablers to achieve desired and lasting effects**

TASK FORCE LEGION



Back-up Slides

CJSOTF-AP "EKG" Model



Effective Targeting Through Time

HVI

-Facilitators
-Financiers
-Enablers
-C2
-Cell Leaders
-Network
Critical Path

Soldiers
Cell Members
Infrastructure

Prosecution of mid-level targeting develops actionable intelligence on network leaders

Network

Leader

Facilitator

Facilitator

Focus on cell leaders and high level facilitators IOT isolate network subsets and effectively disrupt networks

Leader

Facilitator

Facilitator

Network Subset

Technician

Technician

DA Soldier

Continue CJSOTFAP Targeting Methodology

Leader

Leader

Once triggers are exhausted, target cell members IOT drive intelligence for follow on operations

Cell 1

Cell 2

DA Soldier

DA Soldier

Technician

Facilitator

Facilitator

Technician

DA Soldier

DA Soldier

Targeting Vignette



AQIZ Leadership

HVIs

CJSOTF
Net. Subset C2, Tech, Fin, Fac

MNDs
Soldiers, Cell Members

Leader
Leader
Leader
Leader
Leader
Facilitator/ Financier
Facilitator
Facilitator
Facilitator
IED Tech
DA IED

AQIZ moves in new leadership, facilitators and soldiers to rebuild the network subset. New group lacks sophisticated GSM IEDs, despite increase in IEDs detonated, significantly lower casualties; effectiveness is 1 in 9.

IEDs Detonated
IEDs Effective

CJSOTFAP Targeting Results:
- 16 ops over 5 months
- 37 detainees
- Disruption of Abu Ghurayb AQIZ affiliated IED network subset.

Prior to C… Ghuray… activity, … against … advanced IED devices.

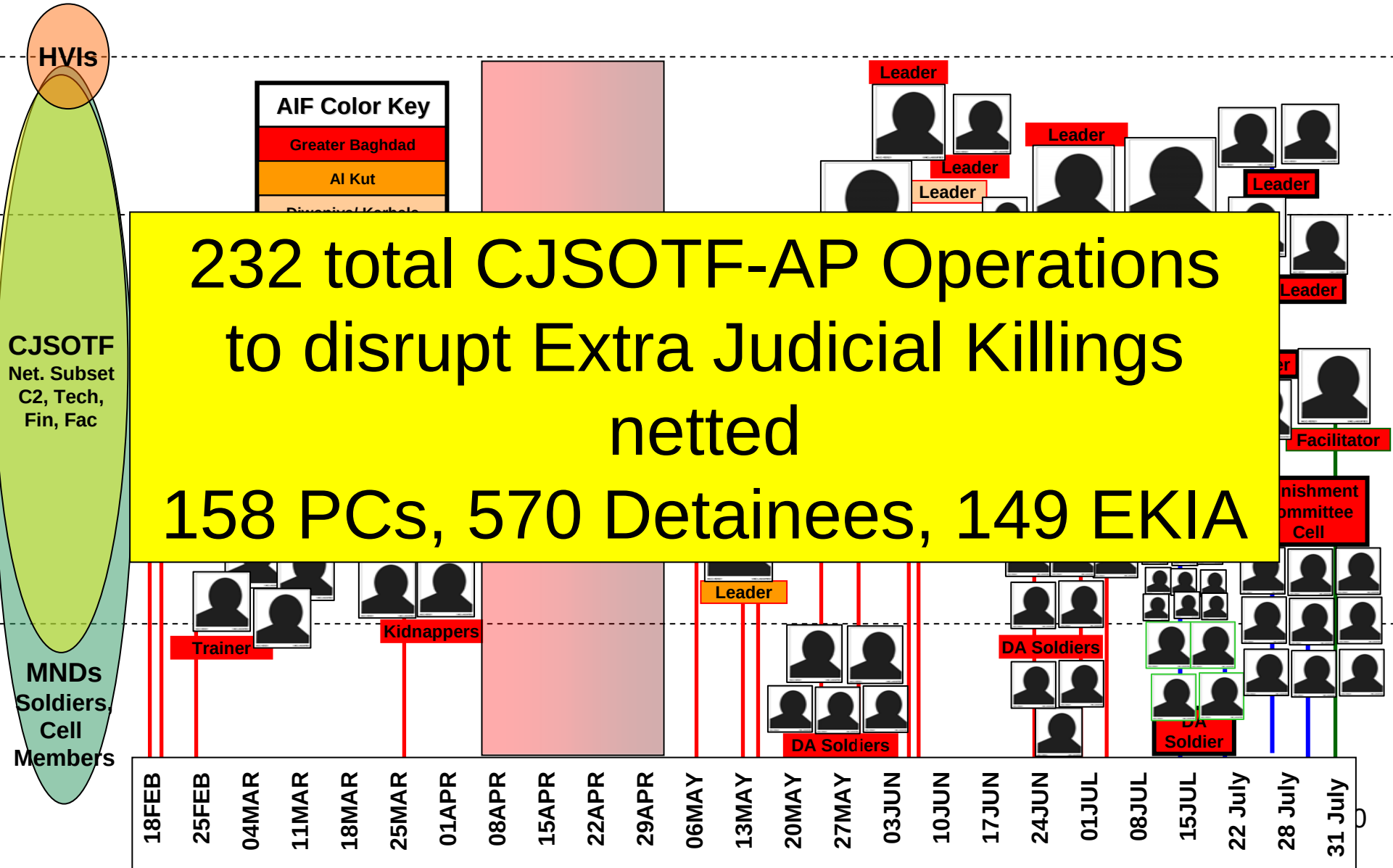
Follow … AQIZ IE… immediate reduction in detonated IEDs.

CJSOTFAP continues to develop and action targets.

20
18
16
14
12
10
8
6
4
2
0

28JAN 04FEB 11FEB 18FEB 25FEB 04MAR 11MAR 18MAR 25MAR 01APR 08APR 15APR 22APR 29APR 06MAY 13MAY 20MAY 27MAY 03JUN 10JUN 17JUN 24JUN 01JUL 08JUL 15JUL 22JUL 29JUL

CJSOTF-AP Operations to disrupt Extra-Judicial Killings (EJK)



232 total CJSOTF-AP Operations to disrupt Extra Judicial Killings netted

158 PCs, 570 Detainees, 149 EKIA

Operational Vignette



Operational Vignette



Operational Vignette





Operational Vignette

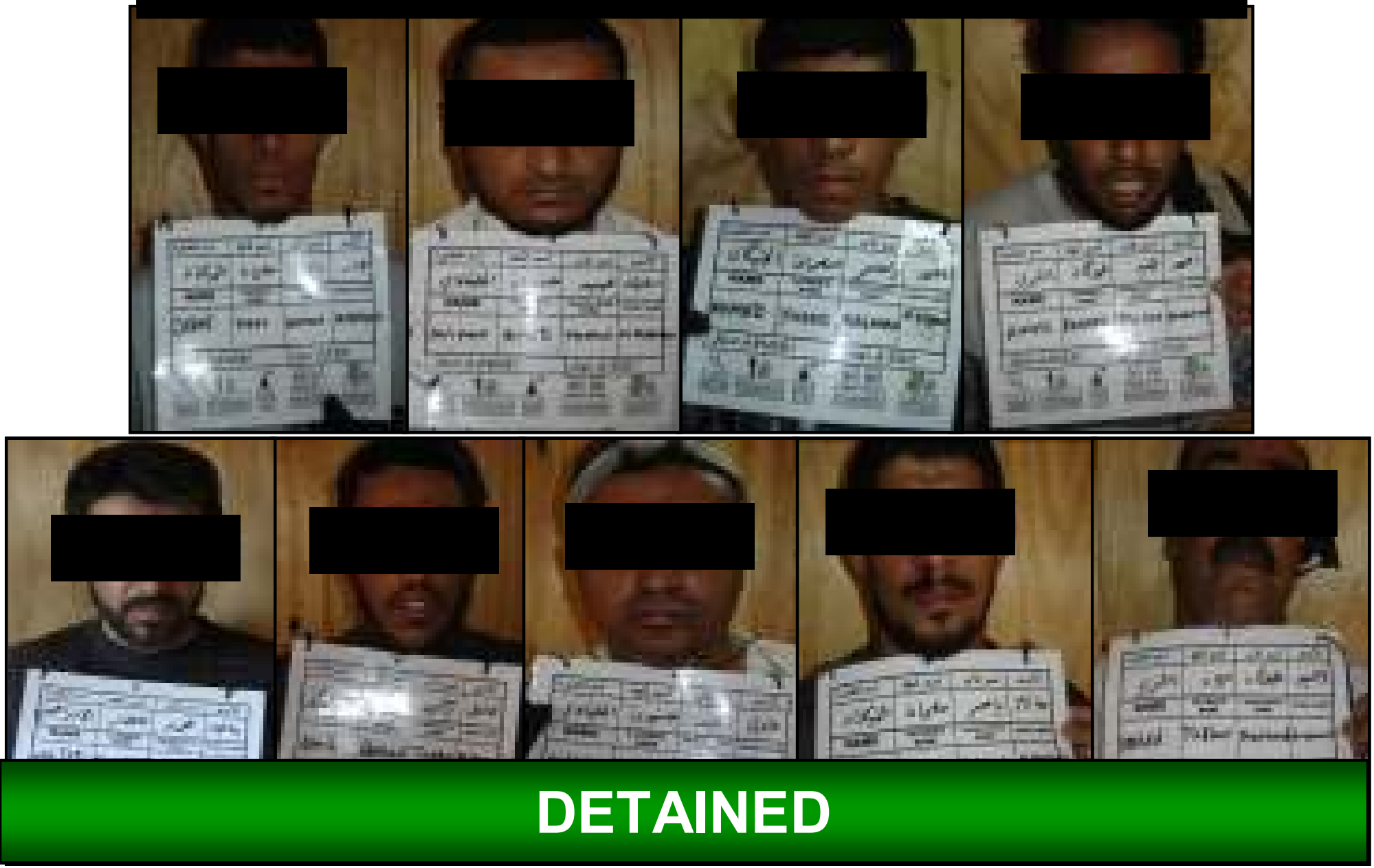


Operational Vignette








DETAINED

TRIPLE CANOPY



Warfare in the Seams

Industry Vignettes

18th Annual SO/LIC Symposium and Exhibition
February 27, 2007

Overview

One man's take on War in the Seams:

Sun Tzu circa 400 BC



"So in war, the way is to avoid what is strong and to strike at what is weak."

"If the enemy is superior in strength, evade him. If his forces are united, separate them. Attack him where he is unprepared; appear where you are not expected."

Know Your Enemy

"We are not fighting so that you will offer us something. We are fighting to eliminate you."

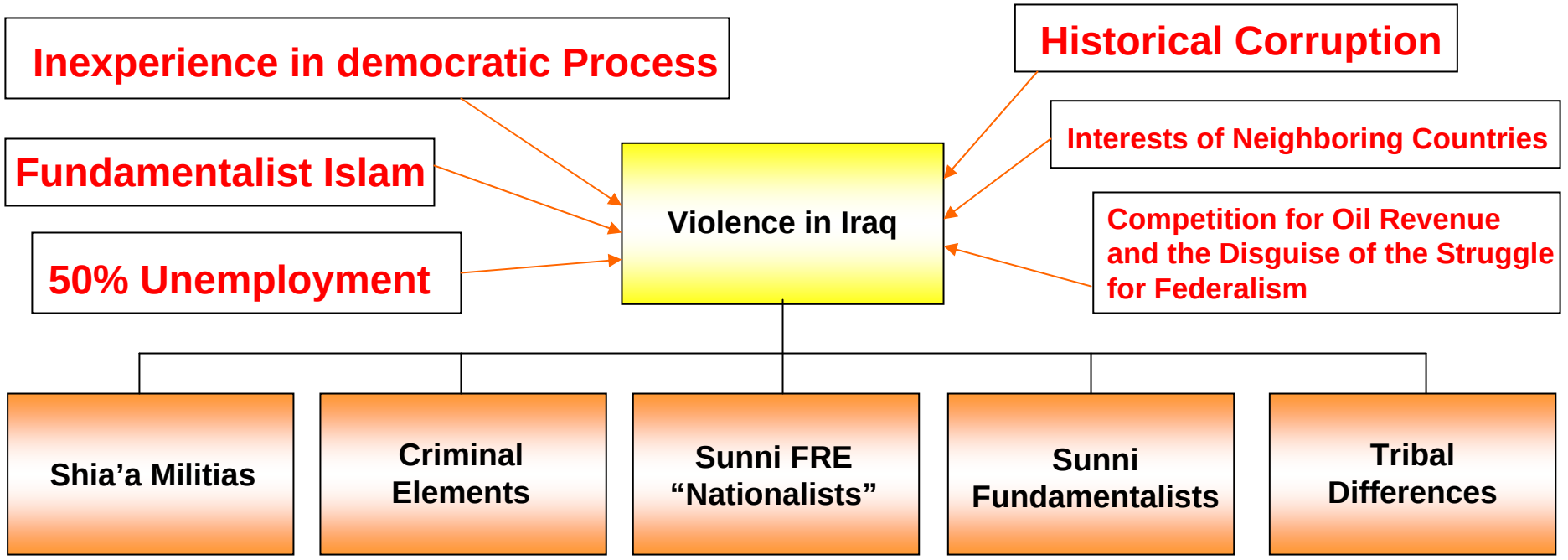
-Hussein Massawi

Former Hezbollah leader

In 1648, the Treaty of Westphalia provided the state with a monopoly on the use of organized violence

Such is no longer the case

Forces Behind Iraq Instability



Defense and Industry Partnering to Win

GEN. PETRAEUS: You then should add in tens of thousands of additional forces that are over there; that provide, of all things, contract security for our embassy... and that frees up uniformed forces to perform other missions.

