Identity Superiority

Morris Hymes

TRANSFORMING NATIONAL DEFENSE - NET-CENTRIC

NATIONAL SECURITY STRATEGY

Transform America's national security institutions to meet the challenges and opportunities of the twenty-first century.

NATIONAL DEFENSE STRATEGY

We will **conduct network-centric operations** with compatible information and communications systems, usable data, and flexible operational constructs.

Beyond battlefield applications, a **network-centric force** can increase efficiency and effectiveness across defense operations, intelligence functions, and business processes...

Transforming to a network-centric force requires fundamental changes in process, policy, and culture.

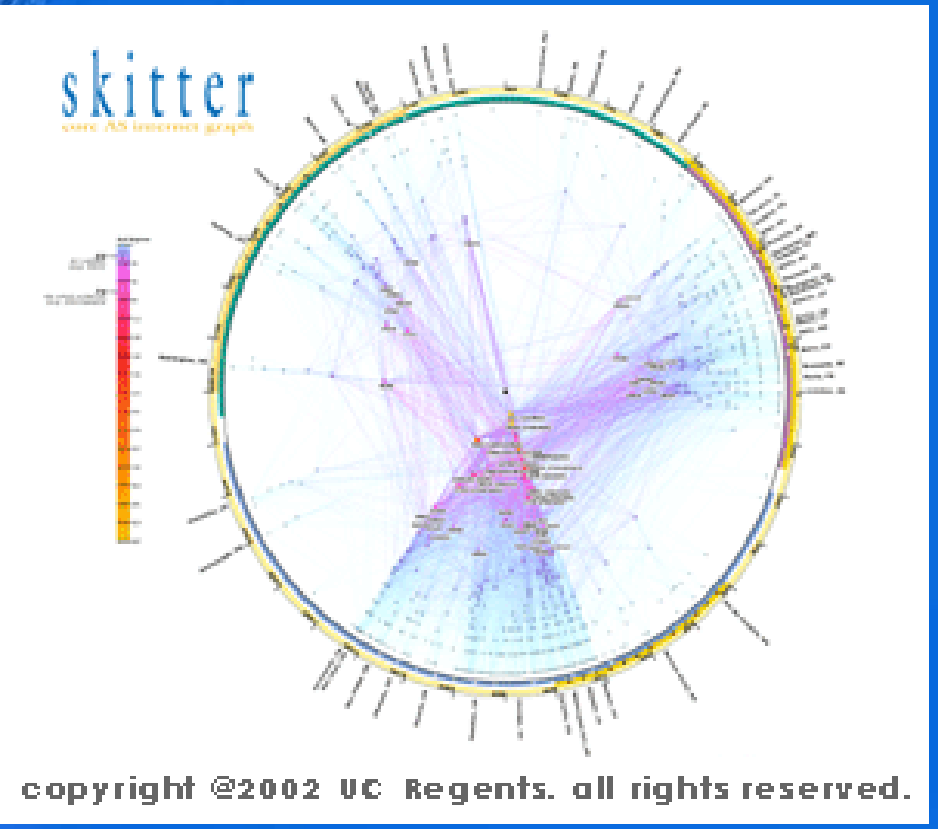
NATIONAL MILITARY STRATEGY

...creation of a collaborative information environment that facilitates information sharing, effective synergistic planning, and execution of simultaneous, overlapping operations... on demand to defense policymakers, warfighters and support personnel.

