



HELLENIC REPUBLIC
National and Kapodistrian
University of Athens

Network Security in the 6G Era

Anna Tzanakaki

National and Kapodistrian University of Athens, Greece

atzanakaki@phys.uoa.gr

Migration from 5G to 6G - Features

- ▶ The deployment of 5G technologies is a reality around the world
- ▶ However, the requirements for interconnection and performance is soon exceeding the capabilities of 5G
- ▶ 6G will support a large variety of applications and offer improved performance in comparison to 5G
 - ▶ Unprecedented connectivity, peak data rates, latency, energy efficiency, etc.
- ▶ 6G will offer ubiquitous infrastructures integrating the most advanced and heterogeneous network and compute technologies
- ▶ Increased Intelligence and flexibility through wider adoption of AI and ML
- ▶ Increased complexity
 - ▶ Need for autonomous operation and self-optimisation
- ▶ New and enhanced capabilities such as localisation, monitoring and sensing of the surrounding environment



Migration from 5G to 6G – Technology Challenges

- ▶ Billions of end-devices
- ▶ Multi-cloud/Heterogeneous Cloud
- ▶ Millions of subnets
- ▶ Open Interfaces & Dissagregation
- ▶ Multi-vendor environments (O-RAN)
- ▶ AI native operation



Migration from 5G to 6G – Threats I

- ▶ Increase of attack Surface across all domains
- ▶ Risk associated with scalability of authentication
- ▶ Physical threats:
 - ▶ The 6G network is highly vulnerable to physical tampering of nodes
 - ▶ Deploying MEC with lightweight devices may compromise both the integrity of the devices and the data they process
 - ▶ IoT systems are susceptible to resource exhaustion, insecure communication, and physical intrusion due to limited computational capacity and security controls
- ▶ The heterogeneous edge/central cloud infrastructure suffers interoperability challenges for security mechanisms as it lacks relevant standardization



Migration from 5G to 6G – Threats II

- ▶ User interfaces: Limited user interfaces in many end devices affect threat awareness and response
- ▶ Weak computation power: Edge devices at the periphery lack robust defense mechanisms
- ▶ Security protocols: Not designed according to 6G requirements such as low-latency, high-speed communications
- ▶ MEC containerization: Containers may run on compromised hosts or dishonestly consume significant resources, incapacitating other containers
- ▶ Edge computing security is complicated due to the mobility of network entities across administrative domains

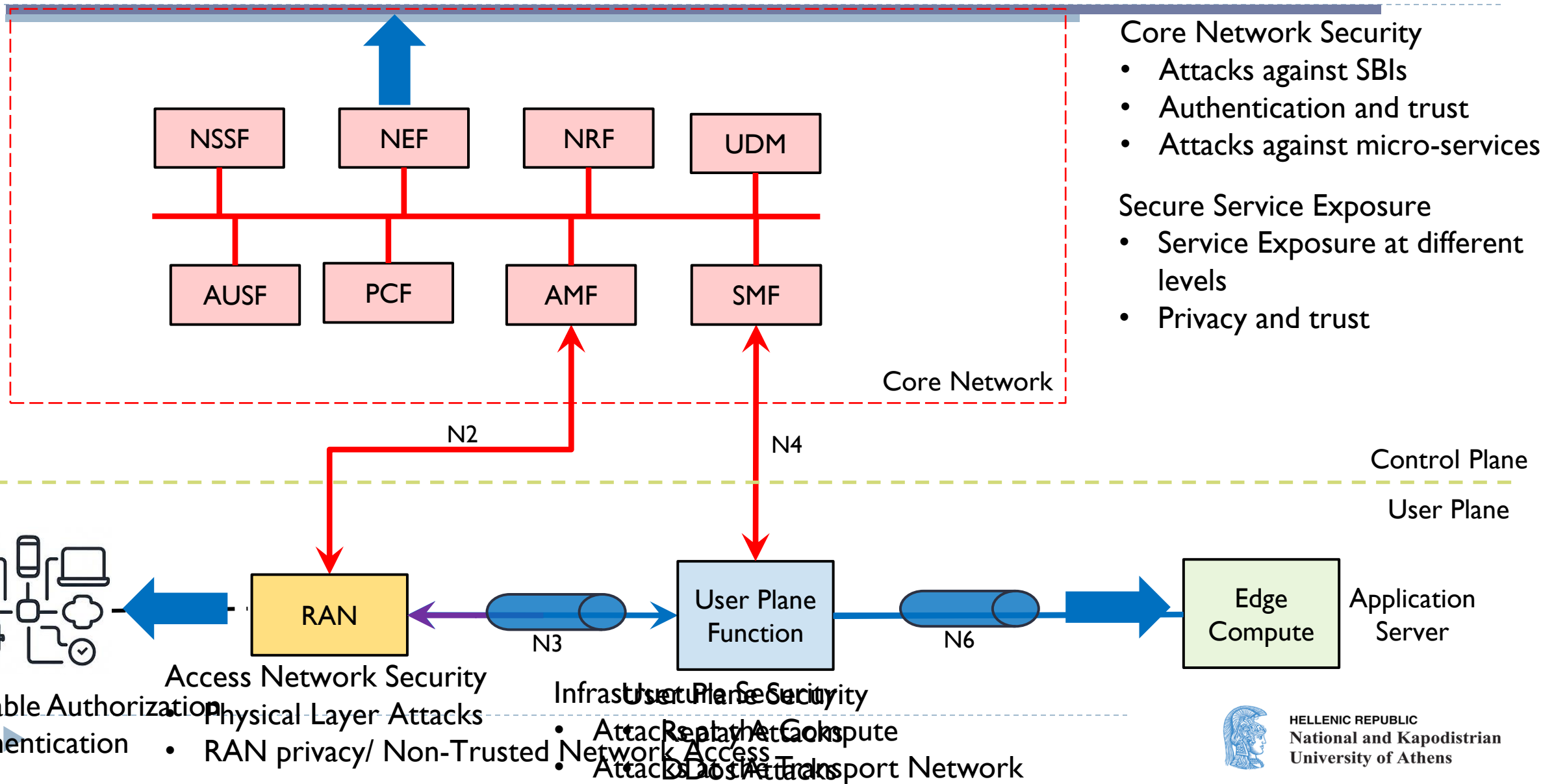


Migration from 5G to 6G – Threats III

- ▶ **Software Defined Networking (SDN):** Decoupling of control and data planes introduces vulnerabilities
 - ▶ SDN switches, with limited memory, are vulnerable to resource saturation attacks
 - ▶ Centralized controllers can potentially compromise network performance and integrity as well as be overloaded and cause network disruptions
- ▶ **Open interfaces:** promoted e.g. by O-RAN expand the attack surface and expose the system to third-party code
- ▶ **Multi-vendor interoperability:** Multiple vendors and service providers can lead to inconsistent security implementation and varying levels of security expertise
- ▶ **Powerful attacks:** Adversarial attacks, exploiting vulnerabilities in AI algorithms can potentially have a very large attack surface in 6G environments



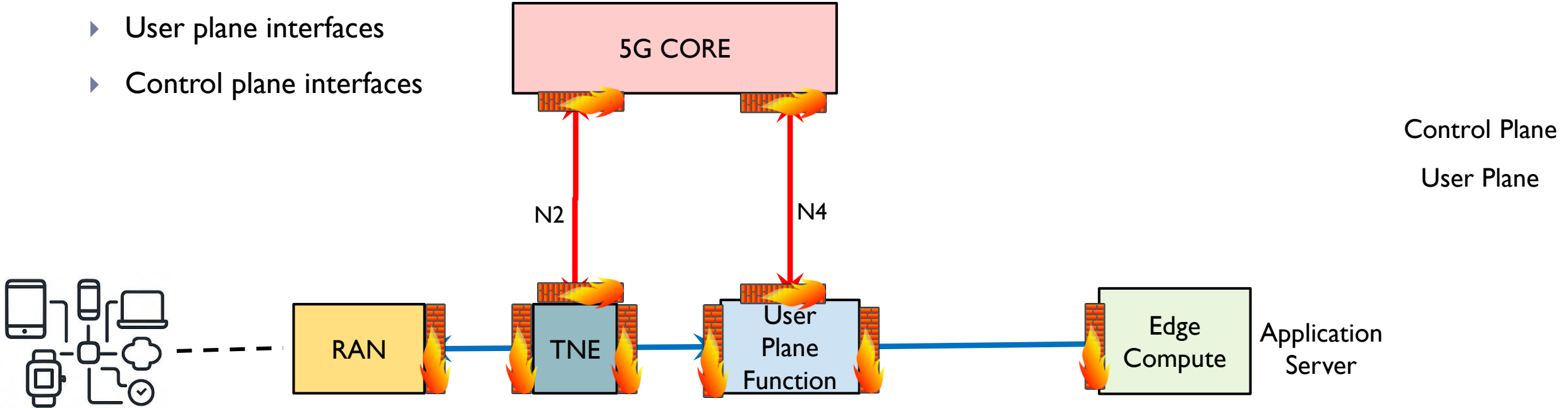
5G Network Architecture



5G Network Architecture Security

- ▶ Protection of SBIs based on Firewall for:

- ▶ User plane interfaces
- ▶ Control plane interfaces



- ▶ Vulnerable against port scanning attacks

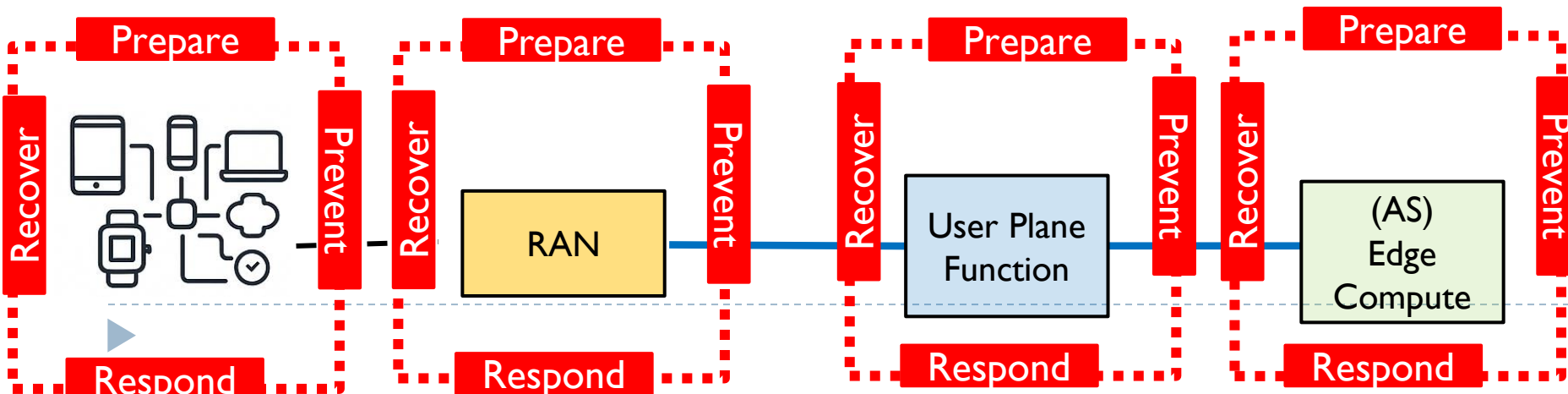
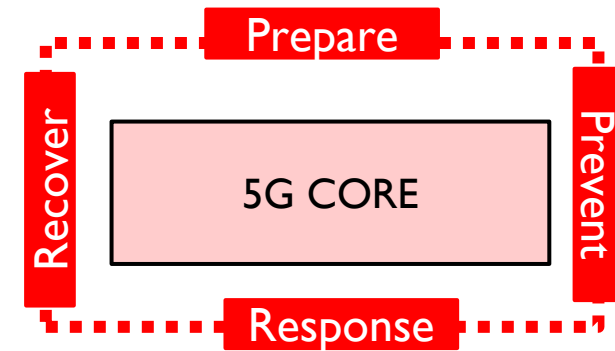
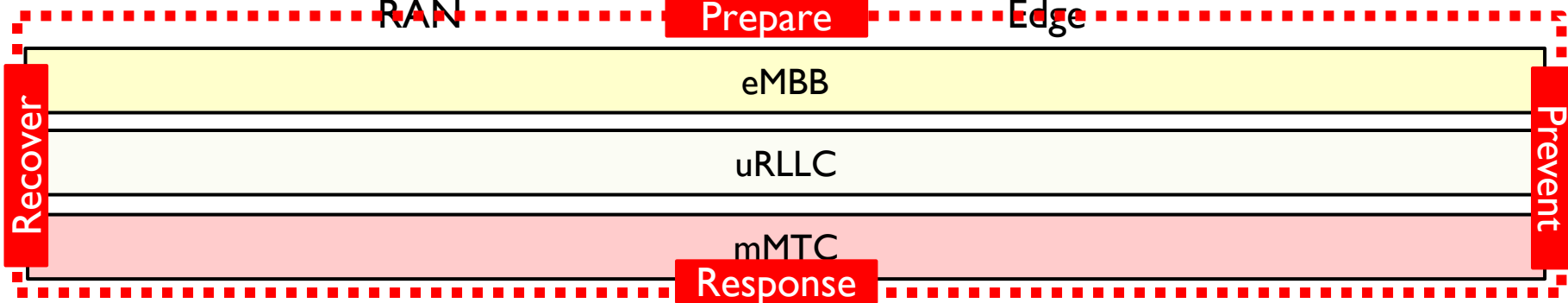
▶ Zero Trust for Private 5G/Edge, <https://www.zscaler.com/products-and-solutions/private-5G>



5G Zero Trust Network approach

- Assume a breach is inevitable (or has already occurred)
- Constantly limit access to only what is needed
- Looks for anomalous/malicious activity everywhere

