Conversation with the Colloquium

June 2012

Deborah Frincke, PhD
Deputy Director, Research Directorate
National Security Agency

Let's Chat …

- NSA Research
- Enlisting your aid
  - Classified Journal
  - Postdoc
- A nod to Big Data and analytics

NSA Mission

Protect

Protect U.S. Secrets

Assure communications and systems against exploitation

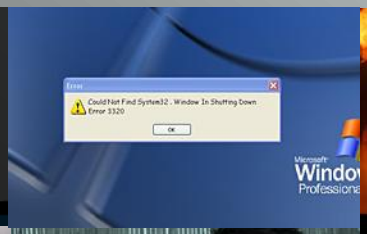
Discover

Discover Adversaries' Secrets
Intercept and exploit Foreign Communications (SIGINT)

Outmaneuver Adversaries in Cyberspace

Wide Array of Threats

Insider Threat



External

Supply Chain

Technological

Environmental

NSA Research Directorate: What We Do

Create research breakthroughs in mathematics, science, and engineering that enable NSA to achieve and sustain intelligence advances against immediate and emerging threats to our national security

The Research Facilities

Research & Engineering
Fort Meade, MD

Laboratory for Physical Sciences
College Park, MD

Laboratory for Telecommunications Sciences
College Park, MD

Center for Advanced Study of Language
College Park, MD

RD Strategic Overview

Seven Thrust Areas:

- Analysis
- Communications
- Crypto-Science
- Cyber
- Enabling Mission
- Technical Health
- Trustworthy Systems

Workforce Breakout:

15% - Forward Deployed to Mission

15% - Near-term Research

(<18 months for deliverables)

70% - Long-term Research

(>18 months for deliverables)