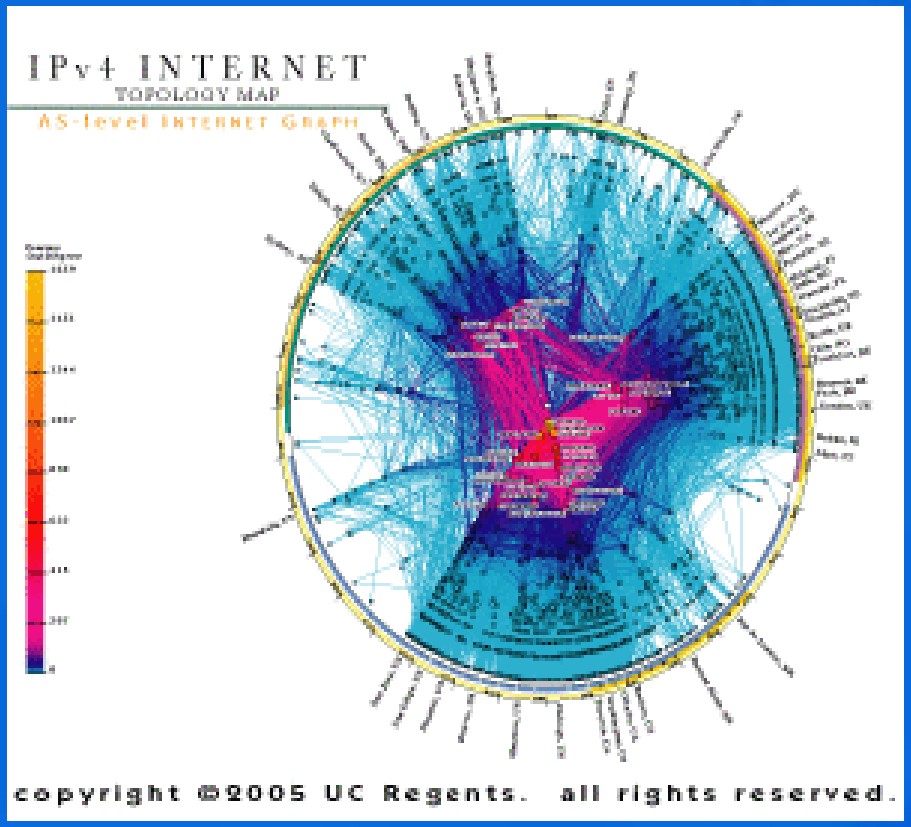
Use of the INTERNET

- Use of Internet has exploded over the last 20 years
- Global War on Terrorism (Iraq/Afghanistan)
  - First extensive use of Internet
  - Adversaries also using Internet
- Trust is most critical element in use of modern communication systems
- Challenge is identifying Red Force from Blue Force on the Internet,
  - but, Internet was not designed with Identity in mind

Explosion of Internet Connections

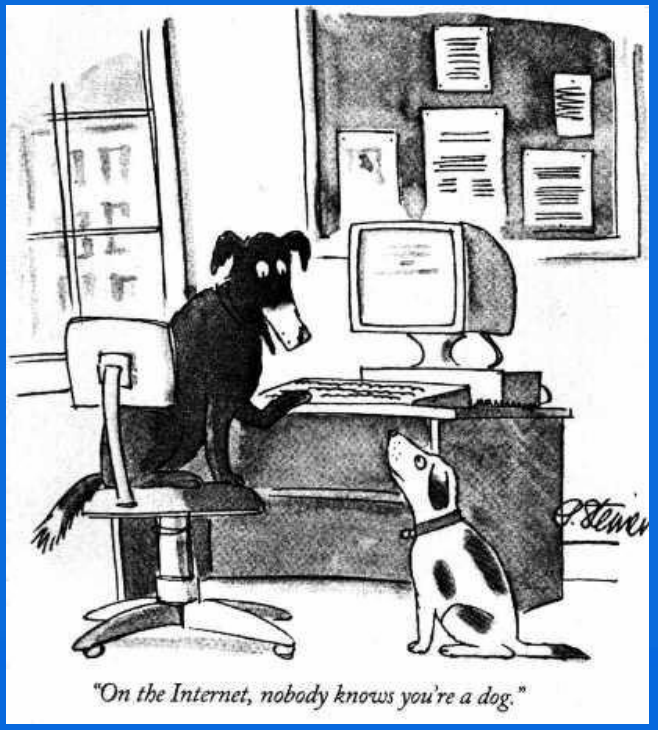


January 2000



April 2005

1990's View of the INTERNET



Peter Steiner's famous *New Yorker* cartoon captioned "On the Internet, no one knows you are a dog," July 5, 1993

DoD IDENTITY PROTECTION & MANAGEMENT SENIOR COORDINATING GROUP

BIOMETRICS

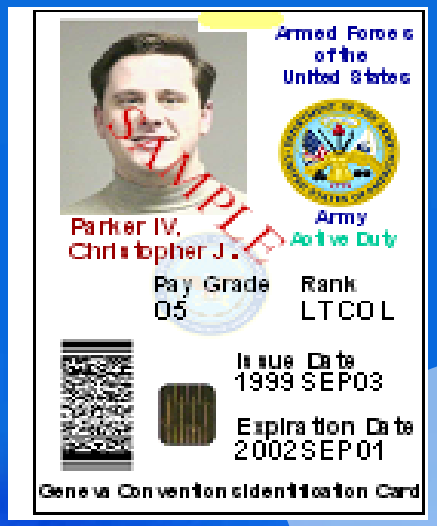
DoD COMMON ACCESS CARD (SMART CARDS)

