Defense Information Systems Agency

Department of Defense

Hard Problems: Information Assurance

Richard Hale
Chief Information Assurance Executive
Defense Information Systems Agency

September 5, 2008

Our IA Goals

(Our Highest Level Hard Problems)

1. Ensuring that DoD and its mission partners can depend on information and on the information infrastructure in the face of physical and cyber warfare

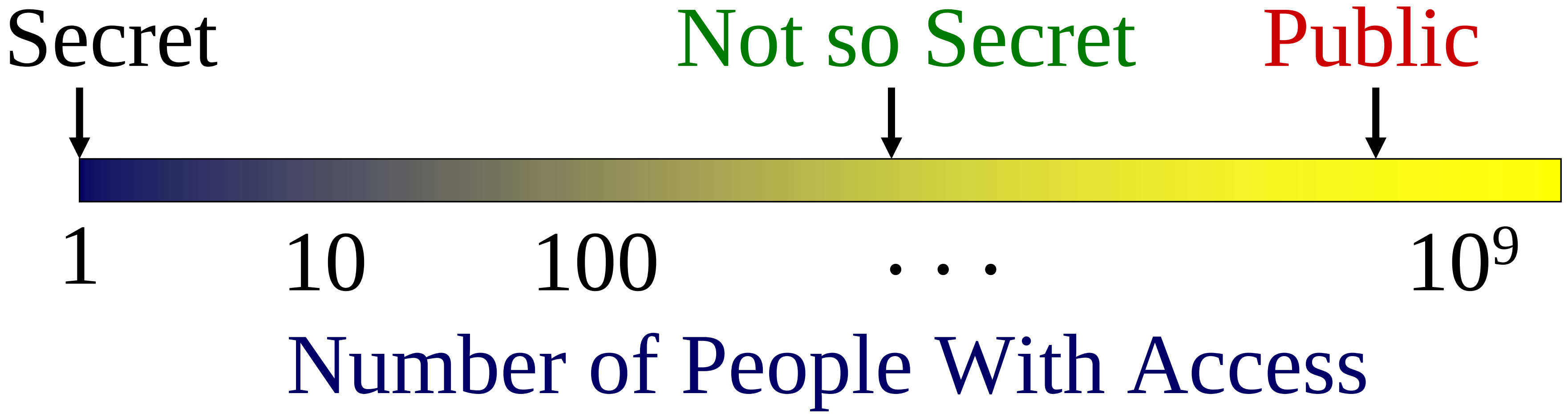
Or, Dependability in the Face of Cyber Warfare

(Aka Mission Assurance)

2. Ensuring that DoD and its mission partners can keep a secret (when we/they want to)

Hard Problem:

Keeping a Secret While Sharing Broadly



My Oversimplification of How DoD Is Pursuing These IA (and sharing) Goals

Part 1

Limit exposure of vulnerabilities by

- ***Removing*** as many of these vulnerabilities as possible (e.g. encrypt when appropriate, configure things securely, remove unnecessary functions, eliminate passwords)

- ***Layering protections*** that incrementally limit the population with access to a given vulnerability (defense-in-depth)

- ***Designing*** what DoD looks like to partners, to the public, to adversaries

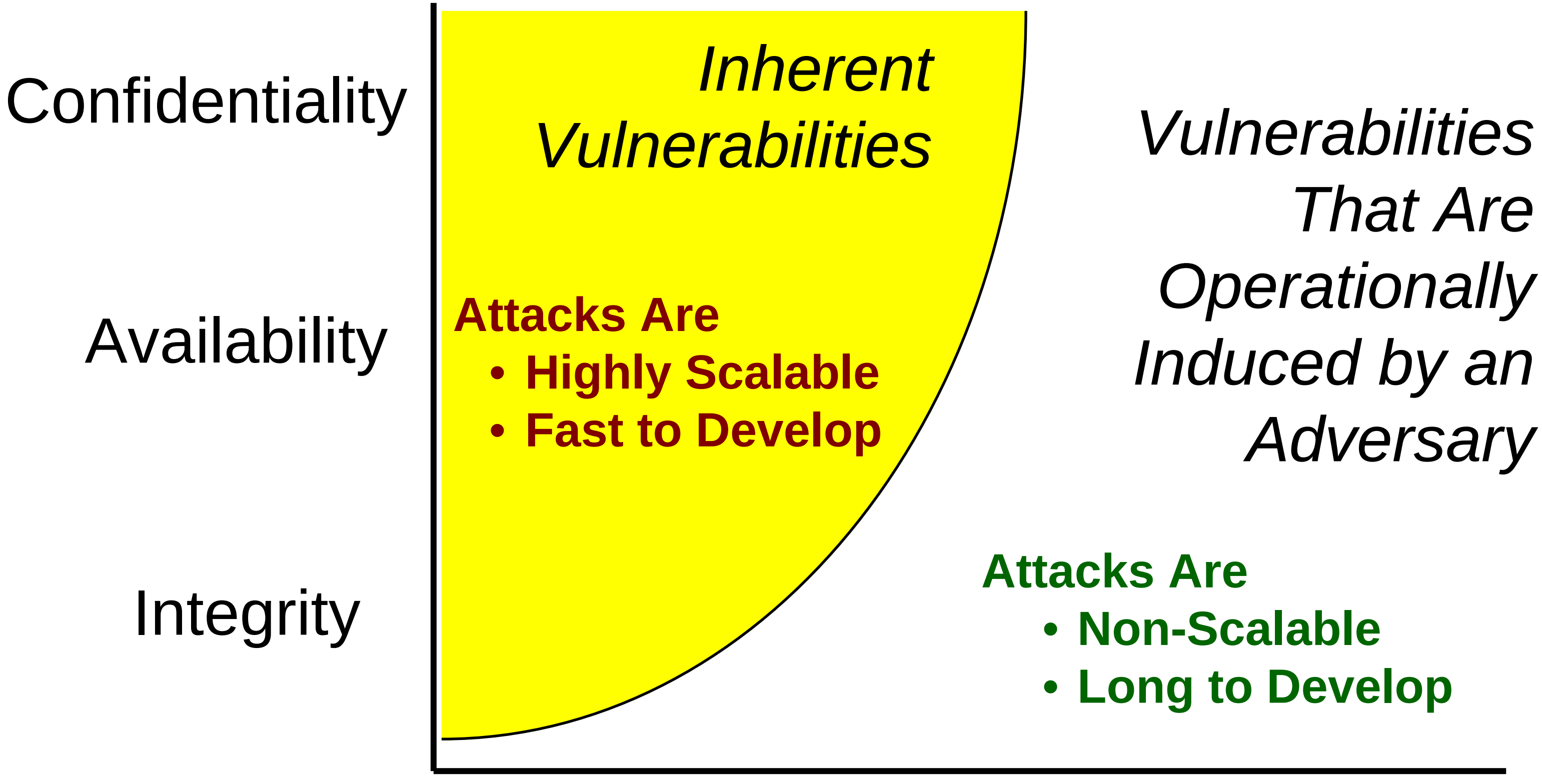
Part 2

- **Drive-out anonymity** (and enable net-centricity and improve sharing) by broad use of non-spoofable cyber identity credentials (aka ***PKI***)
  - Minimize whole classes of worries; brings accountability, *worries some classes of bad guys*

- **Build and operate** an **attack detection and diagnosis** capability that allows rapid, sure, **militarily useful reaction** to cyber attacks

- **Improve joint, coalition, interagency, & industry partner cyber operations/ NETOPS** so the above is possible

Vulnerabilities



Confidentiality

Availability

Integrity

Inherent Vulnerabilities

Attacks Are

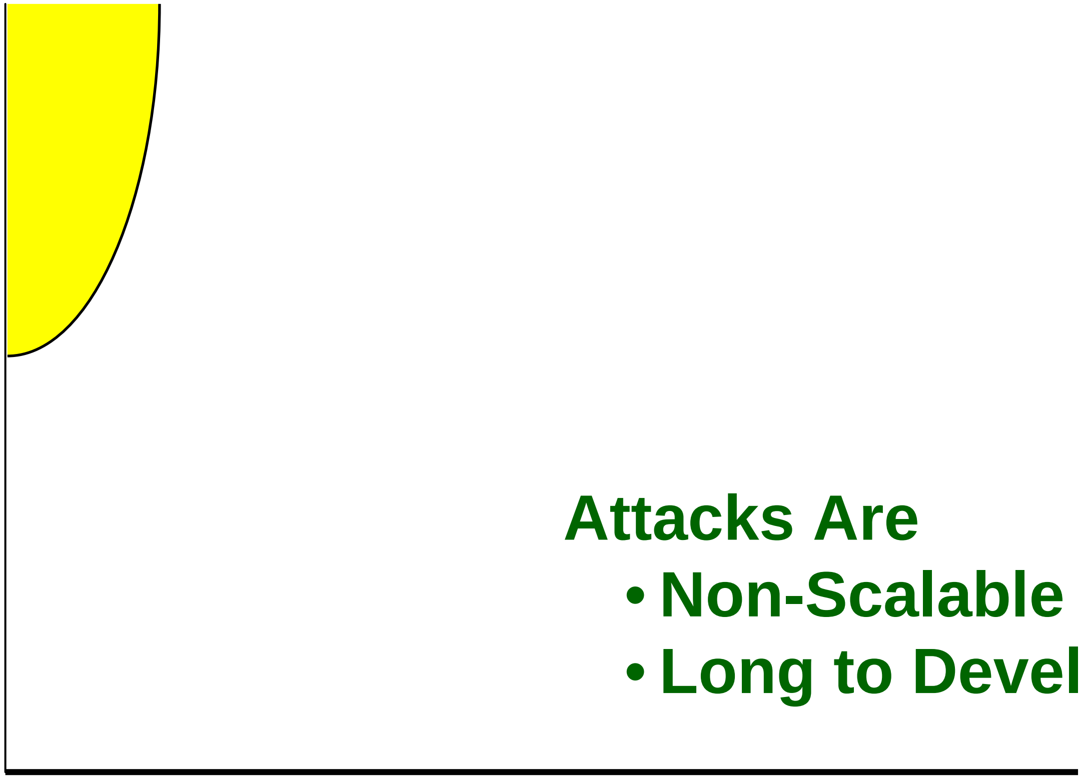
- **Highly Scalable**
- **Fast to Develop**

Vulnerabilities That Are Operationally Induced by an Adversary

Attacks Are

- **Non-Scalable**
- **Long to Develop**

After the Basics:



Attacks Are

- **Non-Scalable**
- **Long to Develop**

Hard Problem: Then What?

