Evolving Optical Transport Network Security

Prepared by:
John Kimmins
Executive Director
732-699-6188
jkimmins@appcomsci.com

May 15, 2012

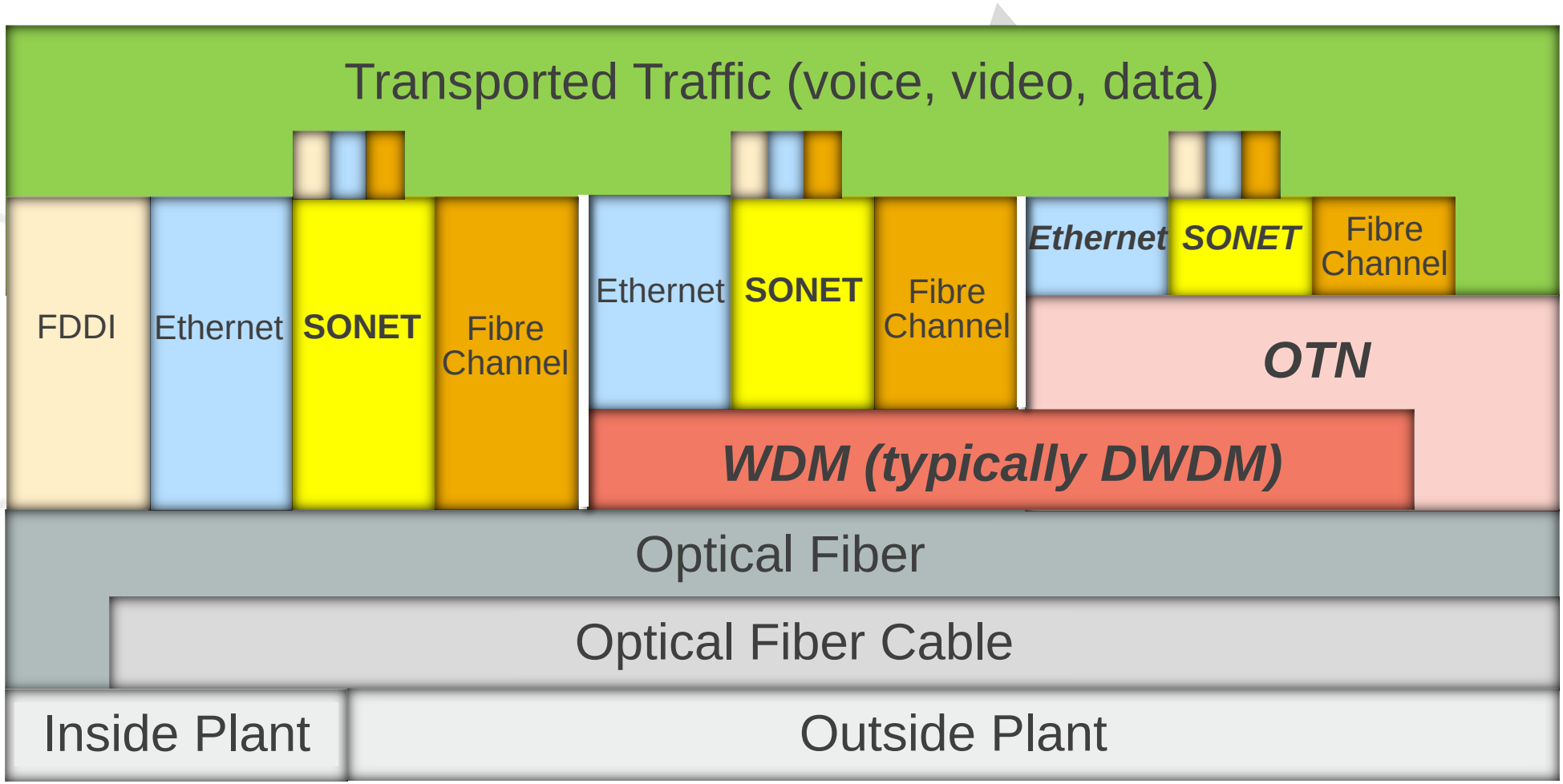
Outline

- Overview of Optical Communications and Transport Networks
- Evolving Transport Network Technology
- Potential Security Issues
- Security Risk Management