Technical Development Programs

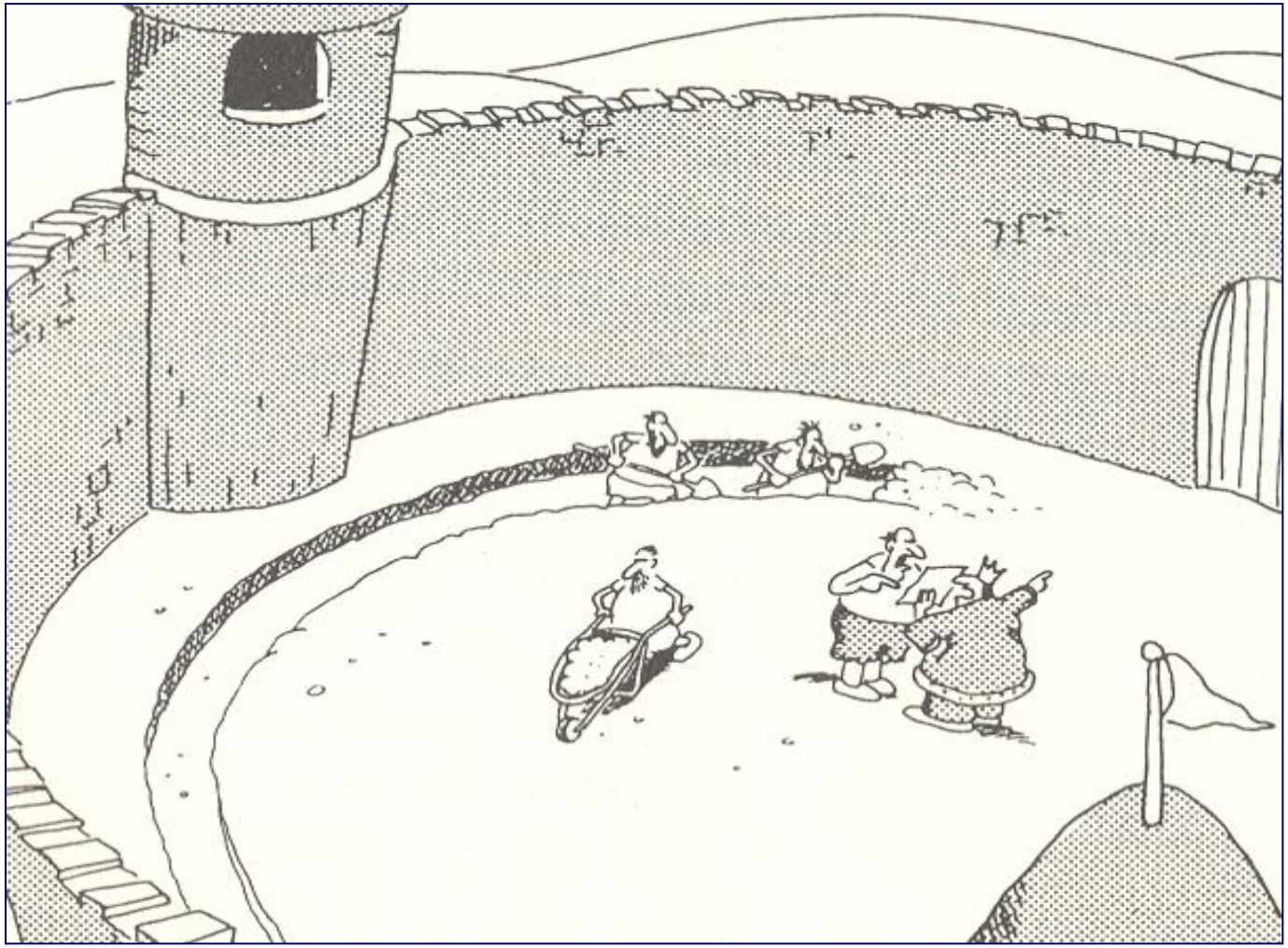
Resident Signals Engineering Program

Applied Mathematics Program

Director's Summer Program

Graduate Mathematics Program

Research Requirements



THE FAR SIDE By Gary Larson

Suddenly, a heated exchange took place between the king and the moat contractor.

Policy – Research Driver

- **E.O. 12333 (1981)** - NSA named executive agent for the communication security of the United States government.
- **Computer Security Act (1987)** – NIST, with NSA technical advice, responsible for developing standards and guidelines needed to assure the security and privacy of sensitive information in Federal computer systems.
- **NSD – 42 (1990)** – DIRNSA named the National Manager for National Security Systems.
- **Executive Order 13587 (EO 13587)** –"Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information."

Sophisticated sensors are now Consumer Goods

Peer Review + Classified Material = …?

