Developing Secure & Resilient Next Generation Communications Networks & Services

Prepared for:

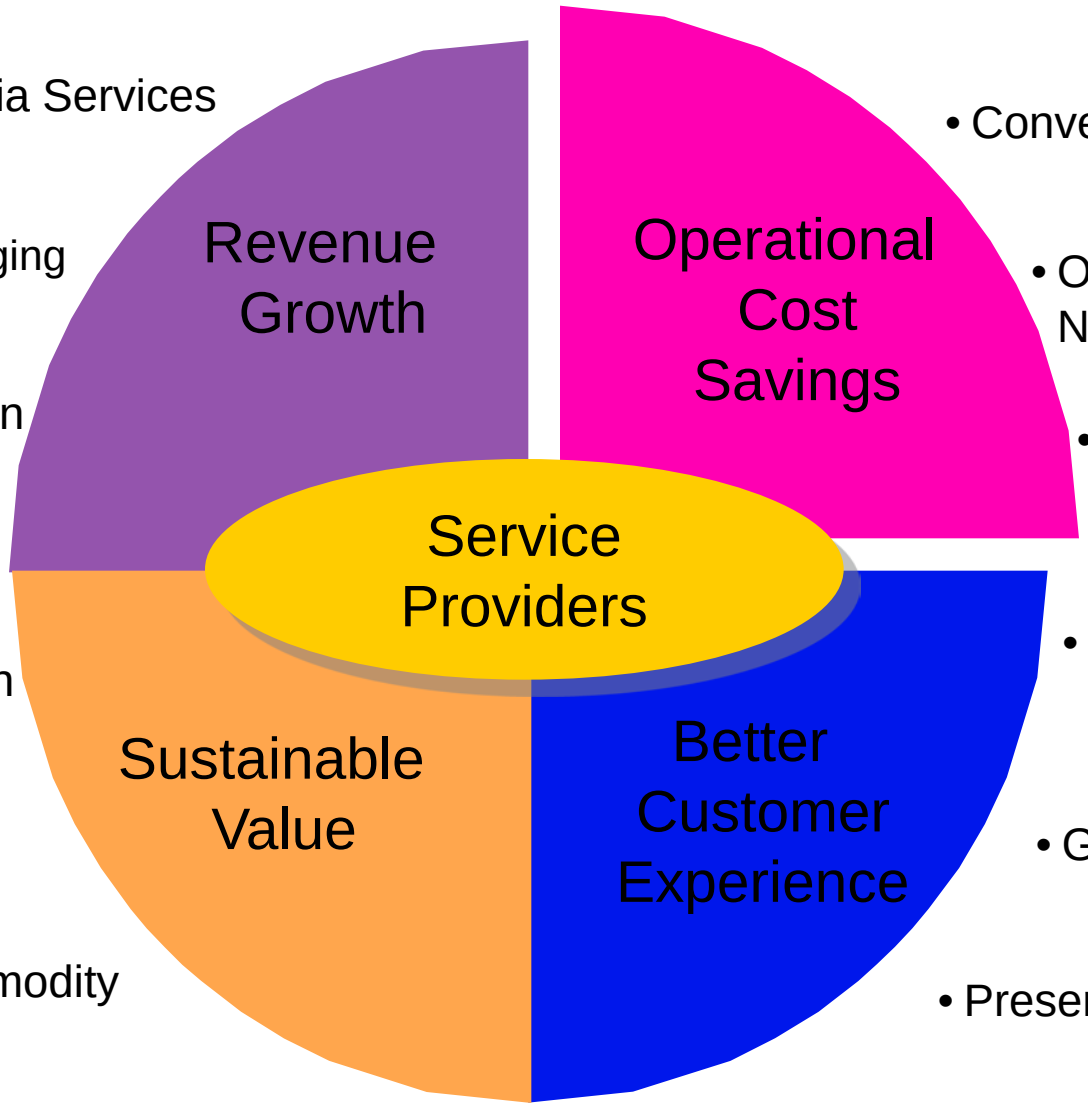
Disruptive Technologies Conference

Telcordia Contact:
John Kimmins
Executive Director/Fellow
jkimmins@telcordia.com
732-699-6188