Drivers for Optical Communications

- Exploding bandwidth demands
  - Annual growth of 50% or more to support services such as
    - 3G and 4G wireless (backhaul)
    - Streaming video
    - Cloud services
    - On-line gaming
  - Capacity of optical systems is hundreds of times greater than that of electrical or radio-wave systems
- Need for agility, scalability and sustainability to meet rising customer expectations
  - Shift from relatively static TDM-based services to rapidly changing IP/Ethernet-based services

Optical Communications Stack Options

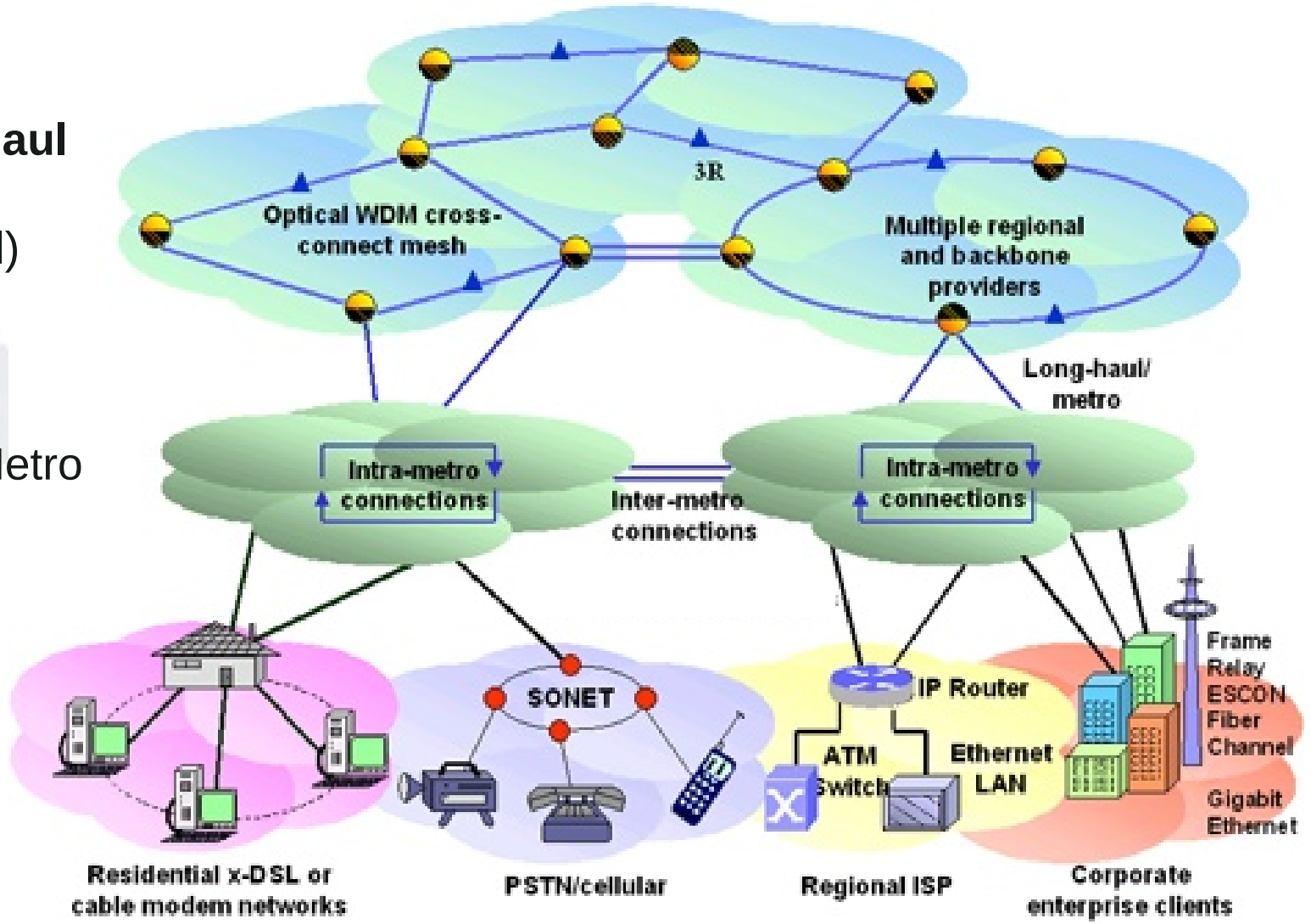


Illustrative Physical Network View

Core/Long-Haul
(undersea
and terrestrial)

