Assessing the State of the Joint IO Enterprise

Mr. Gregory Radabaugh, SES
Director
Joint Information Operations Warfare Center

Agenda

- Current State of US Joint IO Enterprise
- Future Trends Affecting the Information Environment
- Emerging Relationships – IO, Cyber & EW
- Influence Versus Cognitive Combat
- DoD IO Strategy, Investment Framework, Joint Supporting Concept for IO
- Summary

Typical Reaction To JIOWC Briefing

Defining the Terms – JP 3-13

Information Operations: The integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision making of adversaries and potential adversaries while protecting our own.

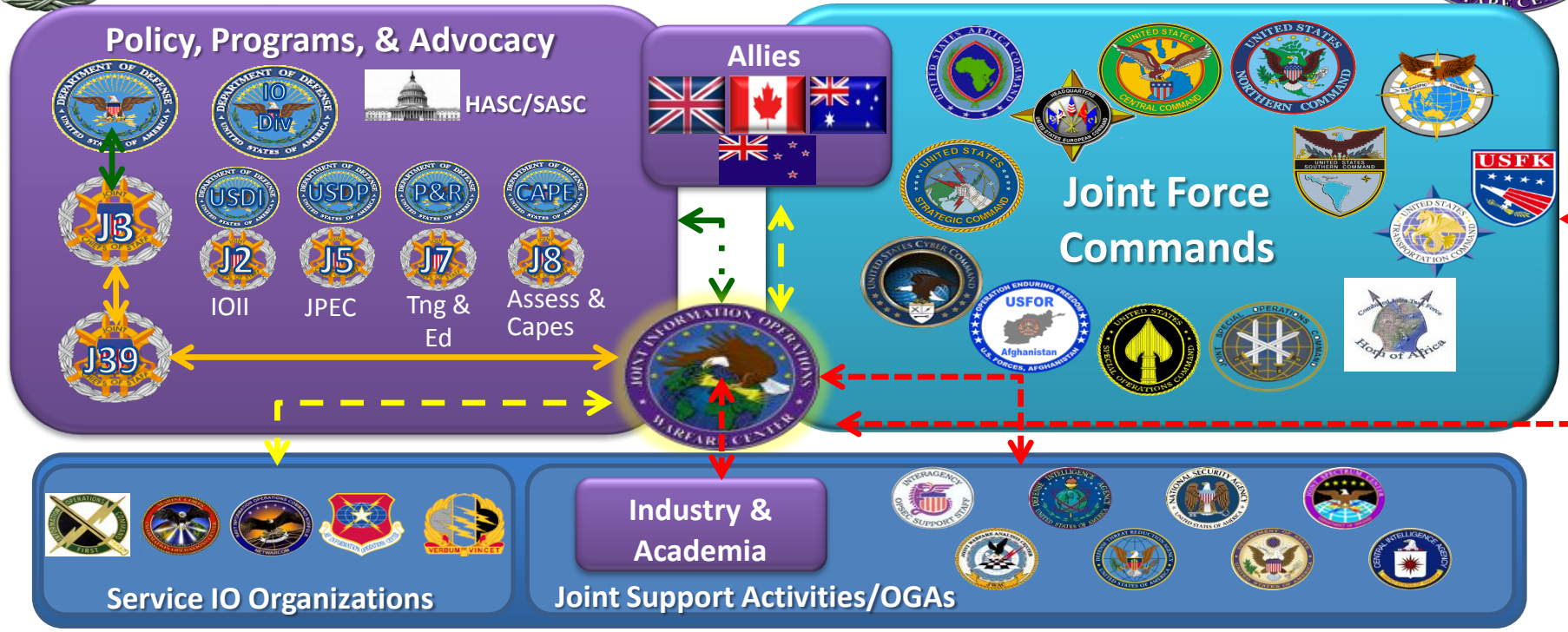
Information-Related Capabilities: The tools, techniques, or activities that affect any of the three dimensions of the information environment.

Information Environment: The aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information. This environment consists of three interrelated dimensions which continuously interact with individuals, organizations, and systems: physical, informational, and cognitive.