Overview

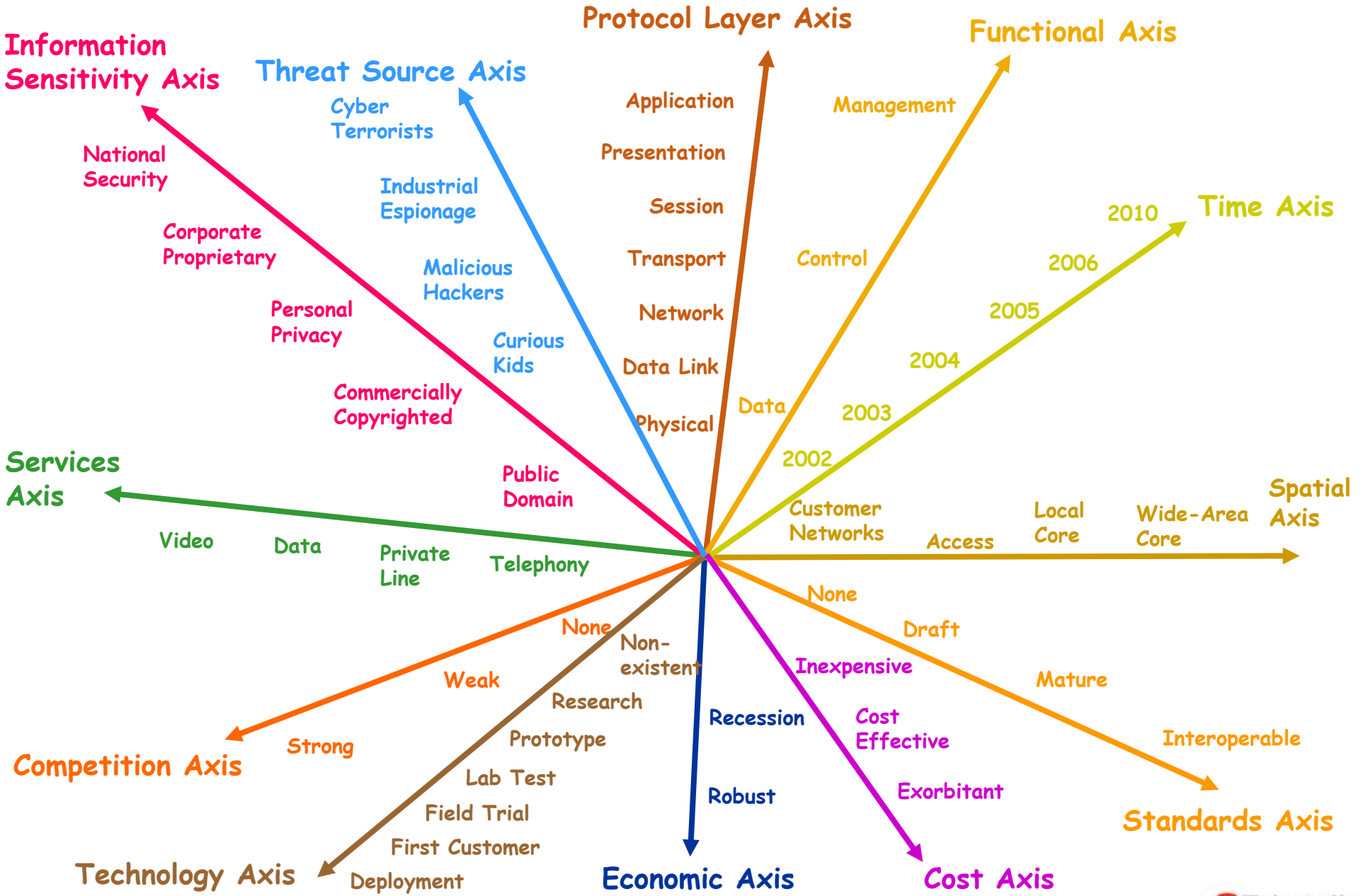
- Network & Services Transformations
- Security Threats
- Technical & Operations Trends
- Current Security Approaches
- Risk Management Framework