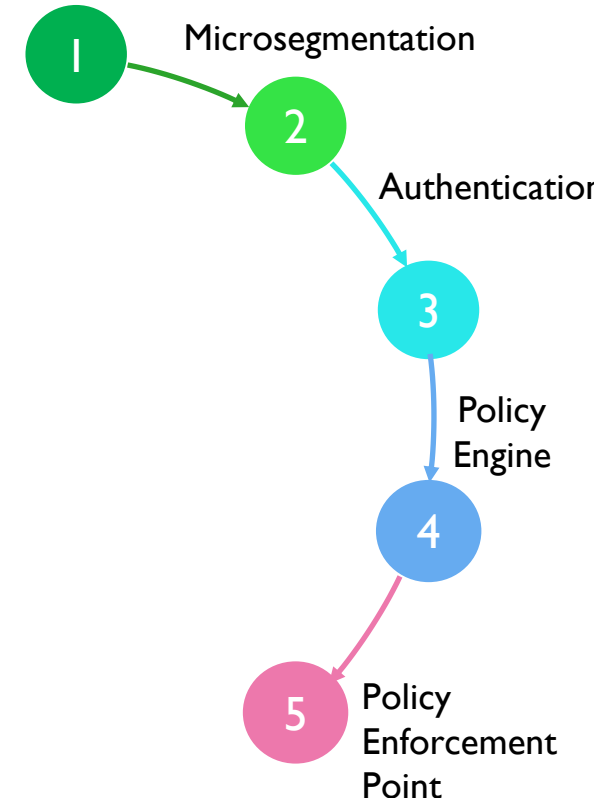
End-to-end protection: Local cybersecurity loops



Zero Trust Architecture: Principles

- 1. Identity and Access Management:** Strong authentication methods to ensure that only authorized individuals can access applications and data
- 2. Microsegmentation:** Divides the network into secure zones to limit movement of threats within the network and isolate compromised devices or segments
- 3. Multi-Factor Authentication:** Requires users to provide multiple verification factors to gain access to resources, reducing the risk of unauthorized access due to compromised credentials
- 4. Policy Engine:** It makes decisions regarding granting access based on policies, user behavior etc
- 5. Policy Enforcement Point:** Strict enforcement of access policies. Policies consider the risk level of each transaction and must dynamically adapt based on user attributes, device posture, and environmental conditions

Identity and Access Management



Zero Trust Architecture: Principles

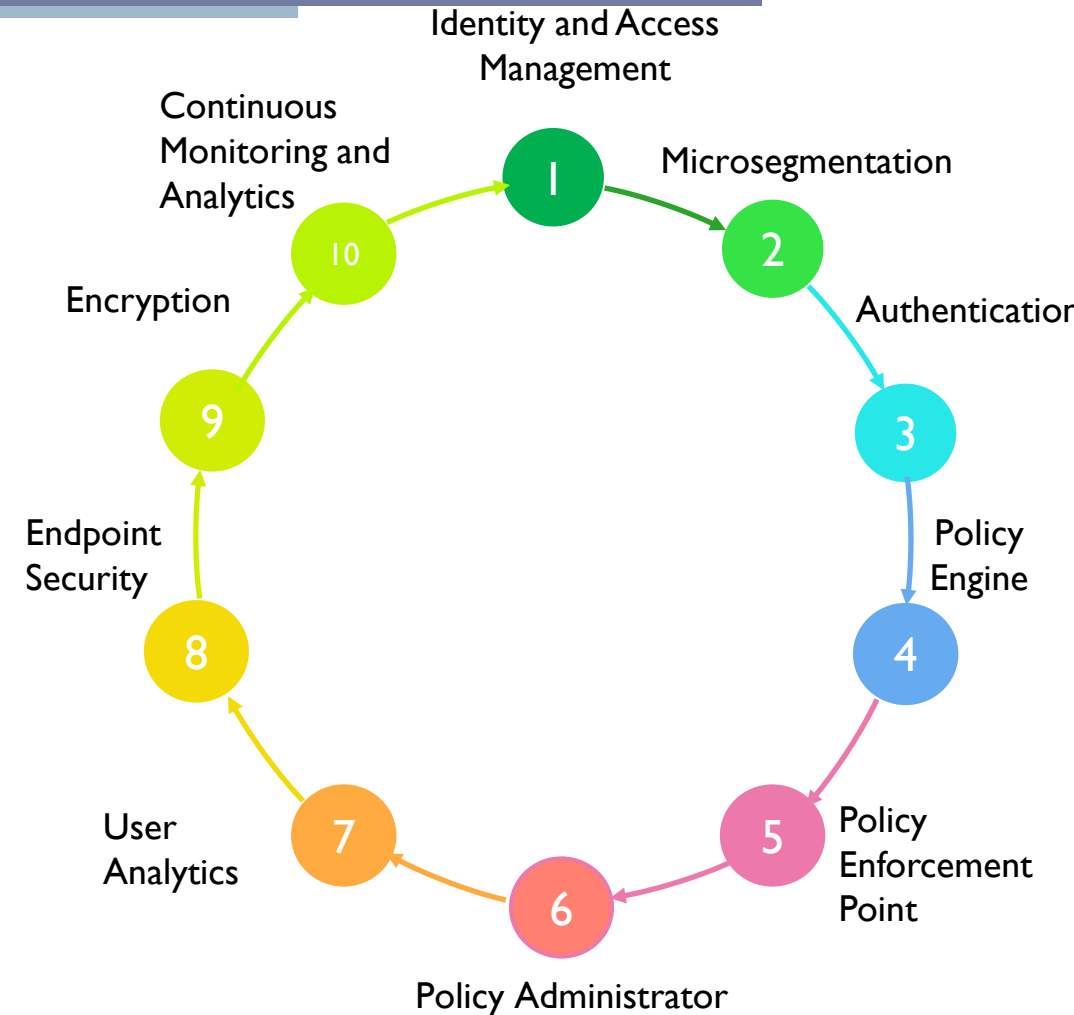
6. Policy Administrator: Establishes and terminates connections between users and resources based on policies set by the Policy Engine

7. User Analytics: Are responsible to analyze patterns of behavior to detect anomalies that could indicate a threat

8. Endpoint Security: Advanced endpoint protection solutions monitor and protect devices from threats. They ensure that only healthy and compliant devices are allowed to connect to the network

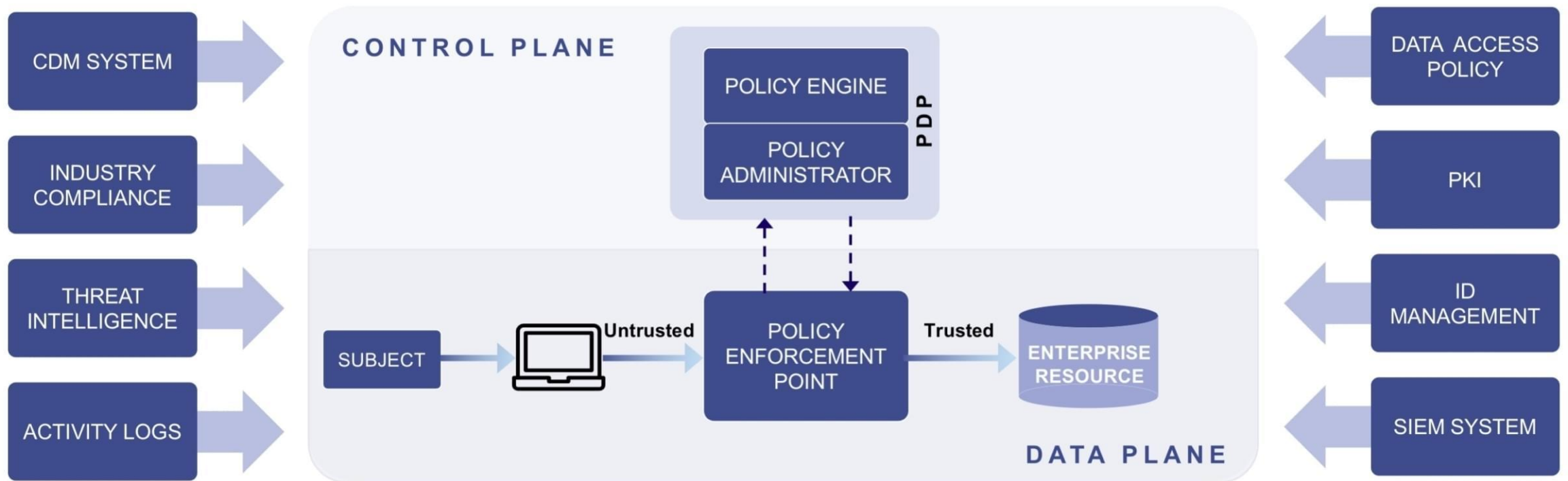
9. Encryption: Data encryption protects sensitive information both at rest and in transit. If data is intercepted, it cannot be easily accessed without the decryption key

10. Continuous Monitoring and Analytics: Real-time monitoring and analysis of network traffic and user behavior to help detect anomalies and potential threats. This facilitates rapid response and risk mitigation.