Information Operations – a Traditional Military Activity

- **Objective in warfare is to influence decision makers to do or not do something**
  - Kinetic warfare accomplishes this through destruction of life/property until adversary yields
  - IO accomplishes this through influencing adversary by affecting information/decision making process (affects can be immediate or long term)
- **Key is to understand how adversary makes decisions/is influenced by information**
  - Cultural/psychological/environmental/peers
  - What information conduits are used/trusted

The Joint IO Enterprise



The Service Perspective

- **US Army**
  - 1st IO Command is the only Army Active Duty IO command
  - Functional Area (FA) 30 is the Army IO officer specialty
  - Focus: IO support to Army and Joint at tactical through operational levels
- **US Marine Corps**
  - Marine Corps IO Center (MCIOC) (FOC Summer 2015)
  - Operational support to Marine Forces
  - Developing Marine Corps MISO
  - Focus: Tactical support to Deployed Marine Operating Forces.
- **US Navy**
  - Information dominance focus
  - Focus: fleet support
- **US Air Force**
  - In flux – ACC divesting IO proponency
  - Rebuilding IO career field (61B – Behavioral Scientist)
  - Focus: AOC and CFACC

Authorities – Who Can Do What

Table 1 - Authorities Affecting DoD Operations in the IE

United States Code	Principal Authority	Examples of Relevance to IO
Title 6 – Domestic Security	Department of Homeland Security	Domestic intelligence and information sharing, cyberspace operations, and defense support of civil authorities
Title 10 – Armed Forces	Department of Defense	Military IO
Title 18 – Crimes and Criminal Procedure	Department of Justice	Countering trans-regional criminal organizations, counterterrorism, and cyberspace operations
Title 22 – Foreign Relations and Intercourse	Department of State	Public diplomacy, foreign humanitarian assistance, and non-combatant evacuation operations
Title 32 – National Guard	State Army National Guard, State Air National Guard	Homeland security and defense support of civil authorities
Title 50 – War and National Defense	DOD C/S/As and IC agencies under the Office of the Director of National Intelligence	Foreign intelligence and information sharing, cyberspace operations

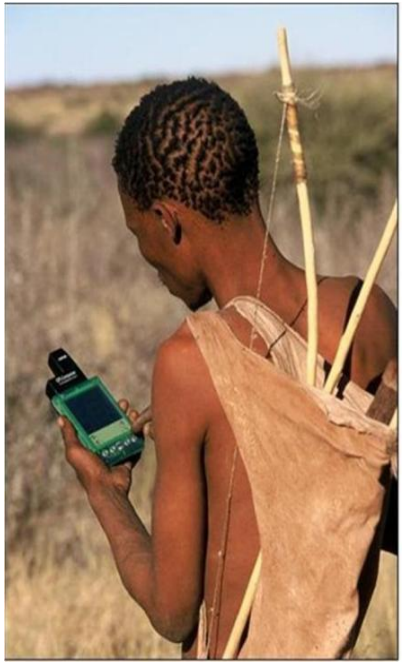
The Assessment Challenge

- **Challenge lies in assessing whether or not IO has been effective**
  - Fairly easy to do with disciplines that can be measured physically (e.g., EW, physical attack)
  - More difficult to do with newer technologies (e.g., CO)
  - Much more difficult with cognition (i.e., how do you know target has changed thinking/behavior)
- **Observe behavior (or lack thereof)**
  - Sounds easy—difficult in closed societies (e.g., DPRK)
  - Public decisions/physical movements
  - Communications/speeches/association with specific individuals

Requires establishing an information environment baseline

Current Information Environment (IE)