A few words about "Big Data" and Analysis…

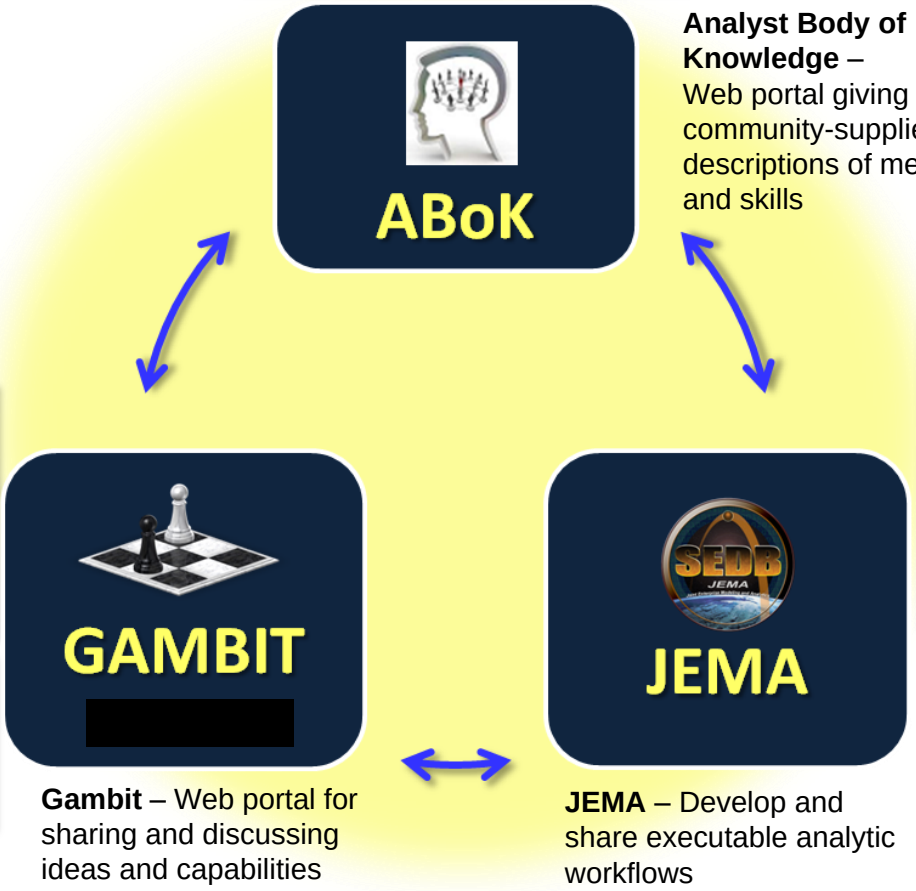
Possibilities…

Fig: Gosler, SNL.

Tradecraft Ecosystem

Detailed explanations
of how to carry out analytic methods
and to use existing capabilities

How do I do that?



Analyst Body of Knowledge –
Web portal giving community-supplied descriptions of methods and skills

Basic descriptions
of ideas and current capabilities

What's out there? Who cares about my idea?

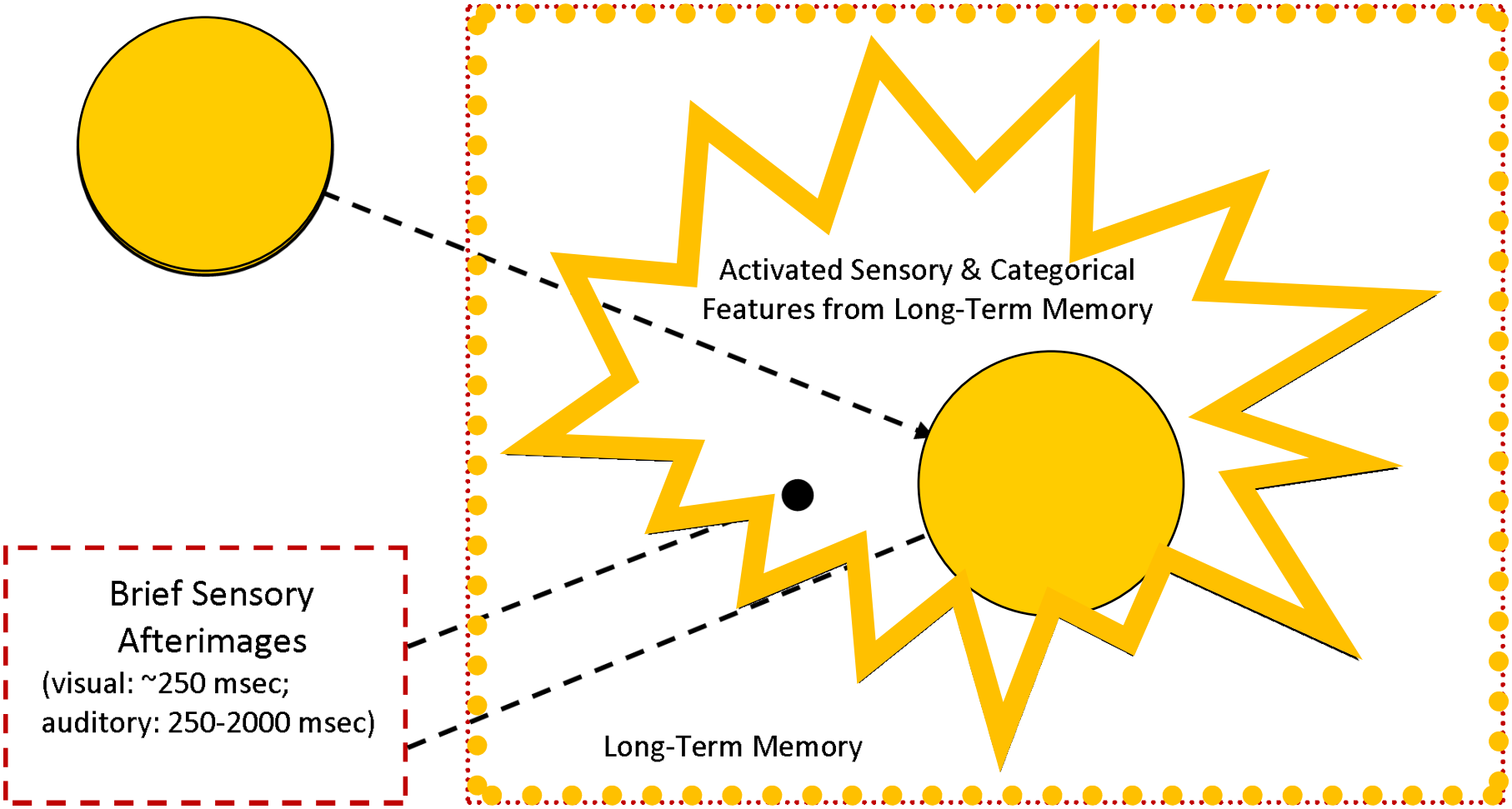
Gambit – Web portal for sharing and discussing ideas and capabilities