Network Transformation:
Market Drivers



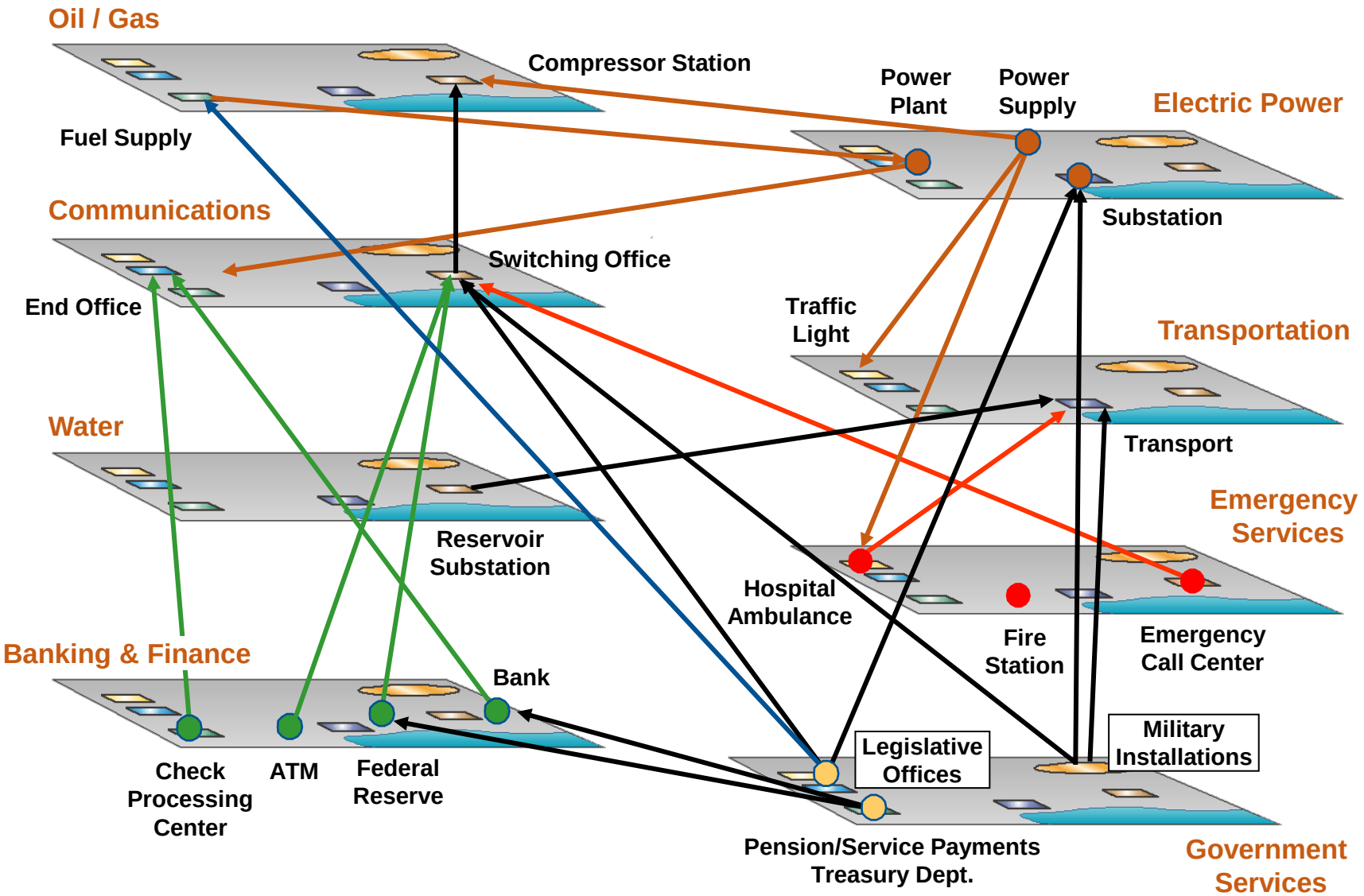
- New Multi-Media Services
- Service Based Charging
- Rapid Service Creation
- Converged Call Control
- Open, Standards-based Network
- Less Operations Staff
- Sell Services, not an "IP pipe"
- Services = Value
- Transport = Commodity
- Access Agnostic (e.g., mobile, fixed, wireless)
- Greater User Control
- Presence & Availability