SEN. PRYOR: Just for the sake of clarity, when you talk about a counterinsurgent, are you talking about anybody that's on our side? I mean, it could be the Iraqi police, obviously, the Iraqi army, obviously, other Iraqi security forces.

GEN. PETRAEUS: That's correct. Yes, sir.

SEN. PRYOR: But it could also be contractors?

GEN. PETRAEUS: If they're performing security functions, yes, sir.

Types of Asymmetric Threats

- Terrorism
- Technology
- Deception
- Disinformation
- Misinformation
- Time
- Guerilla Warfare
- Will
- Training
- Tactics
- Terrain
- Values

Baghdad IZ Checkpoint



Baghdad IZ Checkpoint (Cont)



Office in Basrah



Basrah Checkpoint



Basrah Checkpoint (Cont)



Iraq Concept of Shame and Honor

Shame and Honor

- Govern individual, group relationships and competition. Honor is defined differently in Iraq.
- Honor is exchanged like currency but is not for sale; most valued of resources eclipsing money, jobs and influence.
- Zero-sum exchange: Honor is gained at another's loss of honor and imposition of shame. When one is shamed, he is compelled to act to regain his honor.

Application

- Behaving as an honorable guest will often protect us and our clients, just as becoming known as shameful will often increase odds of attack.
- Important to apply cultural knowledge of shame and honor into all aspects of operational planning, assuring that our clients are respected, and thus protected, whenever possible.

Iraq Culture

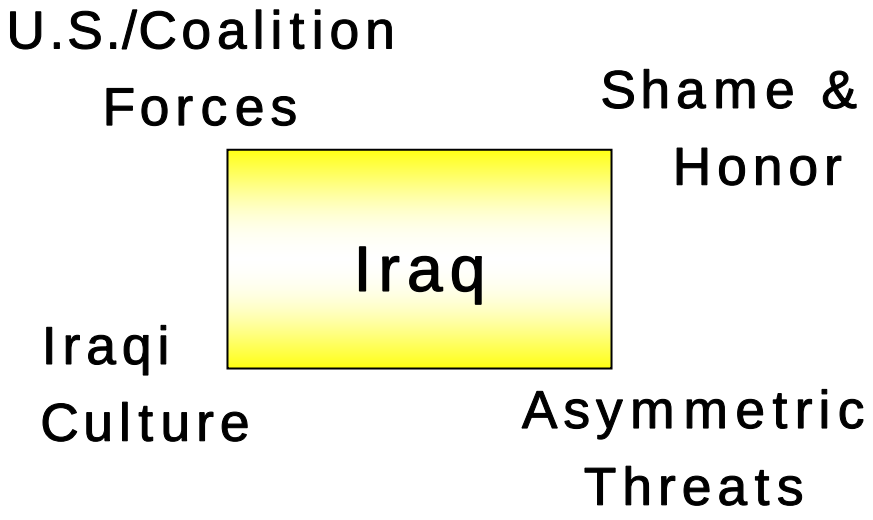
Diverse Traditions

- Iraq behavior is dictated by complex rules combining 3,000 year-old tribal tradition, Sharia (Islamic Law), pre-Saddam civil law, and post-Saddam civil law. Knowing which group adheres to which laws is critical in navigating throughout the country.

Relationships

- *Always* a direct relationship between a large company, a dominant tribe, a politician, an influential cleric and a paramilitary force.
- Though the current strife between Shiites and Sunnis is very real, it does not follow that they have always been at war or always will be. Many tribes have both Shia and Suni members and many continue to inter-marry, though admittedly very quietly these days.

Conclusion


U.S./Coalition Forces
Shame & Honor
Iraq
Iraqi Culture
Asymmetric Threats

Stand-off Nuclear Radiation Detection

Peter E. Vanier
Detector Development and Testing Div.
Nonproliferation and National Security Dept.
Brookhaven National Laboratory

Presented at the
18th Annual NDIA
Special Operations / Low Intensity Conflict
Symposium and Exhibition
Hyatt Crystal City
February 26 –28, 2007

Brookhaven Science Associates
U.S. Department of Energy

BROOKHAVEN
NATIONAL LABORATORY

BROOKHAVEN NATIONAL LABORATORY SITE



BROOKHAVEN
NATIONAL LABORATORY

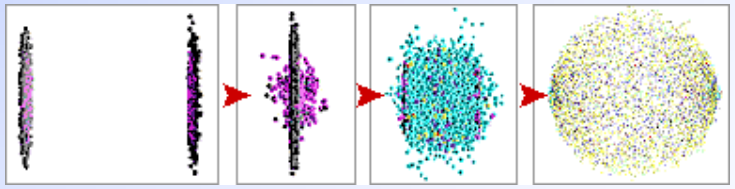


BROOKHAVEN NATIONAL LABORATORY

Camp Upton



- **Established in 1947 on Long Island, Upton, New York, Brookhaven is a multi-program national laboratory operated by Brookhaven Science Associates for the U.S. Department of Energy (DOE).**
- **Six Nobel Prizes have been awarded for discoveries made at the Lab.**
- **Brookhaven has a staff of approximately 3,000 scientists, engineers, technicians and support staff and over 4,000 guest researchers annually.**
- **Brookhaven National Laboratory's role for the DOE is to produce excellent science and advanced technology with the cooperation, support, and appropriate involvement of our scientific and local communities.**



Collision of gold nuclei at RHIC

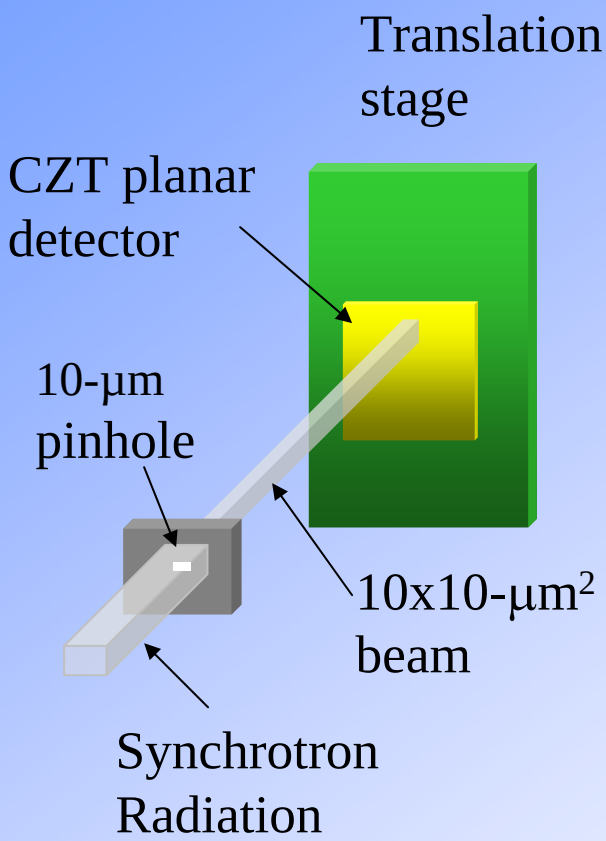
BROOKHAVEN NATIONAL LABORATORY

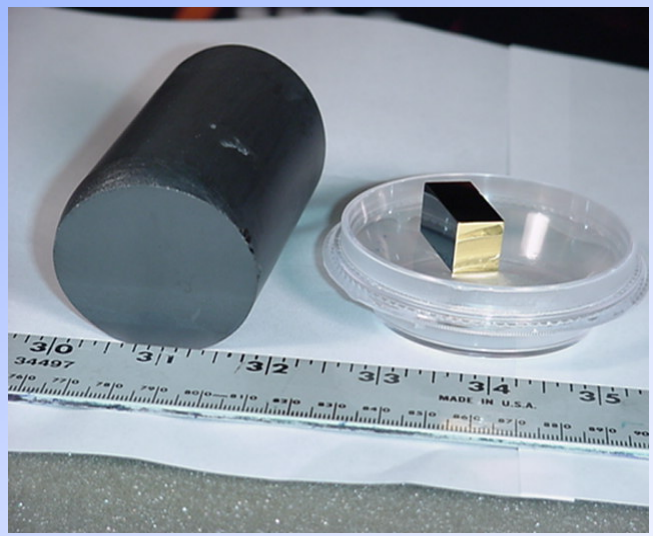
Lab work with Industry:
Radiation Portal Monitor Testing and Evaluation

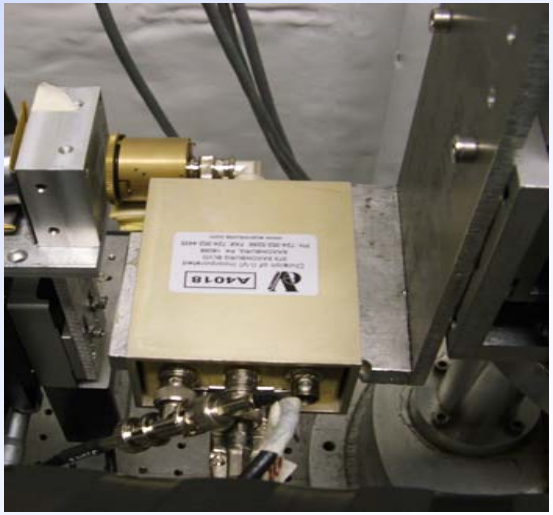


BROOKHAVEN
NATIONAL LABORATORY

Lab work with Industry:
Cadmium Zinc Telluride material evaluation



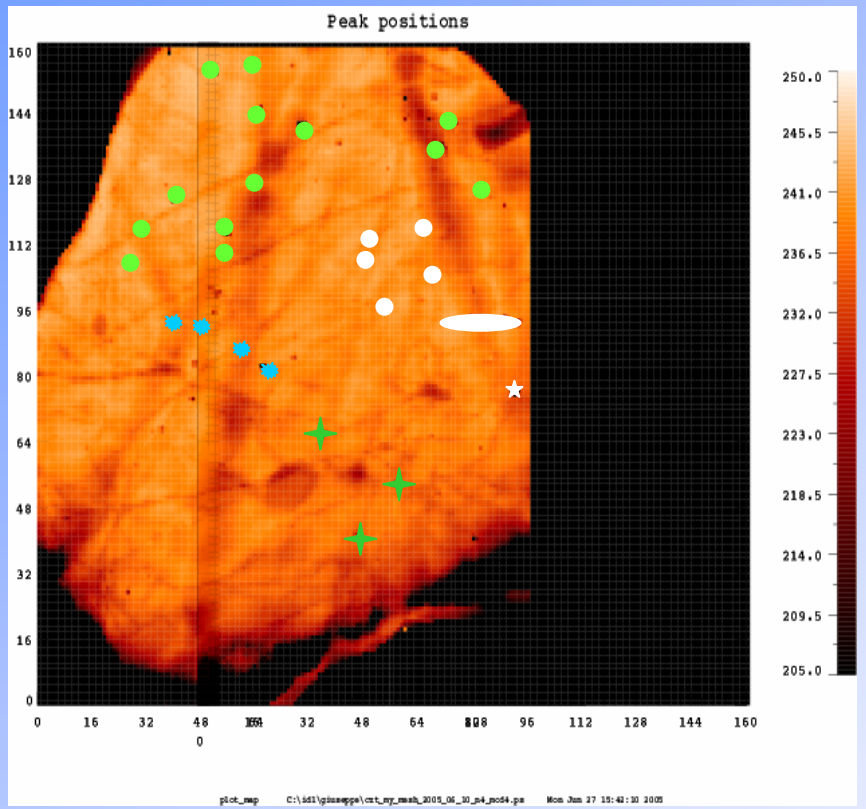


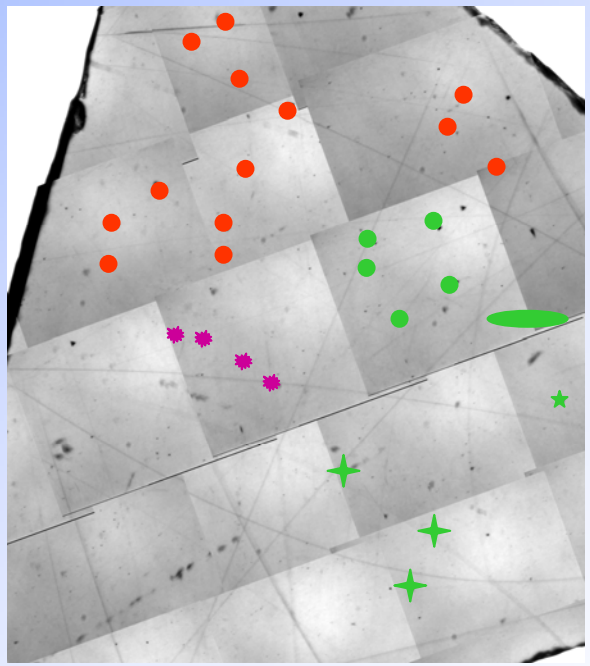


Correlations between x-ray map & IR image

This x-ray map shows the degraded regions precisely correspond to Te precipitates on the right

This IR image shows Te precipitates, which could be identified by shape with IR microscope

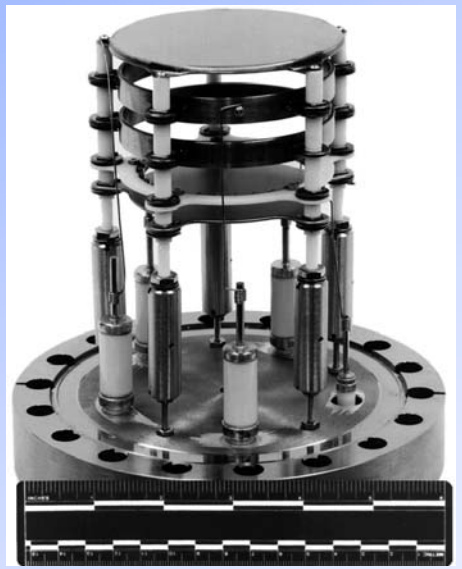




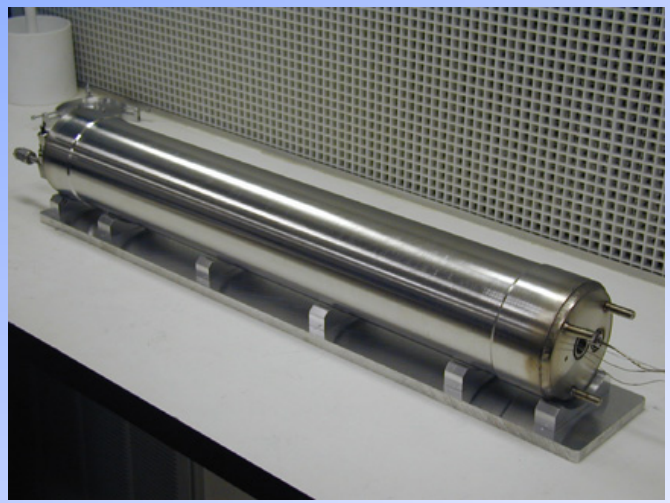
100% correlations were found for all CZT samples tested in this work.