JEMA – Develop and share executable analytic workflows

User-driven analytics (UDAs)
demonstrating how to apply methods and ideas

How can I streamline or automate this as an executable workflow?

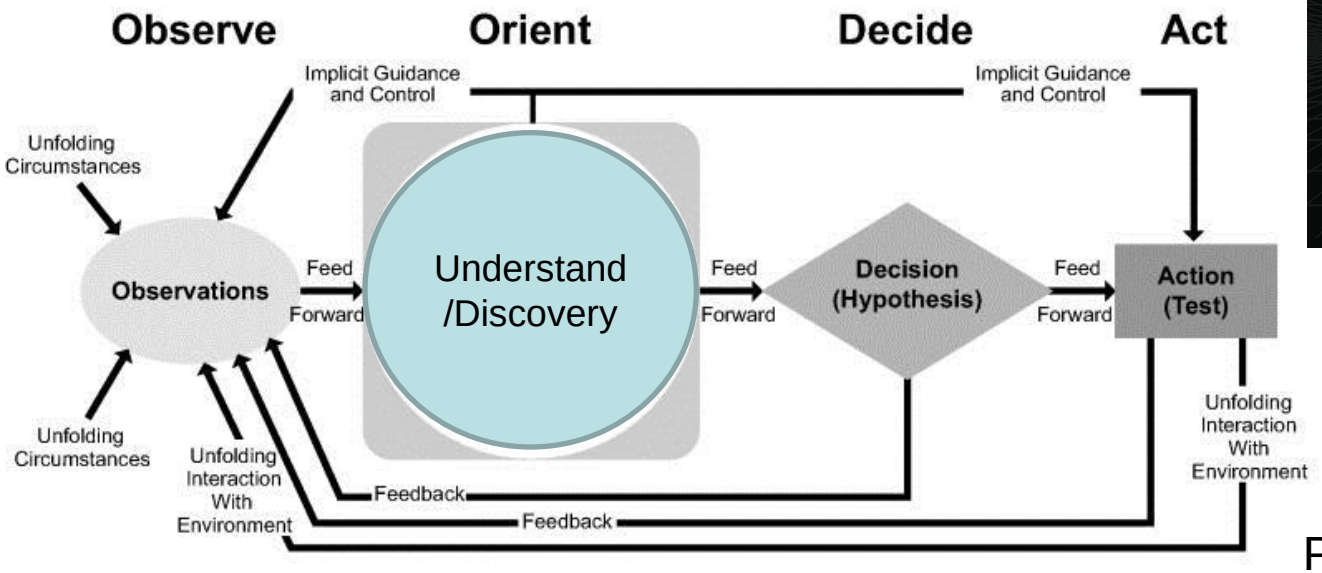
The *Other* Working Memory



e.g., Cowan, 1988, 1995, 2005

Cyber Analytics – Dept of Energy

- Problem: how to *rapidly* discover, understand, and respond to threats
- Solution
  - Methodologies to analyze large volumes of streaming data
  - Advanced visualization tools; techniques to fuse heterogeneous data into coherent displays
  - Novel techniques for signature detection



