Constructive Key Management

Role Based Access to Information by Content Enforced by Cryptography

Tecsec, Inc

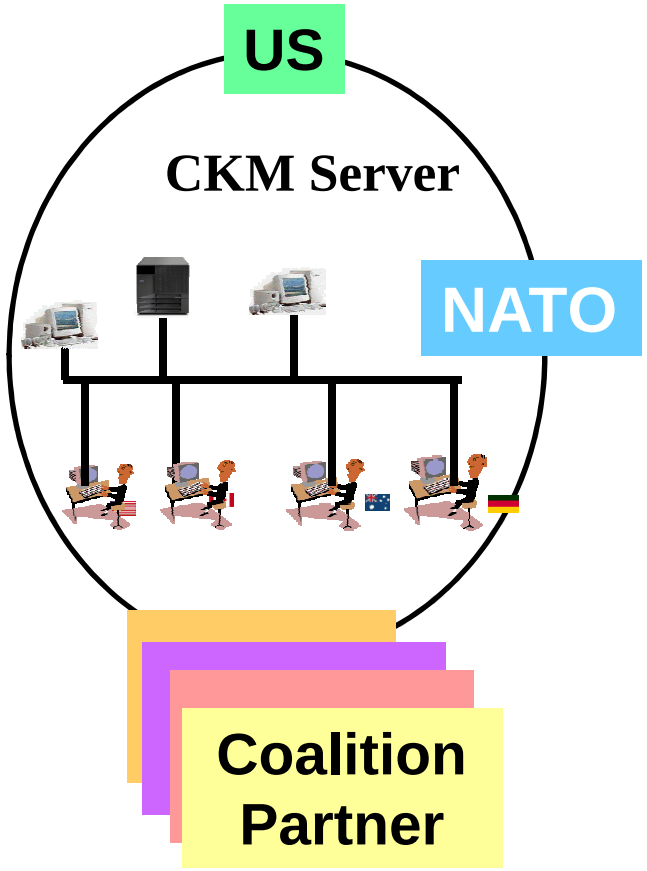
Information Sharing Challenge

Current Situation:

- US/NATO and Coalition forces cannot exchange information over networks
  - Separate networks are built for each new member
  - Very resource intensive
  - Requires "Sneaker Net"
- Coalition operations require a new secure networking paradigm
- Must secure information not networks

Network Centric Security Solutions Prevent the Seamless Sharing of Information among Multinational Partners.

CKM: The Solution



Integrate:

- Marking/Labeling
  - Information marked and labeled based on contents
  - Labels bound to the information
  - Information encrypted based on bound label using NSA approved key management
- IA & A
  - Strong identification, authentication, and authorization
  - Identifies Users and their security attributes
  - Requires something they have (Token), know (Pin) and are (Fingerprint)
- Access
  - Share information based on a match between the content label and the user's security attributes