Possibility? Introduce uncertainty for the attackers in the operationally induced vulnerability area

- If the attack takes time to develop then changes can disrupt the effectiveness of the attack
- (Churn as a defense strategy)

Hard Problem: How?

Related Hard Problem: Spotting and Diagnosing & Reacting to an Engineered-In Attack

Back To The Basics

- Configuring everything properly means we encourage homogeneity owing to opportunities to automate, economies, simpler training, etc.

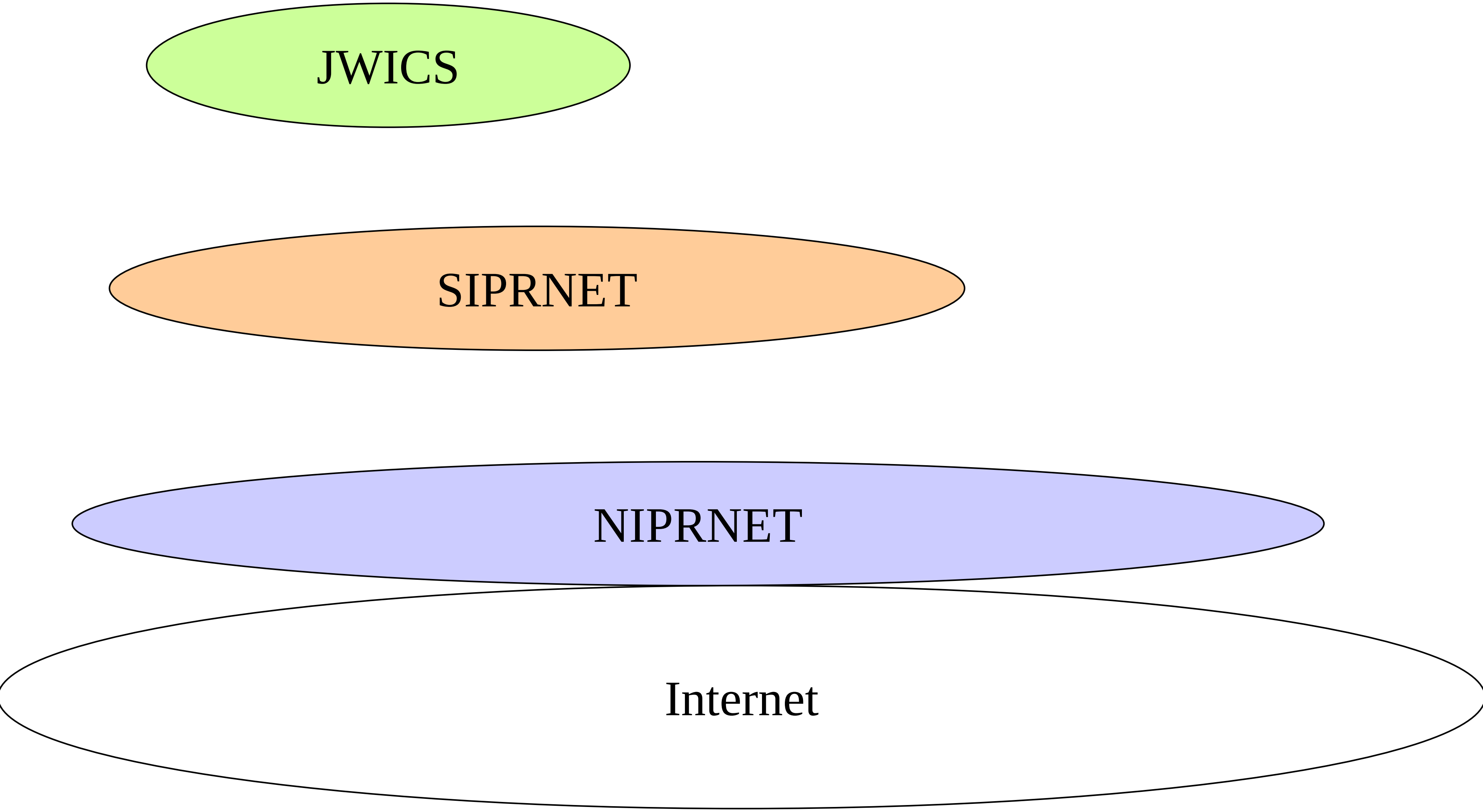
- *Hard problem:* How far can (should) we take homogeneity?

Hard Problems: Software & Systems

- Understanding that complex software or software and hardware is benign
- Or (harder?), understanding how it isn’t but finding ways to use it anyway
- Doing either of the above without good access to design documents, source code, developers, process audits, etc
- Globalized supply chain is a challenge (giant understatement)

Hard Problem: Information Sharing in the Federal Government in the Face of *System High*