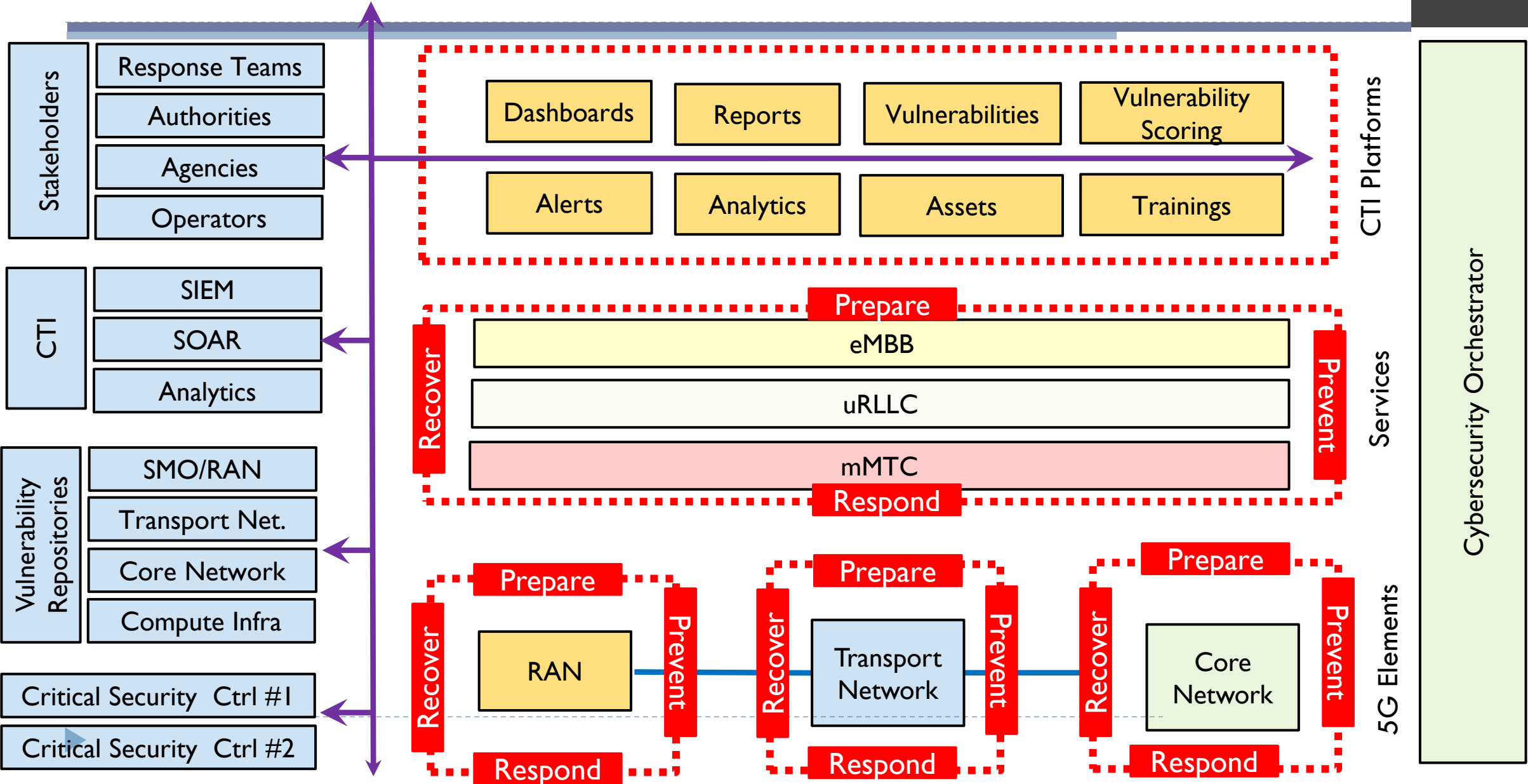


Zero Trust Architecture

- ▶ Policy Engine
- ▶ Policy Enforcement Point

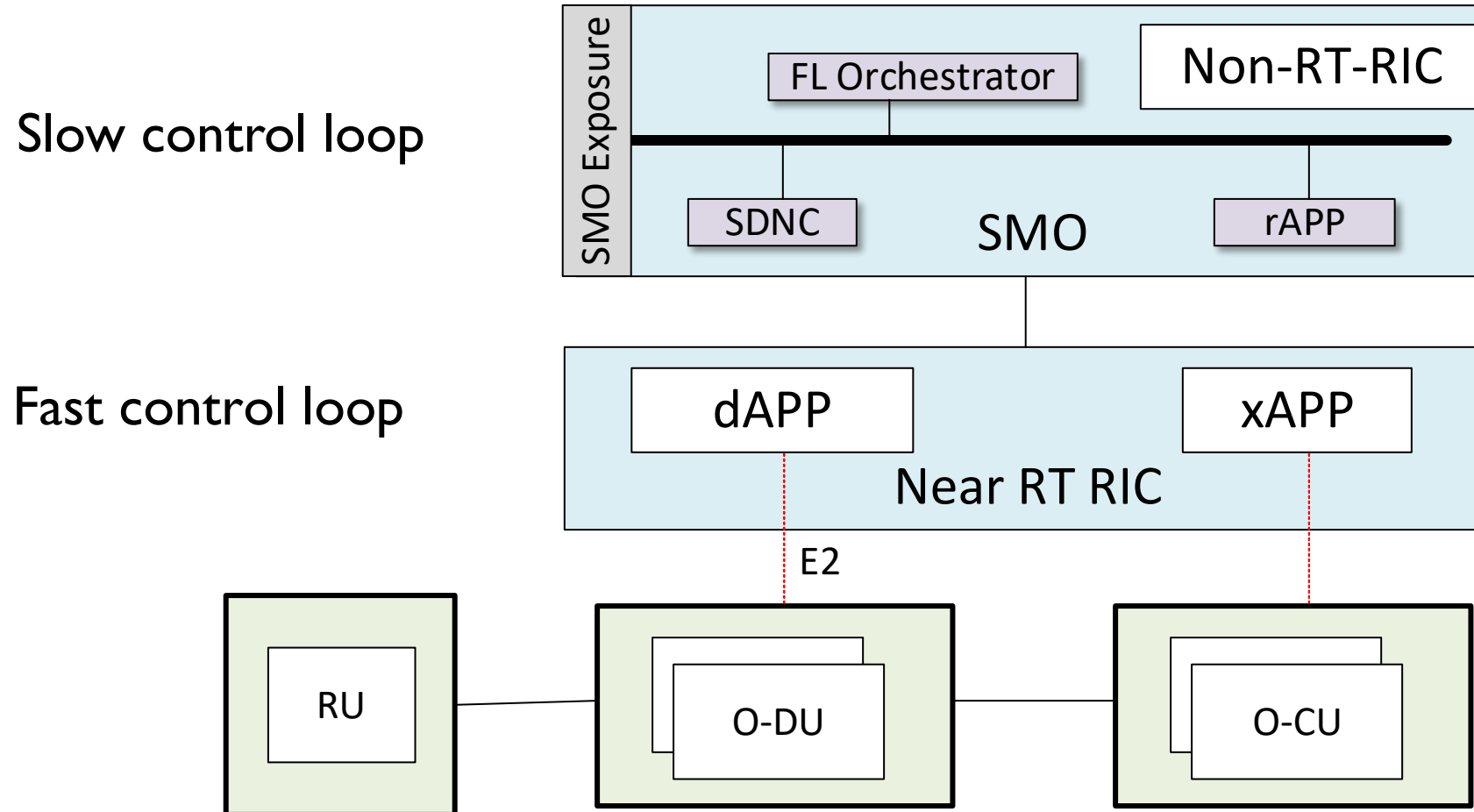


5G TACTIC Security Architecture based on ZTN



Zero Trust Networking applied in RAN

O-RAN architecture



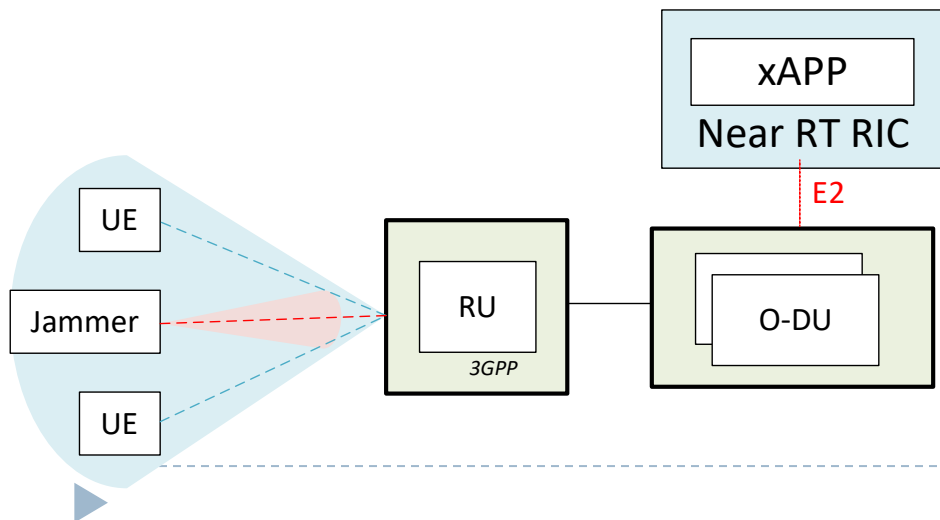
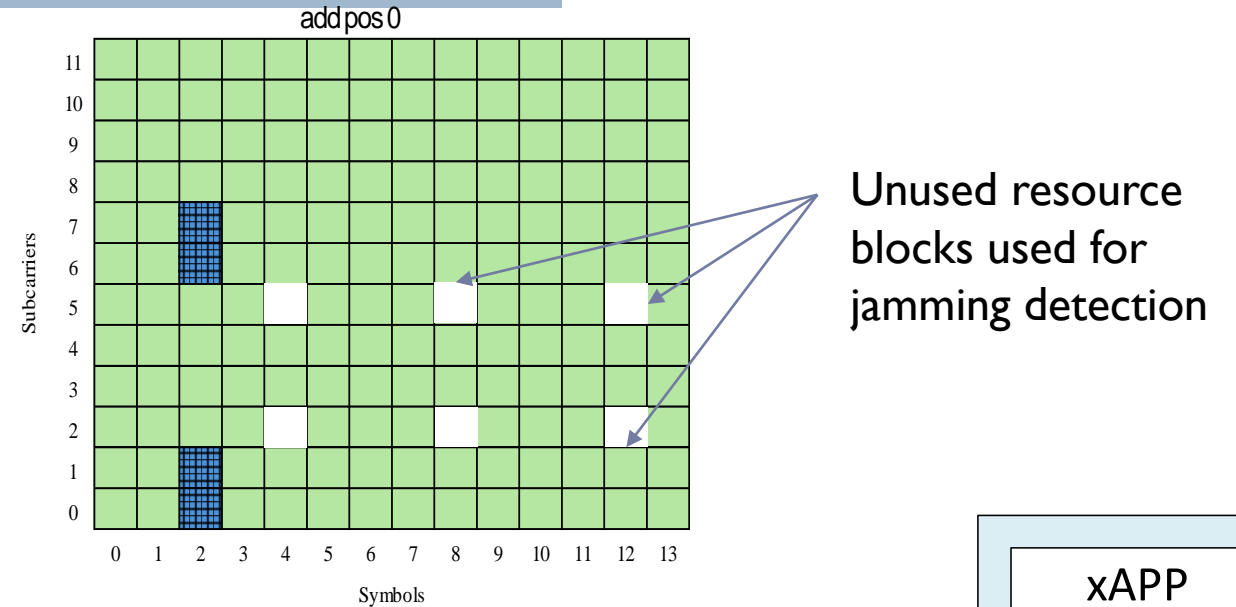
Zero Trust Networking applied in RAN

- ▶ Implement critical Control actions preparing, preventing, responding, and recovering from attacks
- ▶ Test system for vulnerabilities before deployment
- ▶ Protect system as threats evolve
 - ▶ Implemented in the forms of **rAPPs** and **xAPPs**
- ▶ **6G Use Case: Physical Layer Security protecting ISAC services**
 - ▶ Detect sources of physical layer anomaly
 - ▶ Detect and localize jammers/fake targets affecting Comms and/or Sensing Services

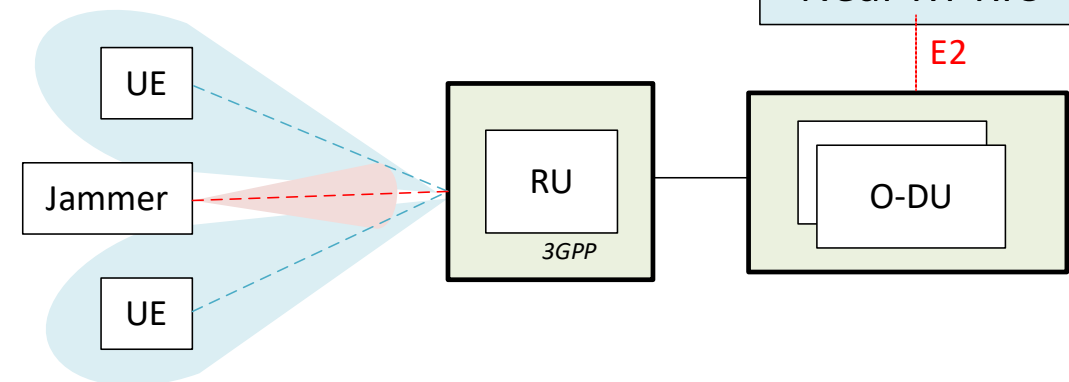


Zero Trust Networking applied in RAN – Comms Services I

- ▶ Jamming Attack Scenario
 - ▶ xAPPs for spectrum monitoring
- ▶ ...and defense

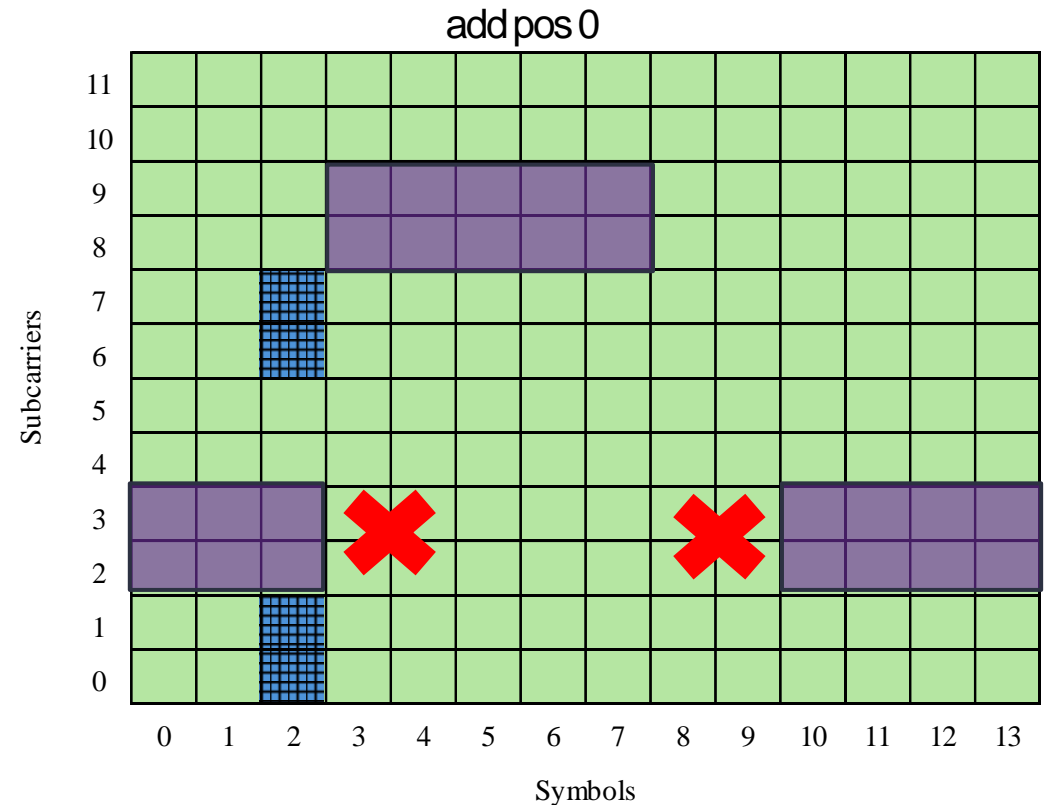
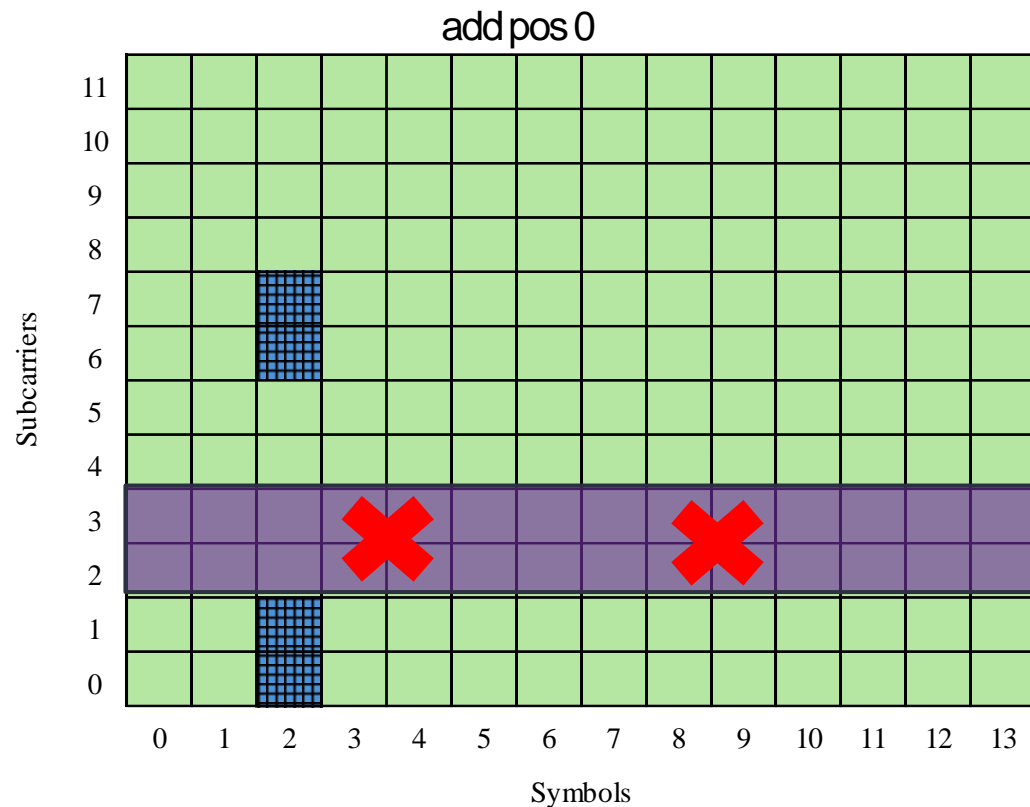