Lab Work with Industry – Compressed Xenon Spectrometers

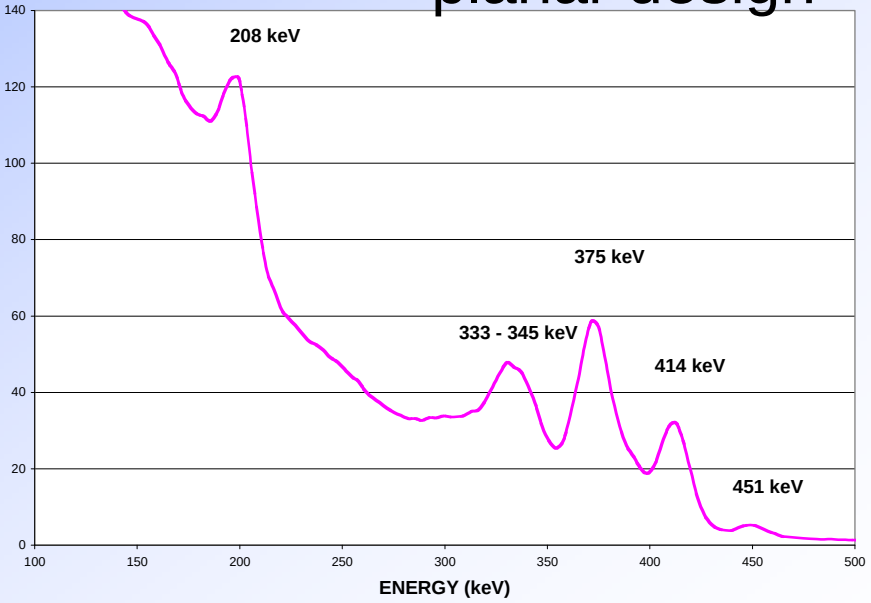
- Operate at room temperature
- Sufficient resolution to identify isotopes
- Scalable to large volumes - increased sensitivity
- Identify special nuclear materials
- Allow passage of medical isotopes
- Allow naturally occurring radioactive materials
- Reduce false positive rate



planar design



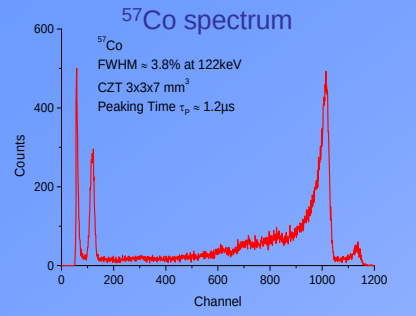
CTC coaxial design

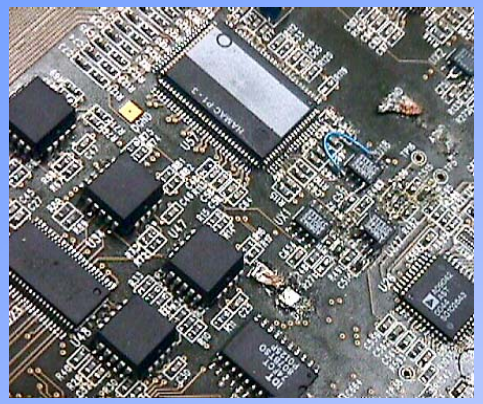


Pu-239 spectrum using xenon

BROOKHAVEN NATIONAL LABORATORY

High-speed, radiation-tolerant sampling/digitizing board

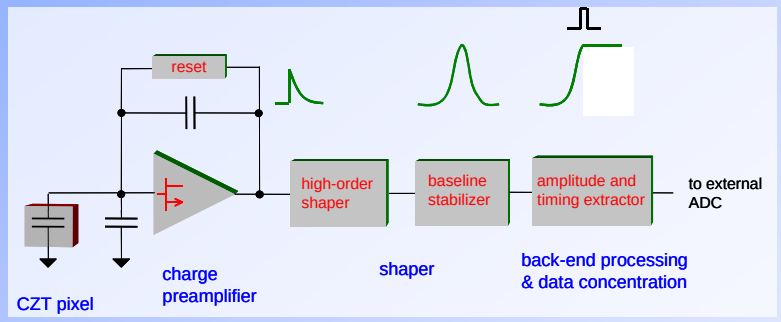






240-channel multichip module for Si drift detector readout

Low-power ASICs



Preamplifier/shaper ASIC block diagram

Microelectronics Group

AREAS OF EXPERTISE

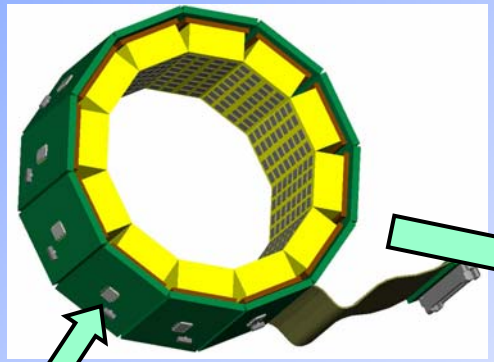
- CMOS monolithic circuits
- charge-sensitive sensor interface
- analog signal processing
- low noise, low power techniques
- VLSI custom design + layout

National Security

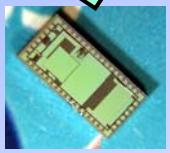
Handheld imaging probe for gamma radiation



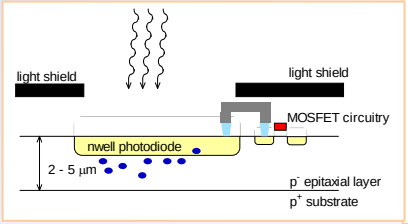
Gamma Imaging



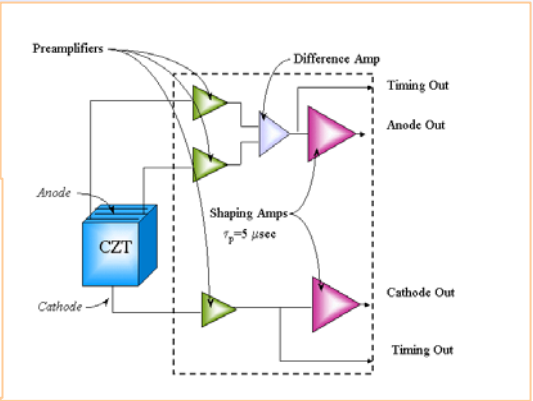




Positron emission tomograph for imaging the awake animal brain



Radiation sensitive pixel readout

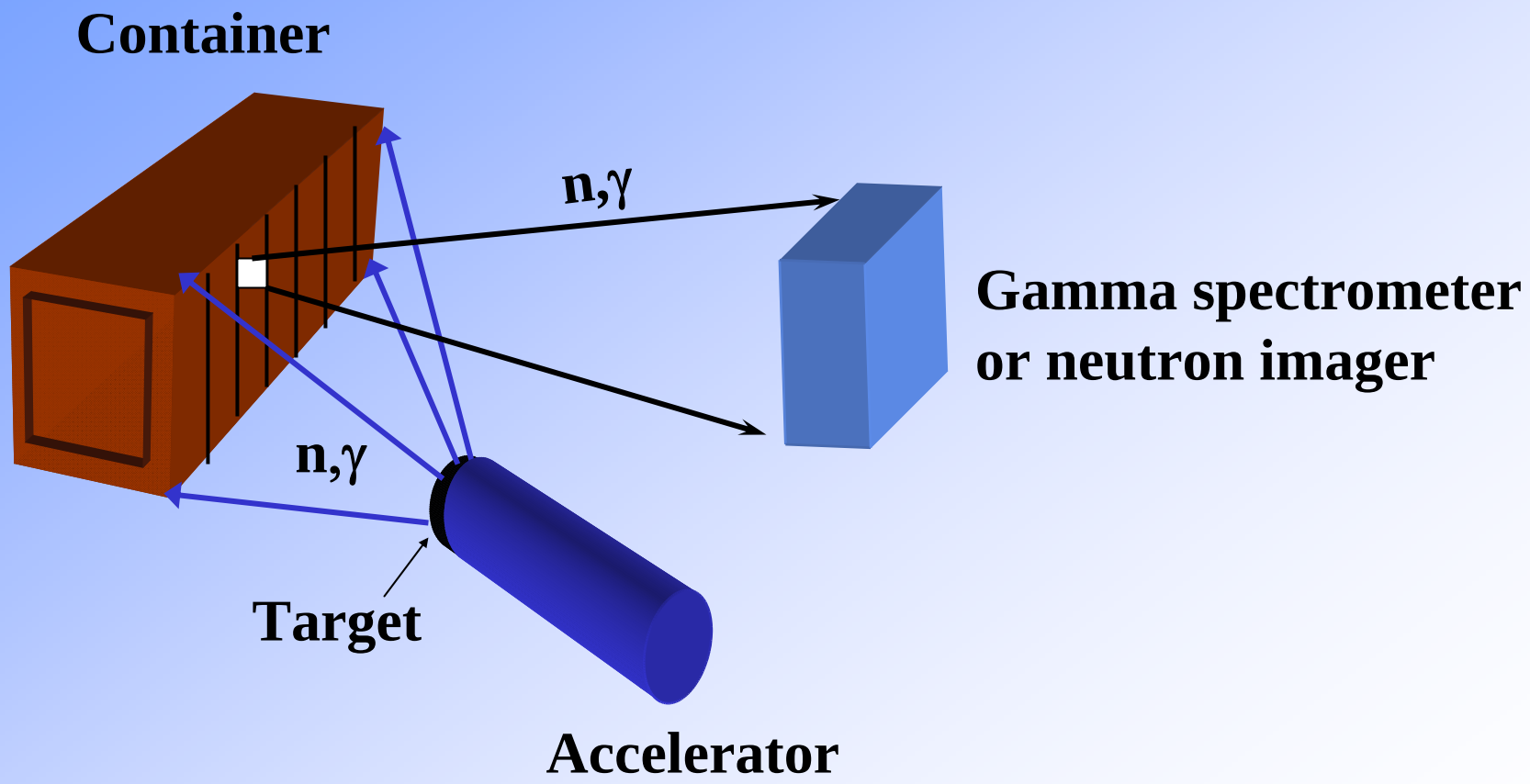


Gamma spectrometer for detection of nuclear materials

Technology investment by BNL that can be helpful in solving SOLIC challenges

- Assume that terrorists will use any means to get attention, including radioactive materials
- Develop of new radiation detectors
  - Gamma spectrometers
  - **Neutron imagers**
- Improve interdiction of radioactive materials traffic
  - Force protection from Radiation Dispersal Devices
  - Force protection from Improvised Nuclear Devices