(Or, ***What System-High Wrought)***



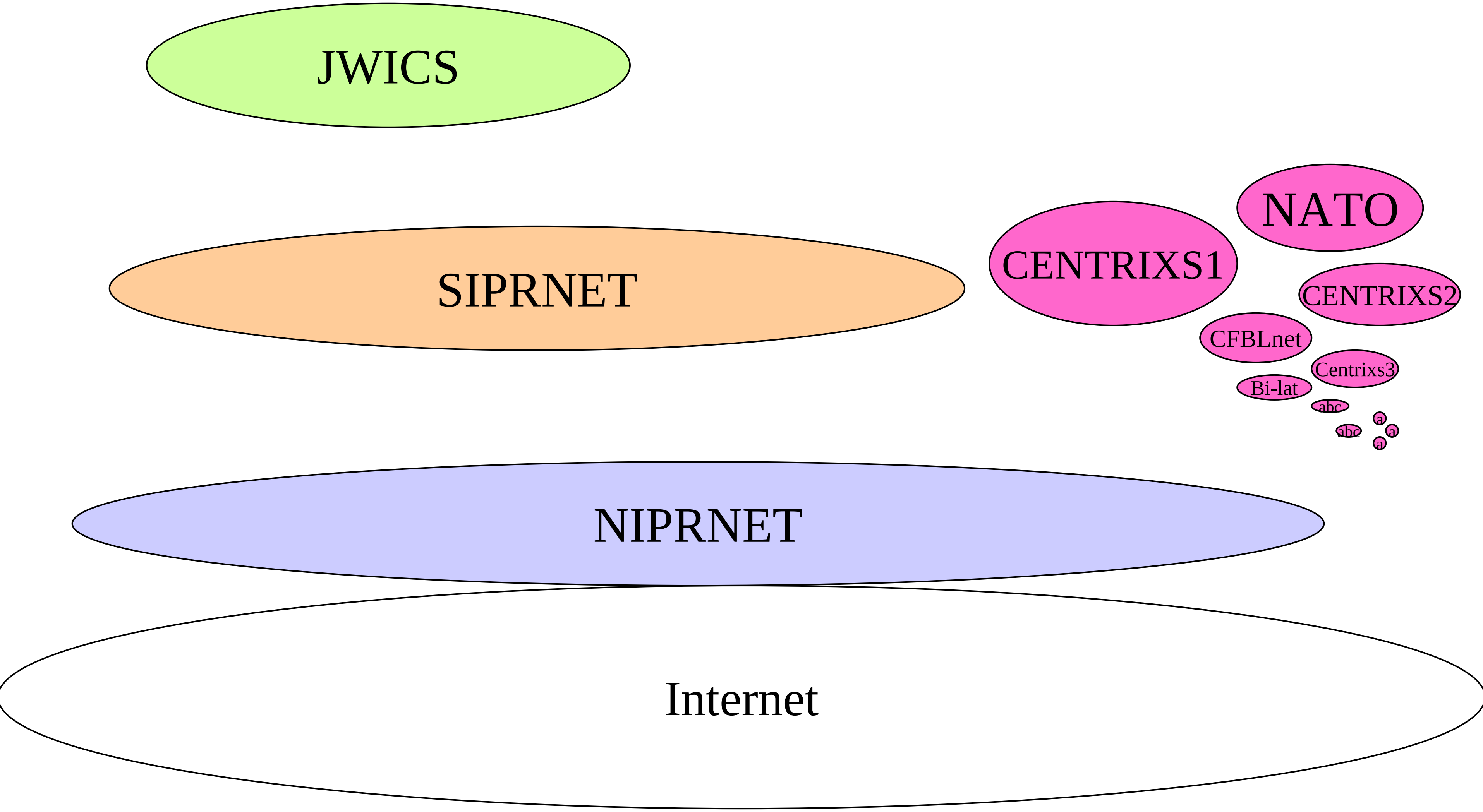
JWICS

SIPRNET

NIPRNET

Internet

Sharing With Allies



JWICS

NATO

CENTRIXS1

SIPRNET

CENTRIXS2

CFBLnet

Centrixs3

Bi-lat

abc

a

abc

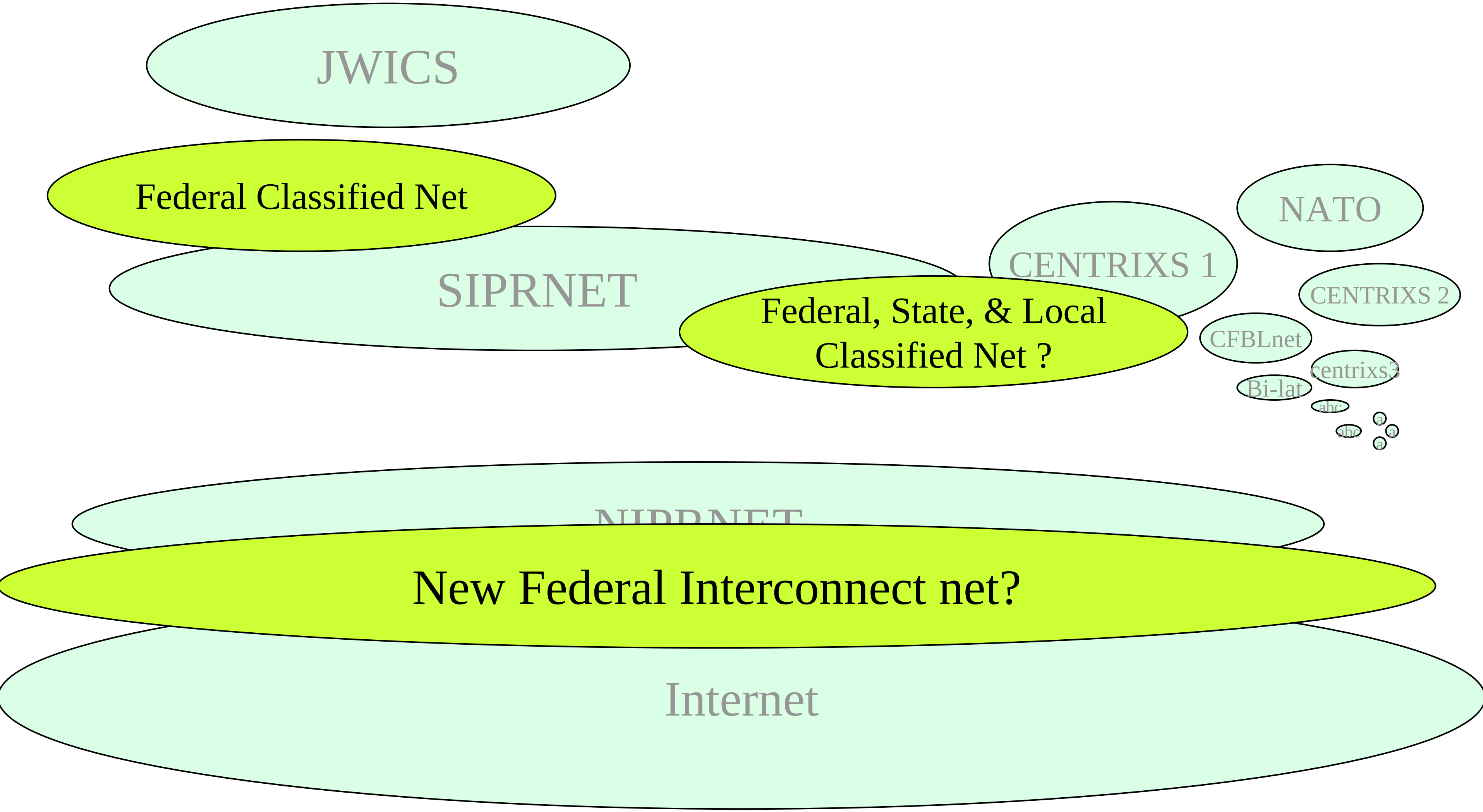
a

a

NIPRNET

Internet

Sharing in the Interagency



JWICS

Federal Classified Net

SIPRNET

CENTRIXS 1

NATO

Federal, State, & Local
Classified Net ?

CENTRIXS 2

CFBLnet

centrixs3

Bi-lat

abc

abc

a

a

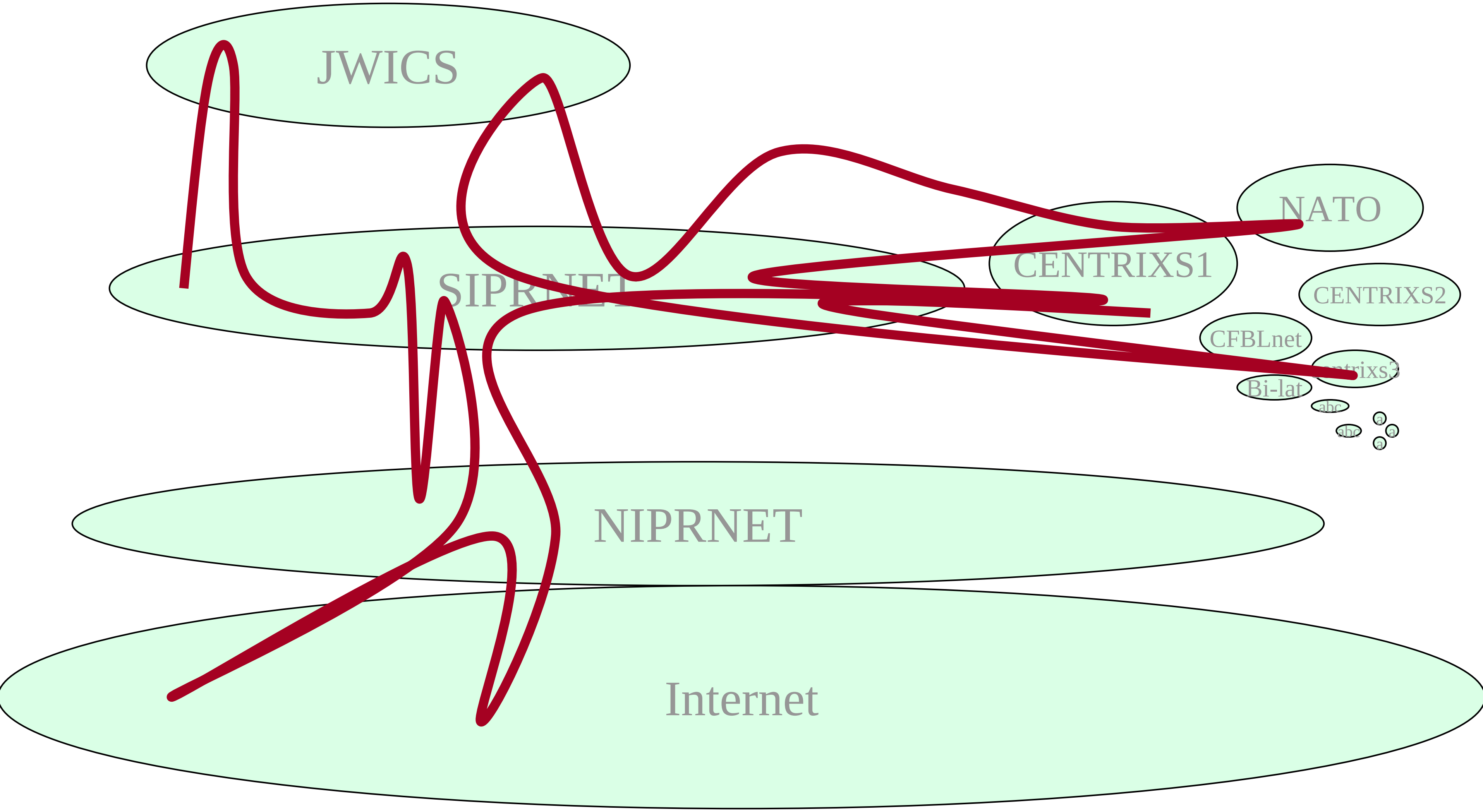
a

NIPRNET

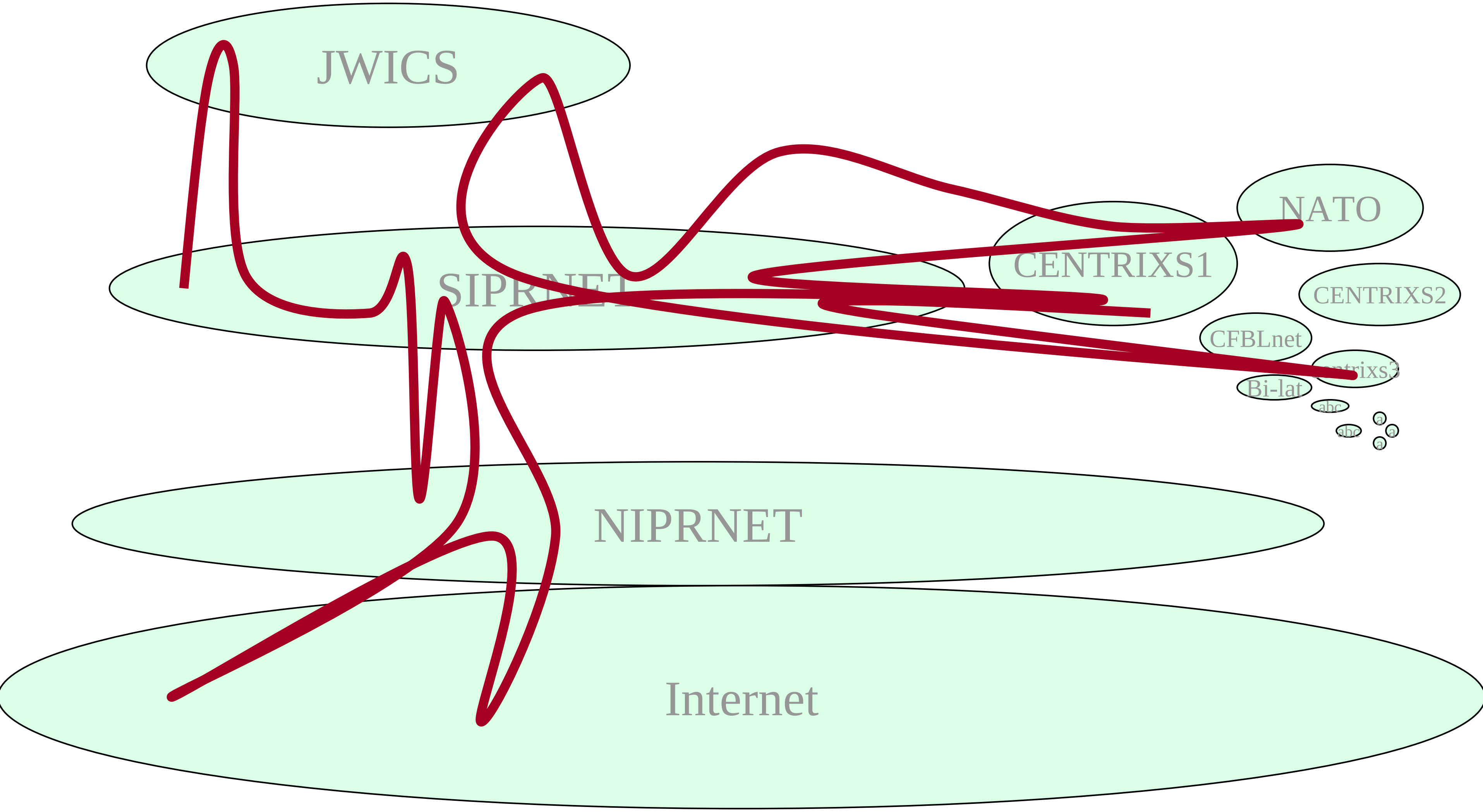
New Federal Interconnect net?