World is a blend of 1st, 2nd, 3rd and 4th Wave societies

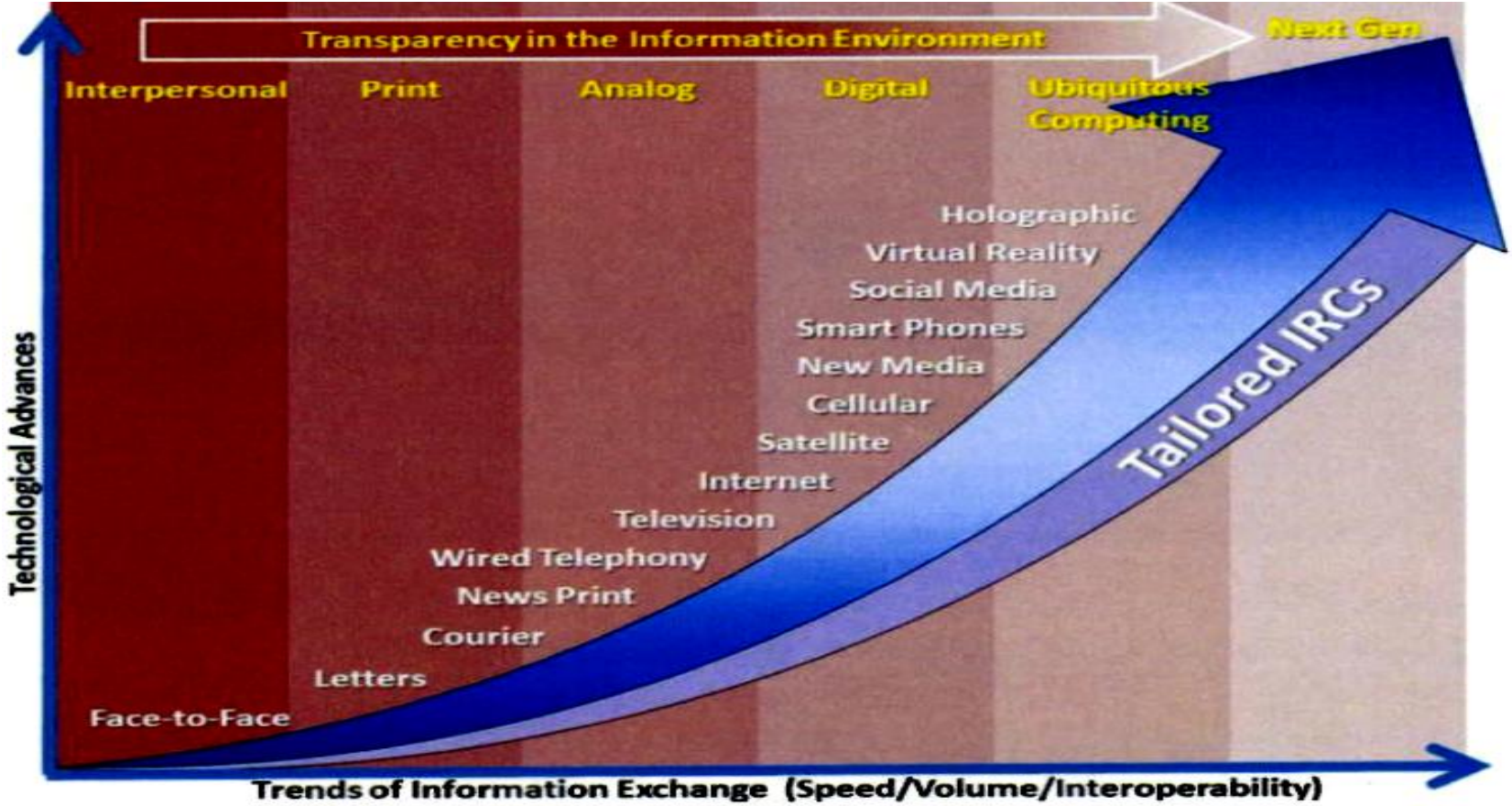


Future IE Trends

- Three major influences on military operations:
  - Volume of information available through all forms of communications media growing in breadth and depth
  - Speed with which information flows through a population
  - Widespread interoperability between digital devices



Future IE Trends



Operating in the Future IE

- **Successful military operations will require:**
  - Integration of organic Internet capabilities within the Joint force
  - Inclusion of stand-off capabilities for operating in anti-access area denial scenarios
  - Immediate adoption of current off-the-shelf technology to pre-empt or disrupt adversary influence
  - Leveraging Partnerships