Multi-Dimensional Challenge



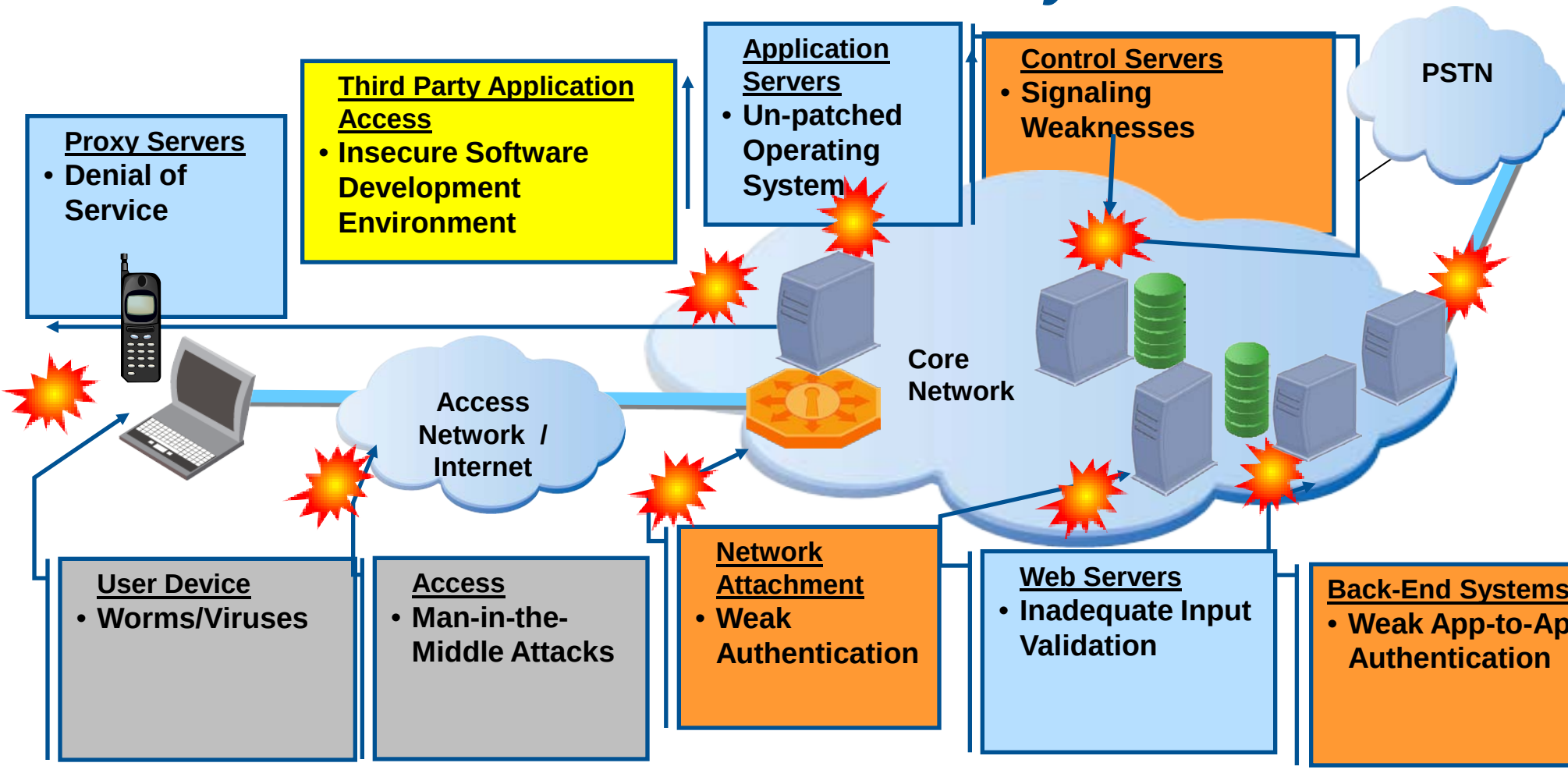
Threats Magnified

Interdependencies & Technology Evolution



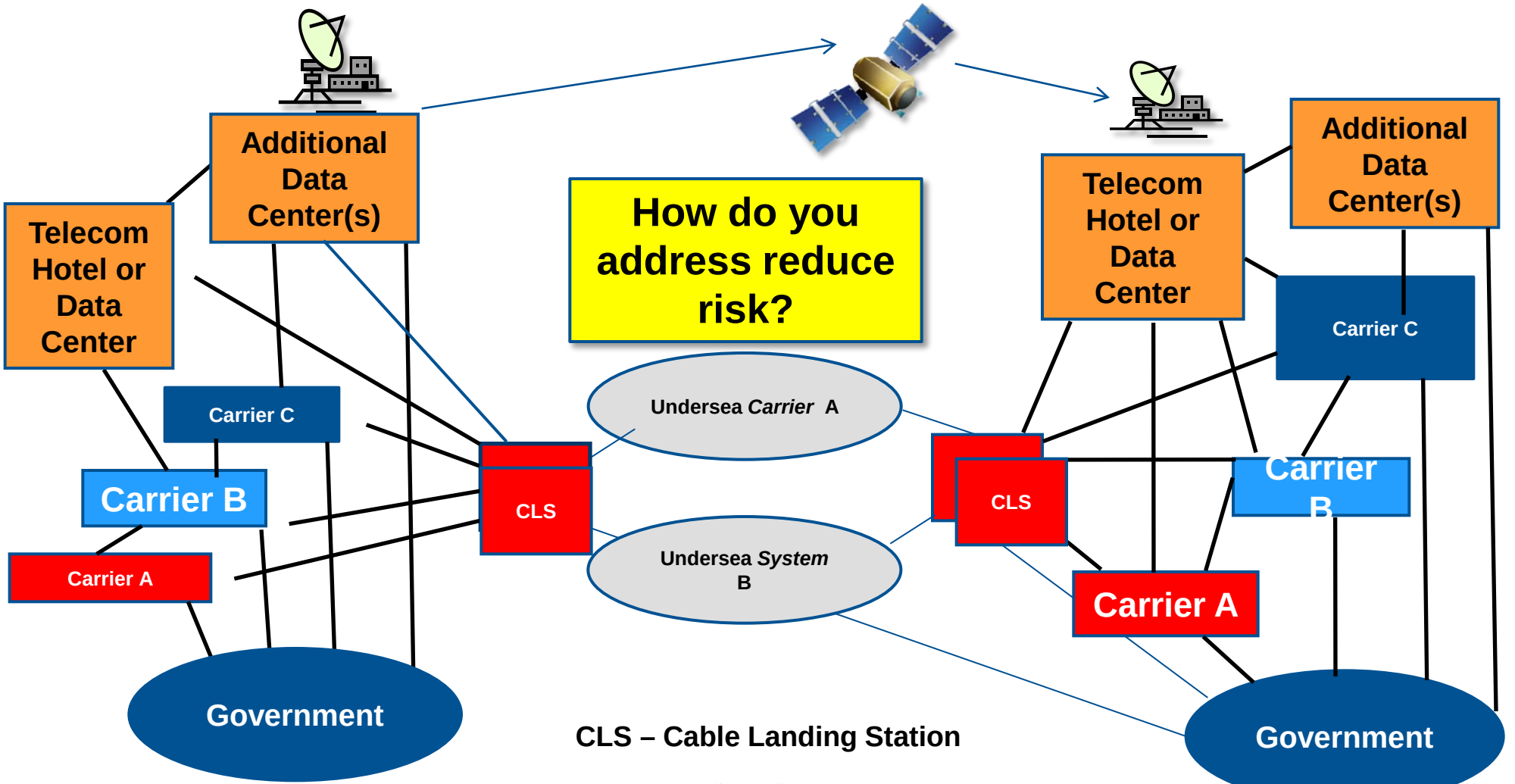
Network Transformation:

End-to-End Infrastructure Security Risks



Network Security & Resiliency Under Attack

"Take Balad Air Base, for example," Colonel Fielden said. "A passing ship anchor cut an undersea fiber optic cable and Balad went from conducting hundreds of combat sorties per day to conducting tens of sorties a day. What do you do when communications systems are down? Not much of anything."



CLS – Cable Landing Station

Next Generation Network (NGN) Deployments

How is Security today?

- **Basic**
  - Baseline security requirements for product vendors are vague
  - Organizational issues are not fully identified and addressed
- **Not mature**
  - Security performance and reliability are critical elements and need to be improved
  - Signaling and media security are not fully recognized by the market
  - Integration of security functionality still evolving
- **Poorly planned and implemented**
  - Implementations inherit traditional vulnerabilities (e.g. Buffer Overflows)
  - Security features to enforce stronger security posture (protocol, user and boundaries) are not uniformly implemented

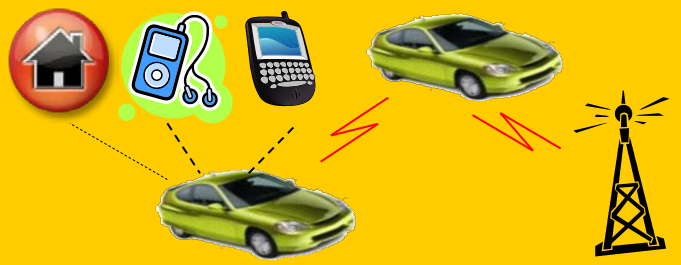
Need to address both NGN and Legacy Network Security

Evolving Wireless Networks & Services

- Besides handset applications there are *new* applications and services infrastructures emerging
  - Vehicle Telematics
    - On-board computers with multiple wireless interfaces
    - Roadside wireless networks
    - Vehicle to Infrastructure & Vehicle-to-Vehicle communications
  - Smart Grid Energy Management Systems
    - Networks linking entities and devices (e.g., sensors, meters) for generation, distribution and usage
    - Automated smart meter management

Wireless Telematics

In-Vehicle System



- In-Vehicle Telematics Architecture
- Applications Software
- Security & Privacy Management