Internet

A Typical Netcentric Mission Thread

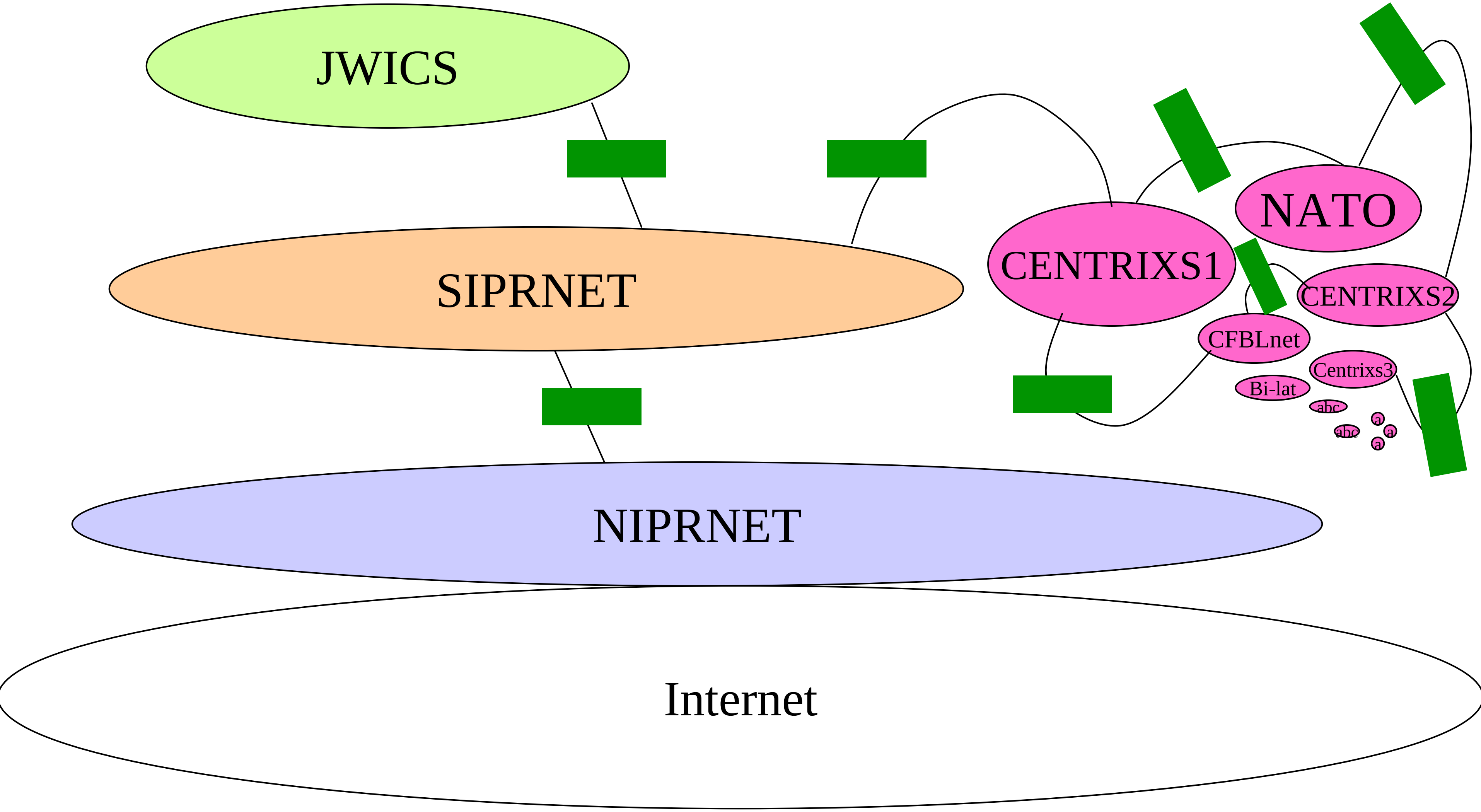

JWICS
NATO
CENTRIXS1
SIPRNET
CENTRIXS2
CFBLnet
centrixs3
Bi-lat
abc
a
abc
a
a
NIPRNET
Internet

(Hard Problem)

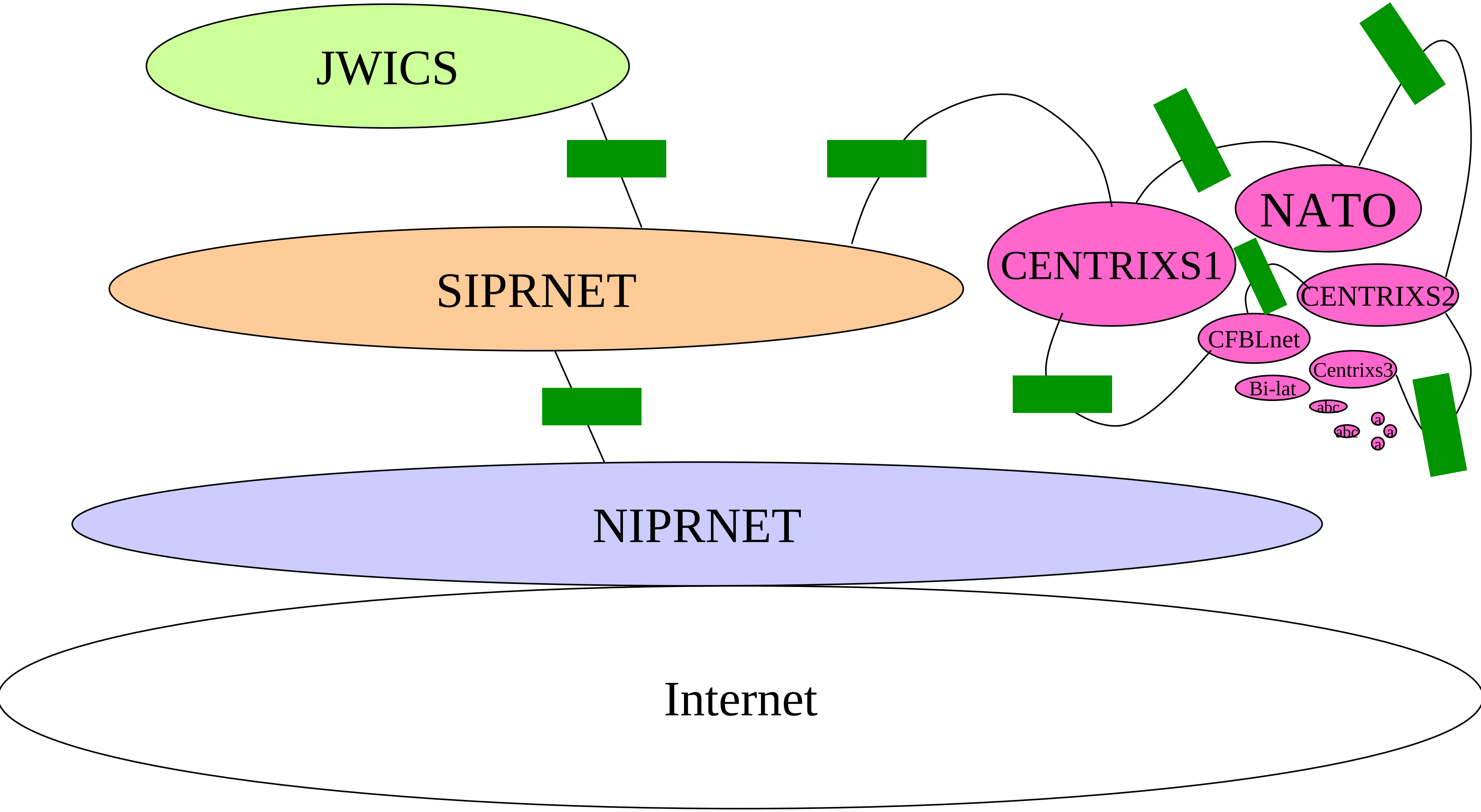


How Exactly Does That Sharing Work Now?

