Society, Law Enforcement and the Internet

Models for "Give-and-Take"

Carter Bullard
CEO/President

QoSient, LLC
150 E 57th Street Suite 12D
New York, New York 10022

carter@qosient.com

ICCS 2010
New York, New York

Carter Bullard carter@qosient.com

- QoSient - Research and Development Company
  - Naval Research Laboratory (NRL), GIG-EF, JCTD-LD, DISA, DoD
    - Network Performance Security Research and Development
    - DARPA CORONET Optical Network Security
- FBI/CALEA Data Wire-Tapping Working Group (2000)
- QoS/Security Network Management - Nortel / Bay
- Security/QoS Product Manager – FORE Systems
- CMU/Software Engineering Institute CERT
  - Network Intrusion Research and Analysis
  - NAP Site Security Policy Development
  - Principal Network Security Incident Coordinator
- NFSNet Core Administrator (SURAnet)
- Standards Participation
  - Editor of ATM Forum Security Signaling Standards
  - IETF Working Group(s), Internet2 Security WG, NANOG

US Cyber Security Focus

- Comprehensive National CyberSecurity Initiative
  - Shifting the US focus from CyberCrime to CyberWarfare
- Strategy and technology focused on new issues
  - Public sector defense, with nation state threats and countermeasures
  - New emphasis on military concepts in Cyber Security
    - Shift from detection to prevention
    - Possible retaliatory mechanisms
- Multi-billion dollar budget will have a significant impact
  - Redefine CyberSecurity for most of the public
  - Compete for best/brightest in security research
  - Determine a new direction for commercial security products

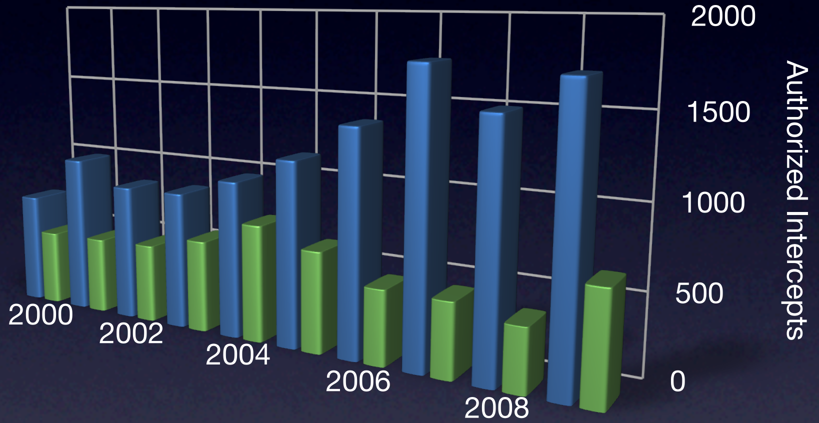
US Cyber Strategy Issues

- Cyber Crime still represents 99% of the cyber problem
- Change in focus may create strategies and technologies that are inappropriate for addressing Cyber Crime.
    - Example: many CNCI initiatives involve enhanced monitoring
        - To support advanced intrusion detection and prevention.
        - Sharing of network monitoring data for enhanced situational awareness.
        - In the pubic sector's .gov, .mil and classified networks, where there is no expectation of privacy. Enhanced monitoring is a very good thing.
        - In the private sector, however, any level of enhanced monitoring is perceived by the public as wiretapping.
- Can the CNCI produce a surveillance strategy that represents an acceptable privacy strategy?
- An old public-private partnership may be able to help

LEAs and Telecommunications

- US Lawful Intercept
  - Pen Register
  - Trap and Trace
  - Content Interception