Multi-Mode Access

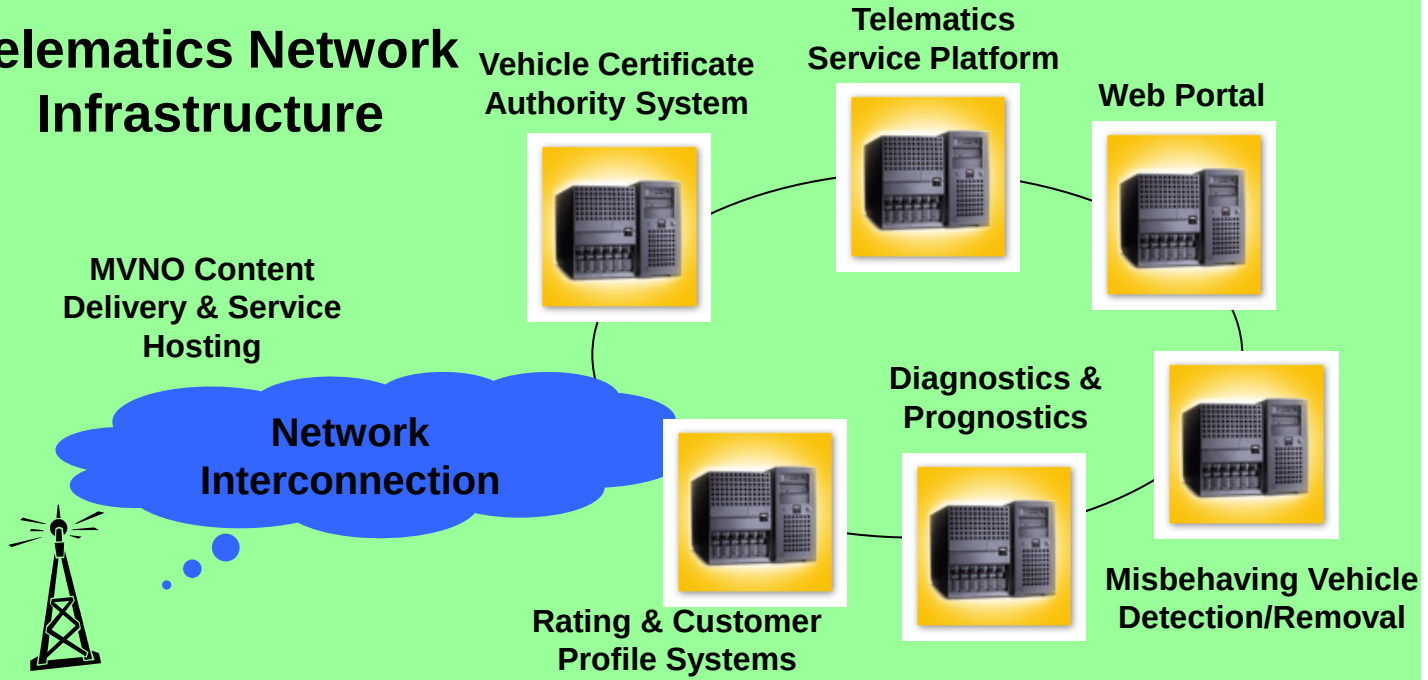
- GPRS
- EVDO
- HSDPA

- DSRC

- WiFi
- WiMAX

- Seamless Mobility
- Secure Mobile IP Sessions
- Integrating Emergency Services / Crash Notification Routing

Telematics Network Infrastructure



Potential Products & Services

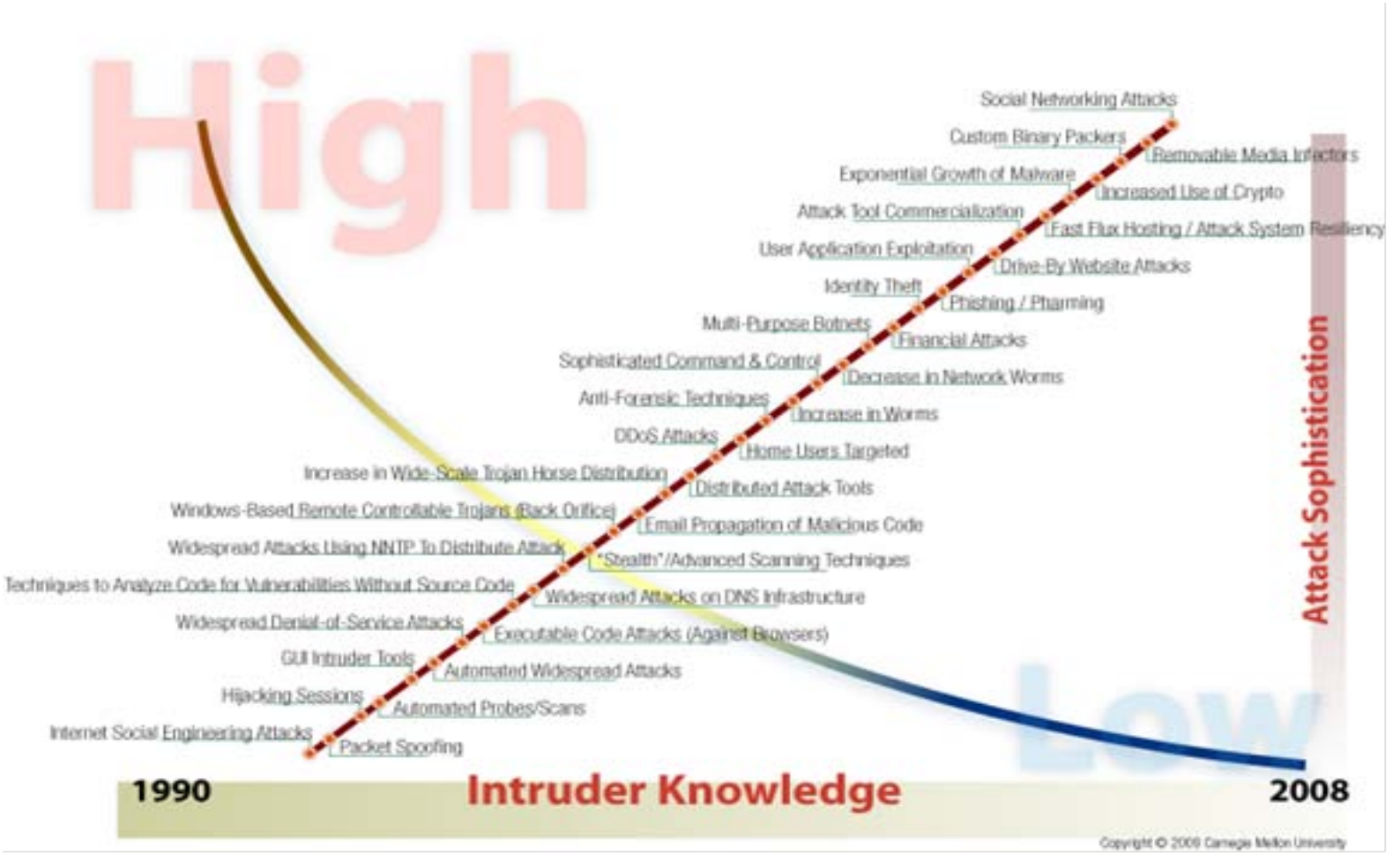
- Telematics Portal
- Vehicle Communications & Network Security
- Telematics Application & Software Development
- Vehicle Diagnostics & Prognostics
- Service Provisioning & Support Systems
- MVNO Content Delivery & Application Hosting
- Transportation Research, Analysis & Modeling