through adaptive beamforming



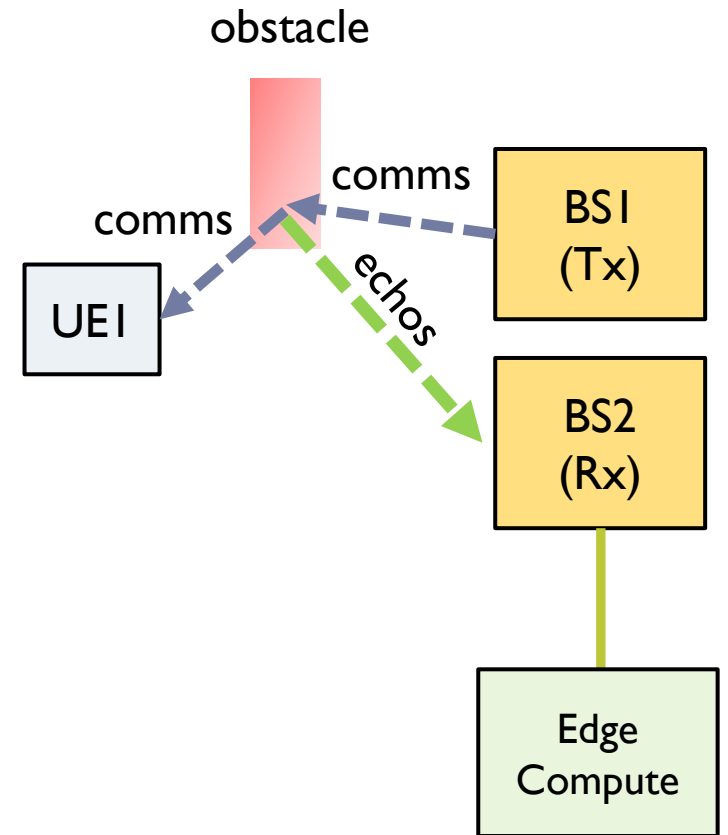
Zero Trust Networking applied in RAN - Comms Services II

- ▶ ...and scheduling mechanisms in the uplink (PUSCH) and downlink (PDSCH) performing frequency hopping for avoidance of sophisticated jamming patterns



Zero Trust Networking applied in RAN – Sensing Services

- ▶ Attacks against (radar-type) sensing services
- ▶ Sensing is performed based on the principle of a distributed passive wireless radar
- ▶ The transmitter and receivers can be physically separated or co-located
 - ▶ 6G BSs generate communication signals reflected on “objects” located in the surrounding area, creating IQ echo streams
 - ▶ IQ echo streams are redirected to an edge compute node for storage and processing



M. Anastasopoulos, J. Gutierrez & A. Tzanakaki, "Optical Transport Network Optimization Supporting Integrated Sensing and Communication Service", OFC 2025, USA, March 2025

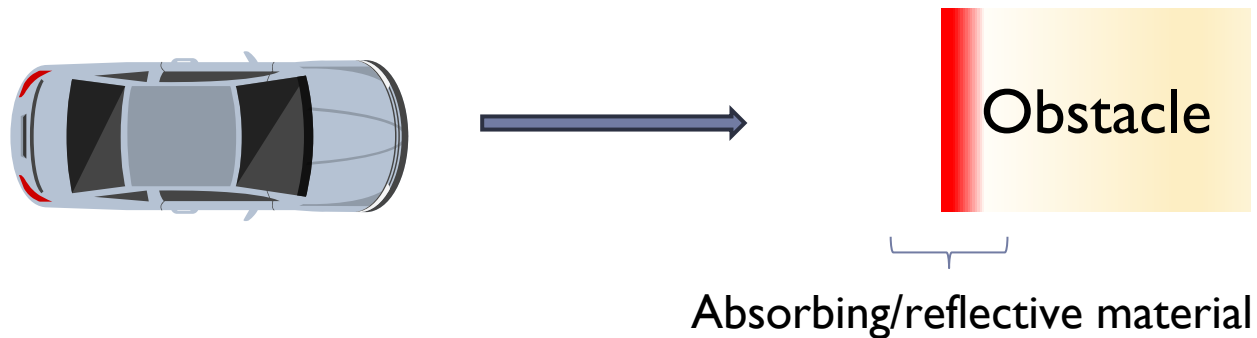
A. Tzanakaki et al, "Optical Transport Networks Supporting Integrated Communications and Sensing in 6G", ECOC 2025, *invited*, Sept 2025, Denmark



Zero Trust Networking applied in RAN - Sensing Services

- ▶ Adversarial attack

- ▶ Create additional input to machine learning models designed to cause the model to mis-classify or estimate wrong distances



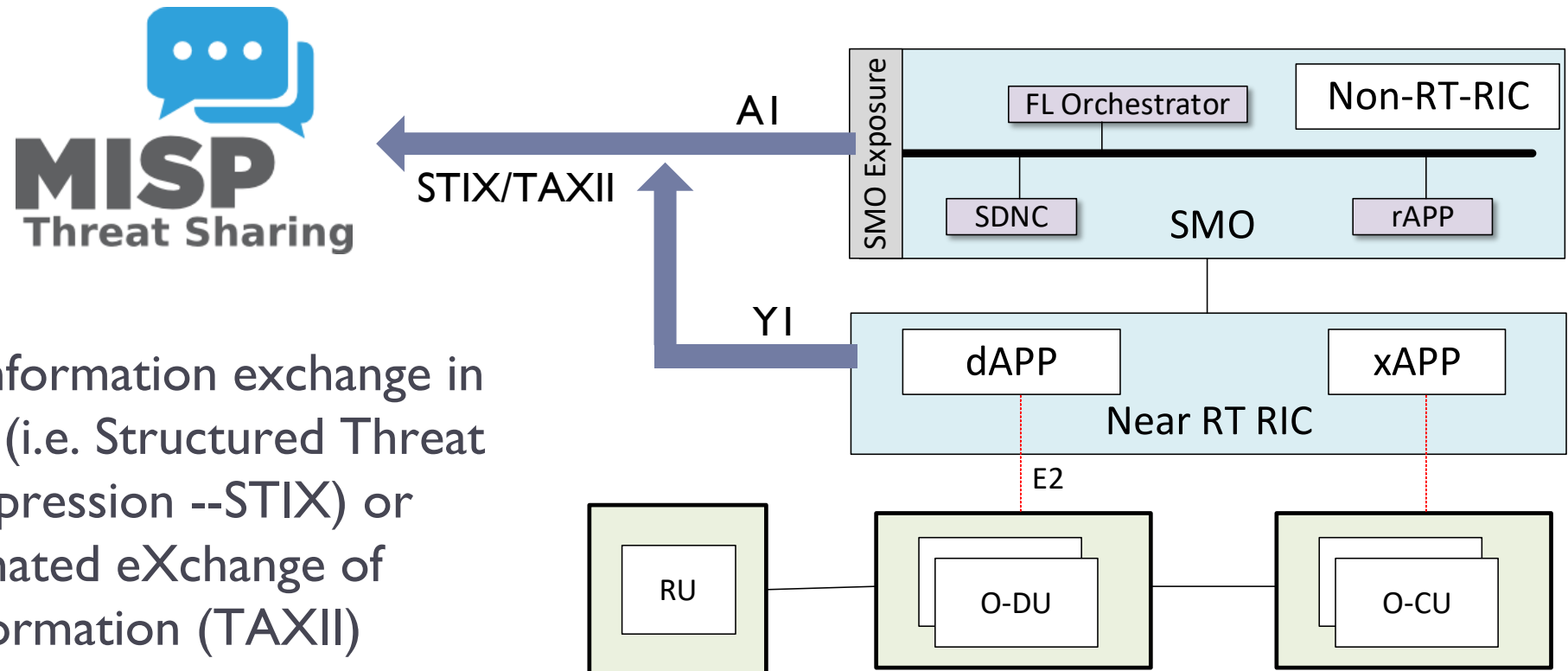
- ▶ Consider it similar to Dazzle camouflage



Zero Trust Networking applied in RAN – Information Sharing

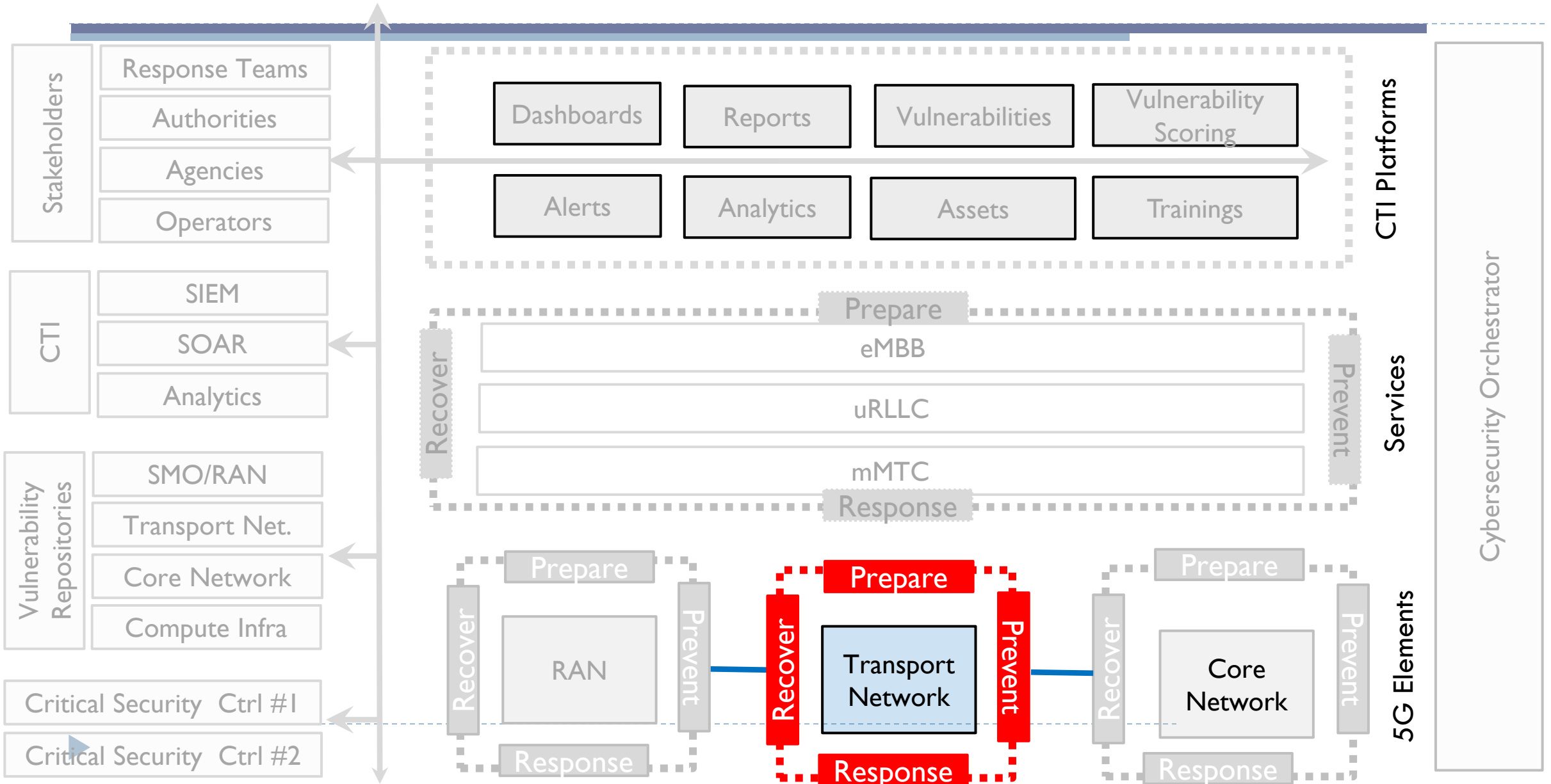
▶ Cybersecurity information sharing from O-RAN

- ▶ Exposure of vulnerabilities from O-RAN to Cyberthreat Intelligence Platforms such as MISP (collecting, storing, distributing and sharing cyber security indicators and threats)