Frequency US Communication Intercepts



Source http://uscourts.gov/Statistics

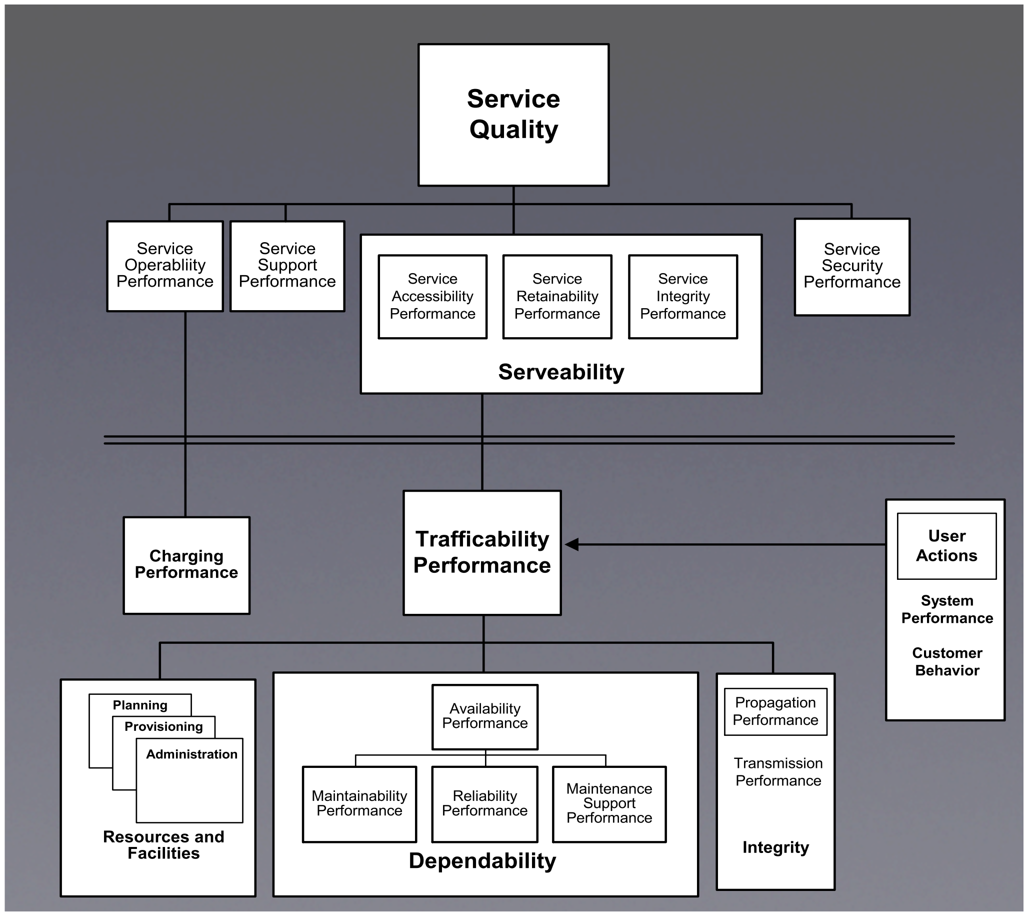
- However, the principal interaction of LEAs with the telecommunications industry are subpoenas of telephone billing records. (over 100X number of Lawful Intercepts)

Private-Public Partnership

- Telephone Billing Records, Call Detail Records (CDR), are a by product of Telco network operations and considered Customer Proprietary Network Information (CPNI).
- Society provides privacy protection for CPNI
  - Of course, the customer can have access to the information at anytime
  - No voluntary disclosure by telco, without customer approval
  - Government can gain access through warrants, or trail subpoenas
- CDRs contain no content, but have high security utility
  - Provide an effective and well recognized deterrent against crime
  - Private and Public sectors rely on CDRs for investigative purposes
    - Provides an enhanced Situational Awareness
    - Used by LEAs to demonstrate need for further investigation
- CDRs directly minimizes the use of Lawful Intercept
- Can CDR equivalent strategies be realized in the Internet?
- Is it possible to enable this partnership in the Internet?
- Can the CNCI use this type of partnership for national Cyber Security?

What Are CDRs Used For?

- Billing
- Traffic Engineering
- Network Management
- Maintenance
- Marketing
- Product Development
- Security
  - Fraud Detection
  - Forensics Analysis
  - Incident Response
  - Non-Repudiation / Audit



From ITU-T Recommendation E.800 Quality of Service, Network Management and Traffic Engineering

Theoretical Security Threats and Countermeasures

Countermeasures		Threat				
		Unauthorized			Degradation of Service	Repudiation
		Use	Modification	Disclosure		
Authentication	Cryptographic	🟥 ×		🟥 ×		
Integrity			🟥 ×			
Confidentiality				🟥 ×		
Access Control		🟨 ×	🟨 ×	🟨 ×	🟨 ×	
Non-Repudiation/Audit		🟨 ×	🟨 ×	🟨 ×	🟥 ×	🟥 ×