PNNL Cyber Analytics/I4

The Analytic Process – High Level

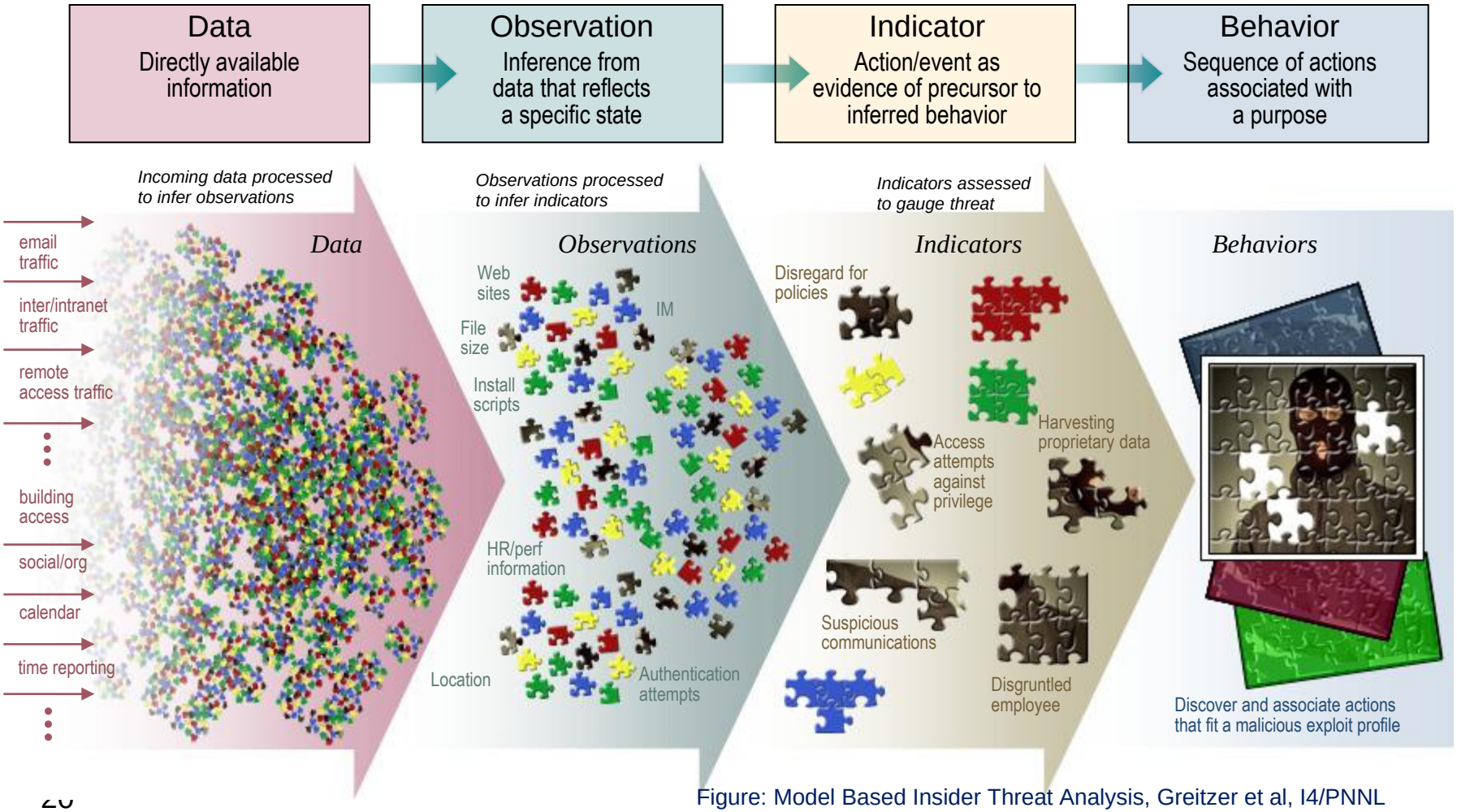


Figure: Model Based Insider Threat