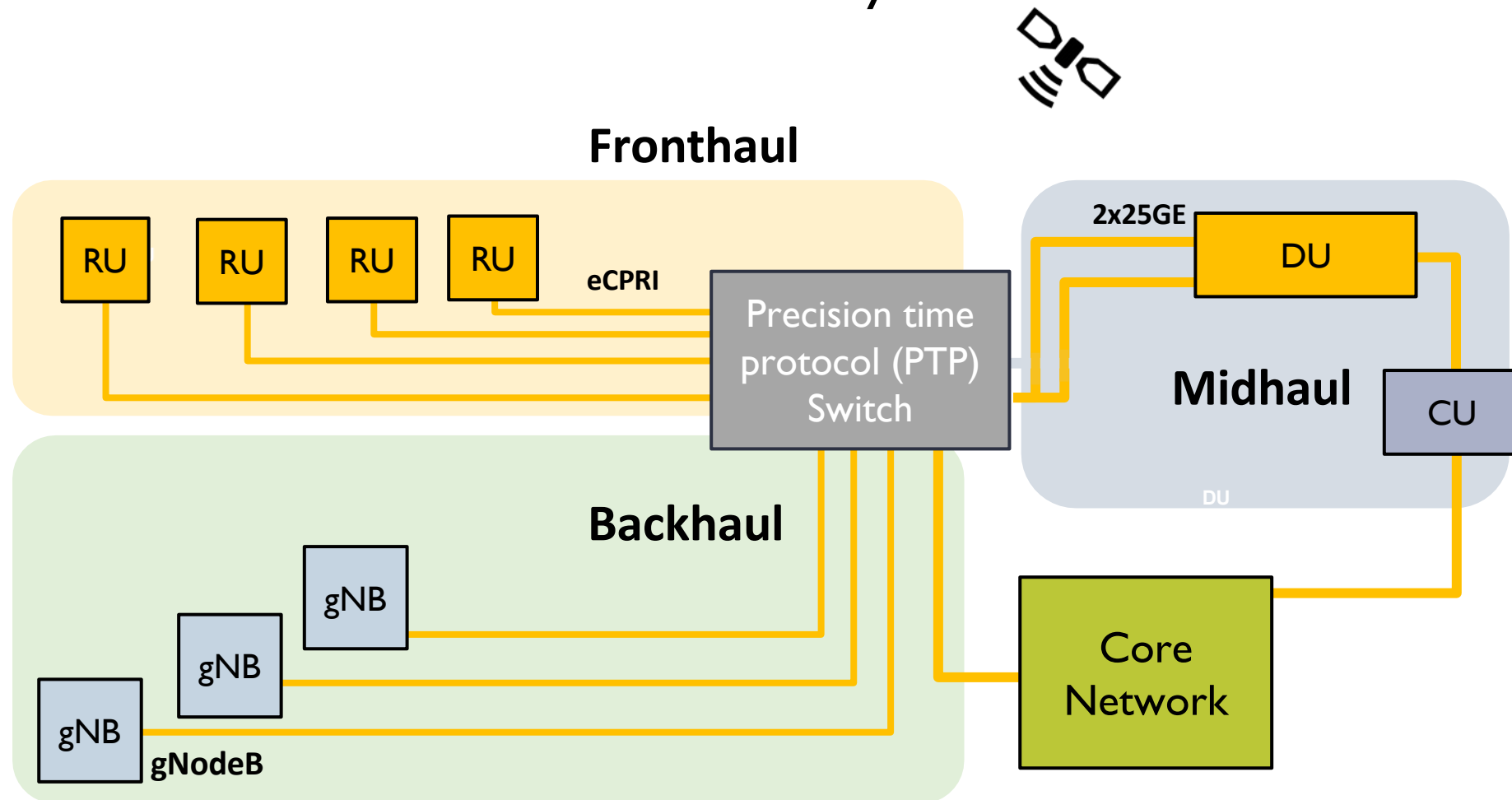
- ▶ Cyberthreat information exchange in specific format (i.e. Structured Threat Information Expression --STIX) or Trusted Automated eXchange of Intelligence Information (TAXII)

Zero Trust Networking applied in Transport Network



Transport Network in Open-RAN

- ▶ Fronthaul/Midhaul and Backhaul connectivity



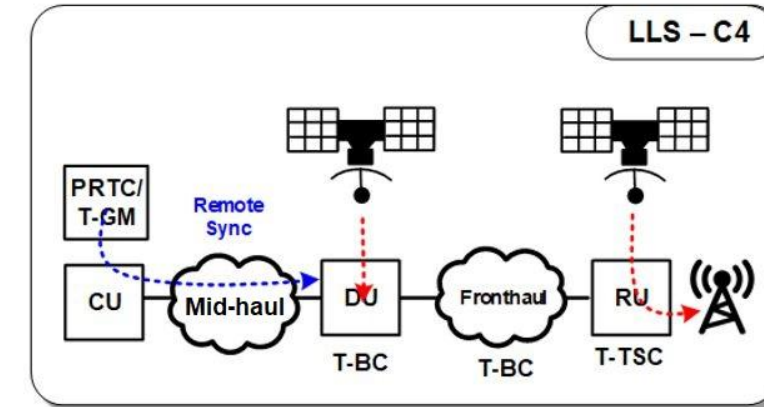
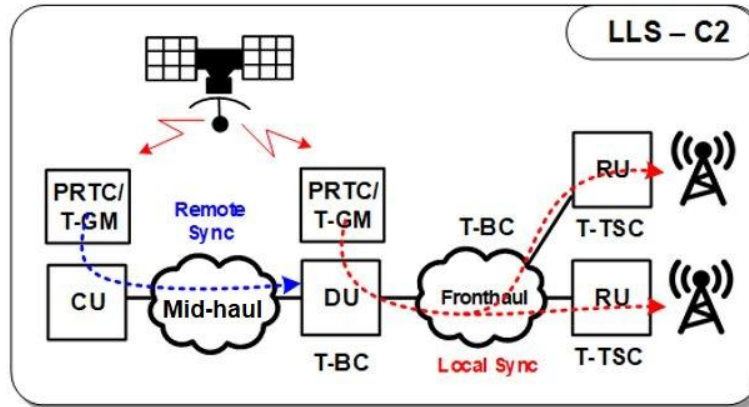
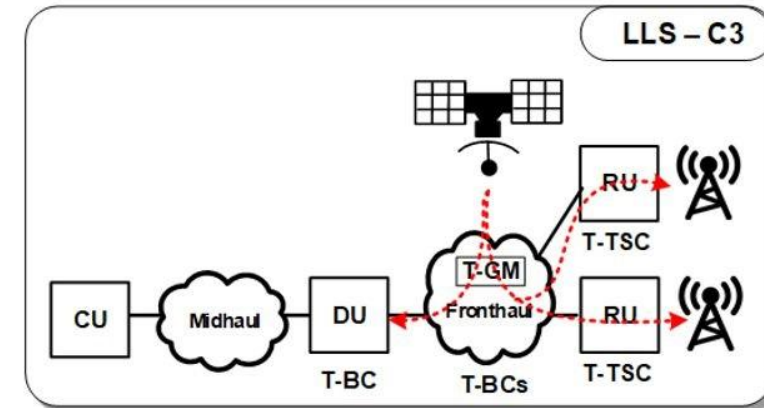
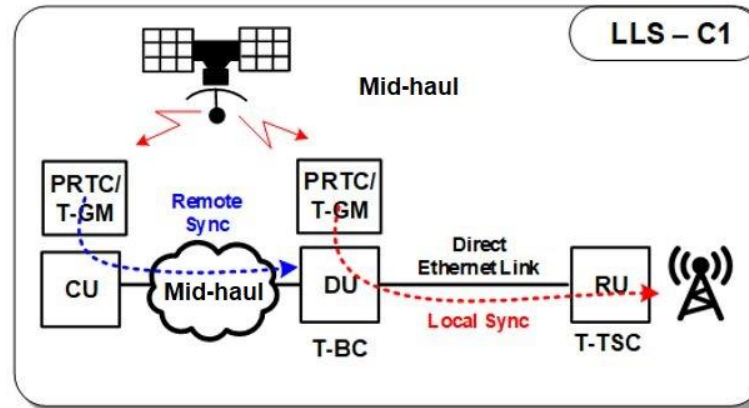
Transport Network in Open-RAN

▶ Timing and Synchronization error requirements

- ▶ Midhaul/Backhaul – 1.1uSec
- ▶ Fronthaul – 260 nSec Time Error

▶ Fronthaul Synchronization options:

- ▶ IEEE 1588 synchronizes the O-DU and O-RU units together, either from a time source in the O-DU (LLS-C1,2) or in a switch within the fronthaul network (LLS-C3)
- ▶ In LLS-C4 uses synchronization based on GNSS



Global Navigation Satellite System (GNSS)

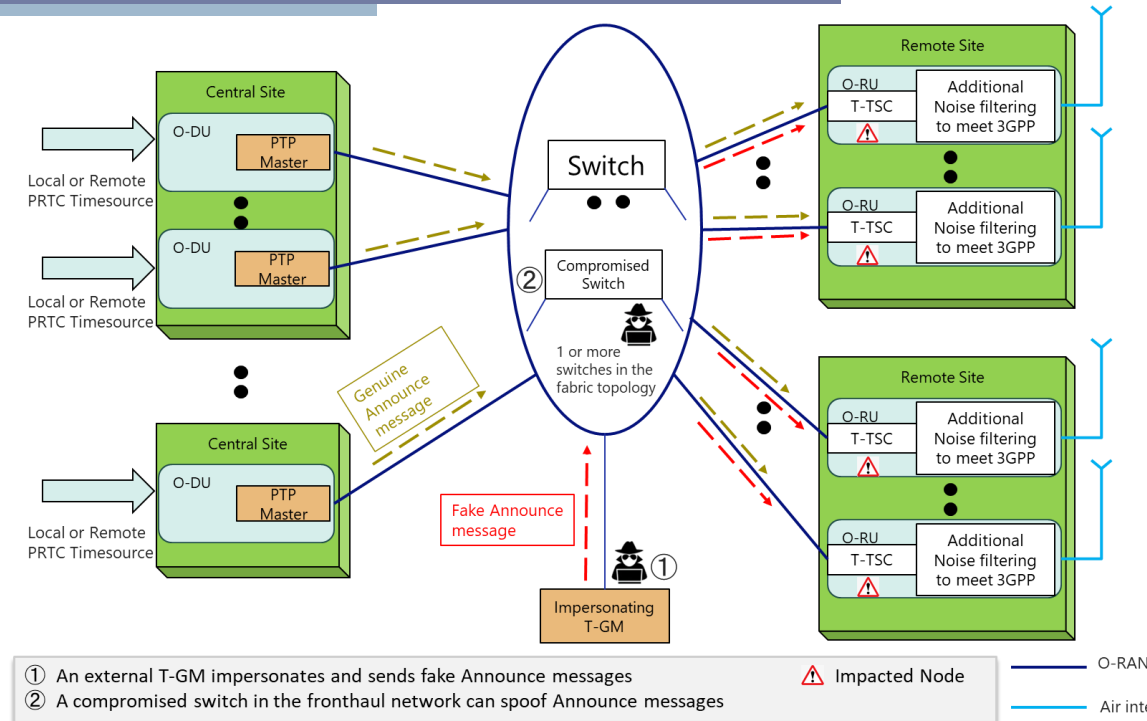
Transport Network in Open-RAN: Attack Scenarios

▶ Precision time Protocol attack scenarios

- ▶ Impersonation of a Time Transmitter clock (Spoofing) within a PTP network with a fake ANNOUNCE message
- ▶ DoS attack against a time Transmitter clock
- ▶ Selective interception and removal of PTP timing packets
- ▶ Packet delay manipulation attacks

▶ Solution

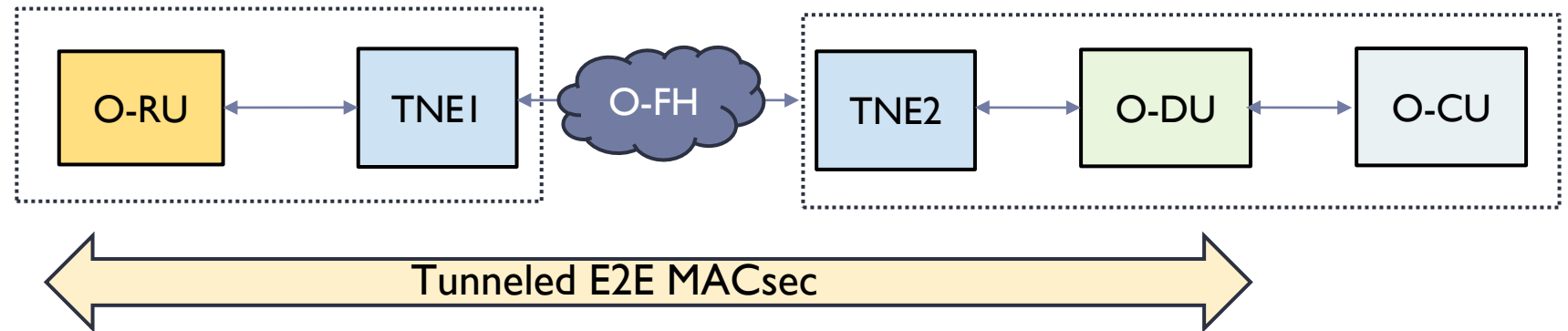
- ▶ Protection of Synchronization-Plane at L2 using **MACsec**
- ▶ Implement authentication and authorization for PTP nodes
- ▶ Provide **redundancy** in Open Fronthaul Synchronization