From ITU-T Recommendation X.805 Security Architecture for Systems Providing End-to-End Communications

🟥	Primary Security Countermeasure
🟨	Secondary Security Countermeasure

Control
Identify
Analyze
Plan
Track
ARGUS

Network Auditing

- Specified by DoD in NCSC-TG-005
  - The Red Book - Trusted Network Interpretation of the Trusted Computer System Evaluation Criteria (1987)
- Goal to provide accountability for all network use
  - Comprehensive audits are Non-Repudiation systems
  - Creates **real deterrence** in formal systems
    - Fear of getting caught is extremely powerful
  - Utility comes from the quality of collected information
- Internet network transaction auditing is emerging
  - Started at the CMU CERT-CC in early 1990's - Argus
  - Directly modeled after the PSTN CDR
  - Aspects of IP network auditing are being standardized

IP Network Flow Information

- All types contain IP addresses, network service identifiers, starting time, duration and some usage metrics, such as number of bytes transmitted.
- More advanced types are transactional, convey network status and treatment information, service identification, performance data, geo-spatial and net-spatial information, control plane information, and extended service content.

- Available IP Flow Information
  - Argus
    - Control and Data Plane network forensics auditing
    - Archive, file, stream formats. (Binary, SQL, CSV, XML)
  - YAF/SiLK - CERT-CC
    - Designed for Cyber security forensics analysis
    - IETF IPFIX stream formats. Binary file format.
  - IPDR - Billing and Usage Accountability
    - ATIS, ANSI, CableLabs, SCTE, 3GPP, Java CP, ITU/NGN
    - File and stream formats (XML).
  - Netflow, JFlow, Sflow
    - Integrated network vendor flow information - statistical/sampled
    - Used primarily for router operations, network management

Why IP Network Auditing?

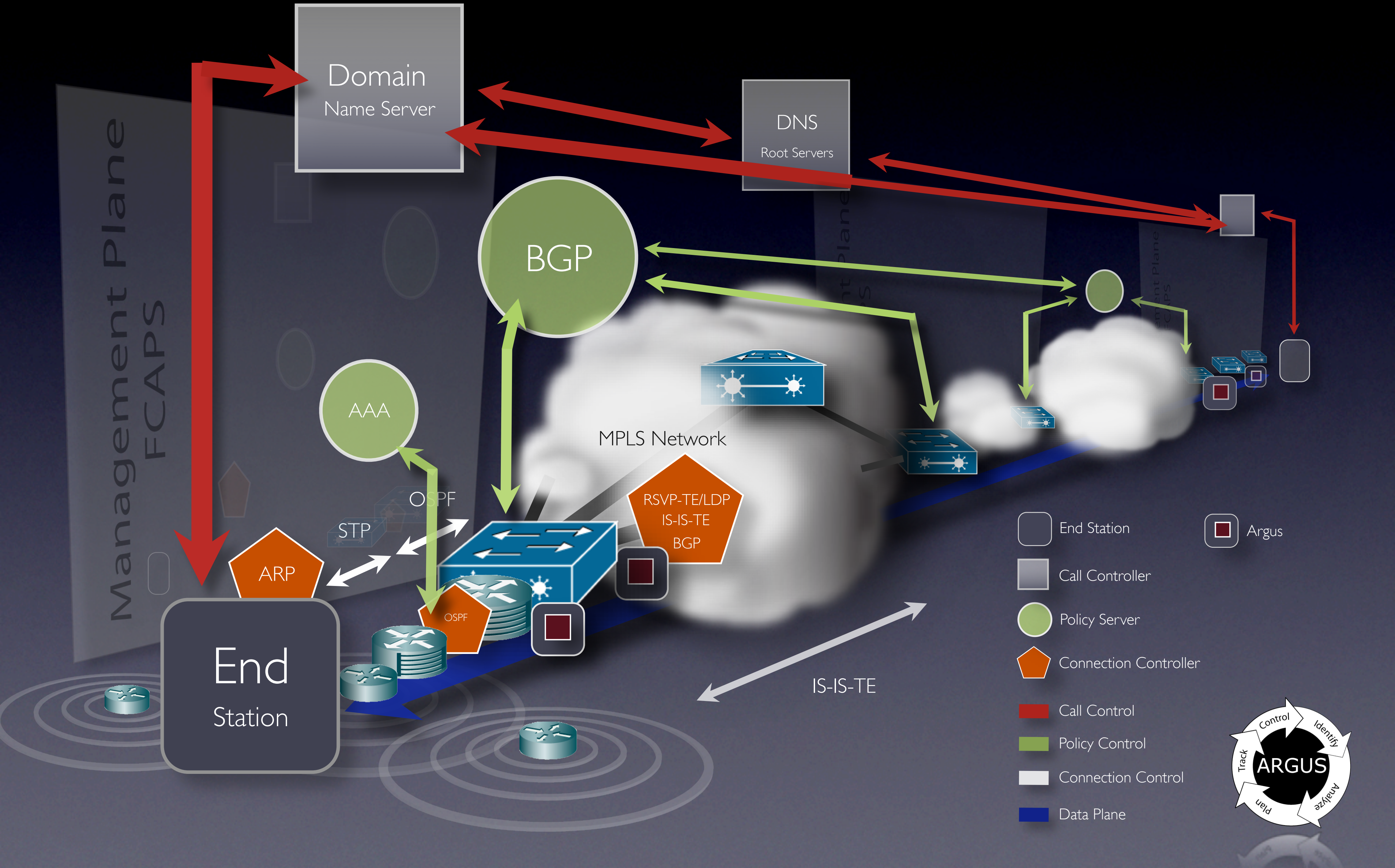
- Effective information for incident response
  - Historical data used for attack attribution
  - Forensic data supports attack identification and cleanup
  - Supports policy enforcement modifications for prevention
  - Near realtime strategies for Zero day vulnerability analysis
- Enhanced network situational awareness
  - Network Policy Enforcement Assurance
    - Are my IPS / IDS / Firewall protections still working?
  - Network Fault Attribution
    - Is it an attack? Is it real? Is it a bug?
  - Network Service Utilization
    - Who's using/abusing my DNS servers?
    - What is generating Email in my enterprise?
    - How much data did that machine transmit last night?
  - Network Non-repudiation deterrent