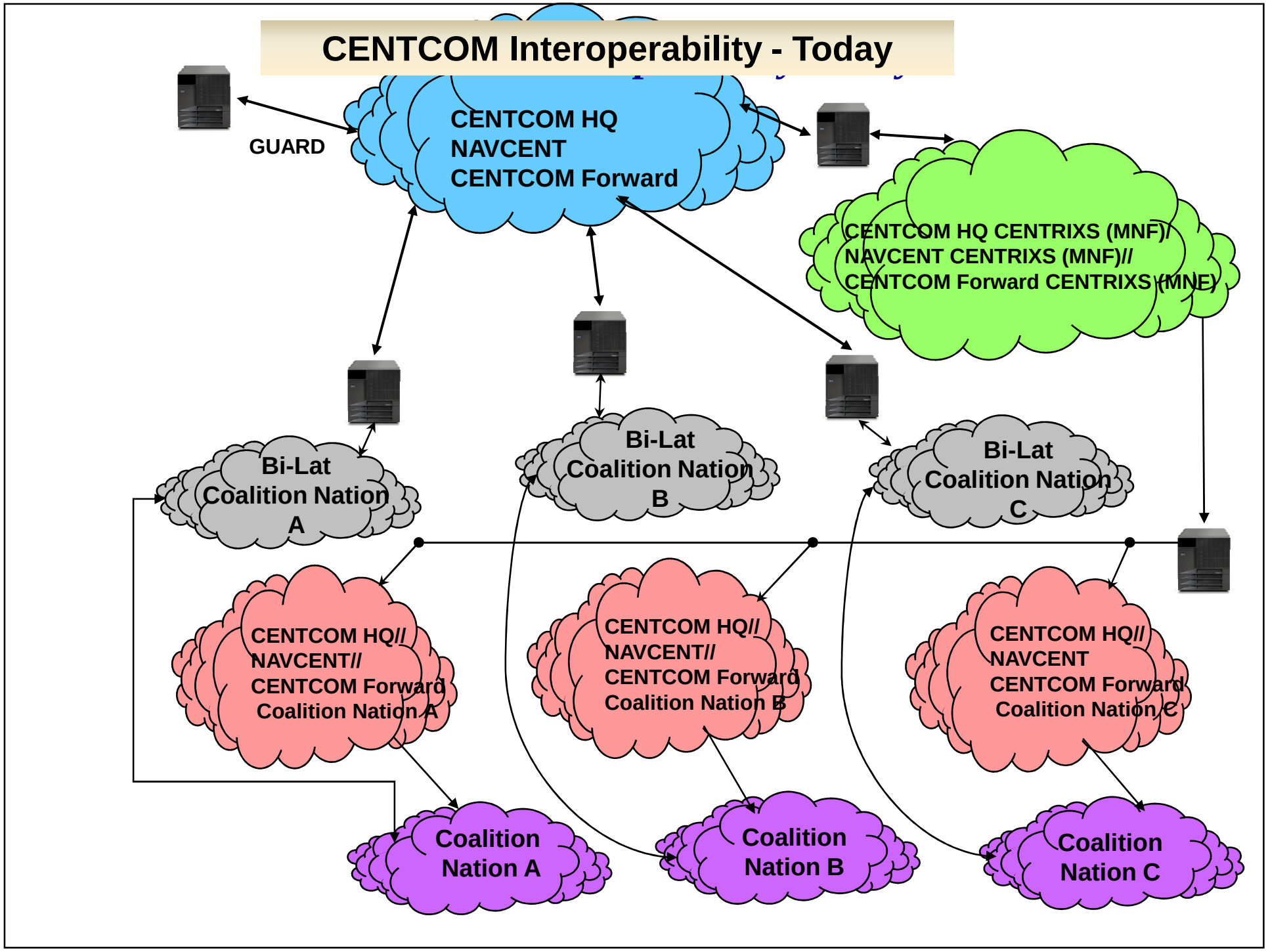
Information encrypted based on its content not the network.

So What?