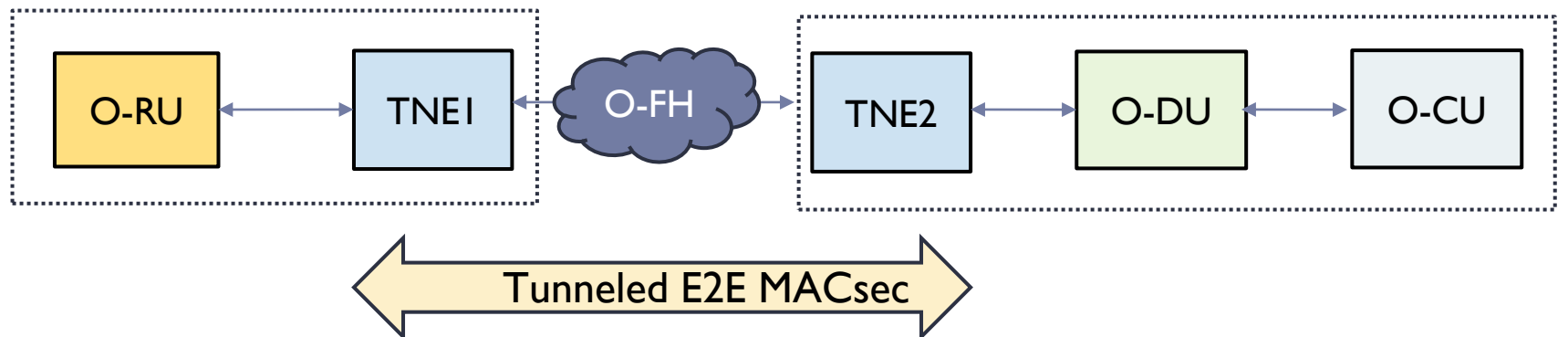
Securing Transport Network in Open-RAN

- ▶ Security at Fronthaul Layer 2 using MACsec
 - ▶ Various deployment options

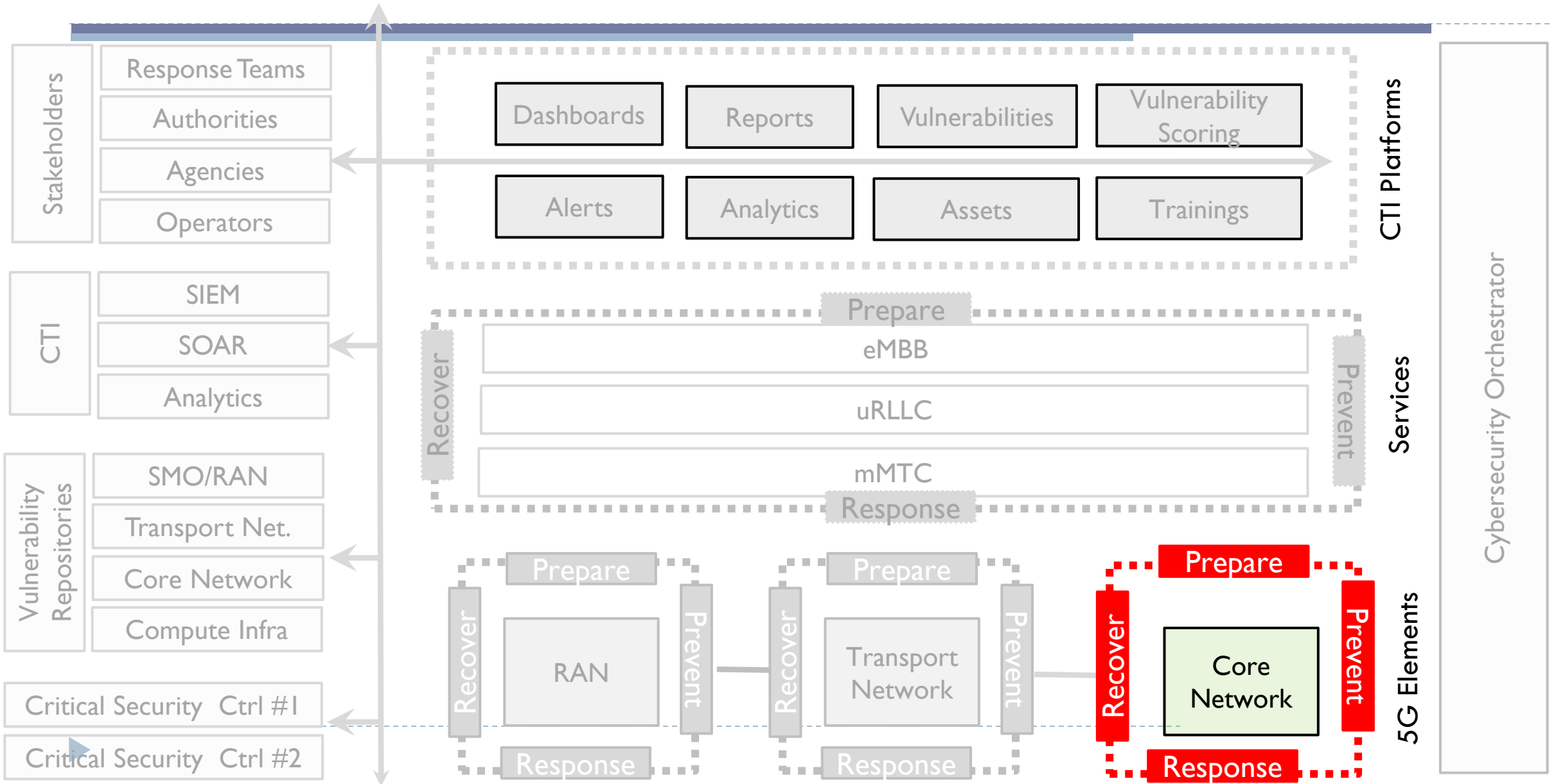
MACsec enabled at O-RU and O-DU



MACsec enabled at edge Transport Network Elements

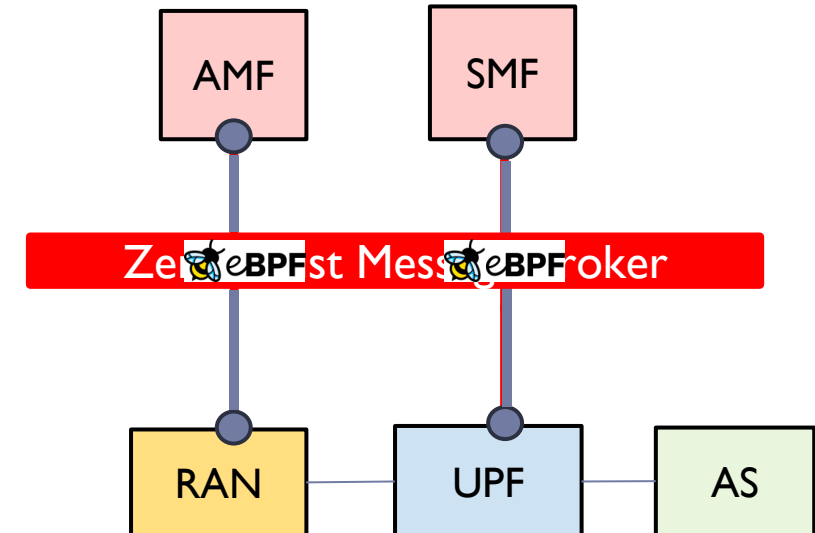


Zero Trust Networking applied in the Core Network



Zero Trust Networking applied in the Core Network

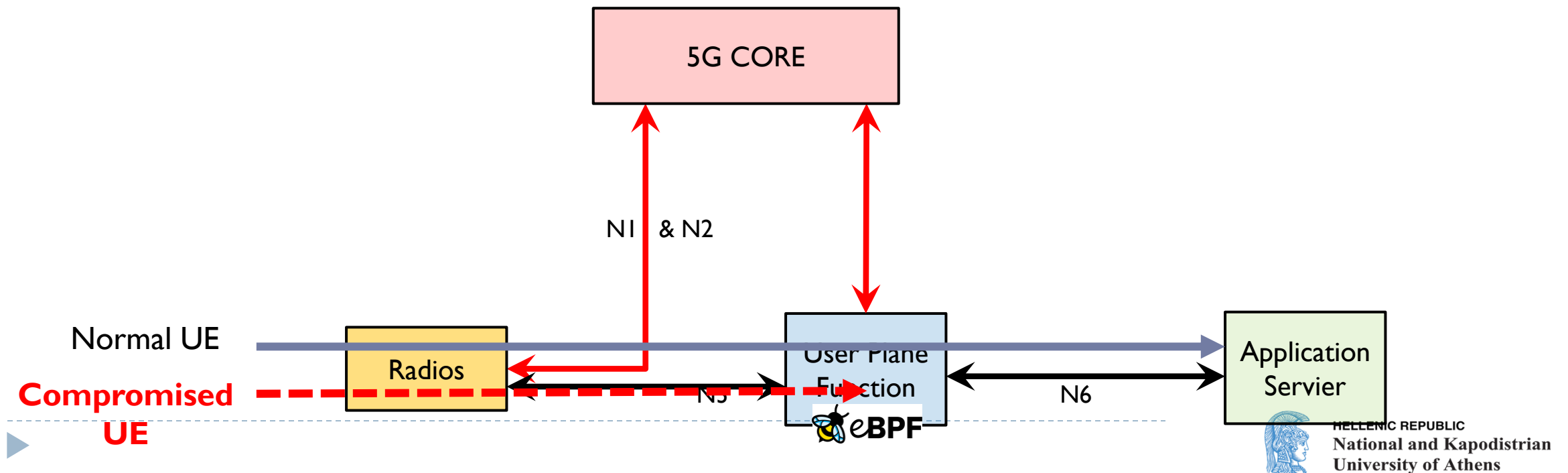
- ▶ Large attack surface
 - ▶ Multiple interfaces interconnecting virtualized network functions
 - ▶ An open system architecture that enables massive device connectivity
 - ▶ A compromised UE may cause significant damage to the system
- ▶ ZTN approach ~ Basic Elements
 - ▶ Zero Trust Message Broker:
 - ▶ Brokers connections between components of the system
 - ▶ Connectors: Deployed in front of microservices
 - ▶ Create secure tunnels from the components to the zero trust message brokers
 - ▶ Tunnels are created based on the available policies i.e., e2e or microsegmented to perform deep packet inspection using eBPF



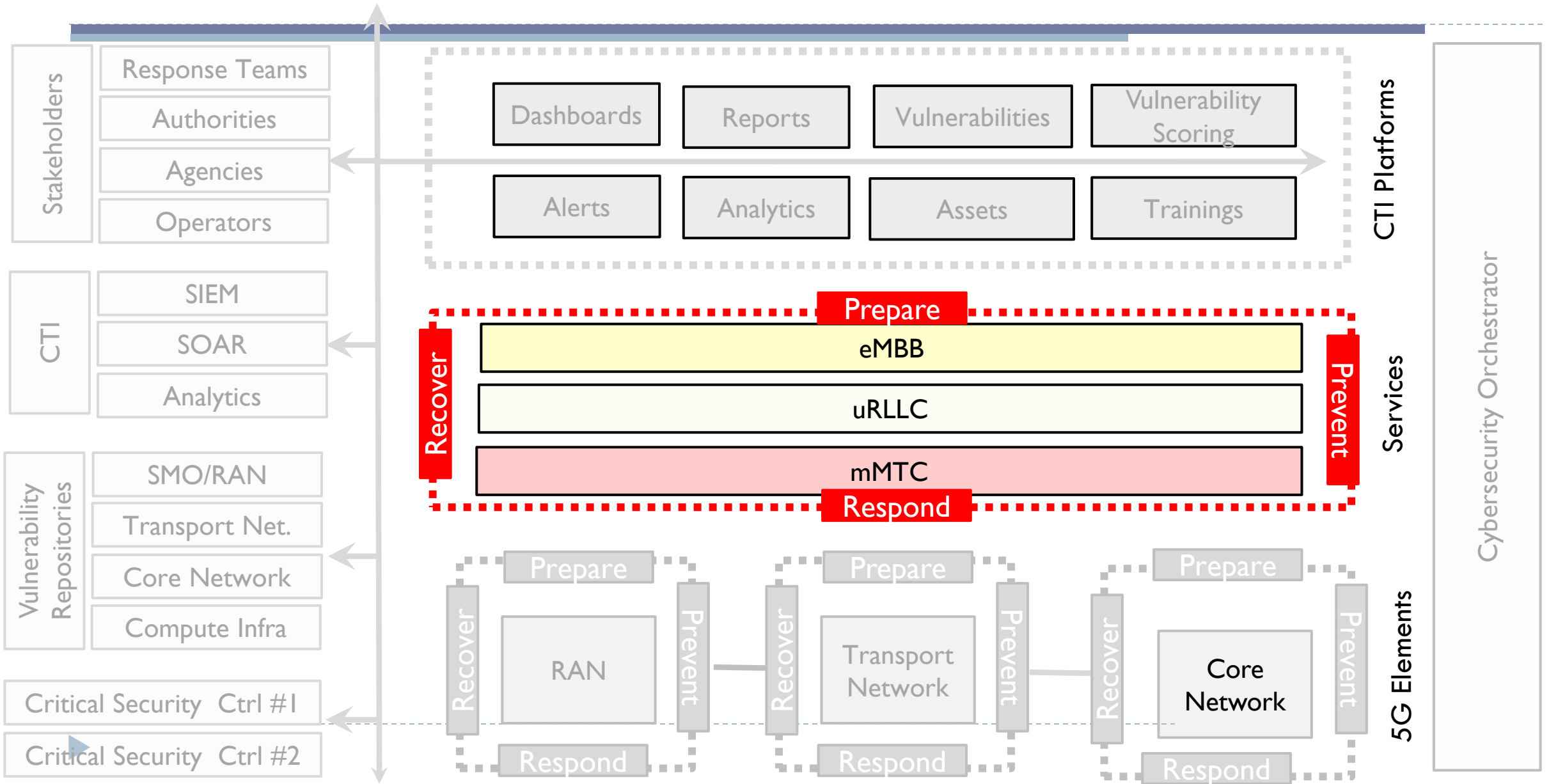
Zero Trust Networking applied in the Core Network

▶ Deep packet inspection:

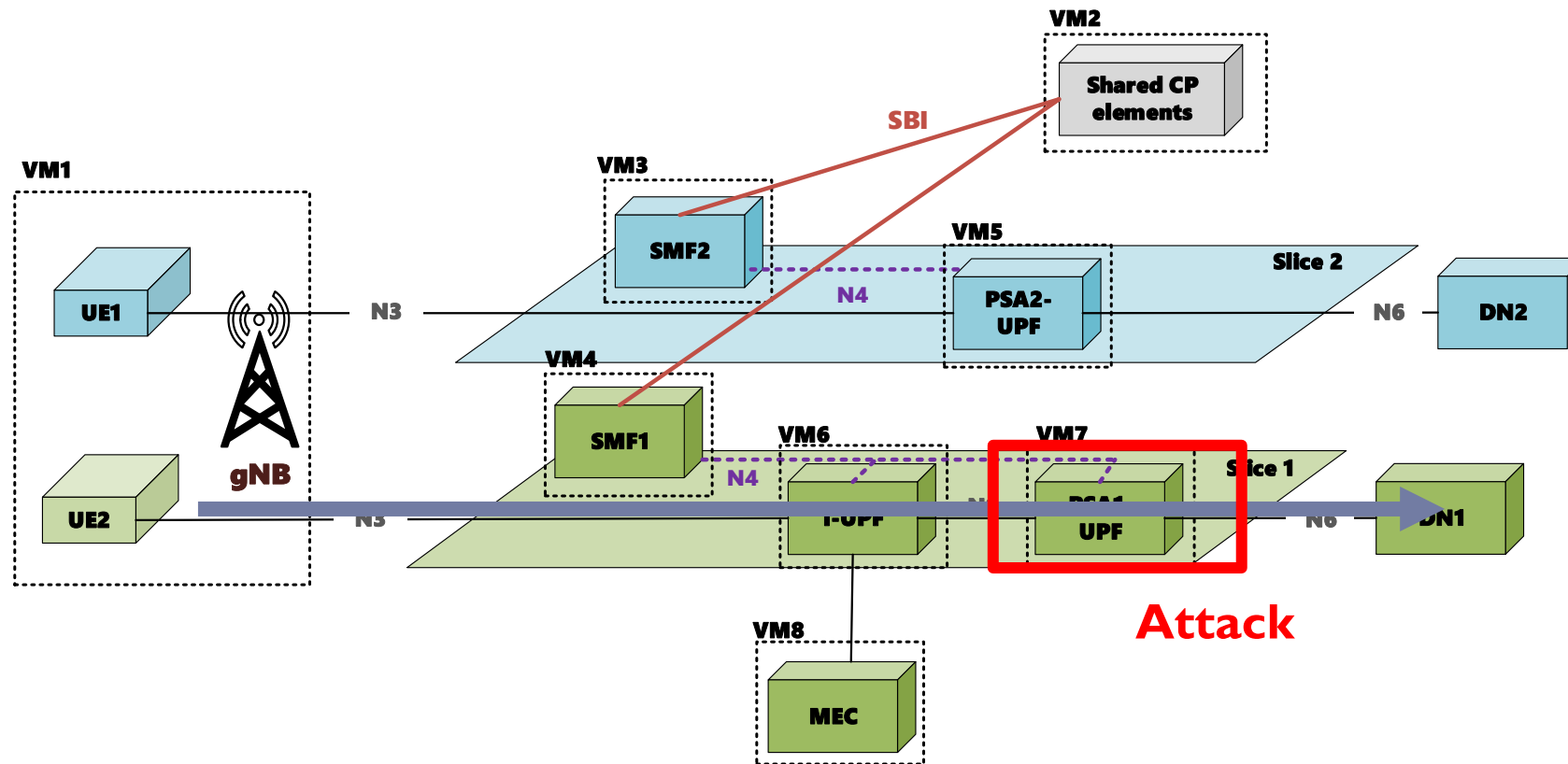
- ▶ Service flows continuously monitored and classified using eBPF.
- ▶ Traffic flows from compromised UEs are detected and dropped from the 5G network with minimal overhead for the network and without affecting the performance of existing services
- ▶ Alerts can be triggered applying policies mitigating risks i.e., setting a UE in an inactive state



Zero Trust Networking applied in Service Slices

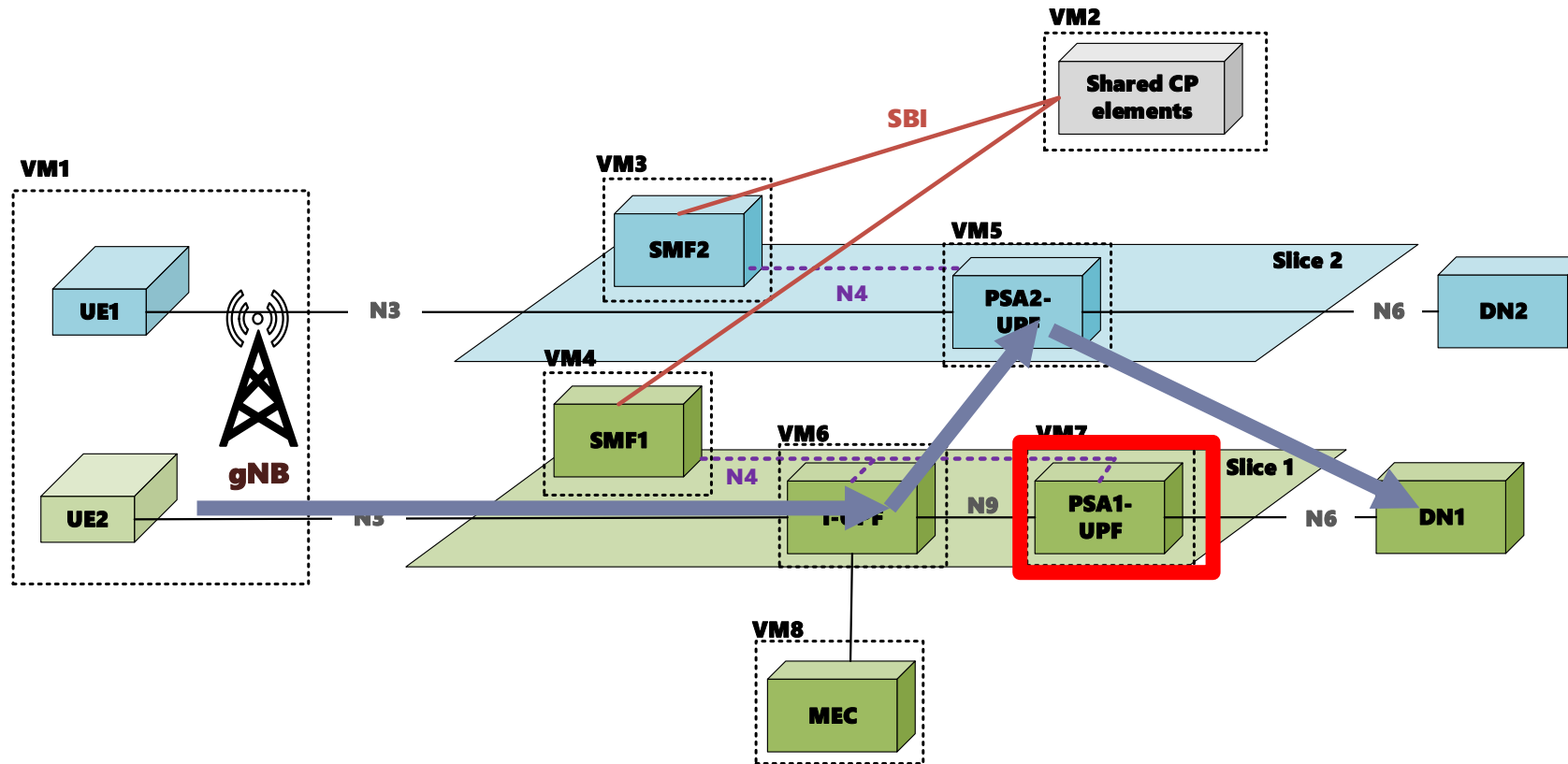


Zero Trust Networking applied in Service Slices: Attack Scenario



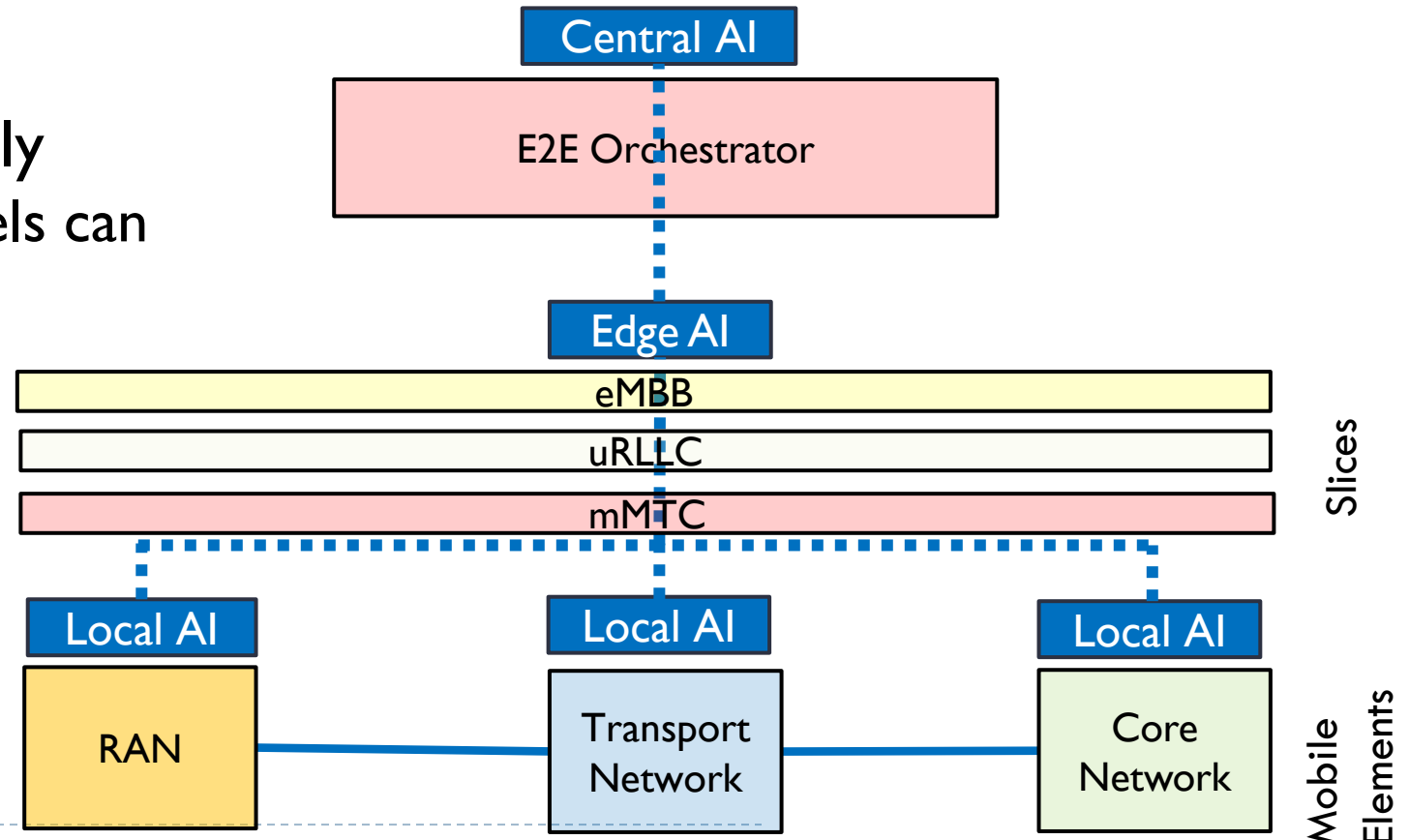
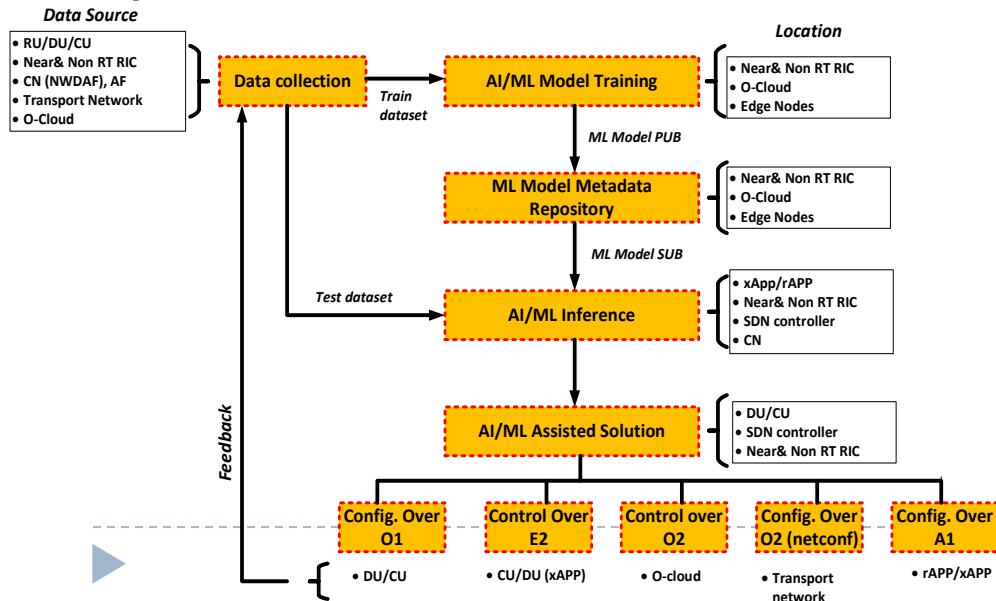
Zero Trust Networking applied in Service Slices: Attack Recovery