PUBLIC KEY INFRASTRUCTURE

PKI's Role in Identifying Individuals

DoD's Public Key Infrastructure (PKI) is part of the larger DoD construct of Identity Management. PKI contributes to Identity Management by generating digital credentials that are:

- unique;
- un-forgeable,
- trusted for use in virtual network transactions



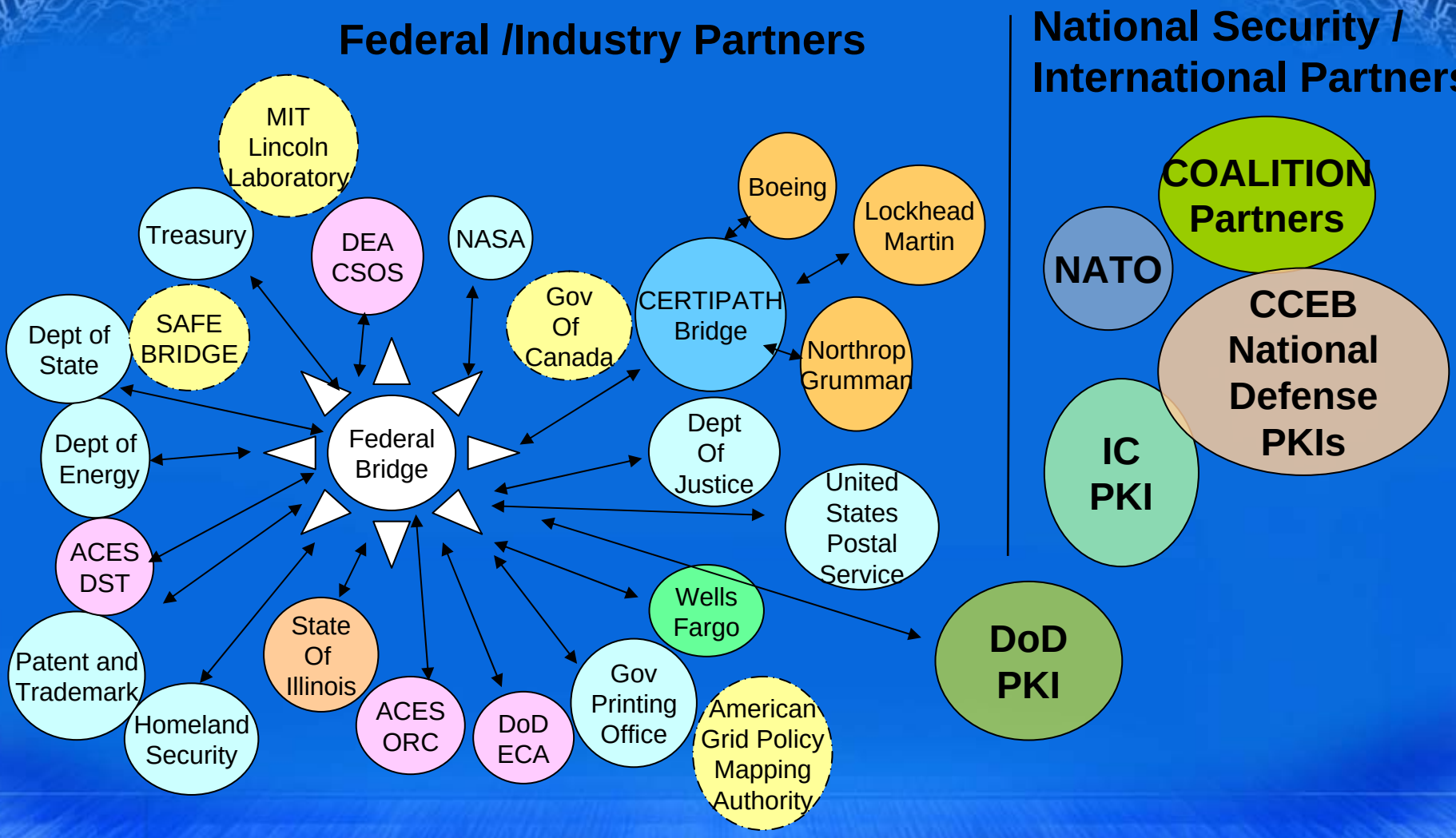
NIPRNET

- Issued 22 million certificates on NIPRNet
- Issued ~ 10M Common Access Card (CAC's)
  (More than 90% of target population now has a CAC)