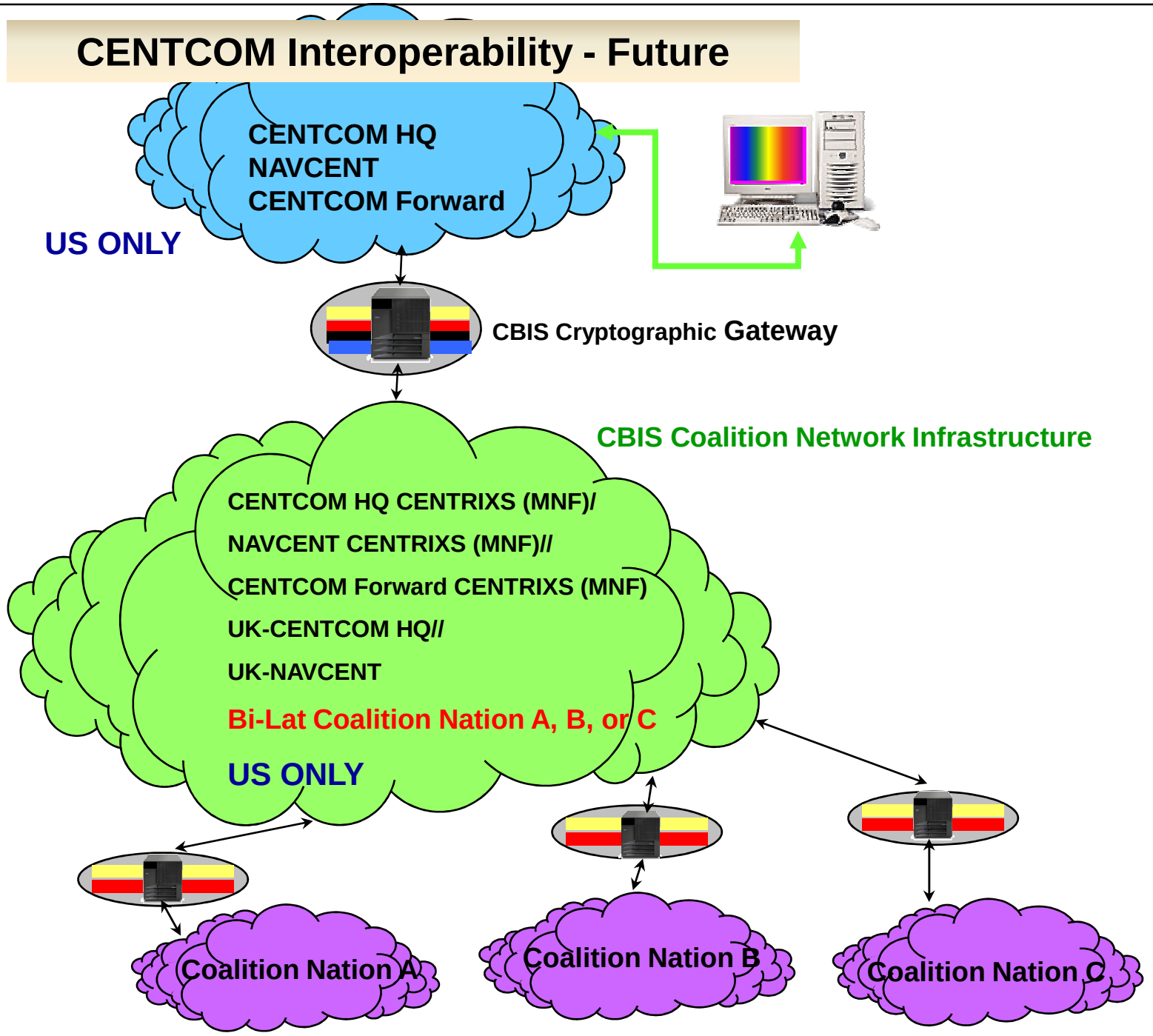
Information sharing not restricted by separate physical networks

- **Operationally:**
  - **Single Network Infrastructure solution reducing manpower and complexity**
  - **Provides commander flexibility to exchange information between US/NATO and other multinational members**
  - **Information protected at the point of origination reducing inadvertent disclosures and compromises**
  - **Controlled information access**
    - **Read (decrypt) information at multiple sensitivity levels**
    - **Write (encrypt) at a single sensitivity level from a single workstation using assured periods separation techniques, (partitioning, multiple CPUs, virtual drives, etc.)**
- **Technically Feasable:**
  - **NSA approved hardware (Type 1) encryption at the workstation**
  - **Symmetric encryption providing a one-to-many capability with asymmetric header encryption for access control**
  - **Provides NSA approved dynamic key management system**
  - **Strong Identification, Authentication & Authorization (IA&A) based on a Token, PIN, and Biometrics**