Information as War

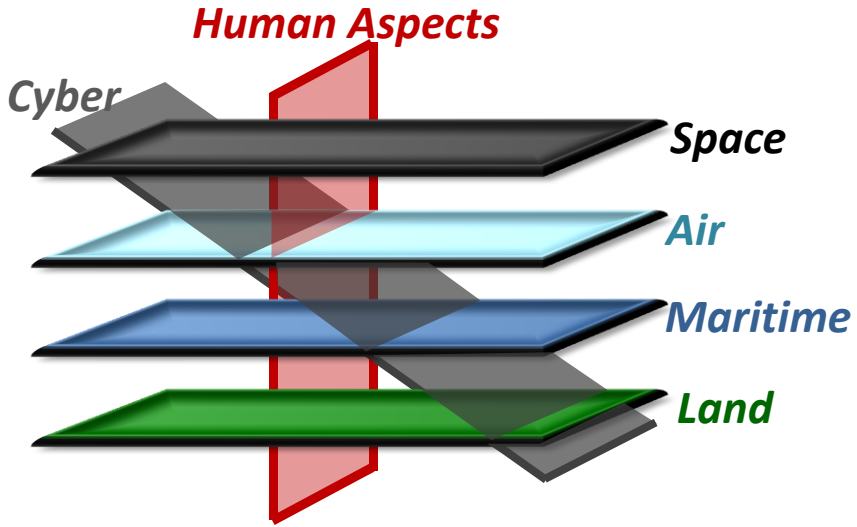
We must now go beyond considering the problem of information in war and consider information as war -

a new discipline in its own right which underpins all other aspects of warfare – Information Warfare.

~ UK Maritime Information Warfare CONOPS

Information as War

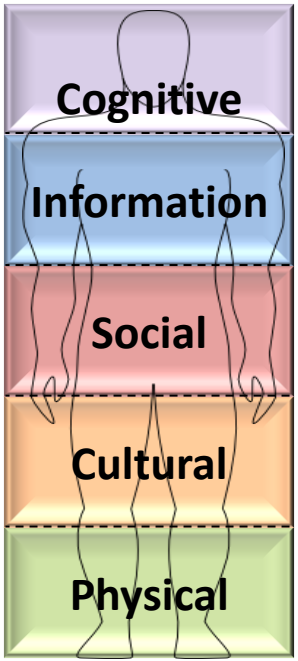
Human aspects of information intersect all domains



Key IE attributes are digital convergence, hyper-connectivity, ubiquitous on-demand media, interpersonal communications

Information as War

Influencing a target audience requires understanding how the target is influenced by multiple domains



Cognitive

- Awareness
- Perception
- Reasoning
- Judgment
- Emotion
- Critical Thinking

Information

- Means
  - Internet
  - Print
  - Radio
  - Television
- Message
- Audience

Social

- Public Groups
- States Institutions
- Local Government
- Civic Groups
- Societal Groups

Cultural

- Ideology
- Tribalism
- Customs & Beliefs
- Ethnicity
- Religion & Rituals
- Language
- Communication

Physical

- Geography
- Topography
- Hydrology
- Urbanization
- Resources
- Climatology

Doing this is really hard as machines can't understand the IE

Information as War

“I tell you we are in a battle, and more than half of it is taking place in the battlefield of the media. We are in a media battle in a race for the hearts and minds of our Ummah.” - Ayman al Zawahiri

In this new reality, TV and the Internet are vital propaganda outlets to disseminate messages and inspire young Muslims to join decentralized and loose networks of local affiliates and cells.

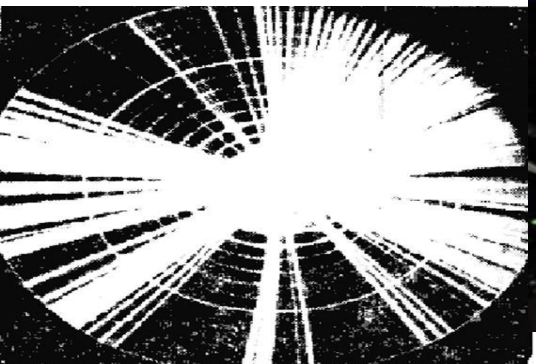
As the terror attack in Ottawa demonstrates, there are subcultures within the overall dominant culture—our adversaries understand that