SIPRNET

- Issued over 50,000 software certificates on SIPRNET
  (Roughly 10% of target population has PKI certificates)

PKI's Trusted Interoperability Environment



Identity Superiority Context

Battlefield extends beyond territorial borders, it include global networks and information.

Authenticated access to facilities and equipment (physical), as well as, networks and servers (logical) is vital.

Web Server

Network domains, ex. .mil
Email

Assured identity credential (cards, PKI certificates, biometrics) are tools to determine and facilitate authorized access to individuals and devices.

Credentials also aid in detecting and determining unauthorized users both trusted insiders and hostile.

Key Tenets

1. Manage -

- **Use identity more effectively in identifying people, system, services and devices**
- **Use identity more effectively to share information and for Force Protection**

2. Dominate -

- **Discover/Generate identities of unknown individuals or resources both passively and actively**

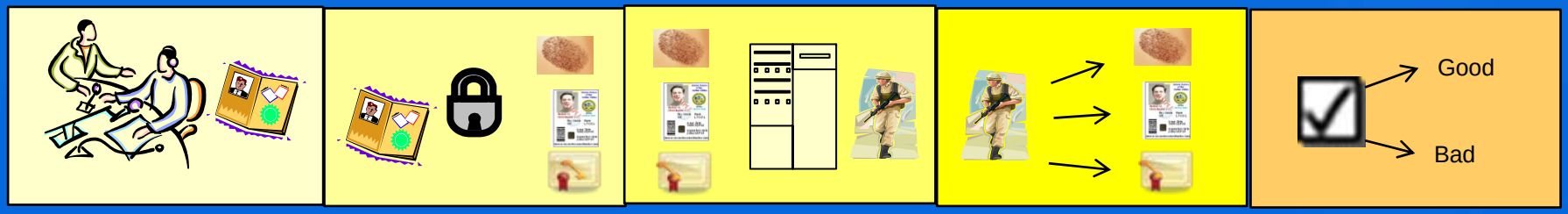
3. Assure -

- **Build a robust ID Superiority Infrastructure that protects** individual information and counters anticipated threats

Process is Key

Process for establishing identity:

1) common across different credential types (biometrics, PKI, smartcard)
2) similar for logical and physical networks
3) applicable to red, gray and blue forces
4) is expensive to replicate



Verifying identity documentation.

Binding identity information with credential.

Associating credential with individual. (Authoritative Source)

Discovering / Presentation of credential.

Validating credential

.

Challenges to Identity in Cyber World

- Privacy
  - American Citizens are very skittish about the government maintaining vast repositories of information for identifying individuals
    - John Poindexter – Total Information Awareness
  - Foreign Countries have laws regarding asking or storing privacy information on citizens
- Internet not designed with individual identity in mind
  - Identity extends to devices and information
- Trusted Infrastructure to support an identity capability not widely established

IDENTITY SUPERIORITY

Identity Mgmt:
Identify (people /systems/ services/ devices) and control with a high degree of confidence

Identity Dominance:
Capture & process Adversary ID information

Identity Assurance:
Protection against range of threats built upon a secure architecture