Cross Domain Stuff

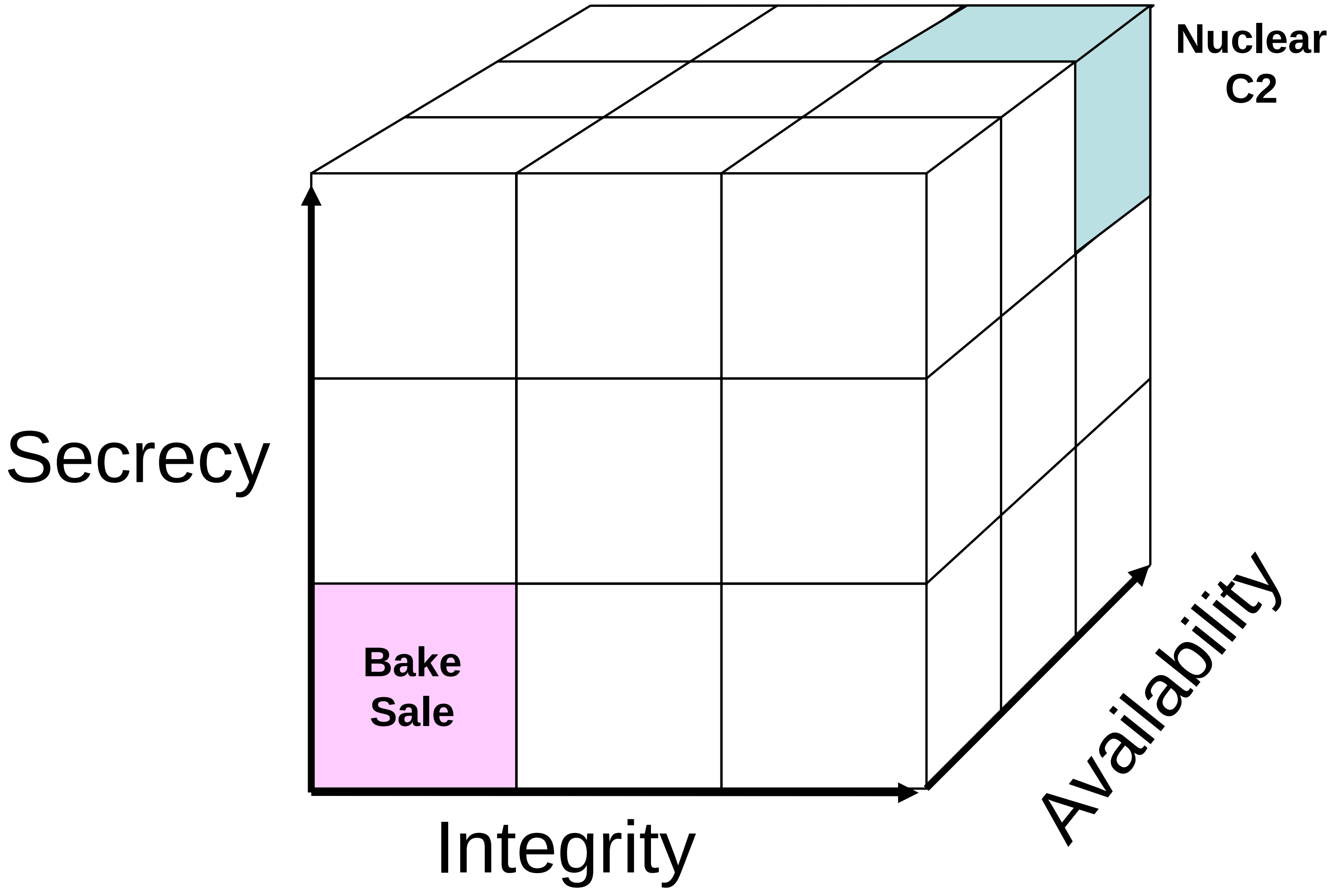


(So, This is a Closely Related *Hard Problem*)

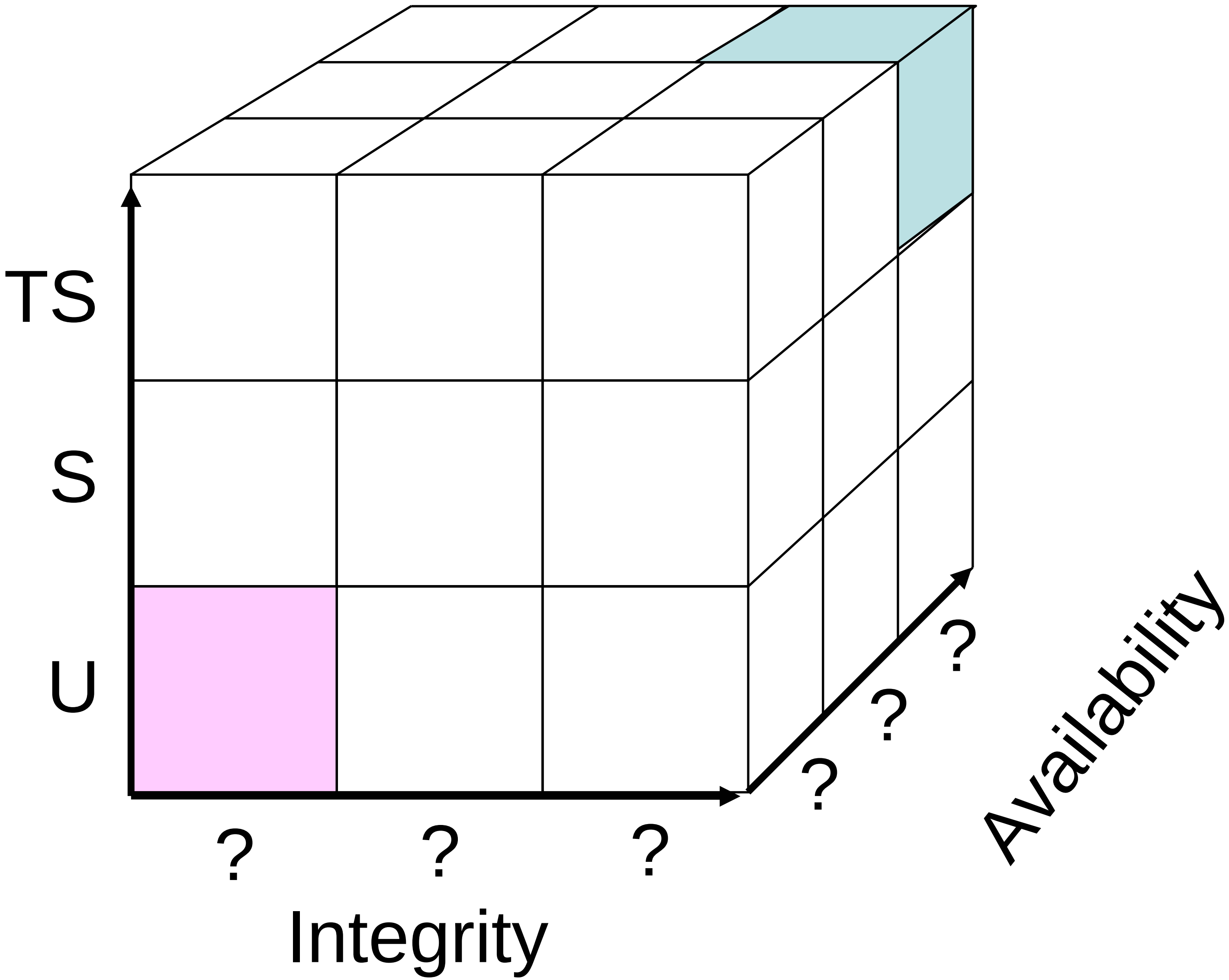


All this System-High stuff is pretty much focused on maybe *half* of Goal 2, that is, Confidentiality (and maybe some of the sharing part)

What’s System-High Got to Do With ***Assured Mission Execution in the Face of Cyber Attack? . . .***


Nuclear
C2
Secrecy
Bake
Sale
Integrity
Availability

How About All Those Missions In the Middle?

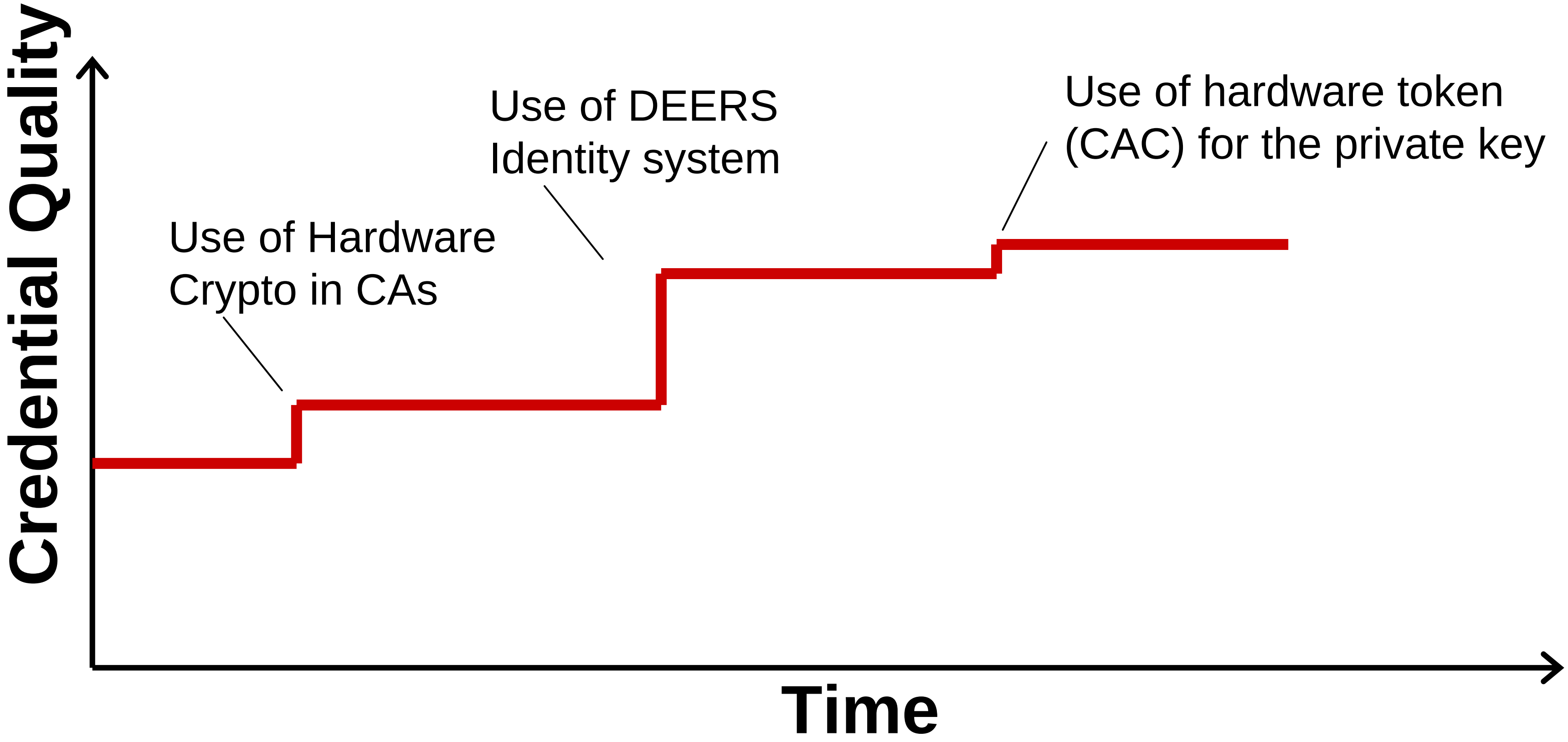


- System-High came from the days before everything was connected to everything else.
- It gives no priority to MISSION, only classification
- *Hard Problems*
  - Is there an overall architectural model for availability? What is it?
  - Ditto for integrity protection

A Little Bit About Driving Out Anonymity (& Improving Sharing?):

Challenge: DoD PKI Credential Quality

(How Much Can I Trust This Credential I've Been Presented?)