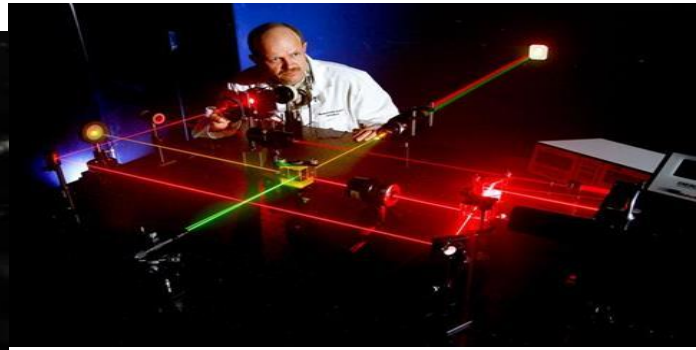
Information as War

More than one target audience intended recipient

Emerging Relationships – IO, Cyber, and EW

- **Cyber and EW provide places and means for affecting the information environment**
  - — Cyber provides both a domain for conducting IO and capabilities
  - — EW provides the means for controlling the electromagnetic spectrum (EMS)
- **EW contributes to success of IO by using offensive and defensive tactics and techniques in a variety of combinations to shape, disrupt, and exploit adversary use of the EMS**
  - — Increasing prevalence of wireless telephone and computer usage extends both threat and utility of EW





The Military Aspect of Cyber

- **Cyberspace is an environment in which military activities take place**
  - Command and control
  - Intelligence, surveillance & reconnaissance (ISR)
  - Data transmission
  - Information Operations
- **Cyber enables military activities or is the military activity itself**
  - Example: ISR for and from cyber
- **The same principles of warfare apply**
  - E.G., It's not cyber targeting, it's targeting
- **However, cyber as a medium of warfare has some distinctions:**
  - Accessibility
  - Volatility of the medium/data
  - Anyone can play

The Intelligence Aspect of Cyber

- **Cyber warfare supports the effect the JFC intends**
  - Requirement may be for non-kinetic, non-attributable effect
  - Requirement may also be for intelligence to support other military operations
- **Cyber targeting is not cyber exclusive**
  - Required effect could be achieved through EW, DEW, kinetic
  - May be easier to put a Mk 84 on the target than go through the difficulty of reaching it non-kinetically
- **Cyber warfare as an "on demand" capability**
  - Analysis required to support cyber operations is extremely detailed
  - Usually does not lend itself to a "pick up" game of warfare in which the COCOM is directed to conducted operations in a short amount of time (e.g., Libya)
    - Very much like IO in that shaping the IE in advance of conflict provides the greater chance of success
  - To achieve this capability will require advanced requirements by the COCOM, prepositioning of analysis and capabilities, and constant refresh

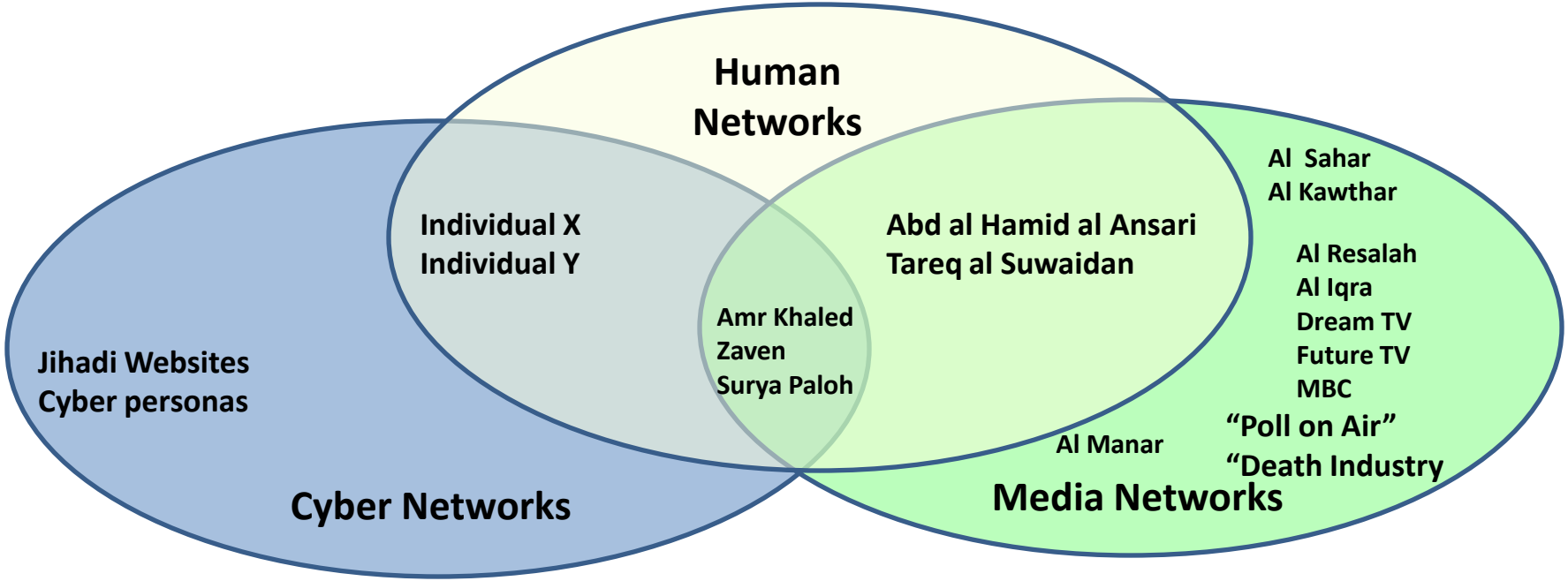
The failure to educate COCOM/JFCs on cyber capabilities will lead to kinetic solutions as the default setting