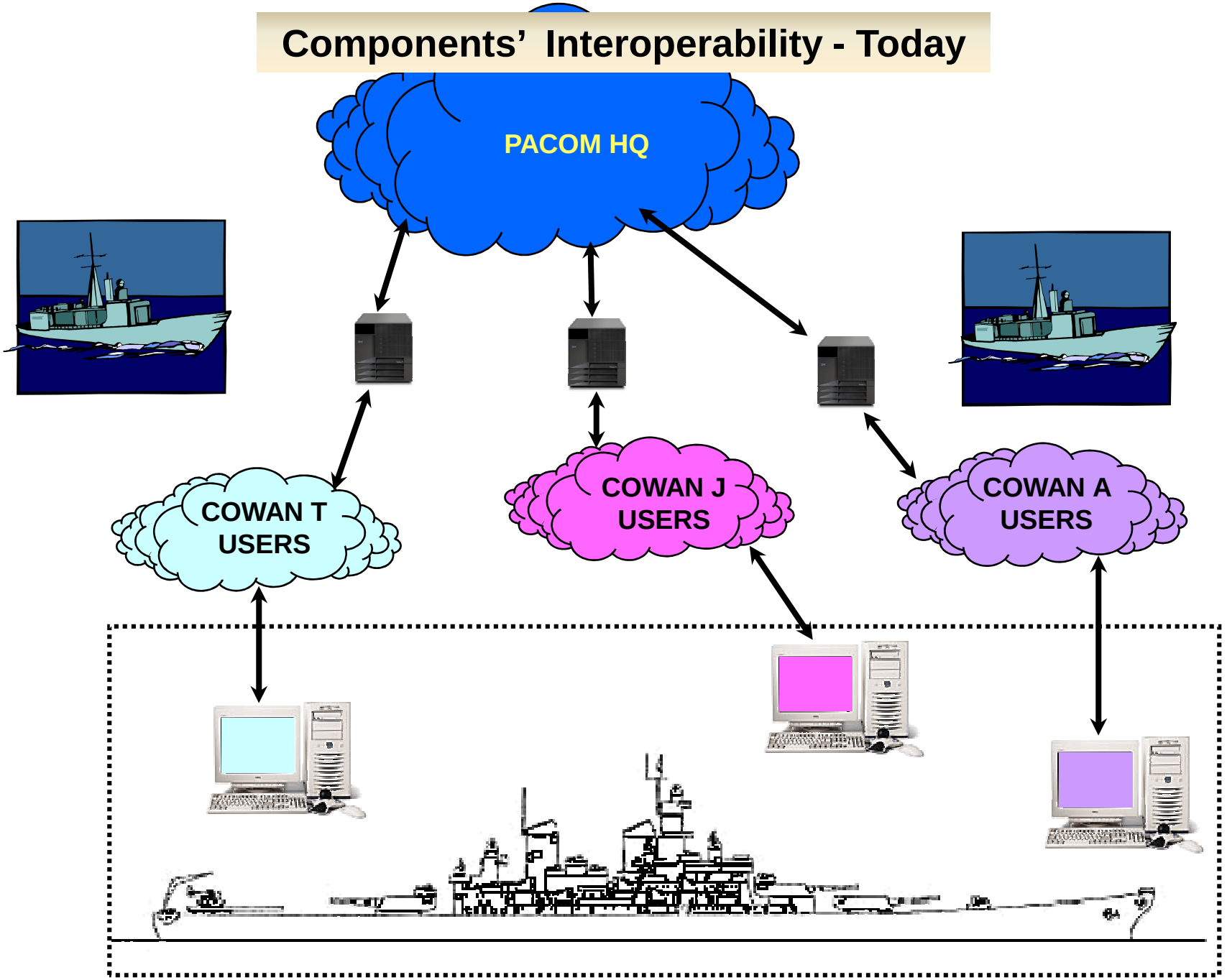
CENTCOM Interoperability - Today



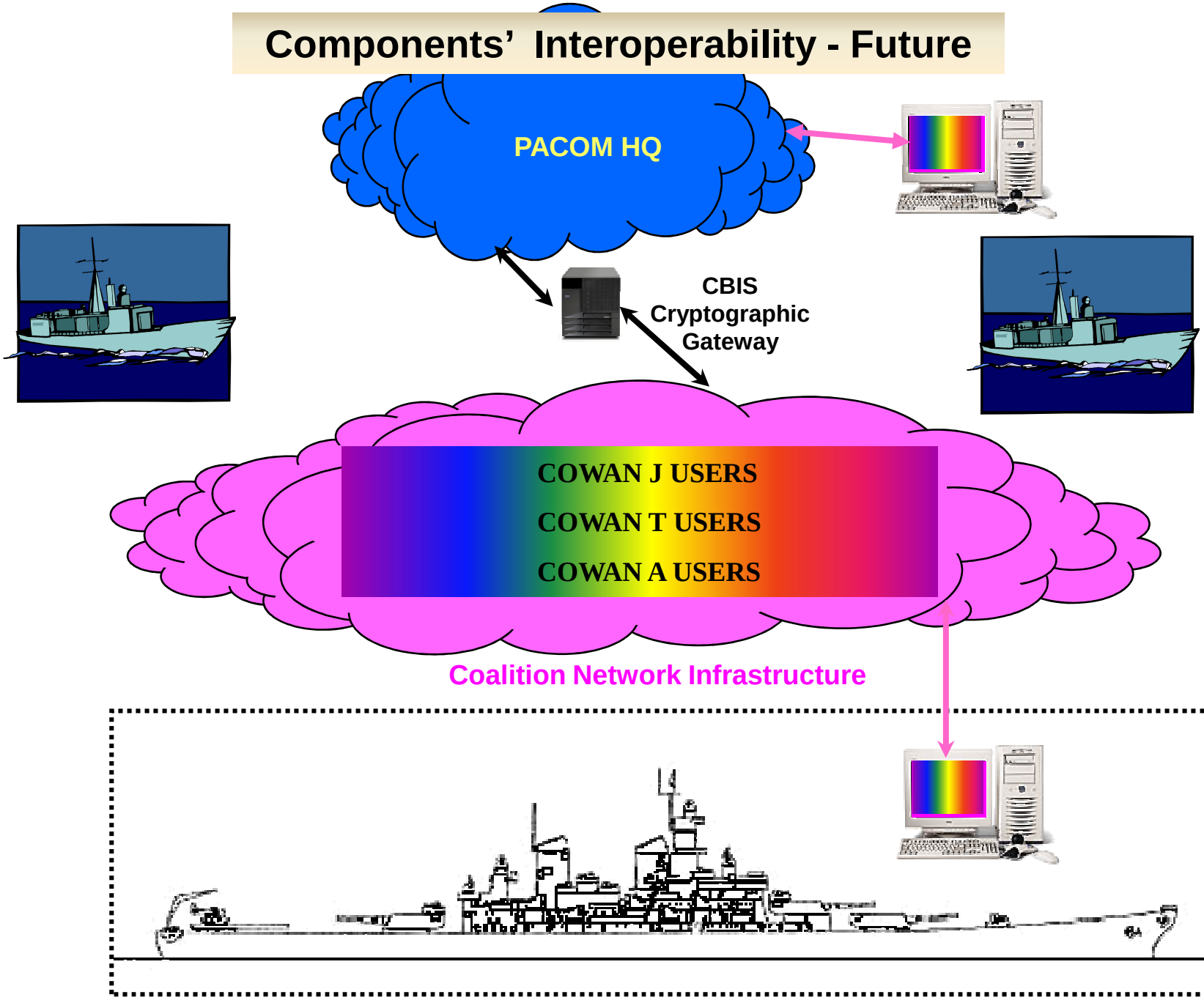
CENTCOM Interoperability - Future



Components' Interoperability - Today



Components' Interoperability - Future

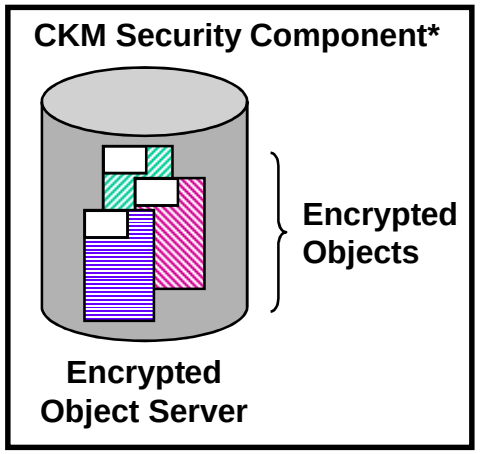


Unique CKM Features

- **Ability to share data with coalition partners using a rule-based access controlled system as a high assurance network overlay**
- **Ability to mark, label and encrypt files/documents at different security levels and partitions**
- **Ability to control publishing of data to coalition server**
- **Ability to use common (commercial) operating systems and applications (MS office, email, any standard network application)**
- **Ability to control access to workstations using an assured process that incorporates three factors:**
  - **Token – something they have**
  - **PIN – something they know**
  - **Biometrics – something they are**