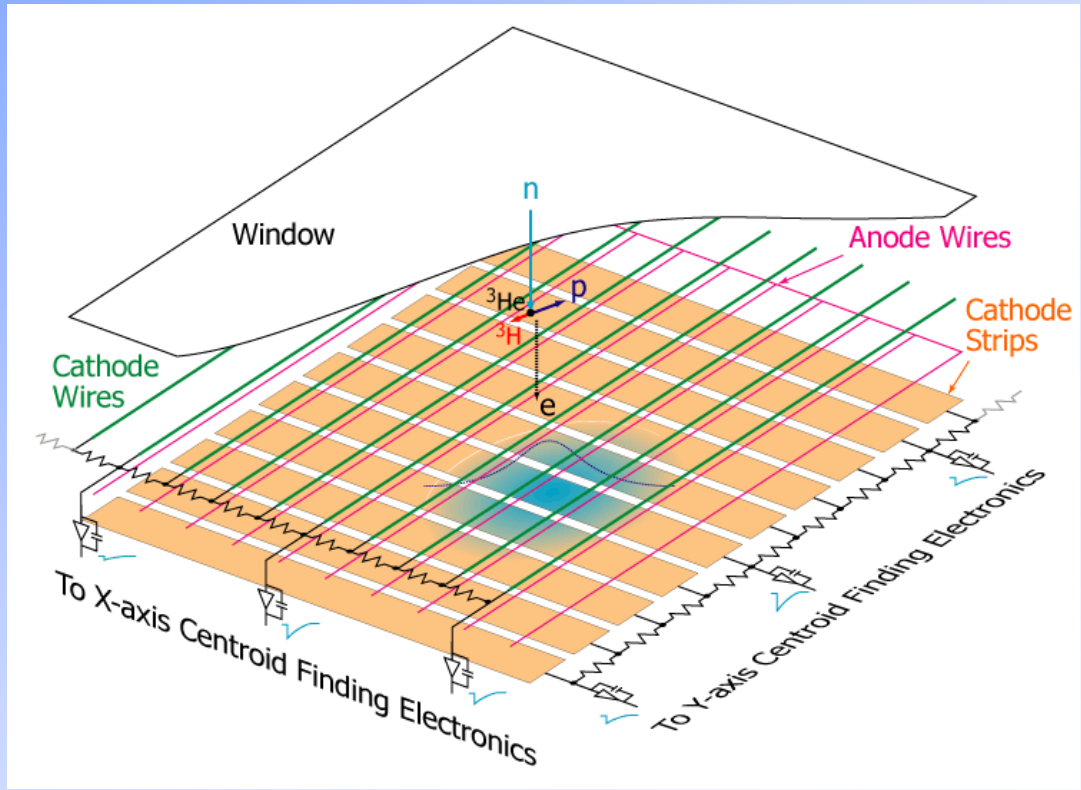
Interrogation of containers and trucks

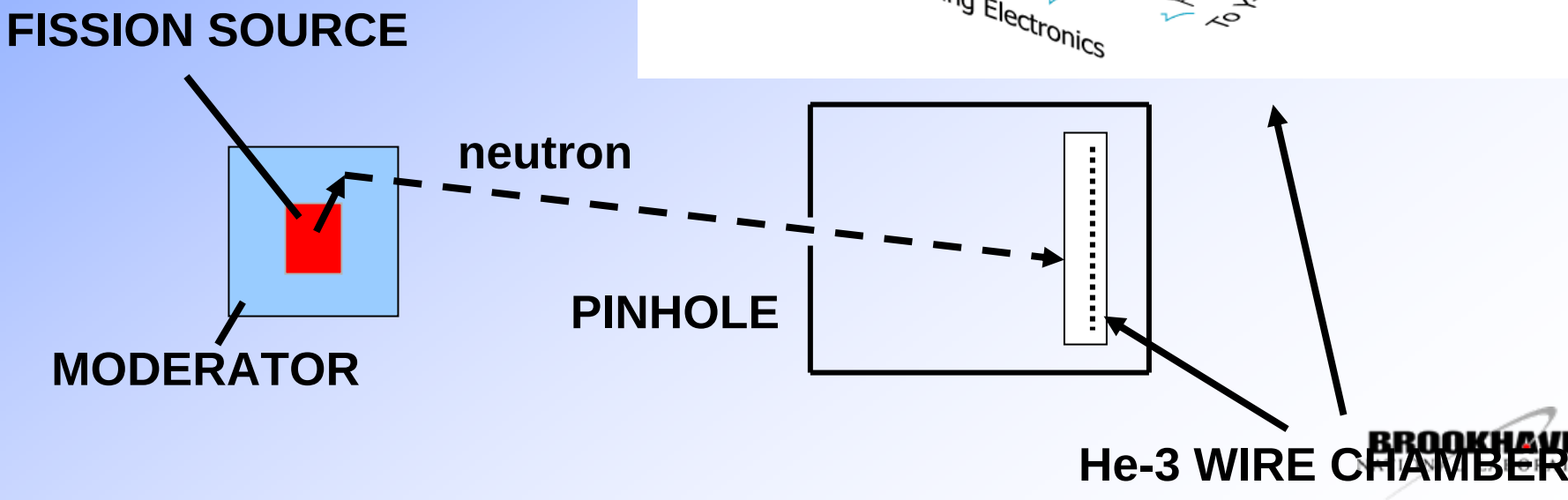


BROOKHAVEN
NATIONAL LABORATORY

Directional Detection and Imaging

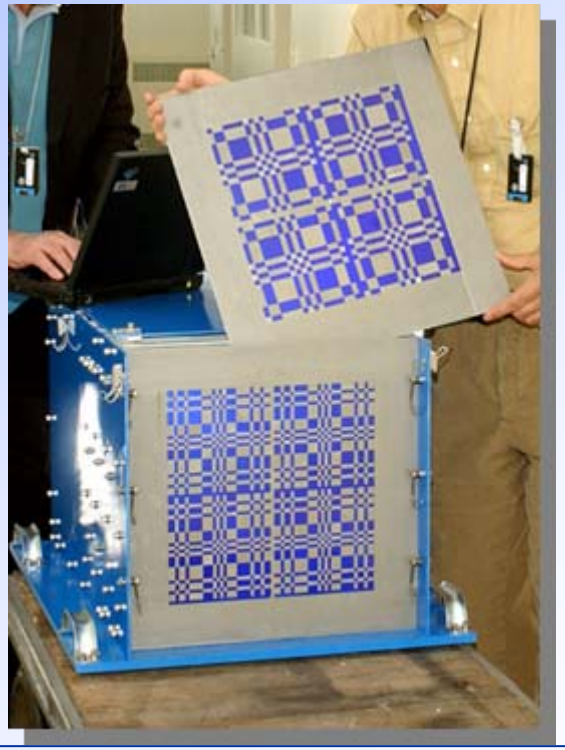
- Pinhole camera
- Poor sensitivity





Thermal Neutron Imager

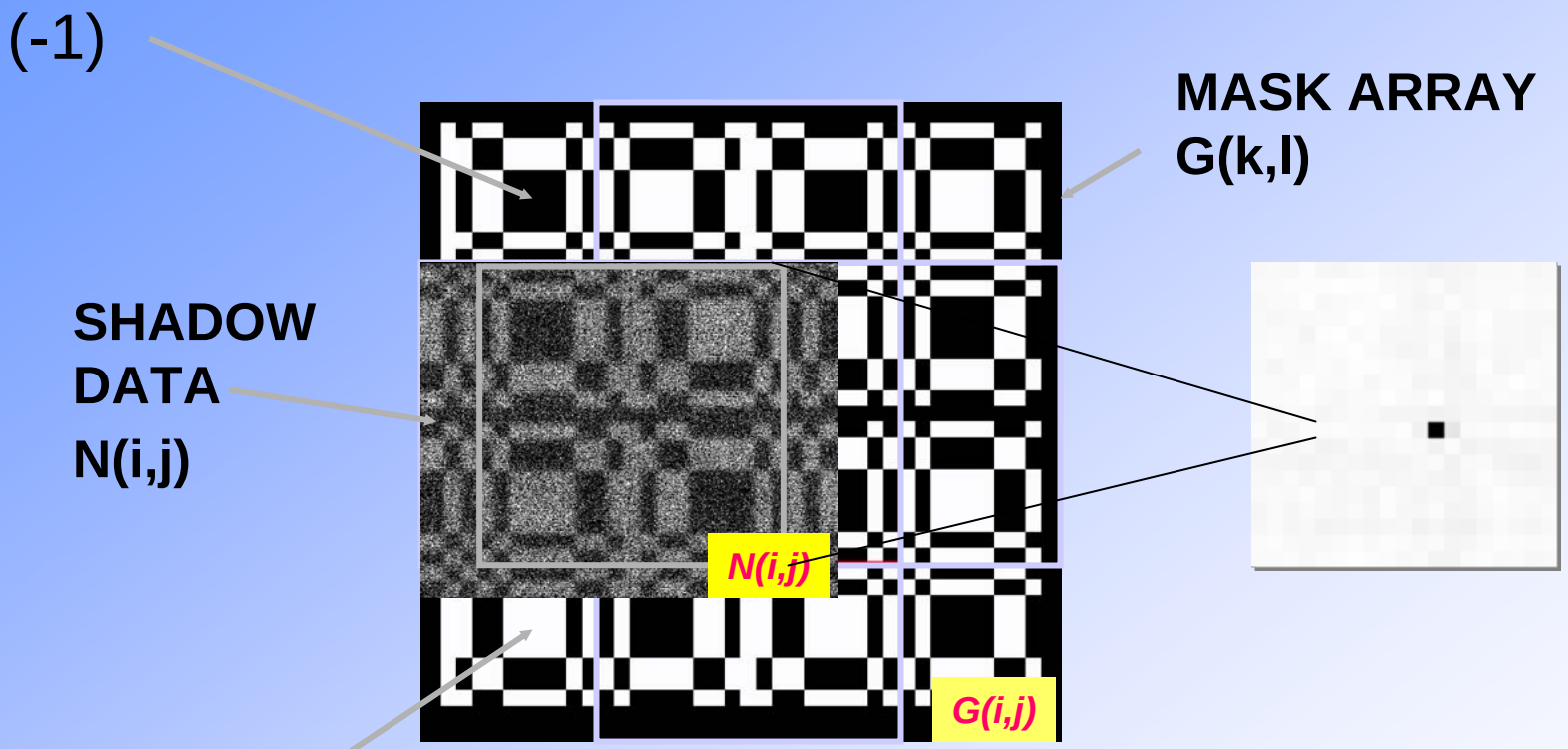




4. Cadmium-lined
coded aperture camera

BROOKHAVEN
NATIONAL LABORATORY

Reconstructing the image from the shadowgram

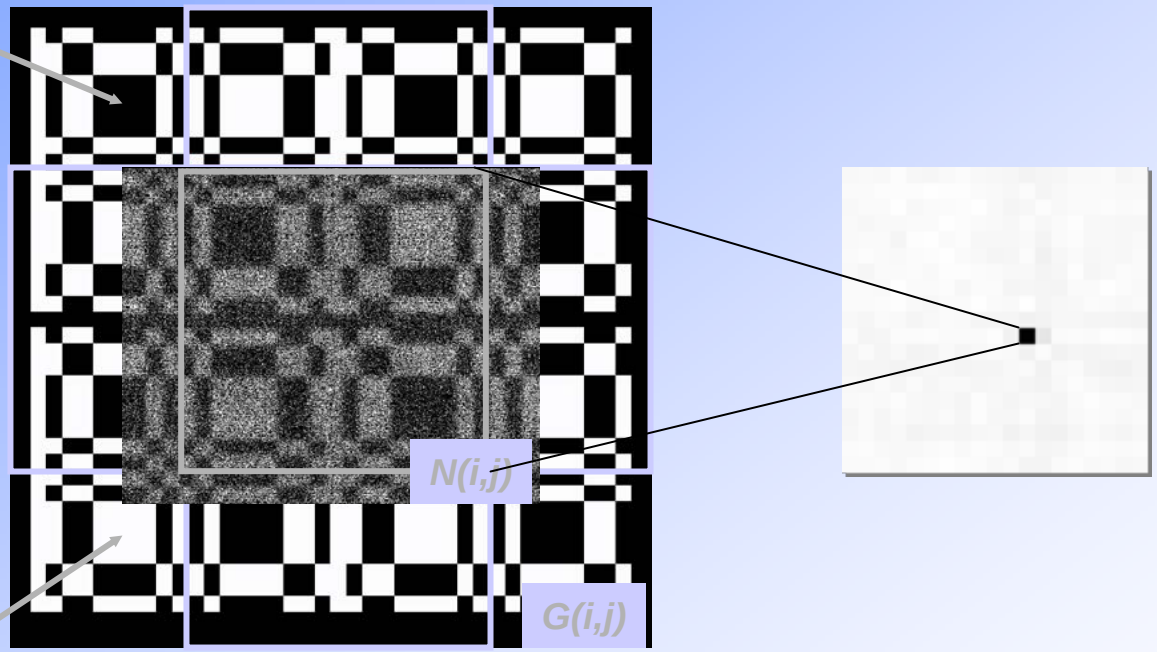


$$R(k,l) = \sum_{i=1}^{r}\sum_{j=1}^{r} N(i,j)G(k+i,l+j)$$

BROOKHAVEN
NATIONAL LABORATORY

Reconstructing the image from the shadowgram

(-1)



(+1)