Distribution/Metro

Access/
Last mile



Evolving Transport Network Technology - 1

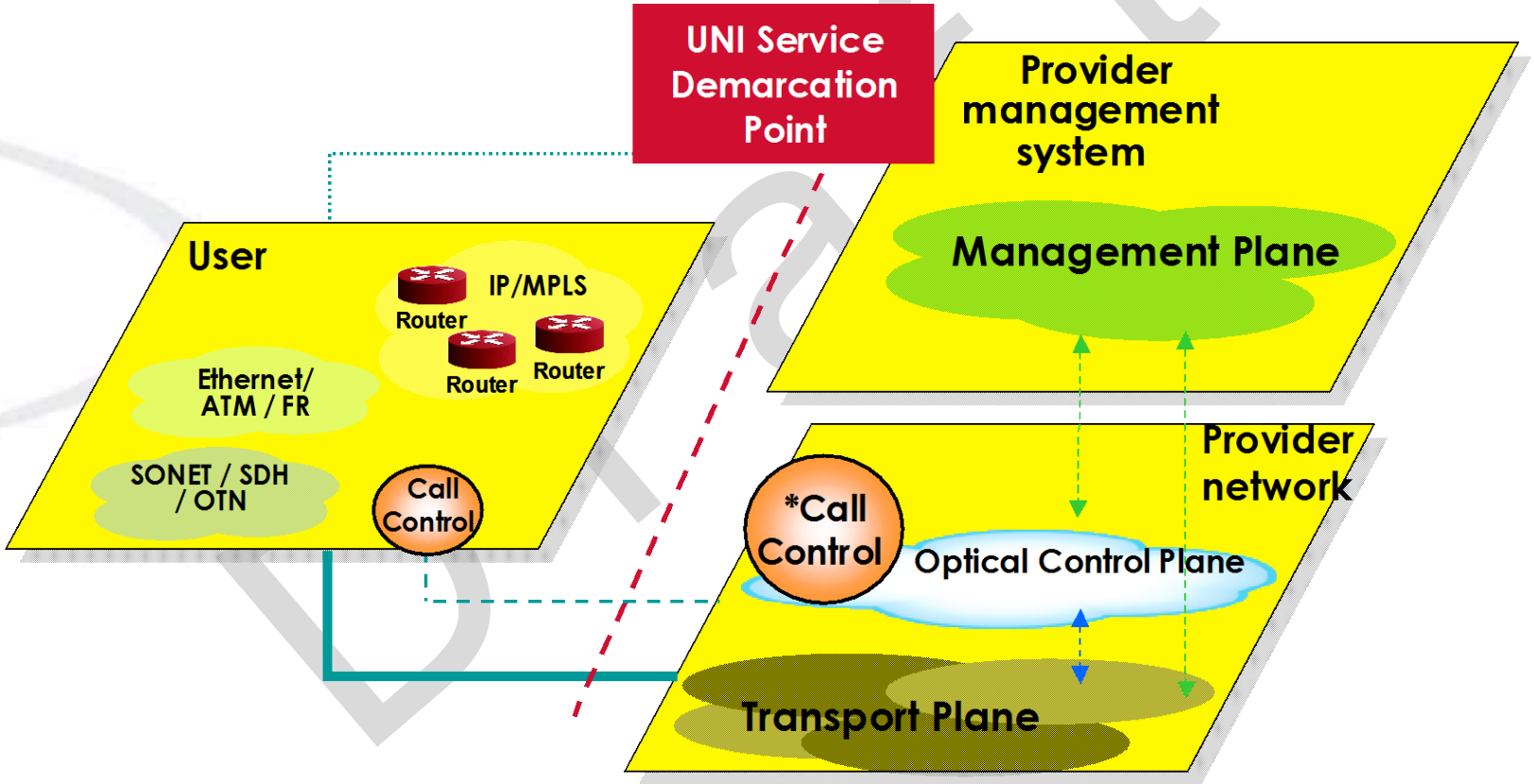
- Automatically Switched Optical Network (ASON) is an emerging control plane technology that
  - Automates discovery and provisioning of network resources and connections
  - Allows for customer control over optical network connections
  - Permits dynamic policy-driven network control
- Transport network changes are initiated by a customer or management system
- Signaling controls the creation and removal of connections
- Customer connects to the transport plane through a physical interface and communicates with the control plane via a User Network Interface (UNI)