Who’s Doing Network Auditing?

- Educational Sites (1000’s of sites world-wide)
    - Carnegie Mellon University
    - Stanford University
    - University of Chicago
    - New York University
        - Enterprise wide near realtime network security audit
        - Distributed Security Monitoring
        - Network forensics security research
- U.S. Government
    - Naval Research Laboratory - Security Incidence Response
- ISPs, Enterprises, Corporations, Individuals
    - General Electric - large scale situational awareness
    - General Dynamics - security forensics
    - Network Service Providers
        - Operational/Performance Optimization

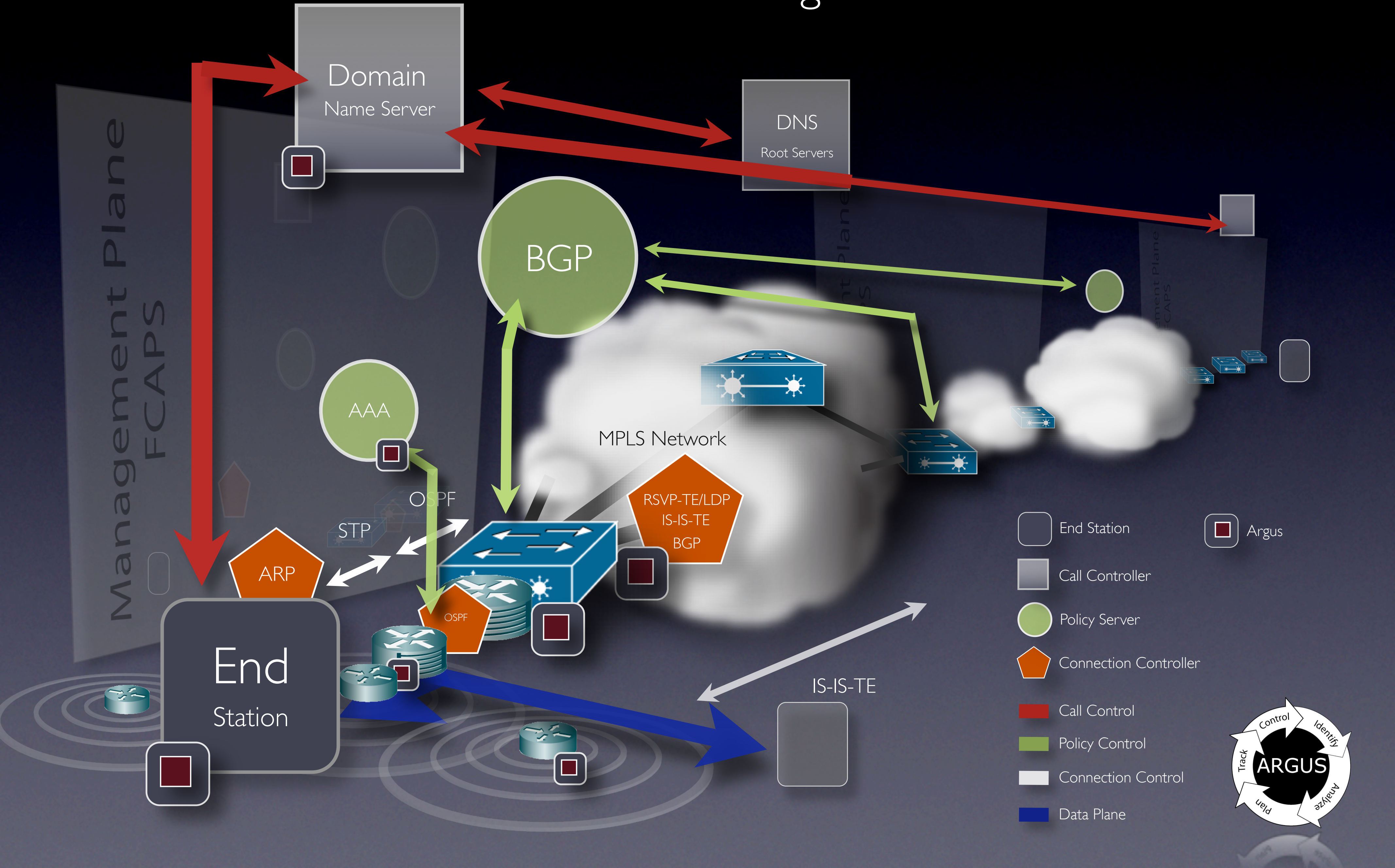
Enterprise Border Awareness

Outside Inside / Them vs Us



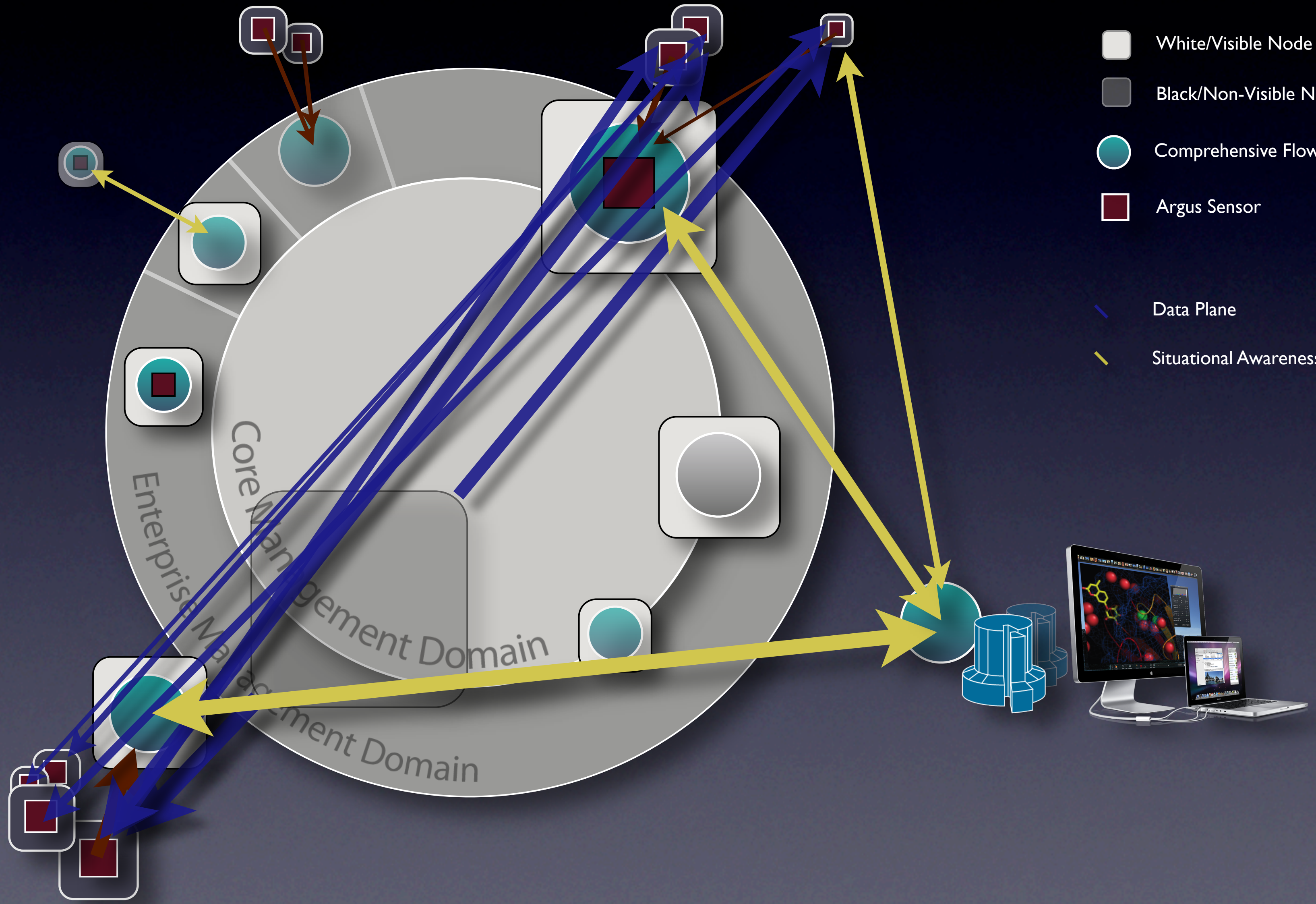
Comprehensive Enterprise Awareness

Dealing with the Insider Threat



Distributed Situational Awareness

Multi-Probe Multi-Site



- ⬜ White/Visible Node
- ⬛ Black/Non-Visible Node
- ● Comprehensive Flow IS
- 🟥 Argus Sensor
- Data Plane
- Situational Awareness Data

Flow Monitoring Infrastructure

- Argus is the predominant tool for network flow monitoring/policy enforcement
- Probes at key points on network
  - Border