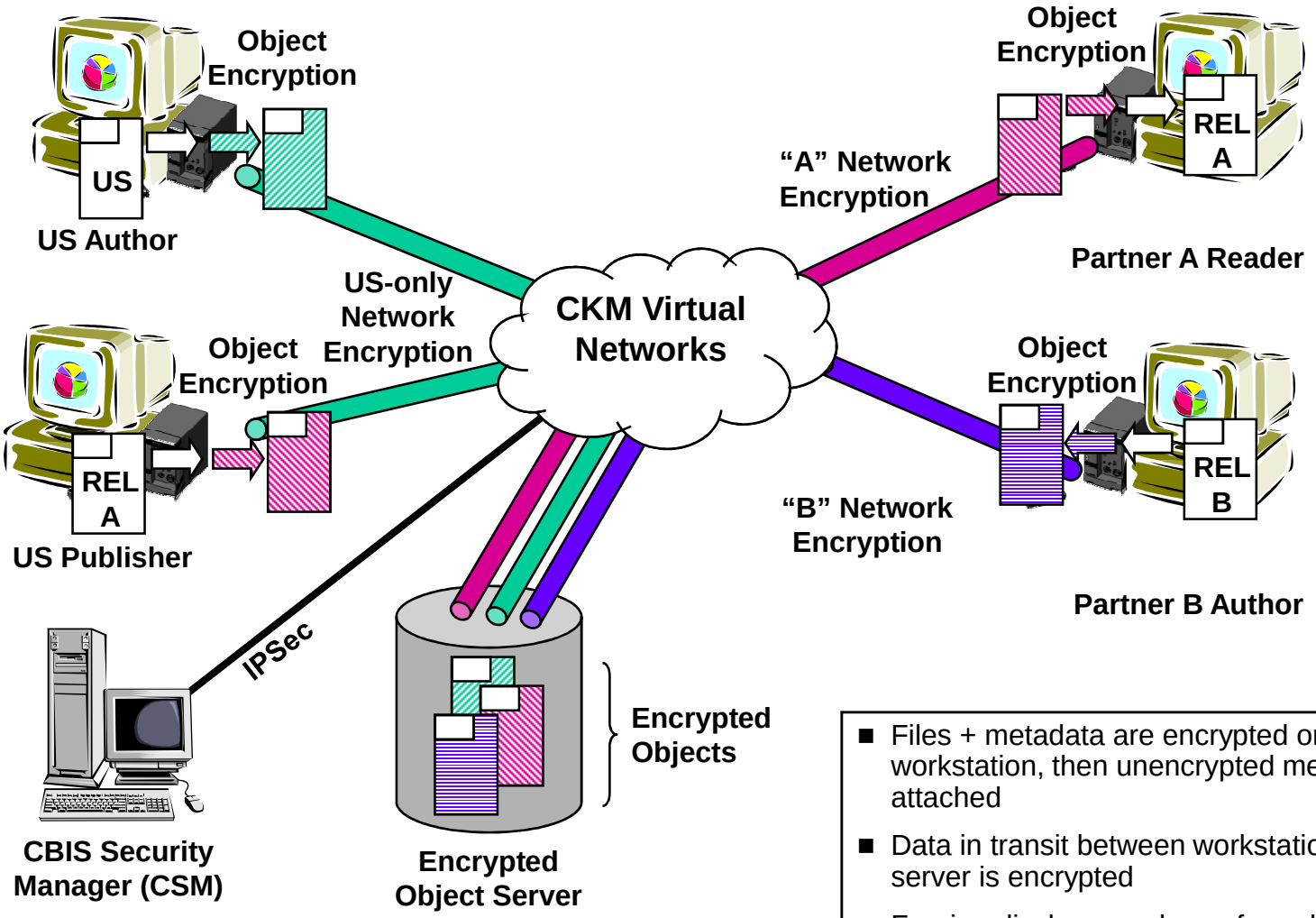
CKM Encrypted Object Server

- **Storage areas for *common storage*, *publisher review* areas, and *local storage***
  - **Data-at-Rest (DAR)-encrypted files stored as database objects (server has no DAR encryption or decryption)**
- **Server security component contains only Data-in-Transit (DIT) encryption modules**
- **Web interface and database search engine provide access control decisions based on metadata attached to encrypted files**
  - **Search results presented to user as a page of hyperlinks**
  - **User downloads file; it is DAR decrypted within the CKM Module located at the users workstation; if the user has the proper key**



* Network only encryption (data in transit)