Hard Problem: Ad Hoc Coalitions

We often don’t know in advance with whom DoD will be working

Yet, we need to begin quickly sharing (…safely) and collaborating (safely) in spite of the lack of information about the other parties

Portion of This *Hard Problem*: How Do I Decide Whether to Accept Someone Else’s Identity Credential?

And harder yet…what do I do when someone has none?

Making an Access Control Decision

Before:

Allowing me to access information,
Allowing me to act in a certain role,
Doing business with me, etc.

Step 1. **Determine that it's *really* me**

Step 2. **Then, *learn things about* the real me**
before deciding to take a risk on me

Step 1: I present my credential (or hopefully I use my PKI private key to authenticate).

Then, all that stuff *about* me comes into play

Who Knows, Who Tells the Things About Me?

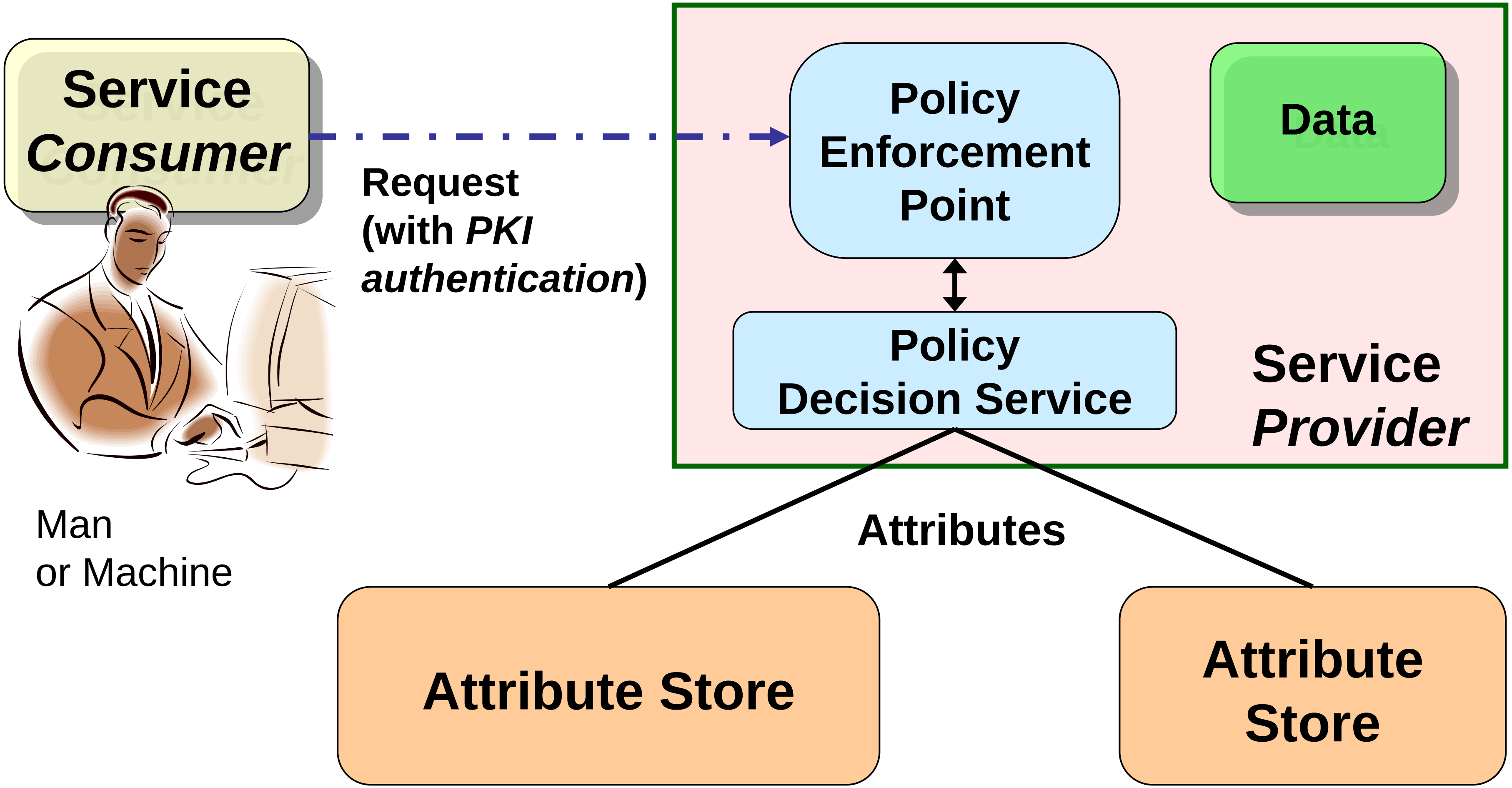
I Do

But if you don't know me, will you *trust* what I say?

Others Do

You *might* trust some of what *others* say about me (attributes about me)

Using Attributes About a Person, an Organization, A Service to Make A Sharing Decision



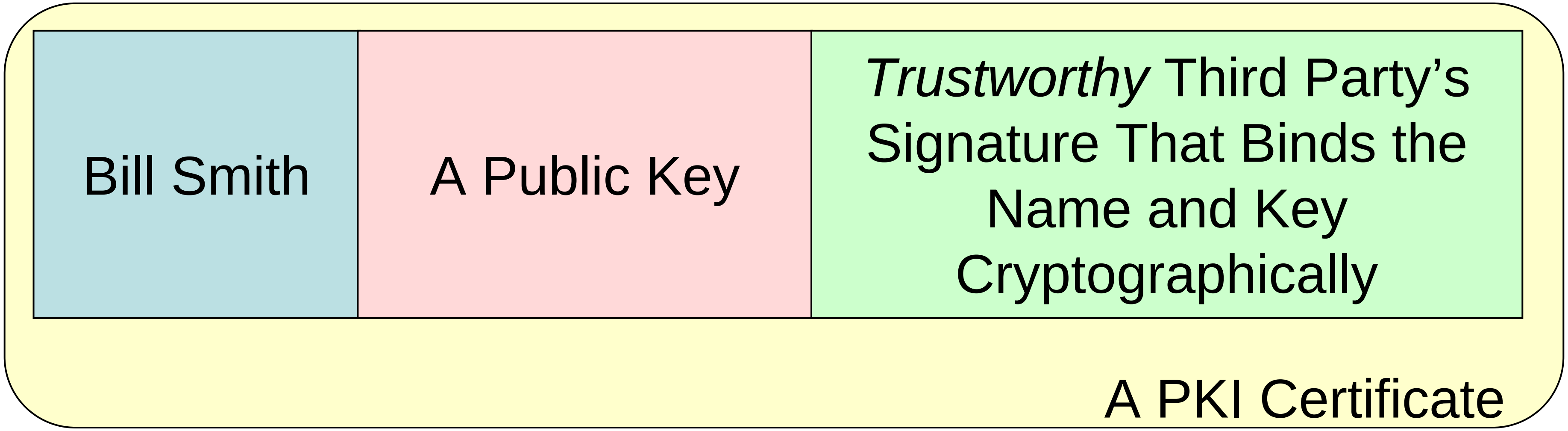
(Attribute-Based Access Control)

End User Hard Problem: Are Those Attributes Worthy of My Trust?

(Can I Make a Good Business Decision With Them?)

Hard Problem: Current cyber technologies don’t give end-users many useful, reliable cues so social engineering and technical attacks against end-users are easy

Background: Those PKI Credentials



Bill Smith

A Public Key

Trustworthy Third Party’s Signature That Binds the Name and Key Cryptographically

A PKI Certificate

Increased *assurance* that Bill’s public key is really his, and not John’s or Sam’s

Attributes and the Directory Problem

- Tight tie between me and my public key provided by my PKI cert (and by careful design of the issuance process)
- *Hard Problem:* **Where's the tight tie between me (my name or some other unique identifier) and an attribute about me?**
- *Hard Problem:* **Who is authoritative** for particular information about me?

How does a relying party know that my credit score, my clearance, my role, my grades, are really mine?

It Gets Harder the Farther From DoD I Go

- Getting authoritative information is harder
- Getting tamper resistant/tamper evident information is harder
- Understanding the reliability of third parties who will vouch for attribute information is harder
- Etc…

Hard Problem: How Do I Use Combinations of High Quality and Lower Quality Data to Make an Access Control Decision?

Fuzzy Attribute-Based (or Other) Access Control?

What About Fuzzy Attributes?

- We “add-up” answers to questions in real life. We make decisions based on a pattern of answers & patterns of experience

So, can we structure our systems so that a pattern of answers, possibly from many sources, adds up to something stronger than any of the answers themselves?