Built Upon

Associated credentials: UserID & PW

Assigned credentials: PKI certificates

Inherited credentials: range of BioMetrics

Infrastructure
Authoritative Sources
Mgt Controls

Applied Against

Logical Networks
Physical Networks

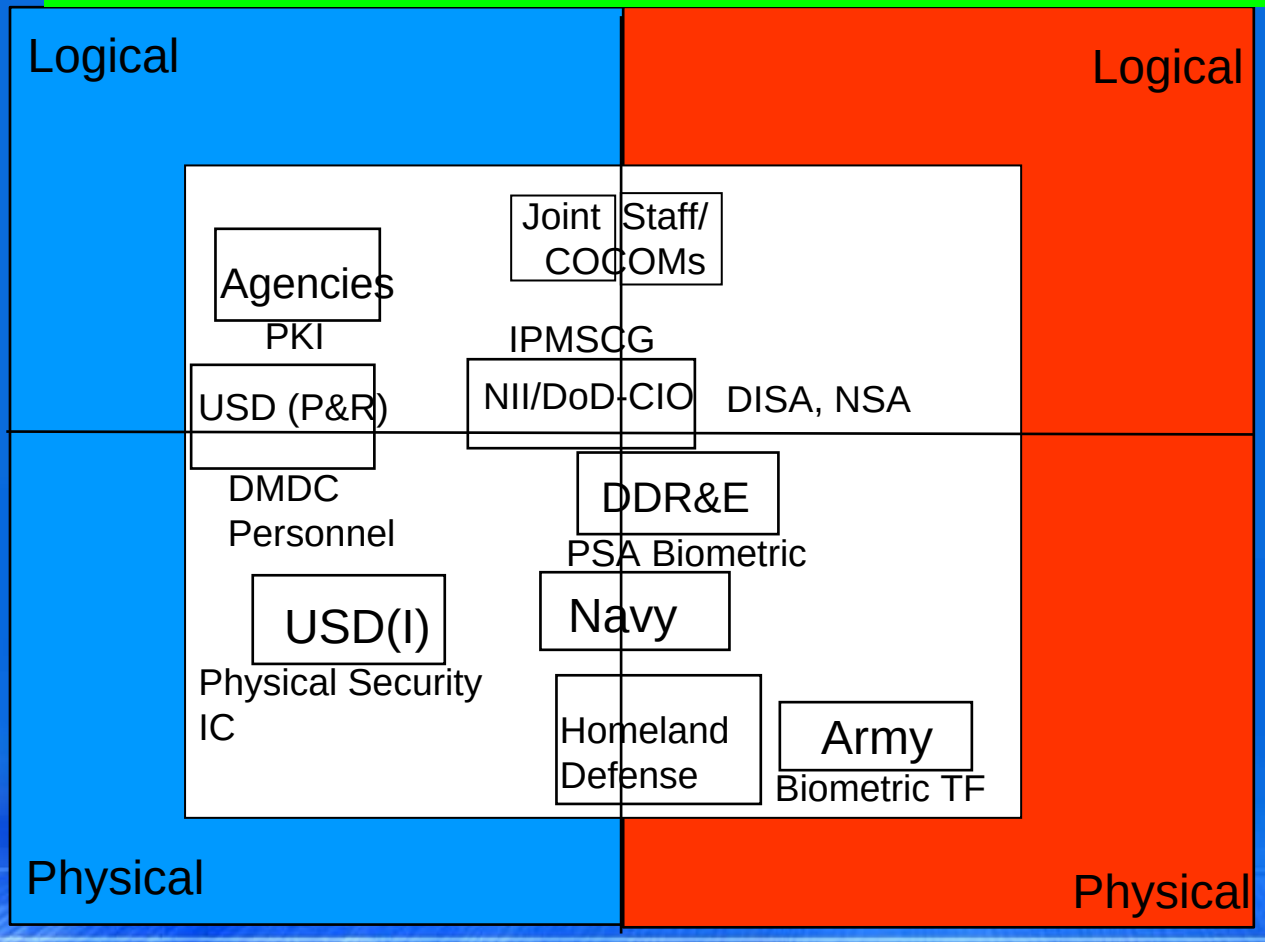
Building a Roadmap

How can we move forward:

1. Leverage common CAC & PKI infrastructure to support biometrics
2. Merge logical and physical networks (change of culture)
3. Protect individual identity information
4. Build a comprehensive view of identity (range of credentials, range of environments)
5. Define and establish authoritative sources
6. Turn ID Superiority into an operational construct (battlefield CONOP)
7. Federated Credentialing (recognize and accept non-DoD based ID credentials)

Virtual Team Organization

Virtual Team Structure => Collaborative effort addressing all stakeholder needs => Consensus



DoD Enterprise Roadmap to ID Superiority - the next chapter

Closing Remarks

- **Possible ISPAB Support**
  - **Encourage the development of guidelines for authoritative sources and protection of biometric information.**
  - **Promote government structure that addresses certification and accreditation challenges across organizational boundaries .**
  - **Consider whether there is a need to create common standards for sharing /accessing identity information. (law enforcement vs operational use)**
  - **Discuss decision support systems that assist with authorization services and address privacy issues associated with aggregating identity information.**