Analysis, Greitzer et al, I4/PNNL

Sophisticated sensors are now Consumer Goods

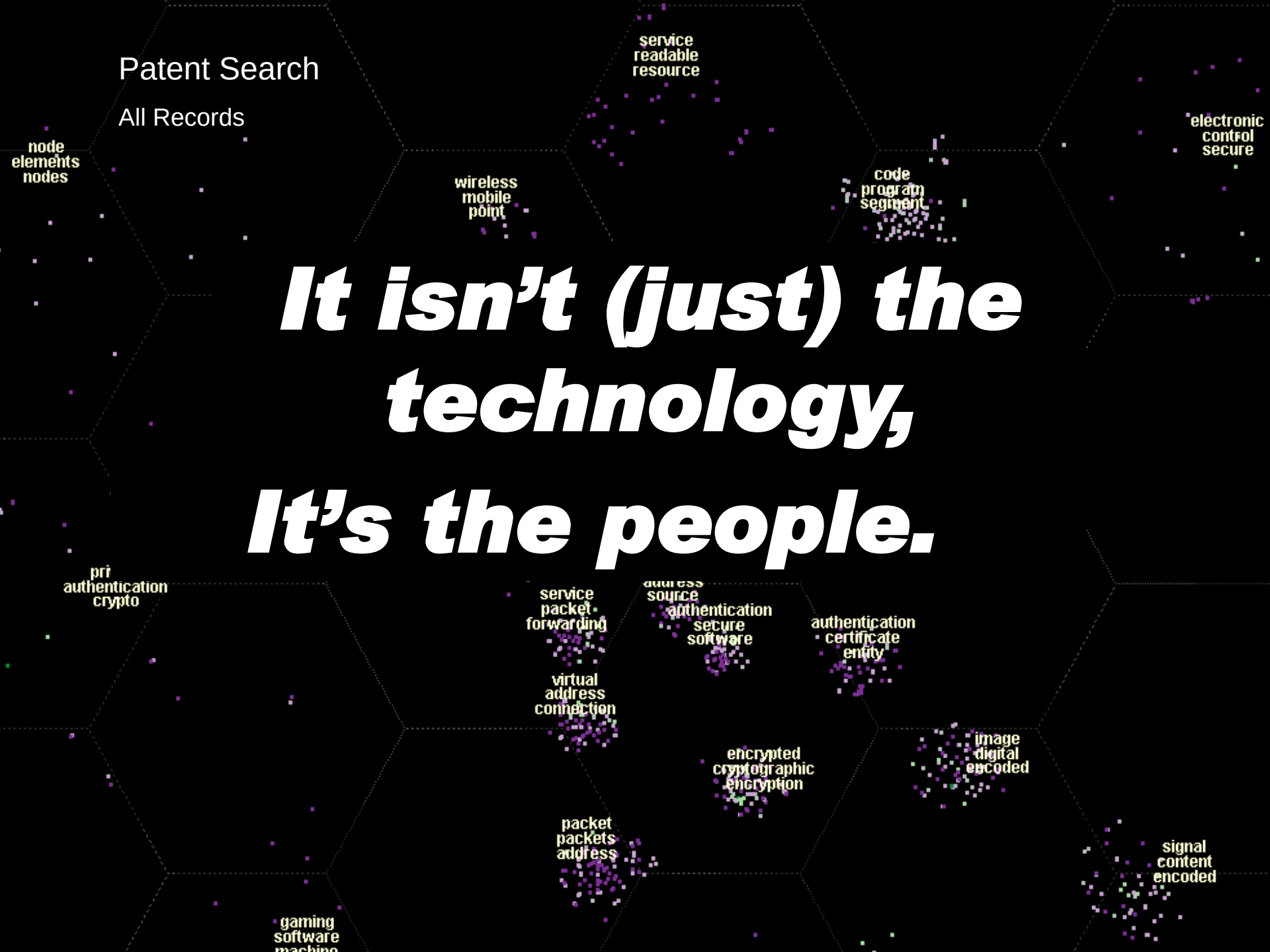
Clouds "In House"