Smart Grid – What is It

- Transform existing energy services using communications technology
  - Remote connects/disconnects
  - Distribution automation
  - Customized user services & billing
- Components
  - Business applications – e.g., generation/supply, SCADA, Usage/demand
  - Computing/IT – e.g., Servers, Web technology, Smart agents
  - Communications Infrastructure – e.g., Home Access Network, WIMAX, Cellular
  - Energy Infrastructure – e.g., Smart Meters, Transformers

Threat Trending

New Targets: Smart phones, STBs, WiFi, Meters, OBEs, etc.



Technical Trends

- Web-based applications & services
- Mobility with different roaming patterns
- New types of intelligent devices
- Signaling extended out to user
- Multi-media protocols
- Third-party software & user interfaces
- Hardware and software security components

What is Sufficient Security?

Security Testing Evolution

Pen Testing is not sufficient

- **Trend towards embedding security functionality into software and hardware with an increasing threat in software/hardware hacking tools**

Protocol Layers

VoIP Application Layer
(Call Managers, SDPs, PSXs…)

VoIP Protocol Layer

Signaling Protocols
(SIP, H323, SS7…)

Transport Protocols
(RTP, UDP, …)

VoIP Supporting Services Layer
(DNS, NAT, QoS, AAA…)

OS and Network Layer
(Linux, Unix, Windows, ARP, MAC, IP…)

Hardware Layer
(Server, SIP hardware)

Verify proper operation through a wide array of vulnerability analysis tools and techniques

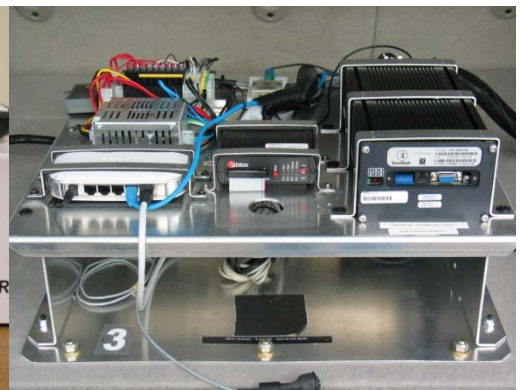
Intelligent User Devices

Embedded Hardware Security Perspective

- Reverse engineering circuit board hardware and firmware
- Exploiting on-chip debugging, JTAG, and in-circuit emulator capabilities
- Accessing and reprogramming FLASH, RAM, and other storage devices
- Stepping, tracing and altering program execution
- Monitoring and inserting data on system and peripheral interfaces
- Extracting / altering keying material, unit identity and other credentials
- Testing PKI functions, such as firmware signatures
- Modifying the circuit hardware to add new devices, remove existing devices, and create new external interfaces
- Re-configuring hardware to masquerade as a different system element