Influence Versus Cognitive Combat

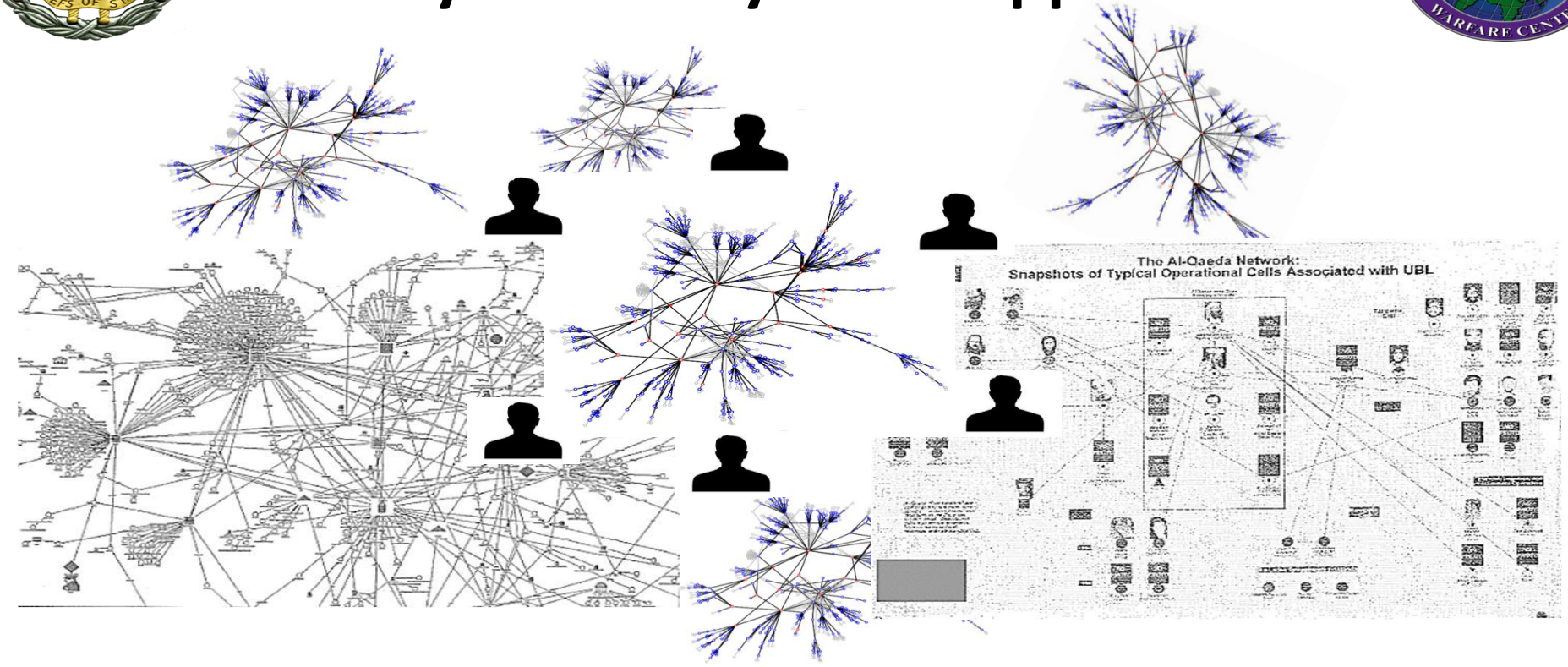
- Influence activities during peacetime
- Transition to cognitive combat during conflict/wartime
- Human influence targeting and the ‘By Name’ war