Evolving Transport Network Technology - 2

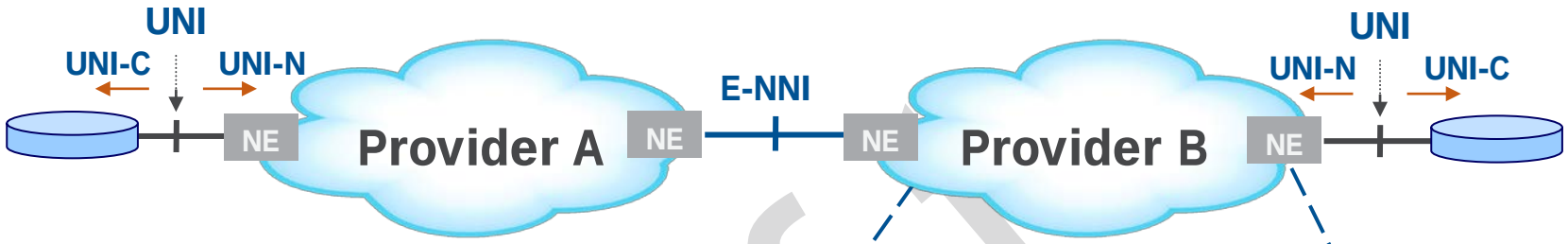
- Automated provisioning allows for
  - Dynamic bandwidth allocation based on demand
  - Quick end-to-end connection setup and teardown
  - Efficient rerouting and resource usage
  - Reduced labor costs associated with manual tasks and customer/service provider interactions
  - Time-efficient response to changing customer needs
- ASON also supports
  - Connection protection and restoration
  - Address and wavelength assignment
  - Traffic engineering
  - Many Quality of Service (QoS) levels
  - Multiple types of traffic (though it may be optimized for IP)

ASON Architecture Interfaces

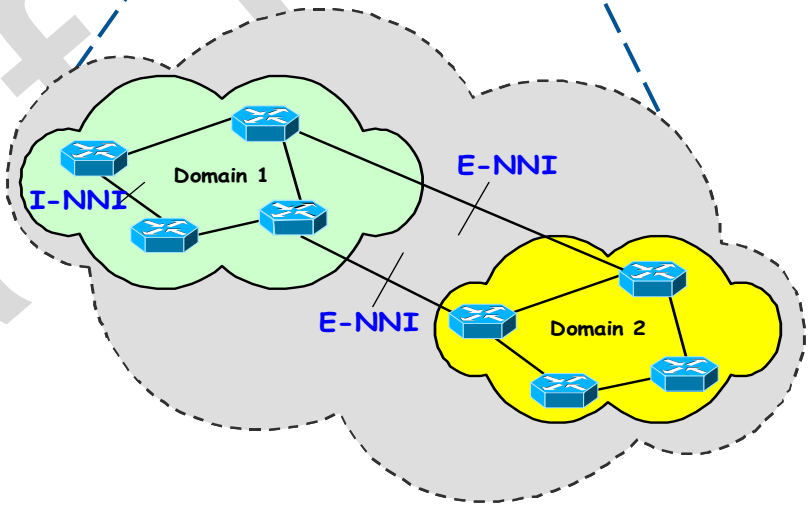
- Service demarcation points are where call control is provided
- Inter-domain interfaces are service demarcation points