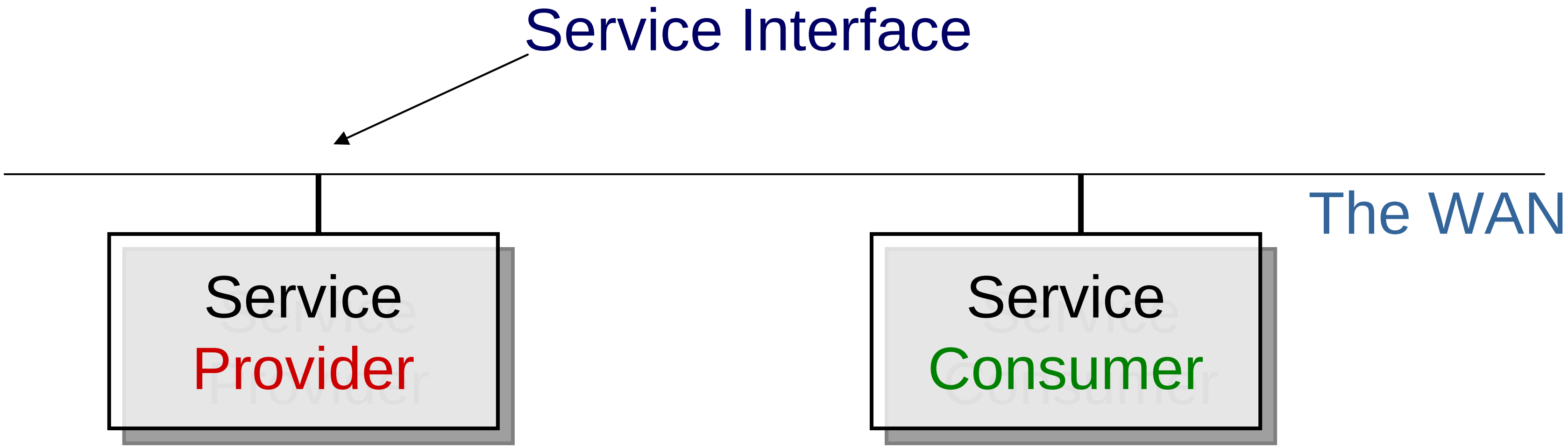
More General Hard Problem: How do we *quickly* establish *sufficient* trust between/among partners (in spite of the anonymity and the uncertain integrity of cyber space) to get work done?

Sharing & Application Agility:

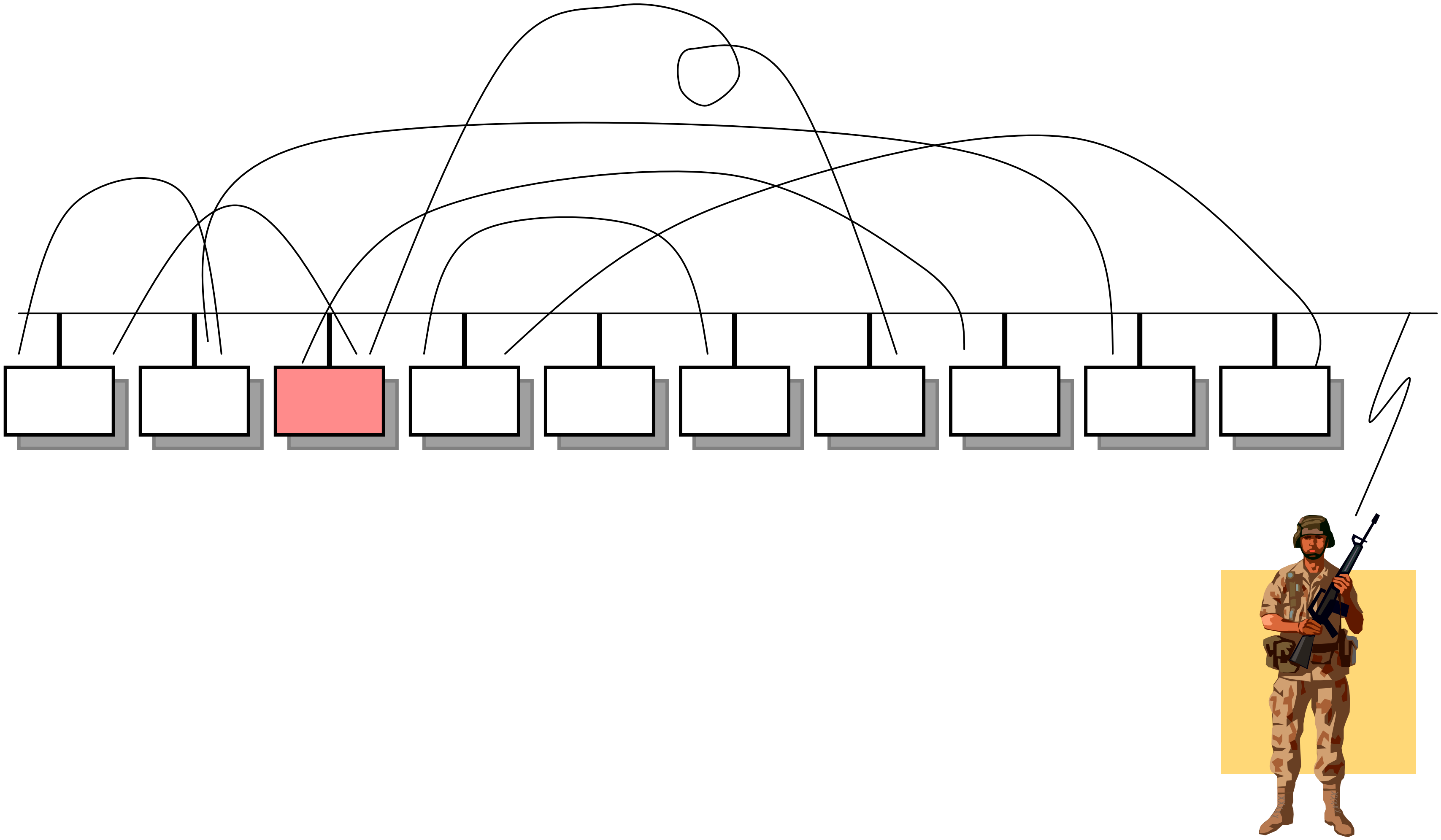
DoD Is Moving To The *Service Oriented Architecture* For Many Functions

Loosely coupled so innovation at the pace of each service provider. Business processes developed fast, especially if only need to compose existing services