Influence Relationships

It takes the physical and non-physical to develop a complete picture



A System of Systems Approach



Operating Effectively In the Future Information Environment Necessitates a Strategy

Congressionally Directed DoD IO Strategy

- "DoD Strategy for Operating in the Future Information Environment"
  - Goal I: People – The Right Competencies in the Right Place…
    - Identify, Sustain, and Evolve the IO Force
    - Field a Trained and Educated IO Force
  - Goal II: Programs – The Right Capabilities at the Right Place and Right Time…
    - Develop the Defense Intelligence Enterprise's Ability to Characterize the IE
    - Develop and Maintain Capabilities to Operate Effectively in the IE
    - Develop and Maintain Capabilities to Assess Operations in the IE
    - Identify and Prototype Capabilities to Operate Effectively in the IE
  - Goal III: Policy – The Proper Guidance…
    - Develop Policy Relevant to IO
    - Develop Concepts Relevant to IO
    - Refresh Doctrine Relevant to IO
    - Review Legal Frameworks and Agreements Relevant to IO
  - Goal IV: Partnerships – The Right Relationships with the Right Partners…
    - Establish and Maintain Partnerships
    - Leverage and Build Partnership Capacities and Capabilities

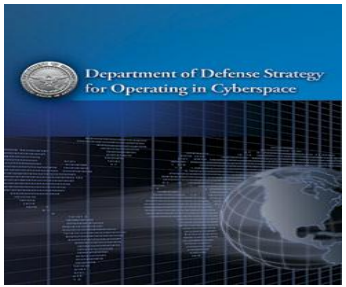
This costs real money—and lots of it—but much less than what it will cost to lose (think peer-on-peer war)

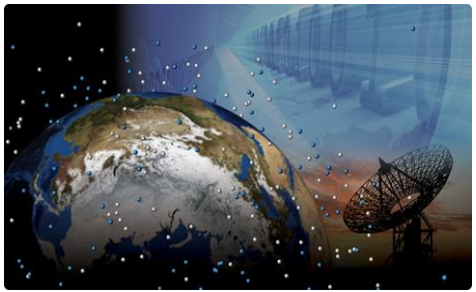
IO Investment Framework – Projected Research Focus Areas

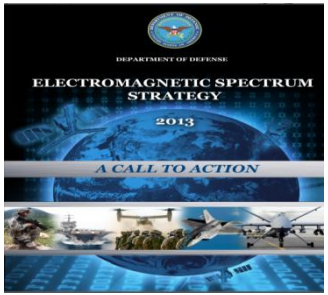
- Understanding/predicting sociocultural behavior
- Detecting influence campaigns and accurately forecasting audience behavior
- Modeling and simulation
- Analyzing and leveraging adversary sentiment
- Psychology, Sociology, and anthropology “apps”
- Exploiting virtual reality
- Cognitive adaptive capabilities
- Automated analysis capabilities

Next Steps

- **IO Strategy Implementation Plan**
- **IO Investment Framework**
  - **Projected technologies/capabilities for Service investment out to 2025**
- **Joint Supporting Concept for IO**
  - **Synchronized with the Concepts for Cyberspace and Electromagnetic Spectrum**







Summary

- Future IE trends, the IO assessment challenge, and convergence of IO, cyber and EW are driving change
- We continue to evolve towards cognitive combat and “By Name” warfare
- As a consequence, DoD is embarked on shaping IO for the Joint enterprise through 2025

The IE hasn’t hit us strategically yet—but someday it will

Comments/Questions?