ASON Network Interfaces

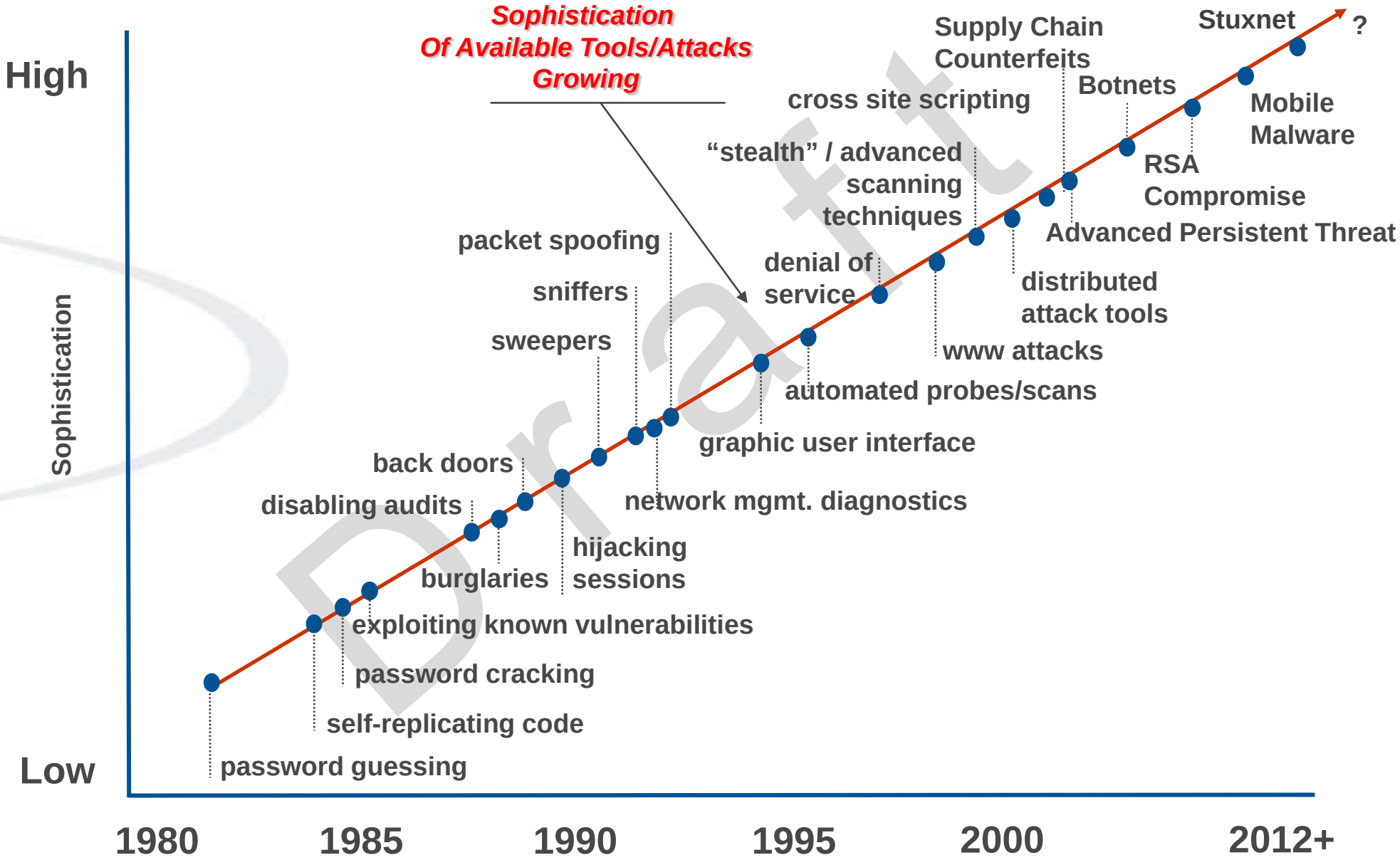


- User-Network Interface (UNI)
  - Separates the concerns of the user and provider
  - Enables client-driven end-to-end service activation
- External Network-Network Interface (E-NNI) enables
  - End-to-end service activation
  - Multi-carrier and vendor inter-working
  - Independence of survivability schemes for each domain
- Internal Network-Network Interface (I-NNI) supports
  - Intra-domain connection establishment
  - Explicit connection operations on individual switches



- UNI and E-NNI are supported by a family of ITU-T and OIF signaling protocols
- I-NNI is considered proprietary