Data Clouds

- **Architecture for large scale search and analytics**
  - **Billions** records/day, **Trillions** of stored records, **Petabytes** of storage
    - *Google File System 2003*
    - *Google MapReduce 2004*
    - *Google BigTable 2006*
- **Design Parameters**
  - Co-mingled data and analytics
  - Performance and scale
  - Optimized for ingest, query, and analysis
  - Relaxed data models
  - Simplified Programmability
- **Implications**
  - New designs required
  - Makes new functionality possible

Utility Clouds

- **Compute and storage services for outsourcing IT**
  - **Concurrent, independent users** operating across **millions** of records and **terabytes** of storage
    - *IT as a Service*
    - *Platform as a Service (PaaS)*
    - *Software as a Service (SaaS)*
- **Design Parameters**
  - Isolation of user data and analytics
  - Portability of data with apps
  - Hosting traditional apps
  - Lower cost of ownership
  - Capacity on demand
- **Implications**
  - No changes to designs
  - Low cost through elasticity


Patent Search
All Records
service
readable
resource
node
elements
nodes
wireless
mobile
point
code
program
segment
electronic
control
secure
It isn't (just) the technology,
It's the people.
pri
authentication
crypto
service
packet
forwarding
source
authentication
secure
software
authentication
certificate
entity
virtual
address
connection
encrypted
cryptographic
encryption
image
digital
encoded
packet
packets
address
signal
content
encoded
gaming
software


NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA


RESEARCH DIRECTORATE
ADVANCING INTELLIGENCE THROUGH SCIENCE

Extras

Research Top Ten IRAD Suggestions

1. Cyber Situational Awareness, Cyber Attribution
2. Massive Data (Mining, Analytics), Statistical Analytics
3. Human Language Technologies – speech-to-text (rare languages)
4. Video – collection, processing, analysis
5. Visualizations and tools to enhance analyst productivity
6. Wireless – especially new mobile broadband technologies – LTE/WiMax
7. Virtualization
8. Secure Mobile Technologies (ideally using COTS devices)
9. Advanced Technologies for HPC
10. Systems Understanding (R/E at the system level)

IAD Authorities

- **E.O. 12333 (1981)** - NSA named executive agent for the communication security of the United States government.
- **Computer Security Act (1987)** – NIST, with NSA technical advice, responsible for developing standards and guidelines needed to assure the security and privacy of sensitive information in Federal computer systems.
- **NSD – 42 (1990)** – DIRNSA named the National Manager for National Security Systems.
- **Executive Order 13587 (EO 13587)** –"Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information."

Center for Advanced Study of Language

CASL is a university affiliated research center (UARC) collaborating across government, academic, and private sectors.

UNIVERSITY OF MARYLAND
CASL
CENTER FOR ADVANCED STUDY OF LANGUAGE

R4 - Laboratory for Telecommunications Sciences

R4 conducts advanced research on all aspects of networking to include next-generation wireless, global telecommunications infrastructures, geolocation, special purpose computing, and high-speed information processing.