$$R(k,l) = \sum_{i=1}^{r}\sum_{j=1}^{r} N(i,j)G(k+i,l+j)$$

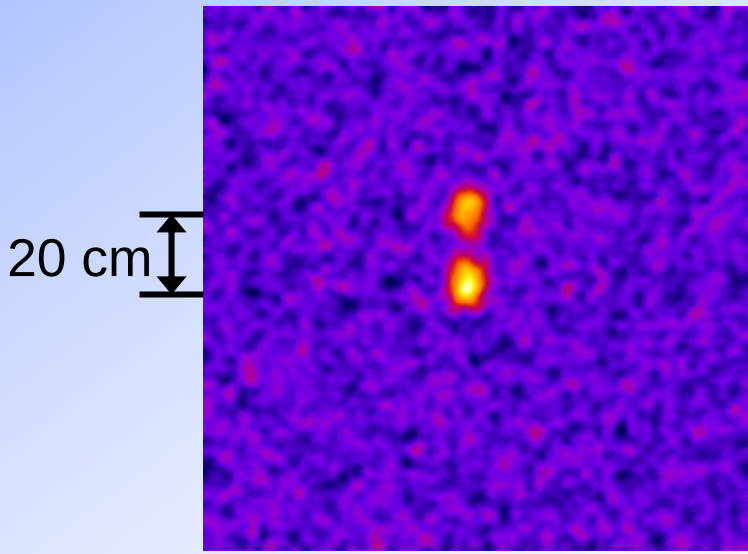
Actually, use Fast Fourier Transforms

BROOKHAVEN
NATIONAL LABORATORY

Lab test of imaging capability



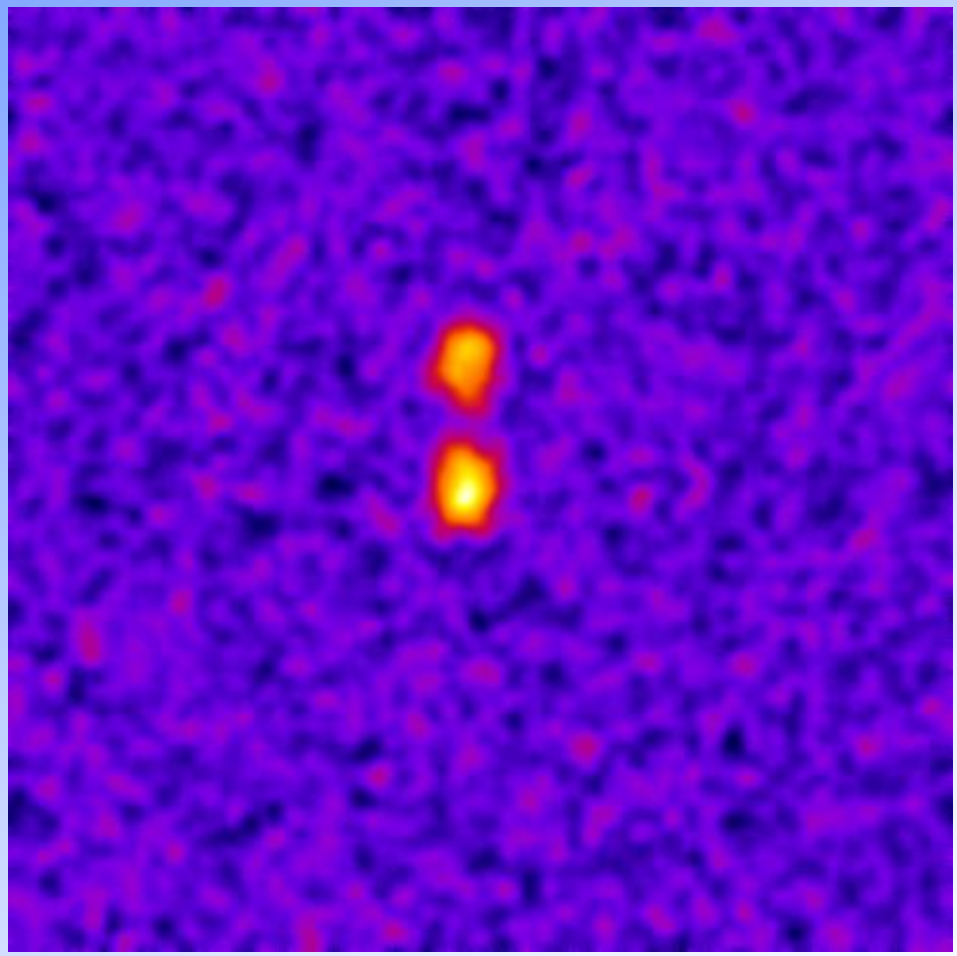
R = 300 cm, f = 30 cm



Neutron image

Three 10-cm cubes of polyethylene, with two Cf-252 sources embedded (courtesy of A. Caffrey, INL)

Neutron image



R = 300 cm, f = 30 cm

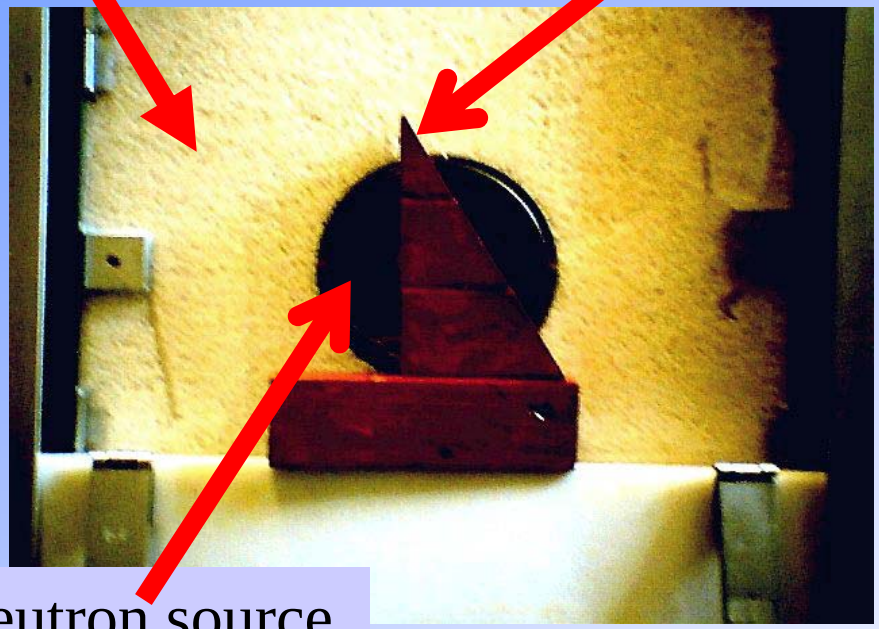
BROOKHAVEN
NATIONAL LABORATORY

Tests in the lab

Photograph

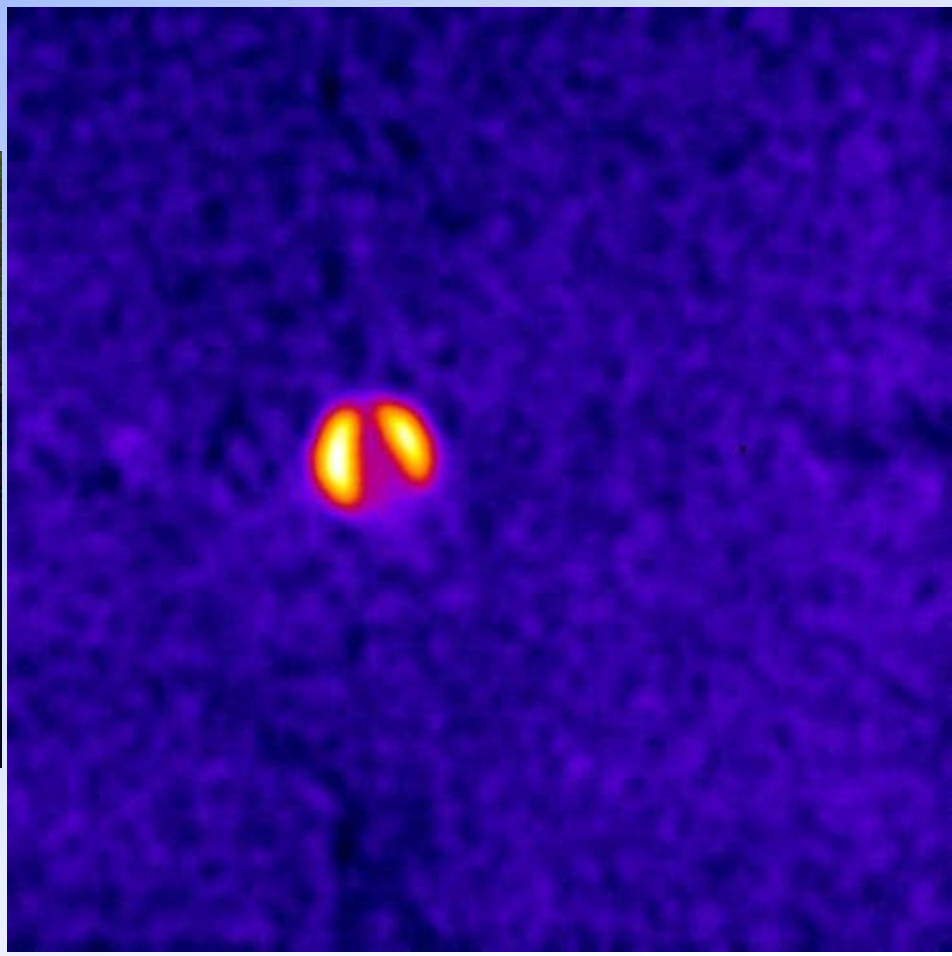
BPE Shielding

Wooden wedge



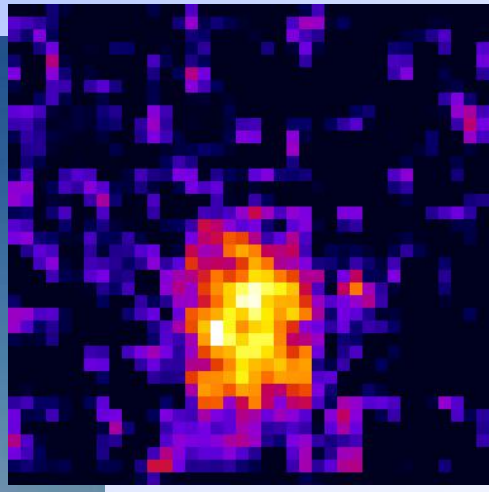
Neutron source behind paraffin cylinder

Neutron Image



Tests in the field



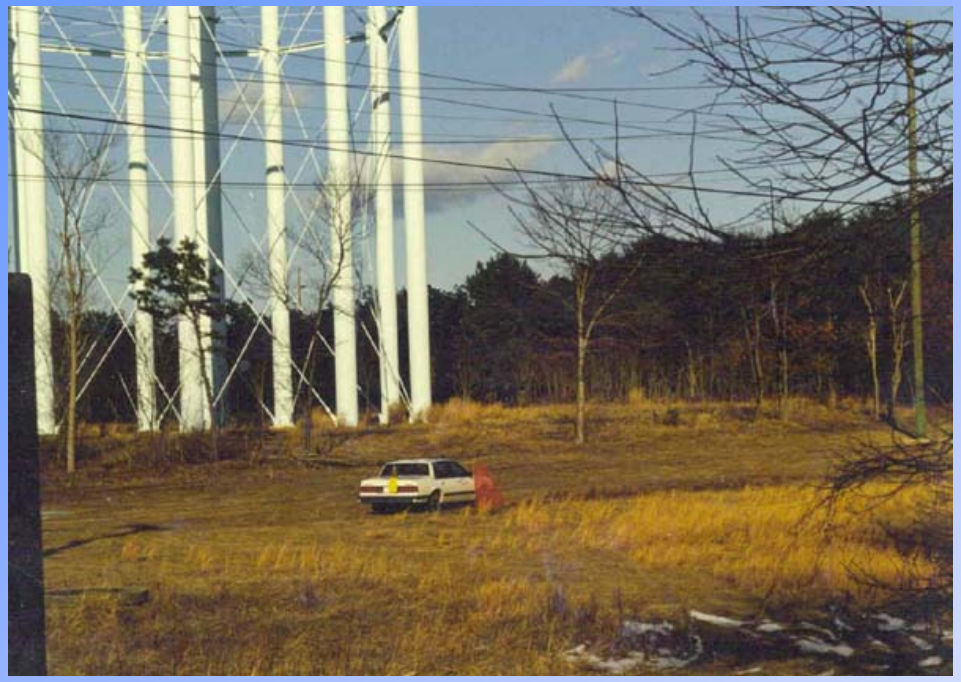


Thermal neutron image

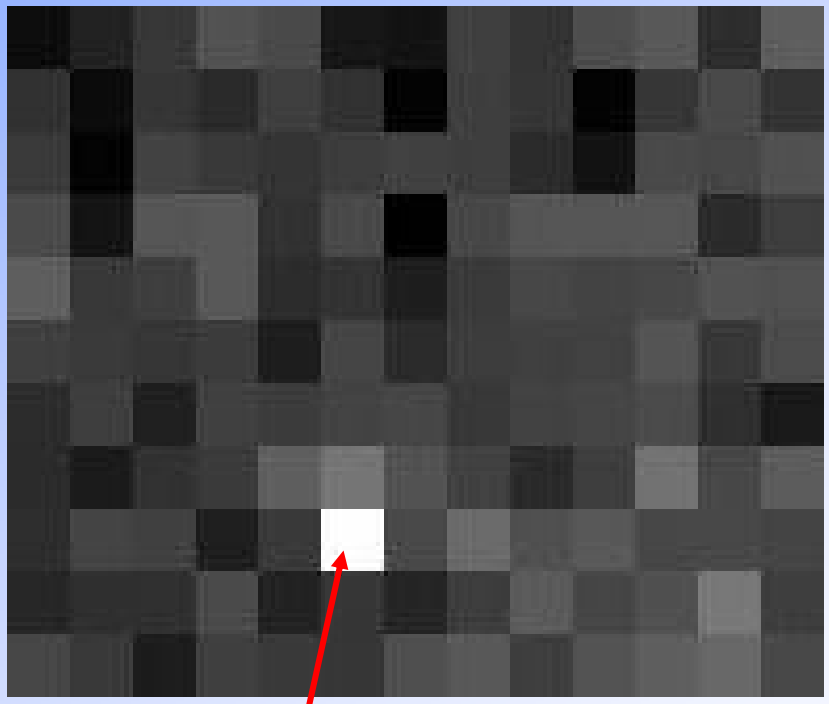
Spent nuclear fuel storage casks at Idaho National Lab