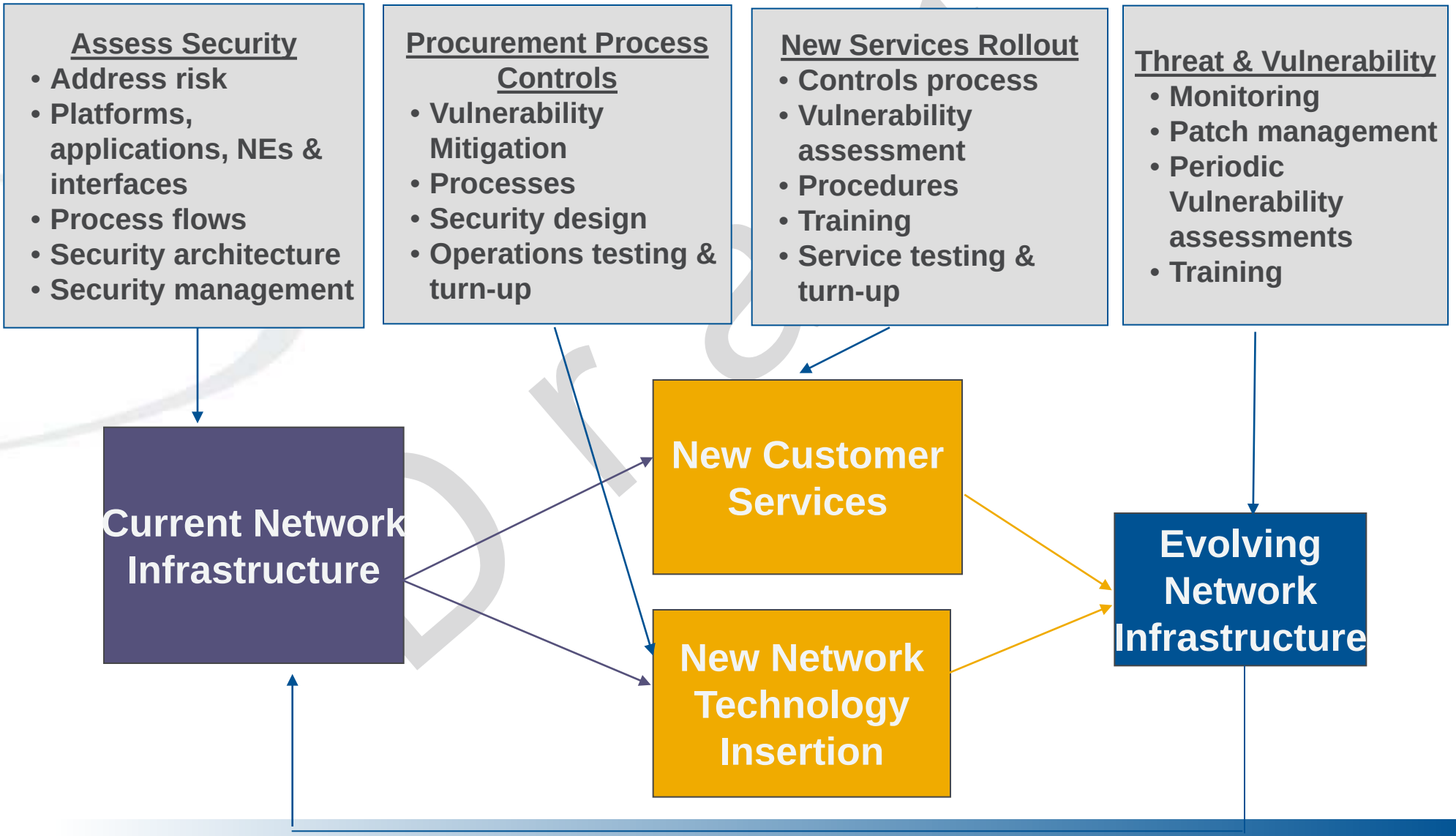
Growth of the Security Threats



Emerging Risks & Impacts

- Increases the exposure of the core optical transport network
  - With new user interface, unauthorized bandwidth requests may enable denial-of-service attacks
  - New routing protocols may not be sufficiently protected and create network instability
  - Network forensics may be more difficult in a dynamic environment
  - Connections may be temporarily set up to support potential attacks and then disappear
- Gateway products will be emerging to mediate network access
  - Testing of security features will be required to determine protection level

Security Risk Management Roadmap



Powerhouse Research. Practical Solutions.