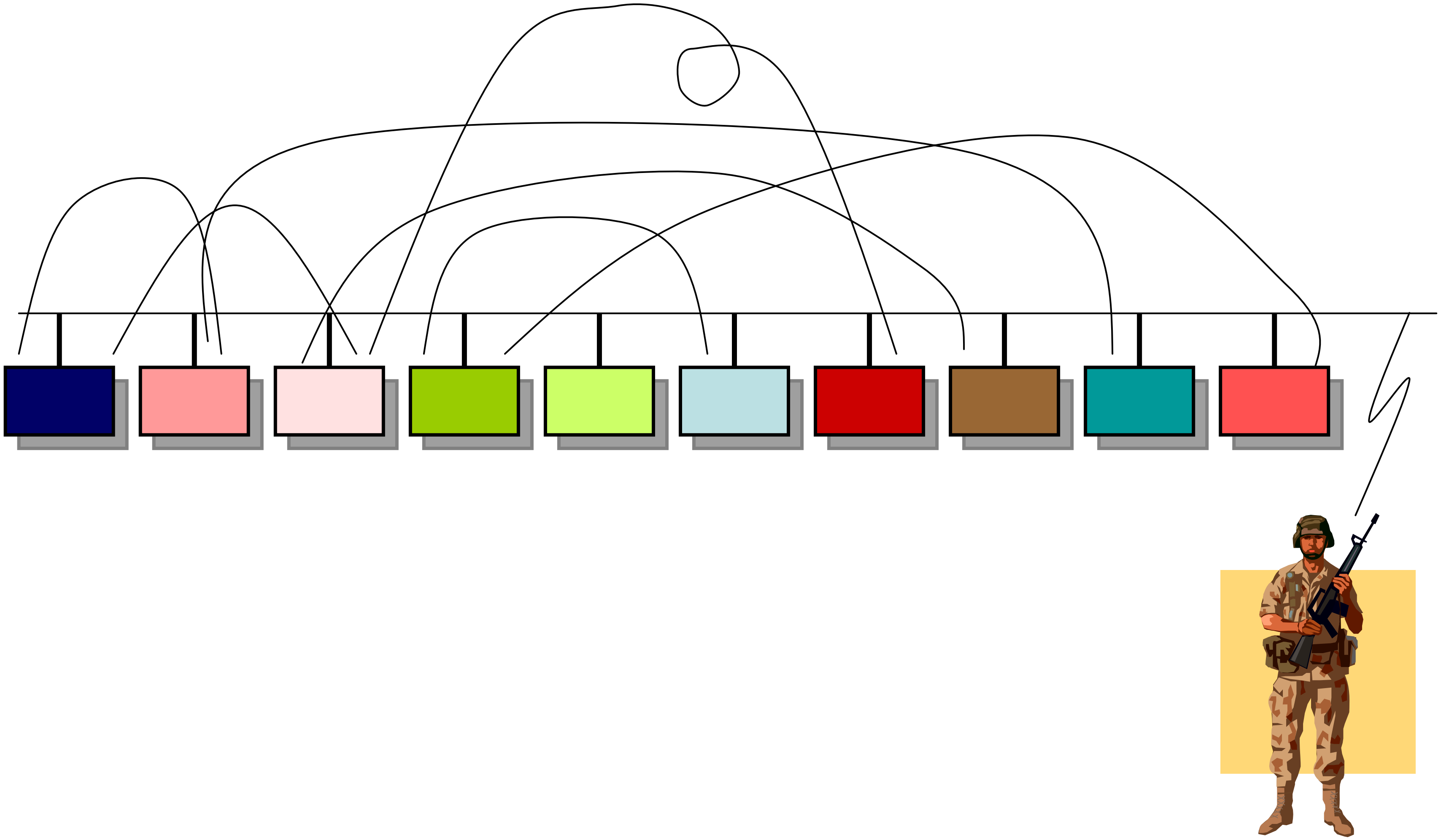
The Simple View of the SOA



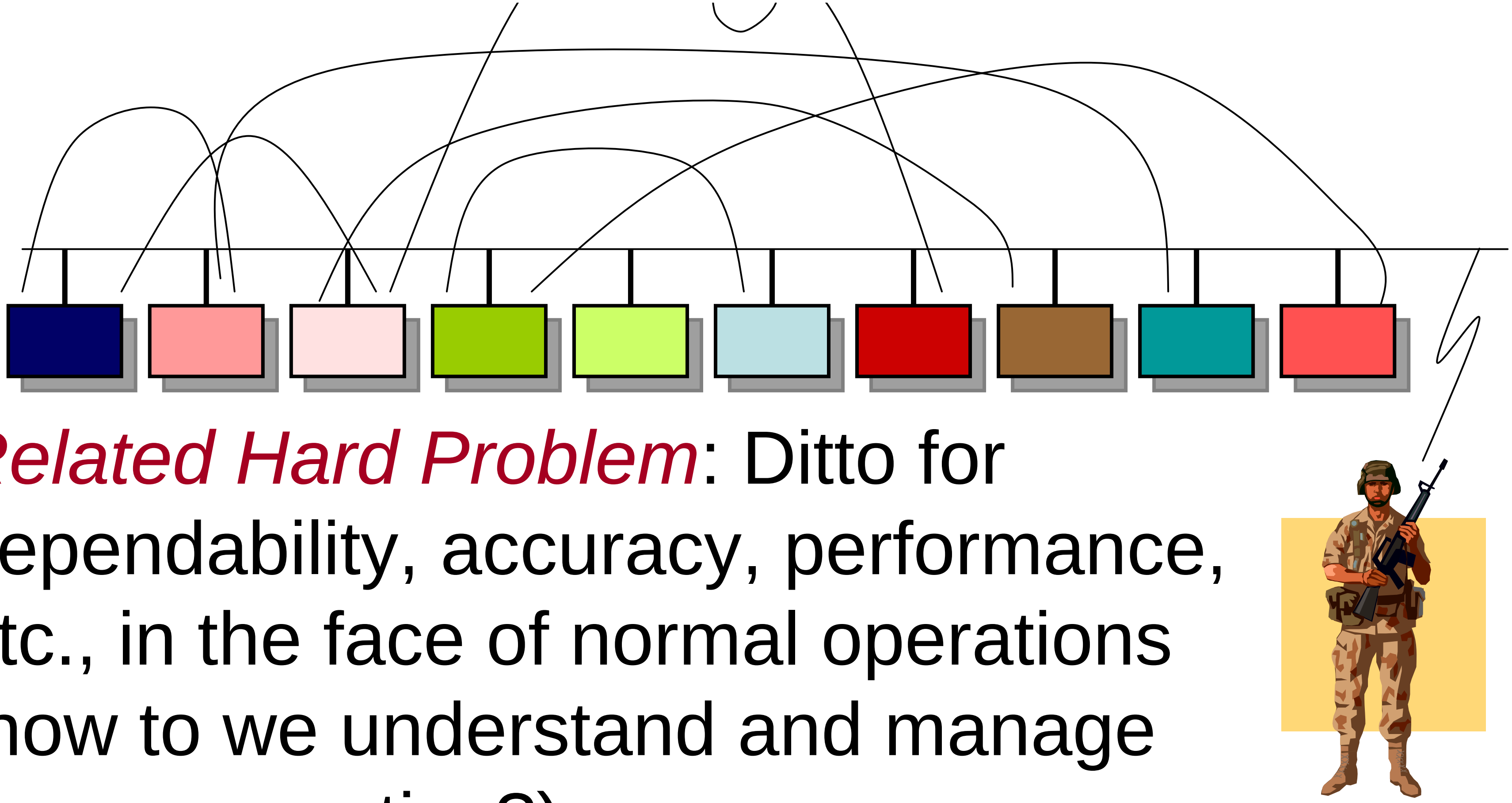
Composition of Services into an Application



Many Service Providers



Hard Problem: Developing, composing and operating for dependability in the face of cyber attack (and in the face of the many possibly independent service providers)



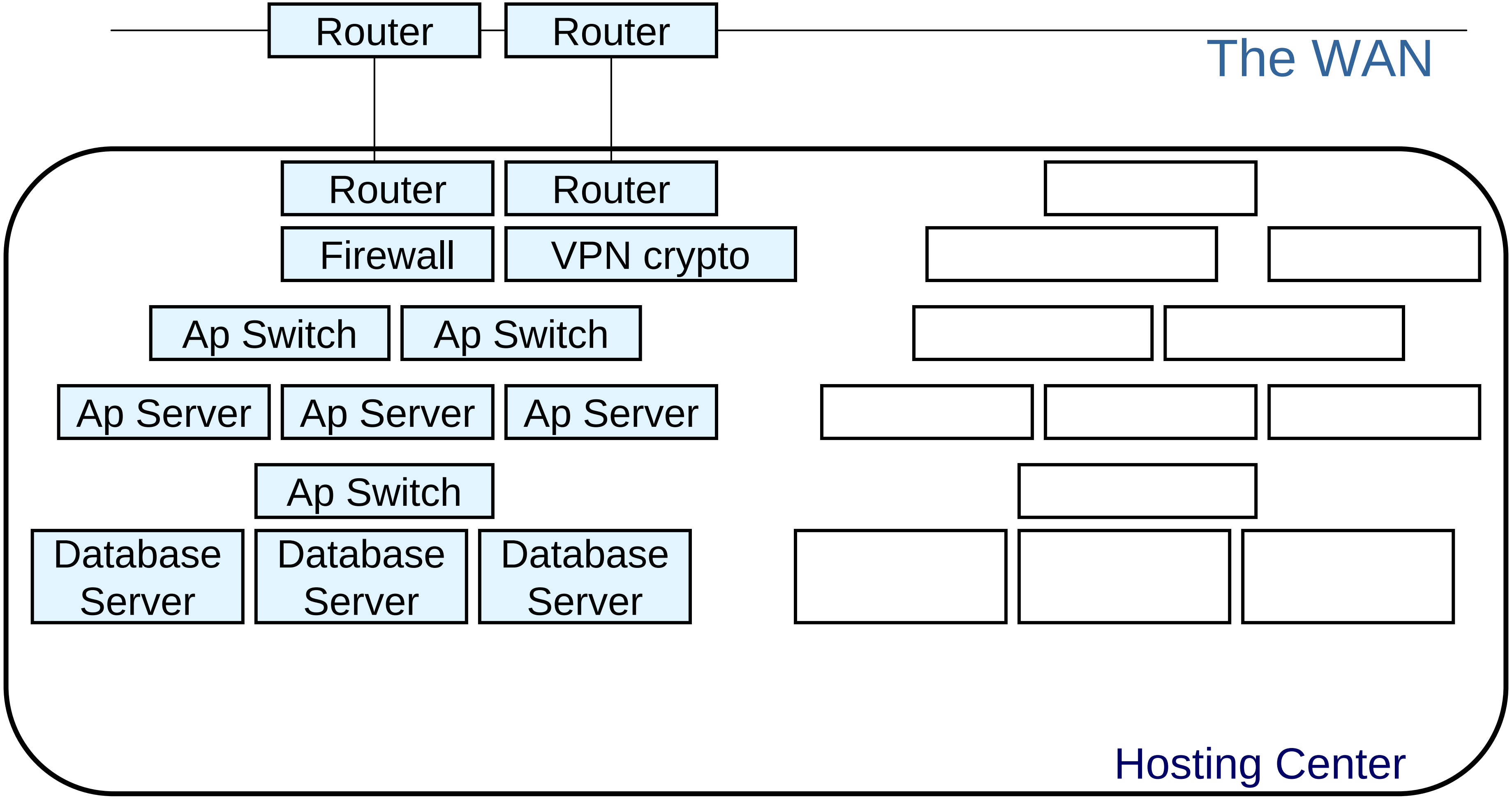
Related Hard Problem: Ditto for dependability, accuracy, performance, etc., in the face of normal operations (how to we understand and manage these properties?)

Related Hard Problems:

1. If there is only one human in this SOA picture, how does each service determine the human is really the entity on whose behalf service is being requested, and how does it make an (attribute based?) access control/service provisioning decision.

2.Can we assure each service provider that that service provider’s policy is being followed?

What’s Behind the Service Interface?



Problem: How Does Identity, Credentialing, Composition, etc. Work and What Can I Trust When All of This Stuff is Virtualized?

(Maybe This Isn’t A Problem)

Hard Problem: Fragility Avoidance as We Deploy All of This Security Stuff (Remember Our Customers)

(CAC PIN reset and my trip from south-western PA to Camp Dawson WV)

Hard Problem: The Network Is Converging

Who do you call when the everything-over-IP network is down? How did you do that again?

Incident & Attack
Detection, Diagnosis, and Reaction

Context for NETOPS

- DoD is really big, really complicated, and really mobile
  - 7 million things with IP addresses for instance
  - Everything has huge quantities of software and incredibly complicated hardware in it
- We're executing missions with thousands of partners who also have complicated organizations and infrastructures

Hard Problem: How Do We Ensure the Information Infrastructure Is Properly Supporting All (or the most important) Missions?

Related Hard Problem: How do we spot, diagnose, and do something about problems, especially cyber attacks in this infrastructure?

Hard Problem: (The Computer Network Defense Process)

- **Detect** the incident or attack or problem (hopefully before it's launched)
- **Diagnose** what's going on
- **Develop militarily useful courses of action**
- **Pick** one
- **Execute** it
- Then **follow up**
- Across all pieces/parts and all organizations that make up a mission thread

All in militarily useful time

To Summarize…

1. Dependability in the Face of Cyber Attack

2. Keeping a Secret

Both While Simultaneously Sharing Information Broadly

DEFENSE INFORMATION SYSTEMS AGENCY

www.disa.mil

iase.disa.mil