Set Top Boxes

OBE for Vehicles



Smart Meters

3G, ISM Wireless

Operational Trends

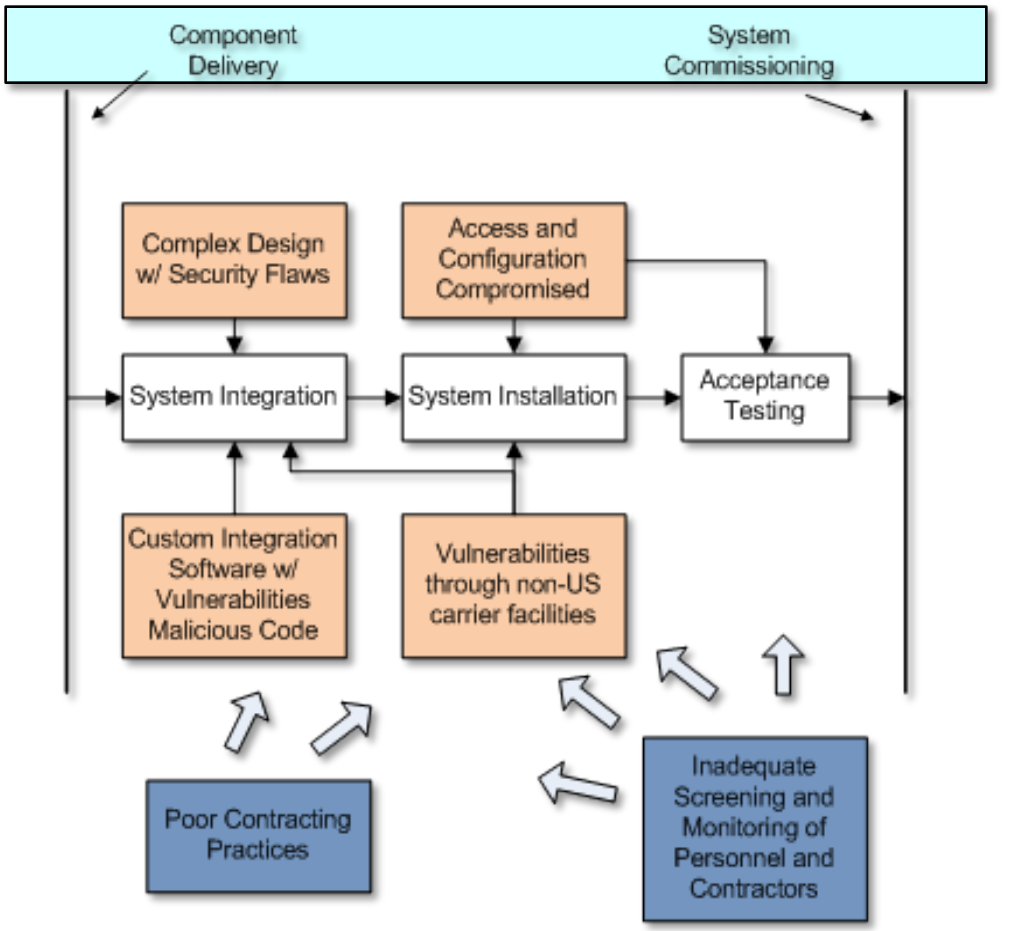
- Primary & Backup NOCs
  - Foreign based NOCs
- Outsourced staff
  - NOC staff
  - Software development
- Lifecycle security across multiple suppliers
  - Supply chain risk management
- Supplier maintaining equipment
- Physical co-location

What is Sufficient Security?

Supplier Assurance

Need for Visible Risk Mitigation Activities

- **Address the insertion of foreign made COTS into networks by feasible architectures, operations, testing & procurement processes**



Current Approaches to Address Challenges

They all have Problems

- Secure Remote Access
- Token-based Access
- Personnel Vetting
- Network Partitioning
- Software & Hardware Testing & Analysis
- Trusted Source Software Releases
- Network Traffic Monitoring
- Filtering Inbound and Outbound Traffic
- Site Inspections
- Physical security assessments

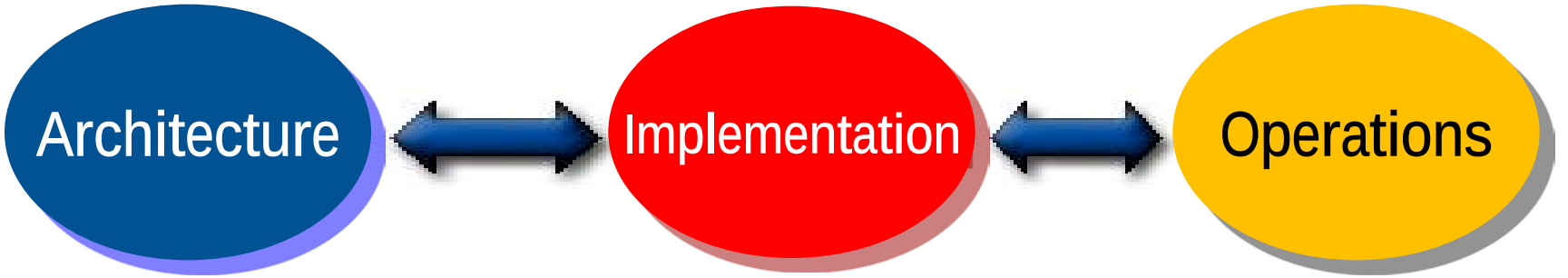
Risk Management Framework

Structured Analysis

- **Network/Service Access Security**
  - User and Device Authentication
  - Personnel & Physical Access Profiles
- **User Platform Security**
  - Hardware/Software Security
  - Management and Services Interfaces
- **Application Security**
  - Service logic integrity and interfaces
  - Information Protection End-to-End
- **Core Network Security**
  - Intra and Inter-Network Security
  - Communications among systems & entities
  - Operational security roles and policy considerations

Holistic Life Cycle-based Security Approach

Broader than IT and Truly End-to-End



- User & Network Authentication
- Integrity & Confidentiality of Signaling and Media
- AAA Architecture
- Management Infrastructure
- Traffic Separation
- Protocol Weaknesses (e.g. SIP)
- Network Resilience
- Maturity/Immaturity of Standards

- Service-Level Security
- Platform Weaknesses & Equipment Shortcomings
- Web Application Vulnerabilities
- Security Policy Enforcement
- 3rd Party Application Interface Vulnerabilities
- Information sharing
- Service Disruption/DoS
- Non-Traditional Vendors
- Software Integrity

- Monitoring for Security, Service Assurance, QoS
- Component Configuration Management
- Vulnerability & Patch Management
- Intrusion Detection & Response
- Maintenance Access
- Physical Security
- Authentication Key Management