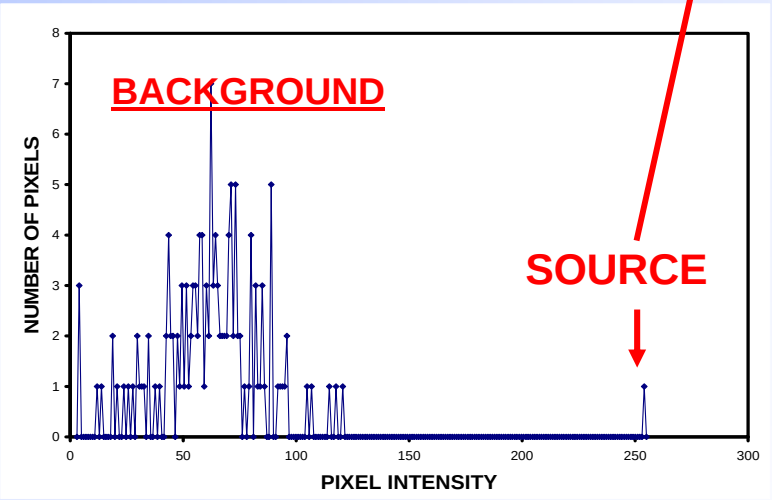
BROOKHAVEN NATIONAL LABORATORY

SOURCE IN TRUNK OF CAR



THERMAL NEUTRON IMAGE

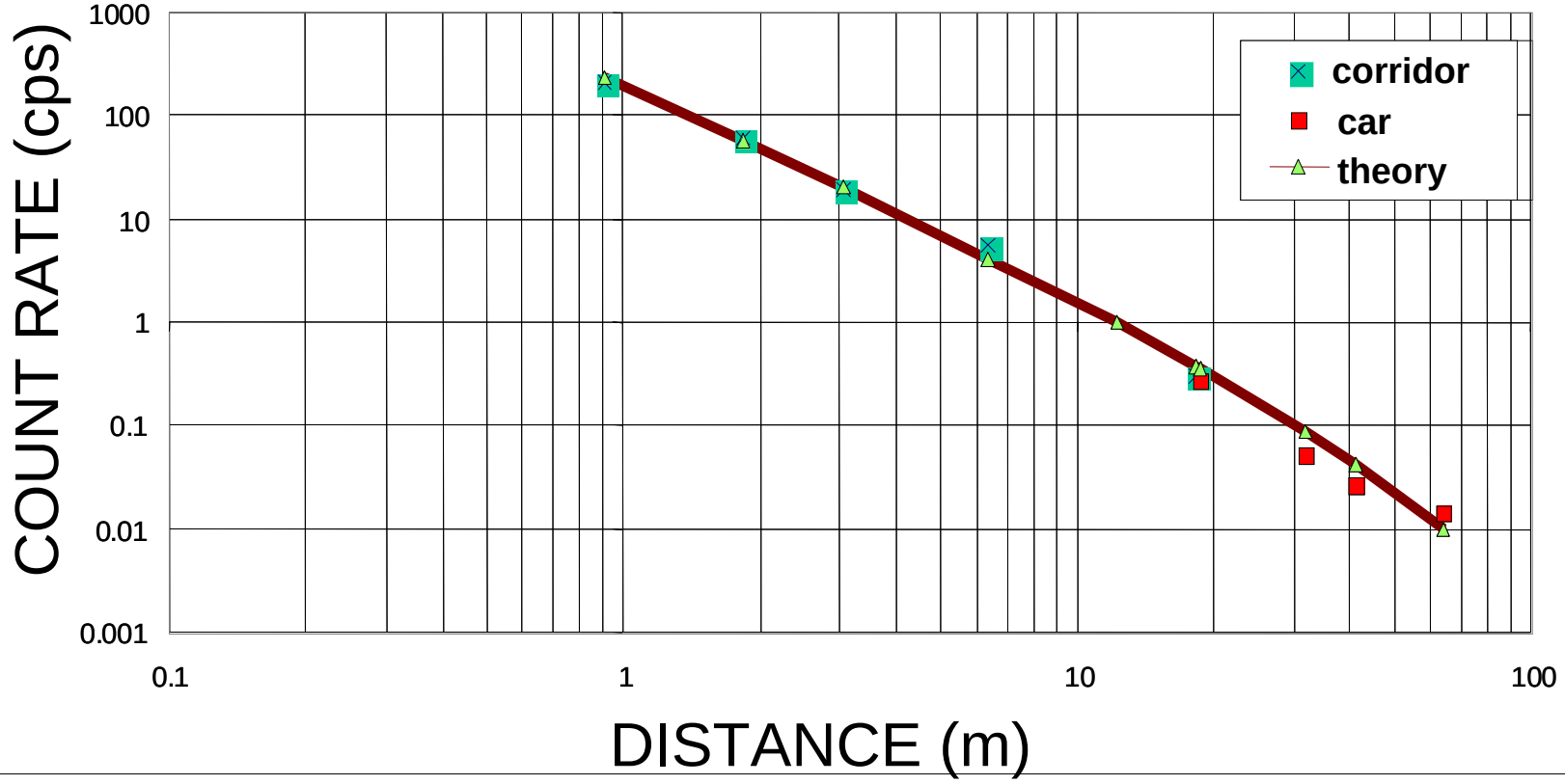




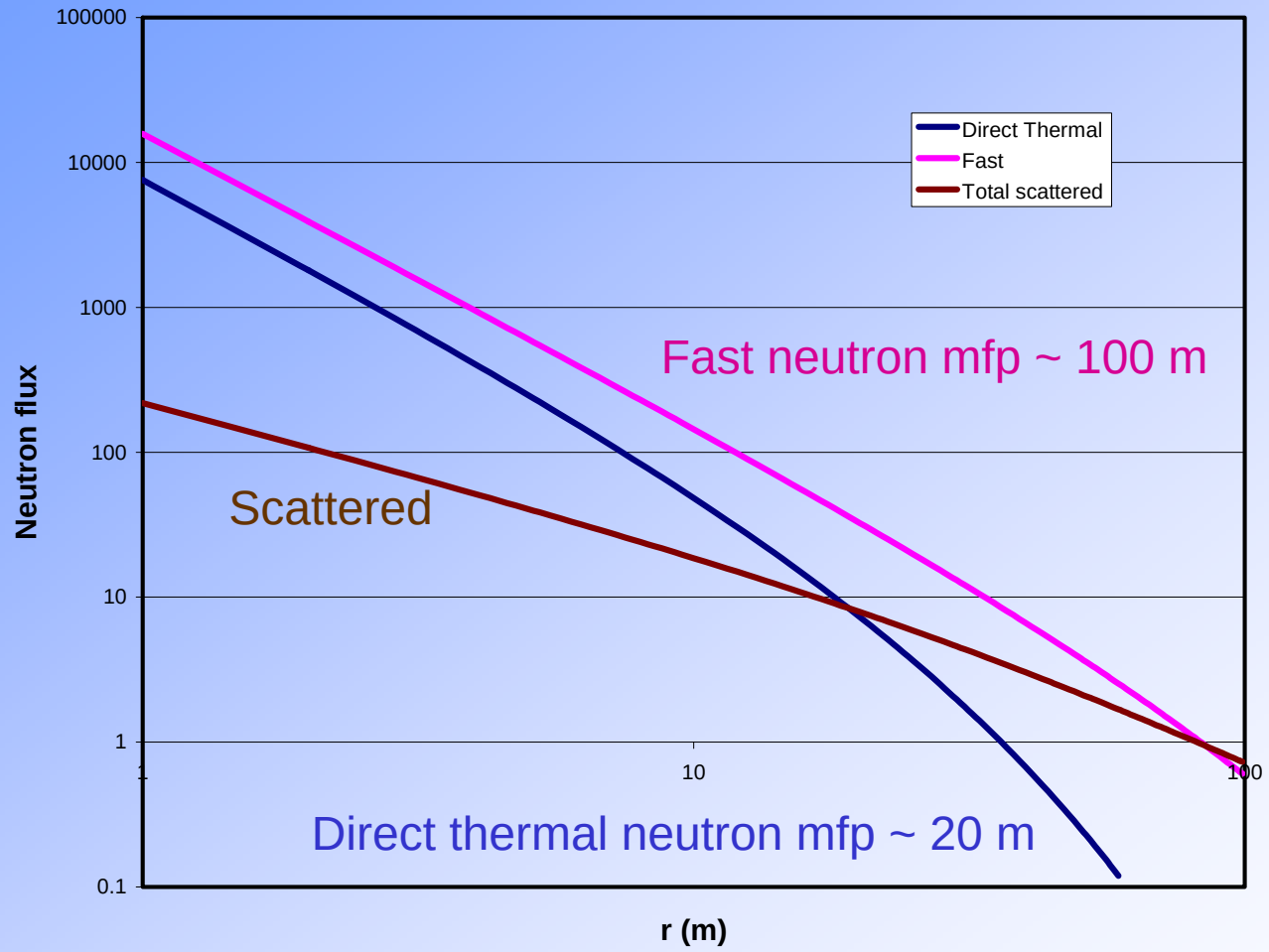
PIXEL INTENSITY HISTOGRAM

BROOKHAVEN NATIONAL LABORATORY

Count rate as a function of distance



Simple attenuation model for neutron point source in air



Detectors can be scaled up to increase count rates



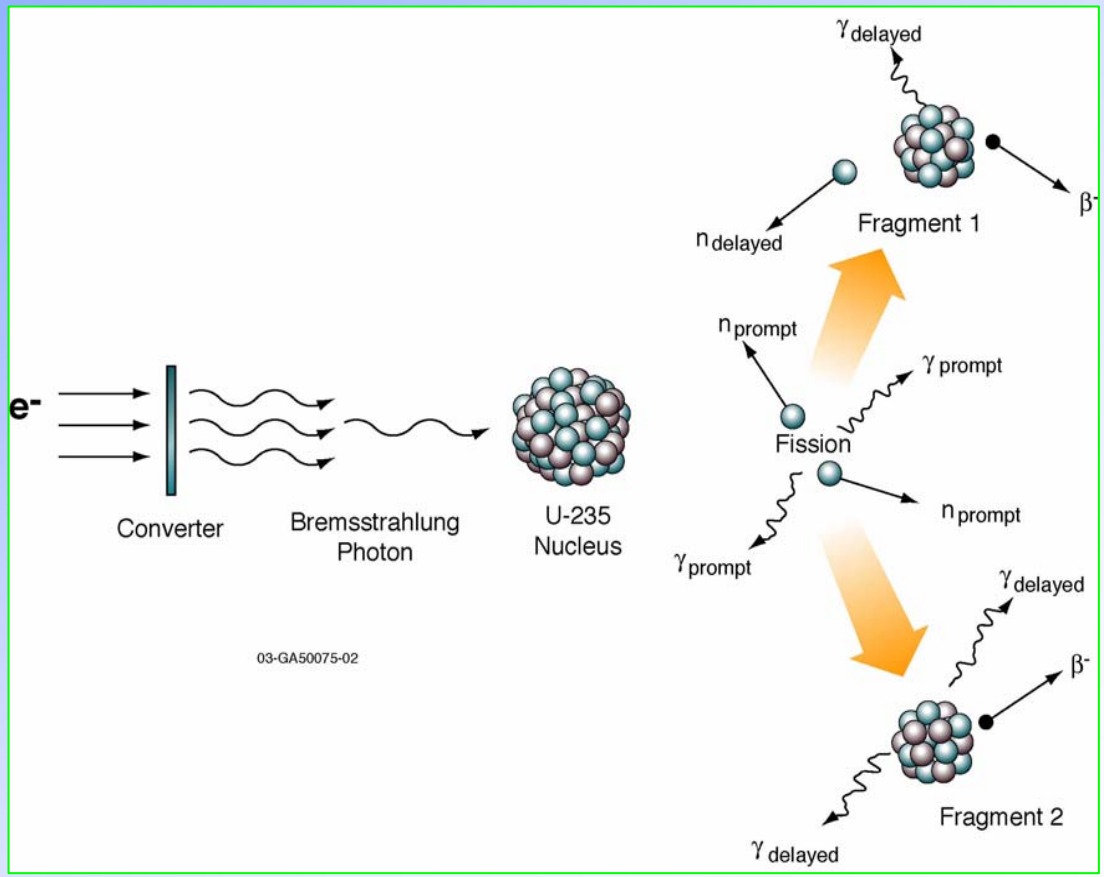
20 cm x 140 cm

100 cm x 100 cm



Active interrogation

- A pulsed electron accelerator produces high-energy x-rays (10-MeV) to generate photonuclear reactions
- Nuclear materials will undergo photofission and generate prompt and delayed neutrons
- The delayed neutrons continue to be emitted after each prompt neutron emission

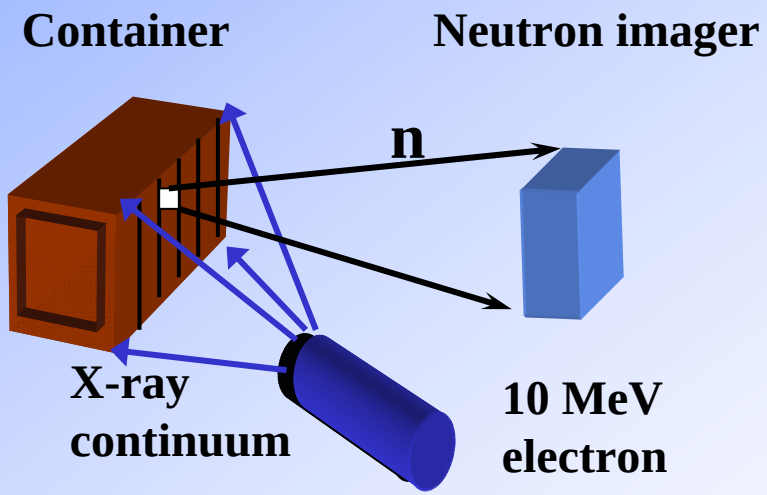


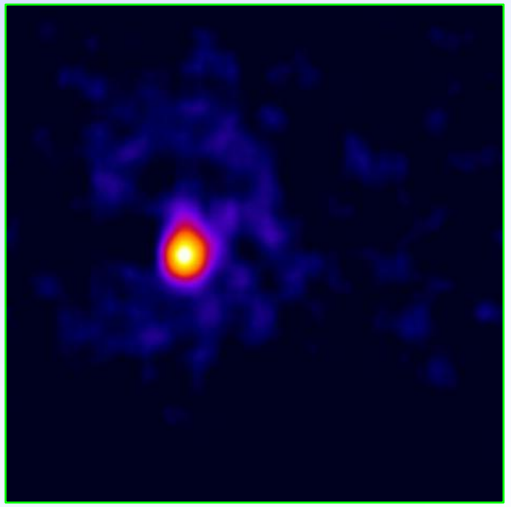
D.R. Norman, J.L. Jones, K.J. Haskell, P. Vanier and L. Forman,
IEEE NSS-MIC Conference Record, October 23-29, 2005