  - Core
  - Wireless network
  - Ad-hoc on edge routers (moved as necessary)

Carnegie Mellon®

Flow Monitoring Infrastructure

- Success stories:
  - Forensic examination of compromised machine traffic
    - Determining size and scope
    - Correlating with other events
  - Auditing correct router ACLs
    - Examine real time flows on both sides of the router
  - User consultations regarding bandwidth usage
    - Reports of machine traffic can be generated
  - Configuration issues with VPN infrastructure
    - Examining flows identified source of problem

Private-Public Partnership

- With enterprises generating and collecting IP network flow data, for their own Cyber Security purposes, we have a key part of the puzzle.
- CDR data equivalents can be realized for the Internet
  - Can IP network flow data minimize the need for content capture?
    - Enterprises are effectively identifying, analyzing, and responding to CyberSecurity incidents using some IP flow audit strategies.
  - Question is can LEAs get the same level of utility
- Can Society accept the similarities of IP network flow data and Telco CDRs, and give IP network flow data equivalent considerations?
  - Public debate and legislation can address this issue.

New Public-Private Partnership?

- The private sector is generating and collecting its own IP network flow data for most of the same reasons that the PSTN processes CDRs.
- Society has learned how to effectively use IP network flow data for its benefit, giving up some aspects of privacy in order to achieve a higher level of general privacy protection through minimizing Lawful Intercept.
- The private sector actively contributes to national Cyber Security through controlled sharing of its own network session data.
- Adoption of this public-private partnership enables a historically recognizable deterrence to crime.

Going Dark

- Changes in technology and billing models in the traditional PSTN are driving some telcos to consider stopping CDR collection and retention.
- Because there are no current statutes or regulations to compel telcos to collect and retain CDRs, assuring CDR availability may be difficult.
- Should we recognize this as a national security vulnerability?
- The CNCI strategy may need to consider more than just data network security issues.

Questions?

- For more information please visit

  http://qosient.com/argus

- Contact me directly via email

  carter@qosient.com