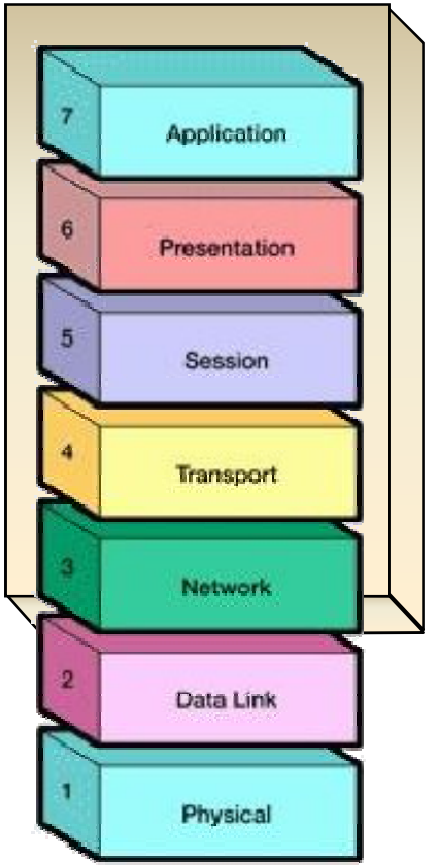
CKM Overview



* Network only encryption (data in transit)

- Files + metadata are encrypted on the workstation, then unencrypted metadata is attached
- Data in transit between workstations and server is encrypted
- Foreign disclosure rules enforced via two-step author + publisher process

Impact on Legacy Networks



- **CKM requires an existing network infrastructure to provide OSI layer 1, 2 and 3**
- **There is no logical interface with existing network infrastructure**
- **CKM virtual networks can utilize IP layer encryption using High Assurance IP Encryption (HAIPE) standards established with the NSA**
- **CKM unique network components remain isolated using high assurance IP encryption**