BROOKHAVEN NATIONAL LABORATORY

Active Interrogation with Imaging



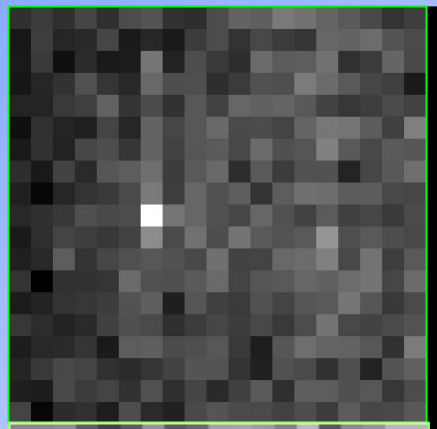


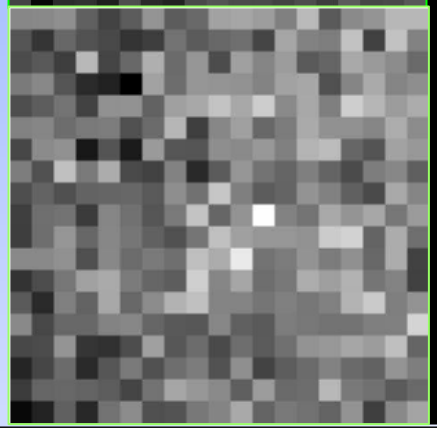


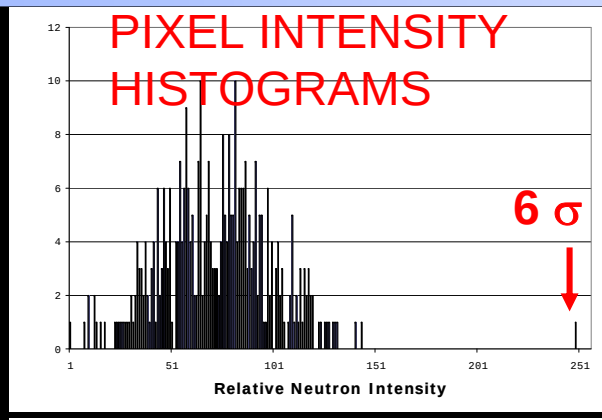
D.R. Norman, J.L. Jones, K.J. Haskell,
P. Vanier and L. Forman,
IEEE NSS-MIC Conference Record, October, 2005

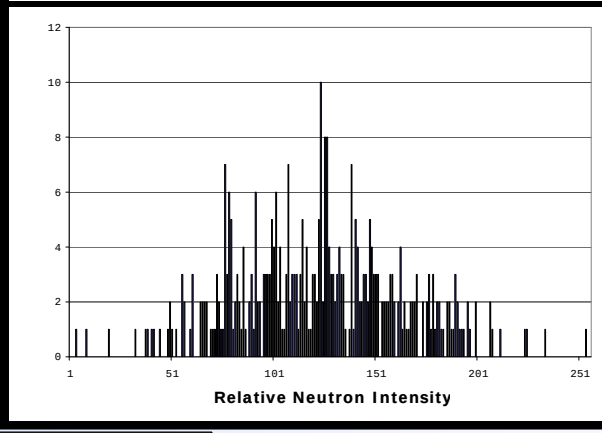
Image analysis

- Depleted uranium in polyethylene
  - 6.5-17.5 ms image window
  - 69k neutrons, mean = 72, σ = 28
- Tungsten in polyethylene
  - 6.5-17.5 ms Image window
  - 17k neutrons, mean = 122, σ = 41

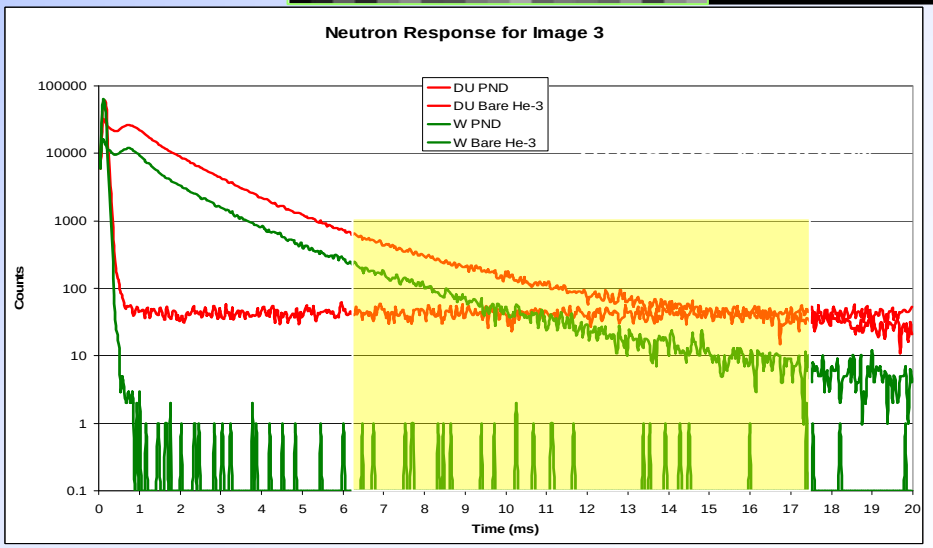






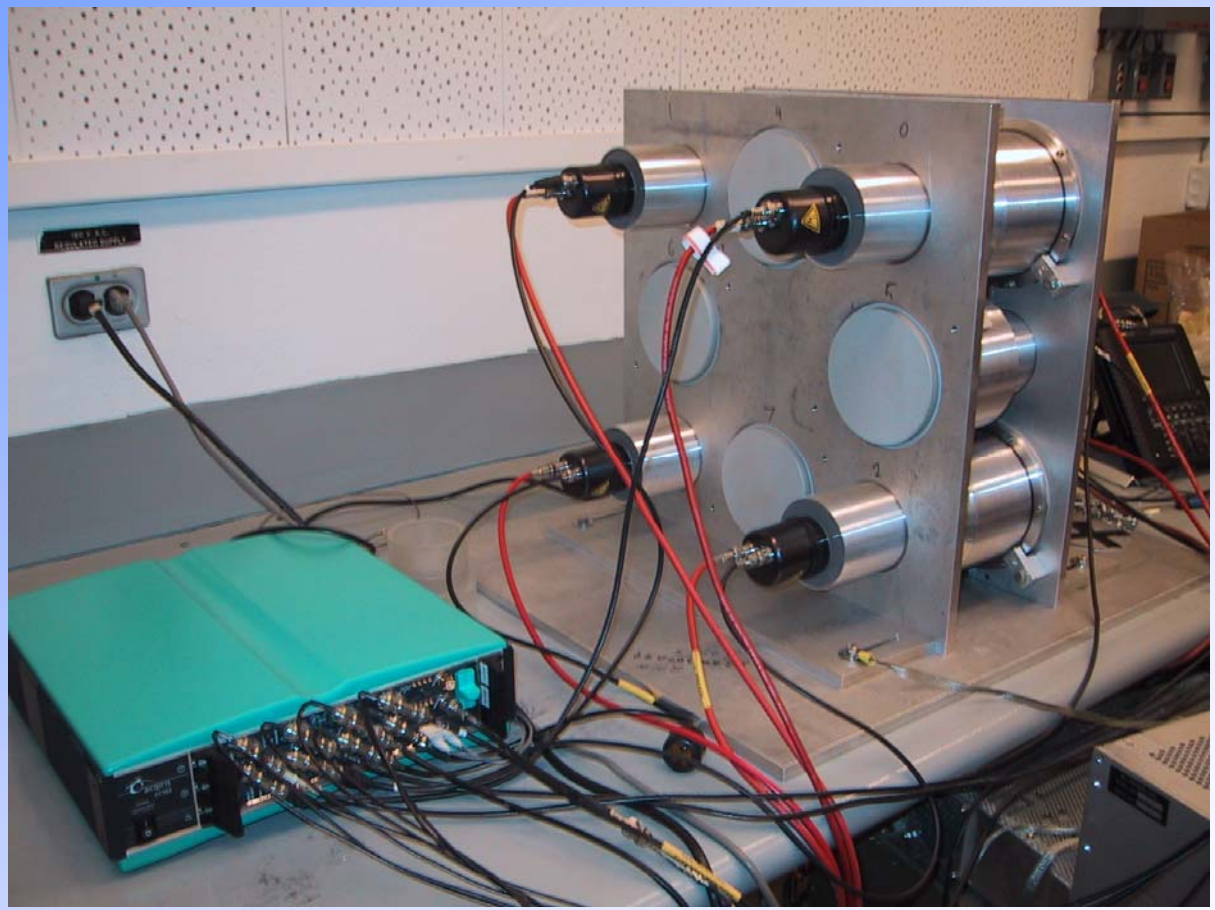


• Use time gate to distinguish prompt neutrons from delayed fission



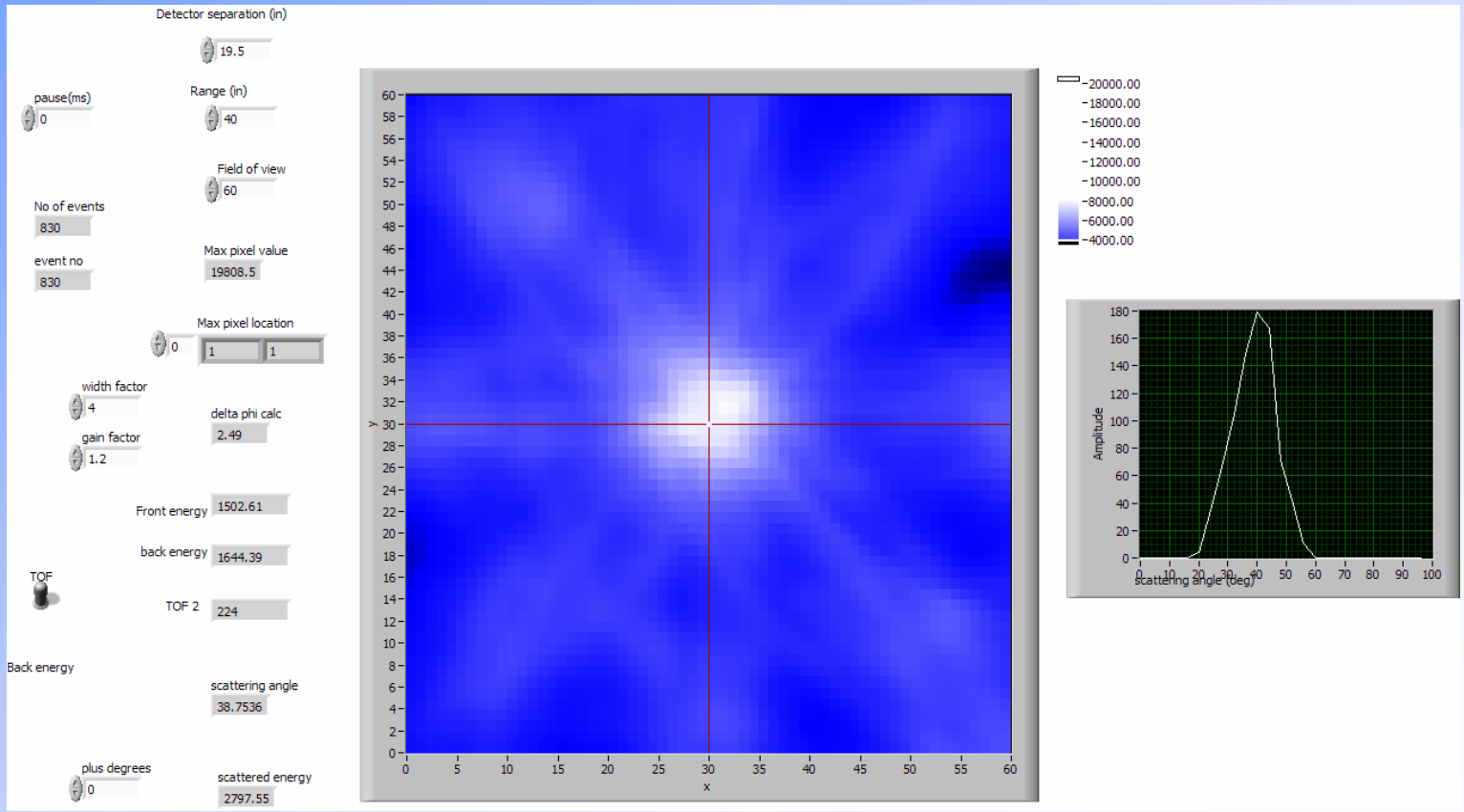
BROOKHAVEN NATIONAL LABORATORY

8-element fast neutron double-scatter spectrometer



BROOKHAVEN
NATIONAL LABORATORY

Experimental data,
Fast neutron source centered



Plane spacing = 50 cm, Range = 100 cm

BROOKHAVEN NATIONAL LABORATORY

Large area fast-neutron double-scatter directional detector



Area 40 cm x 100 cm
Modular design is expandable

CONCLUSIONS

- Directional detection helps find a neutron source in a uniform background
- There are few naturally occurring neutrons
- Ongoing issues
  - Detector size
  - Efficiency
  - Angular resolution
  - Uniformity
  - Gamma rejection
  - Spectroscopy

Acknowledgement

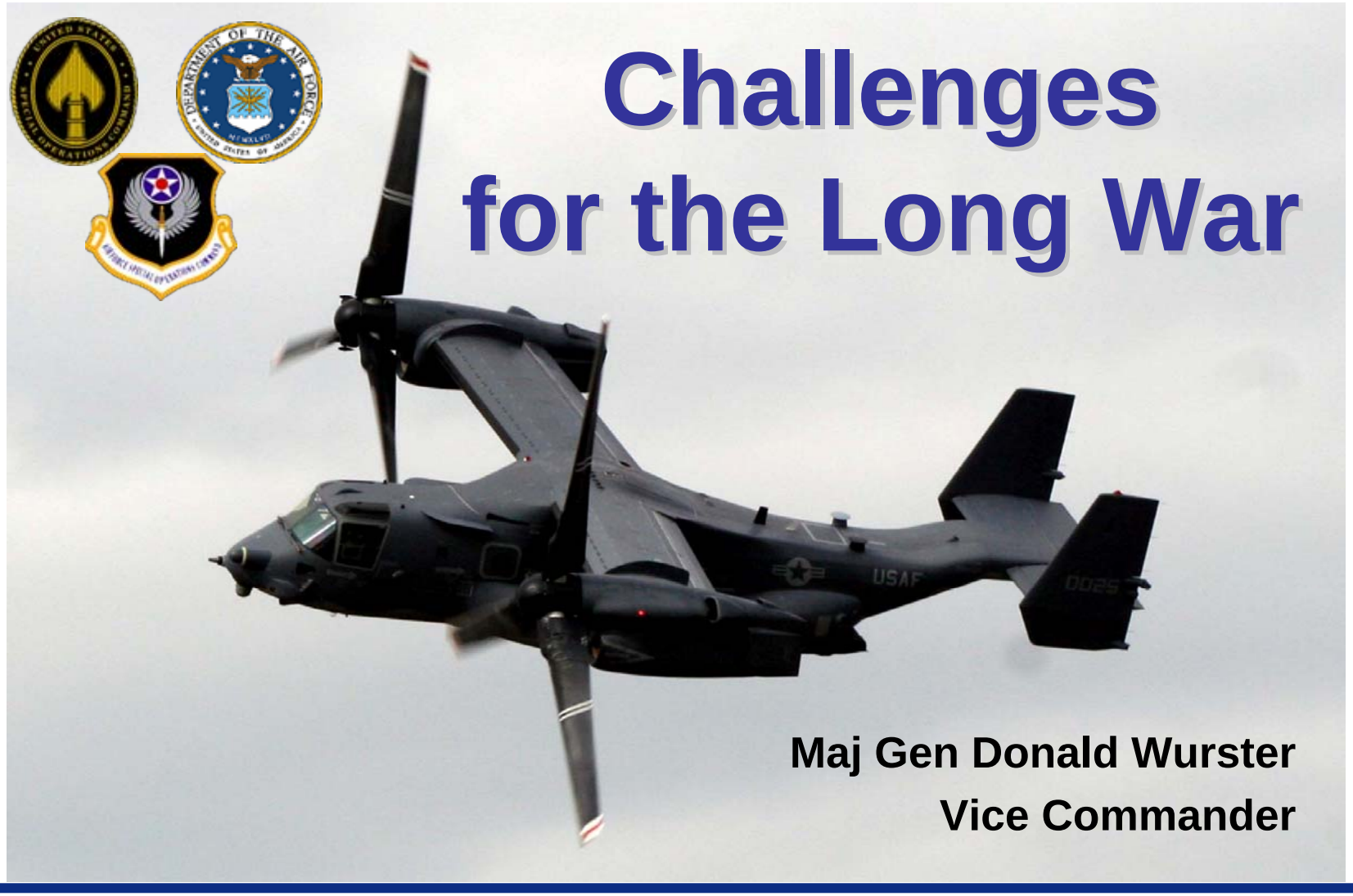
The BNL Detector Development and Testing Division is grateful for continuing support from

DOE NA-22, DHS and DTRA

BROOKHAVEN NATIONAL LABORATORY

AIR FORCE SPECIAL OPERATIONS COMMAND

Air Commandos



Challenges for the Long War

Maj Gen Donald Wurster
Vice Commander

This briefing is: UNCLASSIFIED

America's **Specialized Airpower**

Air Component to Special Operations



AFSOC Weapons Systems

Overview

























Gunship Operations

Weapon Systems



AC-130H/U

Precision requires Training



“You can run…but you’ll only die tired”

Precision Fire Support
Way Ahead

Near Term Upgrades:
- 30mm replacing 25mm & 40mm
- Replace ALLTV with GMS2
- Improve UAV collaboration







Change in Paradigm
- Variable effects (non-lethal to lethal)
- Higher threat areas
- Multiple, simultaneous targets
- All-weather, day/night
- Directed energy

Mobility – Infil / Exfil / Resupply

Weapon Systems



MC-130E/H/W

Fixed Wing Mobility
Way Ahead



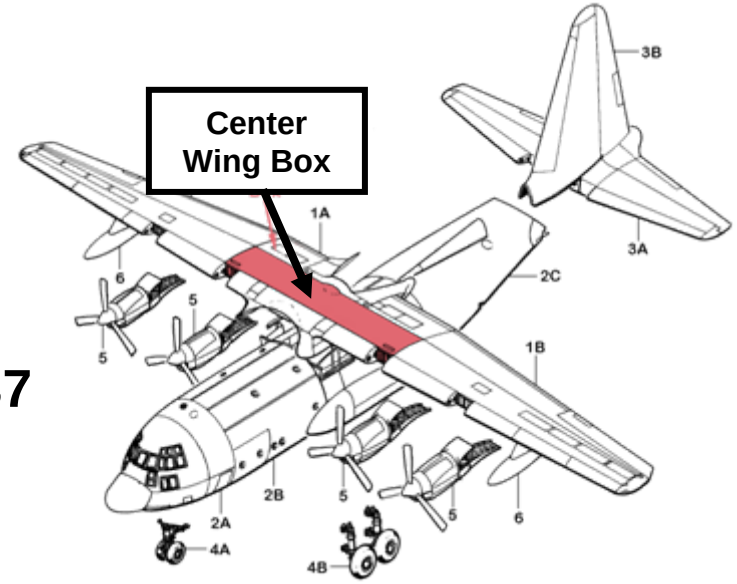
- Increase Commonality
- Center Wing Box Issues
- MC-130W
- SOF Tanker Recap



Recapitalization Requirement

23 X MC-130P Replacements
14 X MC-130E Replacements
12 X SOF Tanker QDR Augments
12 X MC-130W Replacements
61 SOF Tankers

37



Intelligence Surveillance and Reconnaissance



3rd SOS

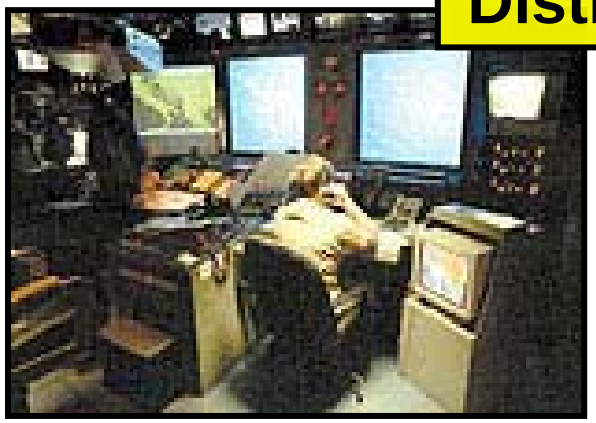
Tactical ISR support of Special Operations Forces





Intelligence Surveillance and Reconnaissance

11th Intelligence Squadron
SOF Dedicated
Distributed Ground System





"Specialized Intel for Special Operations"







Providing Near Real-Time Intelligence directly to Operators

Transformational Mobility



CV-22 Osprey

- Farther and faster in one period of darkness
- 1st CV-22 delivered to Hurlburt in Nov 06





8 SOS is 1st Operational CV-22 Sq



Theater Mobility

Weapon Systems



319th SOS

Tactical in-theater support of Special Operations Forces









Battlefield Airmen
Overview



Family of Airmen

Combat Controllers

Combat Weathermen

Pararescuemen





- Enable Air Power
- Advanced Skills Training
- BAO Kit



Highly Trained Personnel

Why We Succeed

- Highly skilled, mature operators
- Regional orientation, cultural sensitivity, language skills
- Creative and Adaptable
- Small, flexible, joint teams











"The nation that will insist on drawing a broad line of demarcation between the fighting man and the thinking man is liable to have its fighting done by fools and its thinking done by cowards."

Sir William Francis Butler

Aviation Foreign Internal Defense

Overview



6 SOS

Assess

Train

Advise

Assist

Integrate



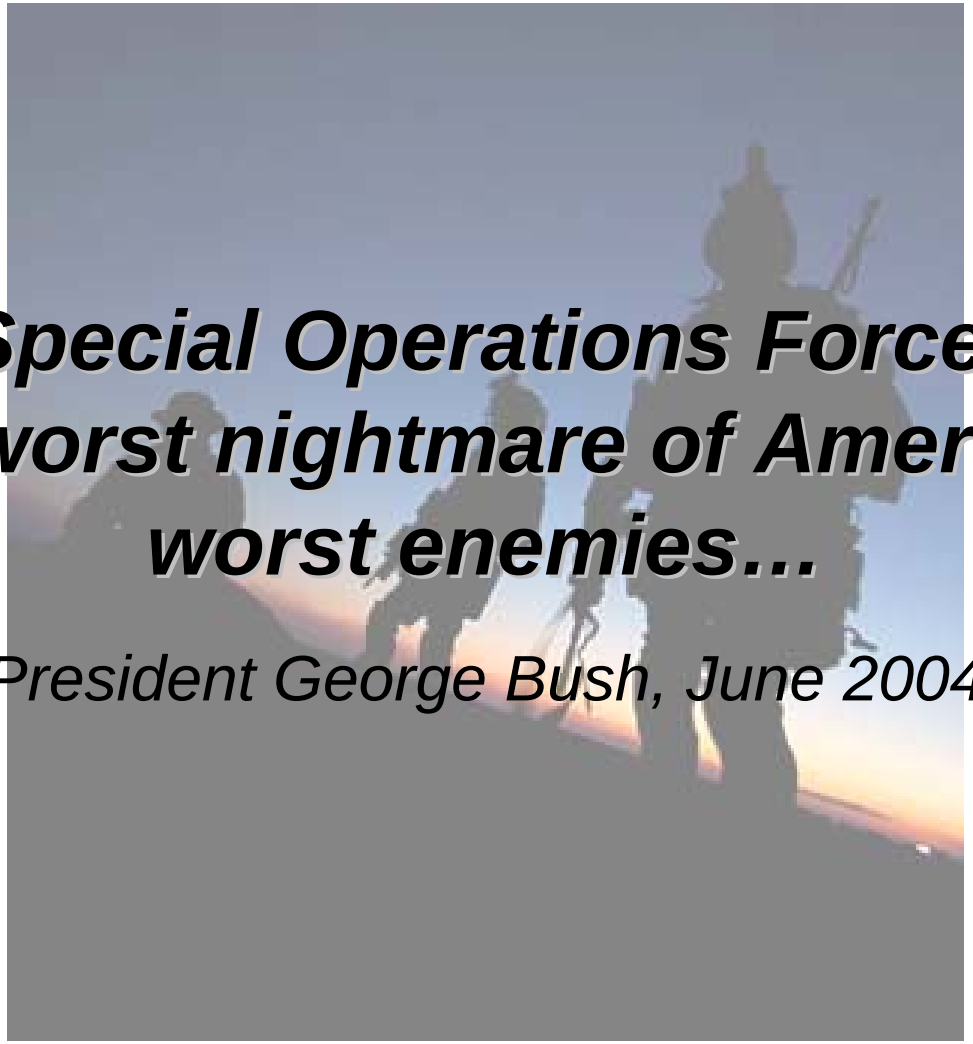


6TH SPECIAL OPS SQ

COMMANDO



Current Operations



Our Special Operations Forces are the worst nightmare of America's worst enemies…

President George Bush, June 2004

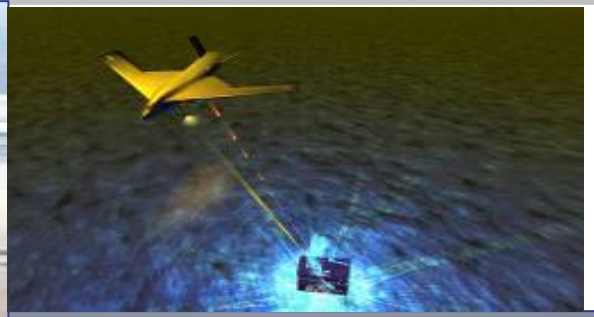
A Bad Day to be a Terrorist…

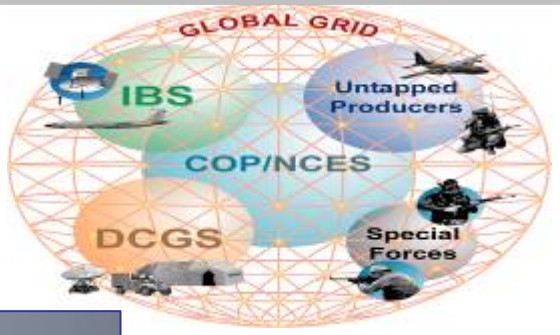


AFSOC Transformed

…Joint, Integrated, and Relevant to GWOT



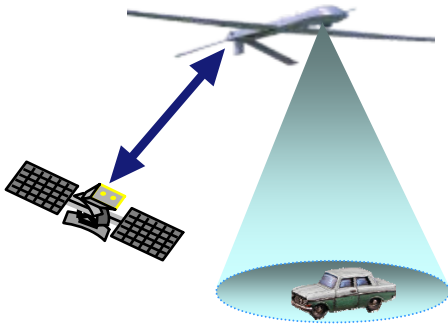






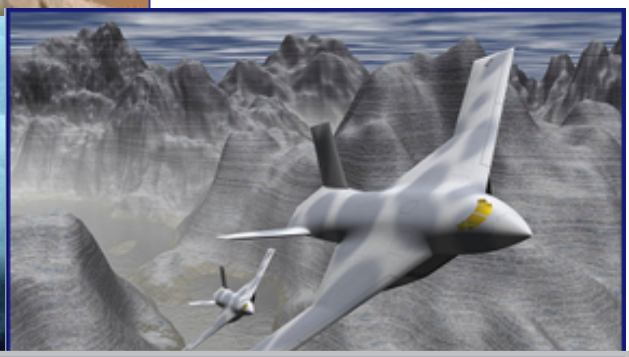












"…Our Special Ops, The Worst Nightmare of America's Worst Enemies" President Bush