- ▶ Policies are applied to isolate the affected service



Network Intelligence: Native AI

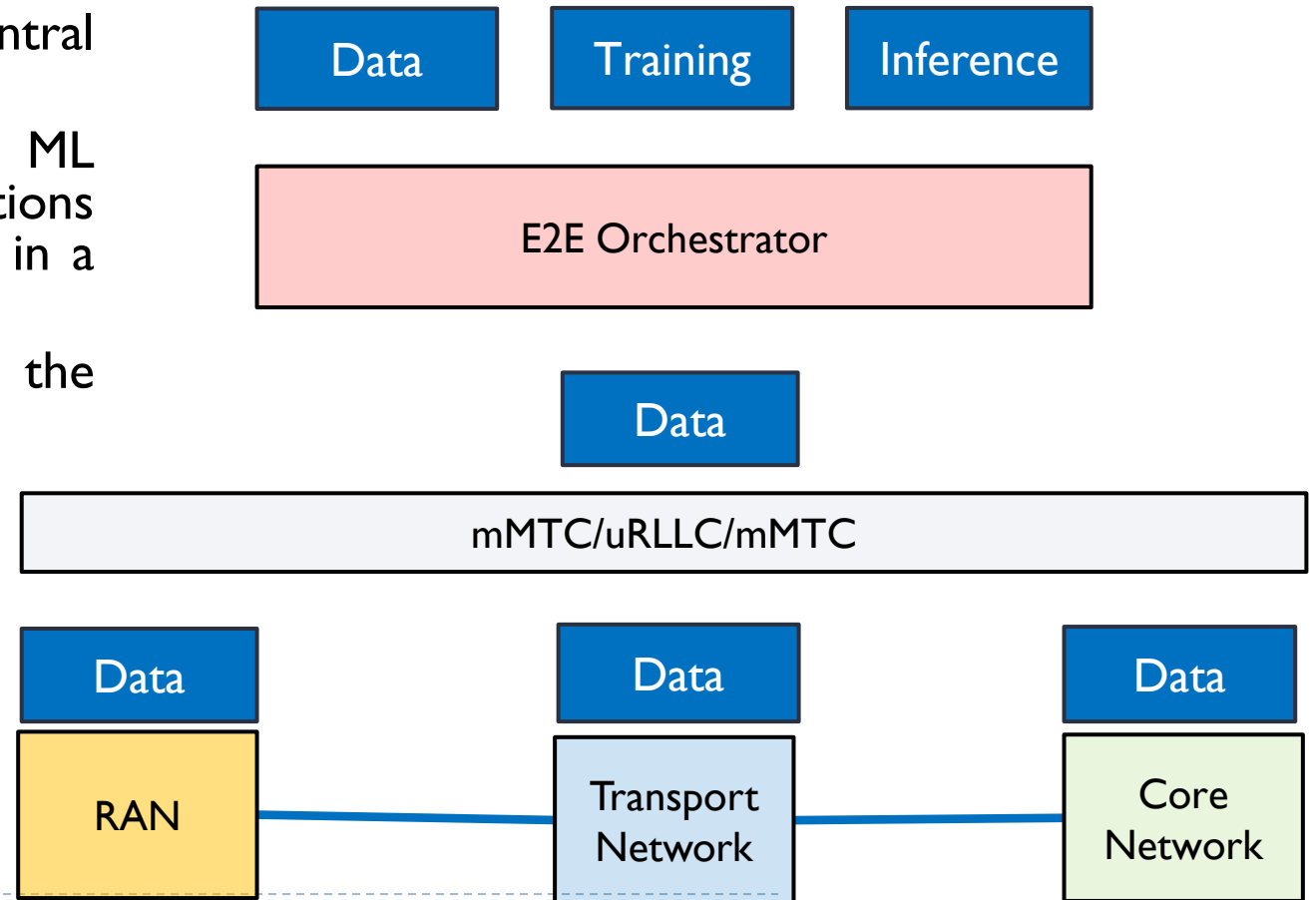
- ▶ AI models providing intelligence for the operation of:
 - ▶ Mobile elements and their supporting infrastructure i.e., RAN, Transport and Core Network
 - ▶ Network slices
 - ▶ E2E Orchestrator
- ▶ AI models deployed hierarchically
- ▶ Training and inference for AI models can be performed at different locations



Centralised Knowledge Management

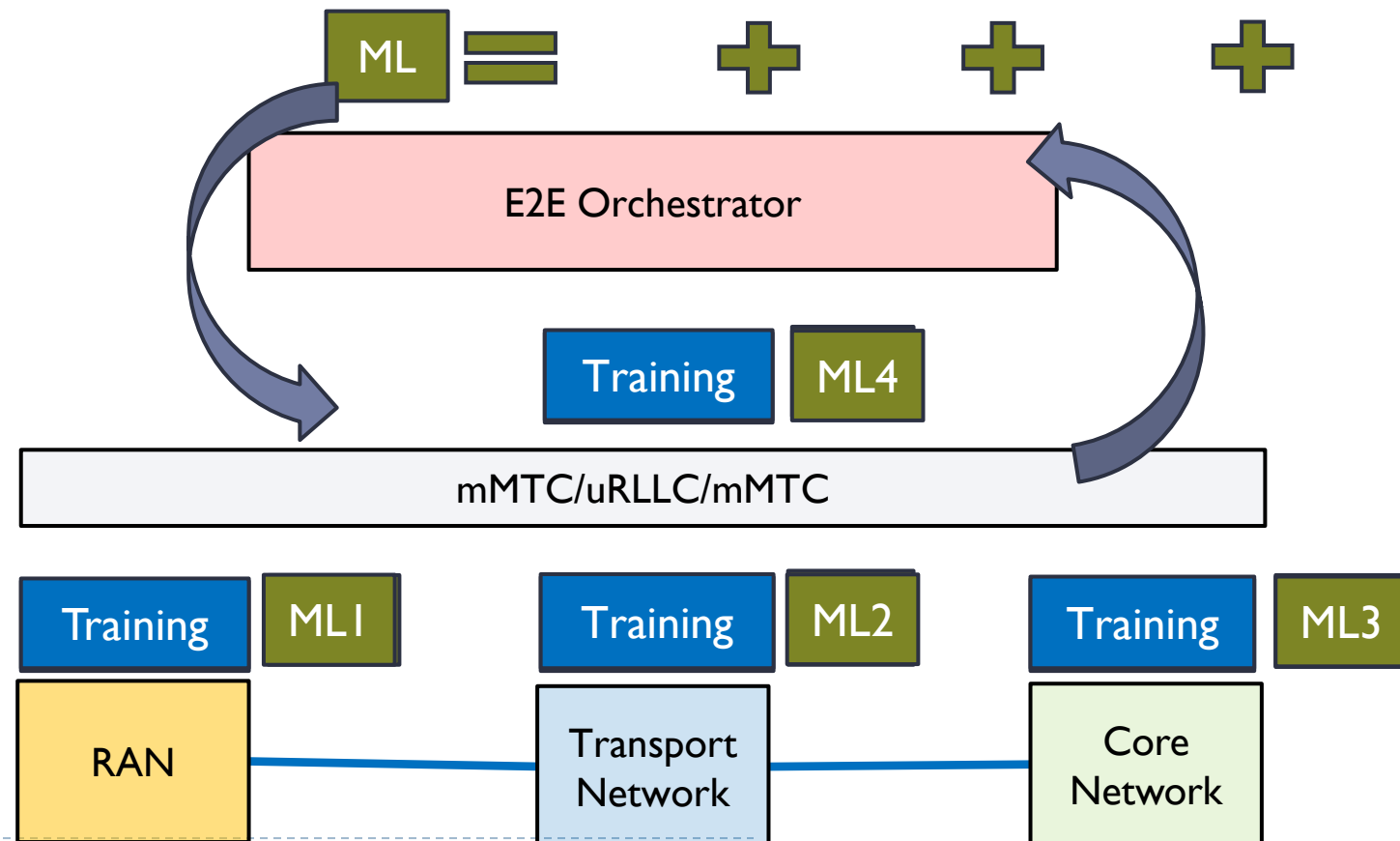
▶ Centralized data collection and processing

- ▶ Measurements from multiple elements are collected and stored in a central location
- ▶ Based on the full dataset a set of ML models are trained to make predictions for all building blocks of the system in a centralized fashion
- ▶ Trained ML models are deployed in the system



Distributed Knowledge Management: Federated Learning

- ▶ Measurements are stored locally
- ▶ Based on the local datasets, each element trains a ML model for a specific time duration
- ▶ Locally trained ML models are transmitted to a centralized server that aggregates the received models creating a new global ML model
- ▶ The global model is transmitted to the elements
- ▶ Based on their local datasets each domain creates an updated ML model transmitted back to the centralized server
- ▶ The process is repeated for several rounds until a certain prediction accuracy is achieved



ML Threats

▶ Data Poisoning

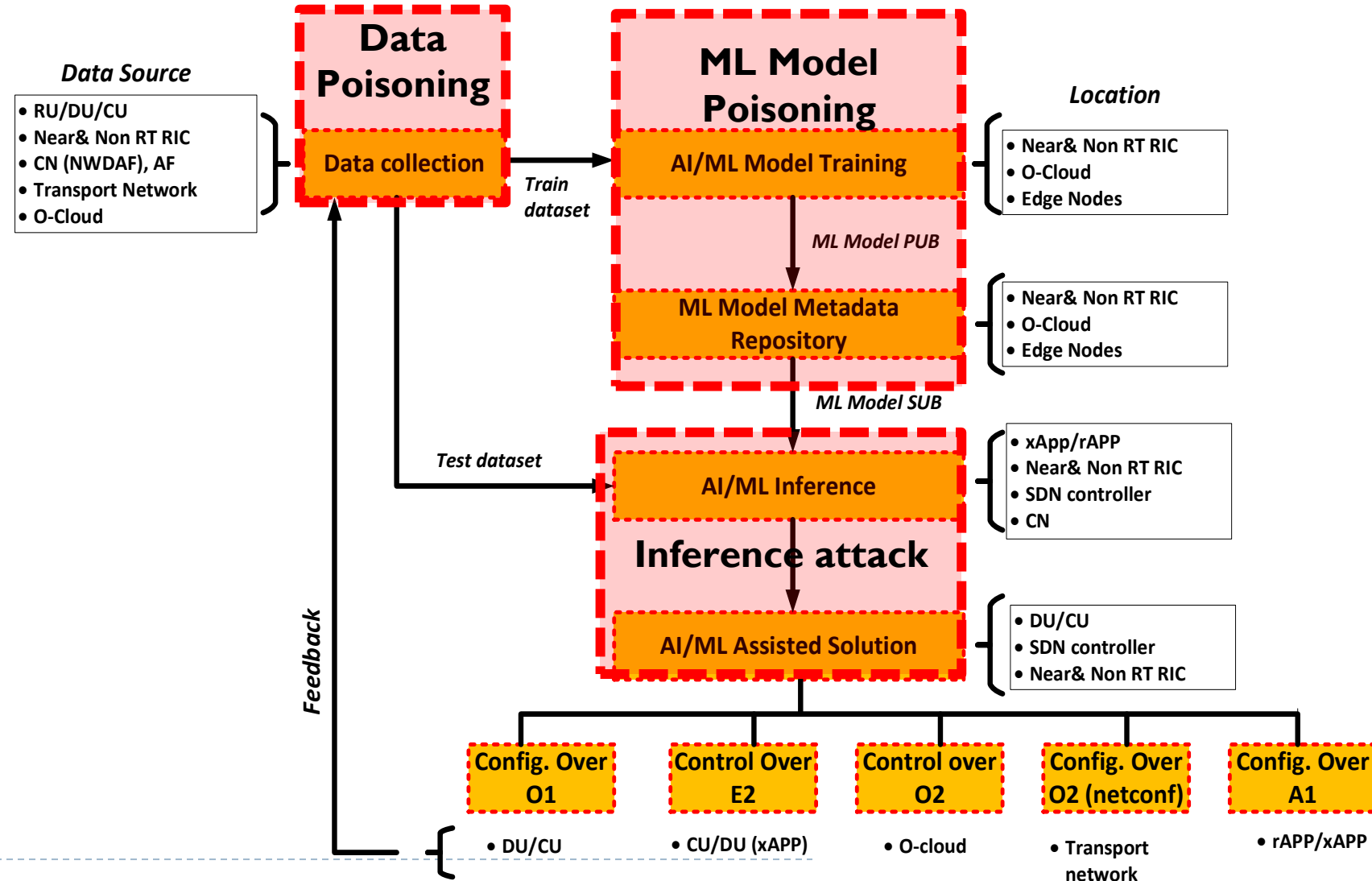
- ▶ Malicious actors tamper training data: insert, modification, or deletion data used for ML training

▶ ML model Poisoning

- ▶ Change of ML model hyperparameters and metadata

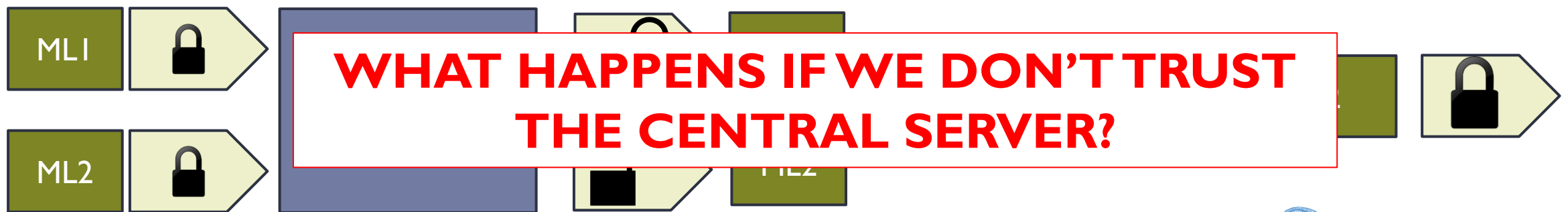
▶ ML Inference attack

- ▶ attacks that aim to extract sensitive information on the model's training data, attributes, or correlations



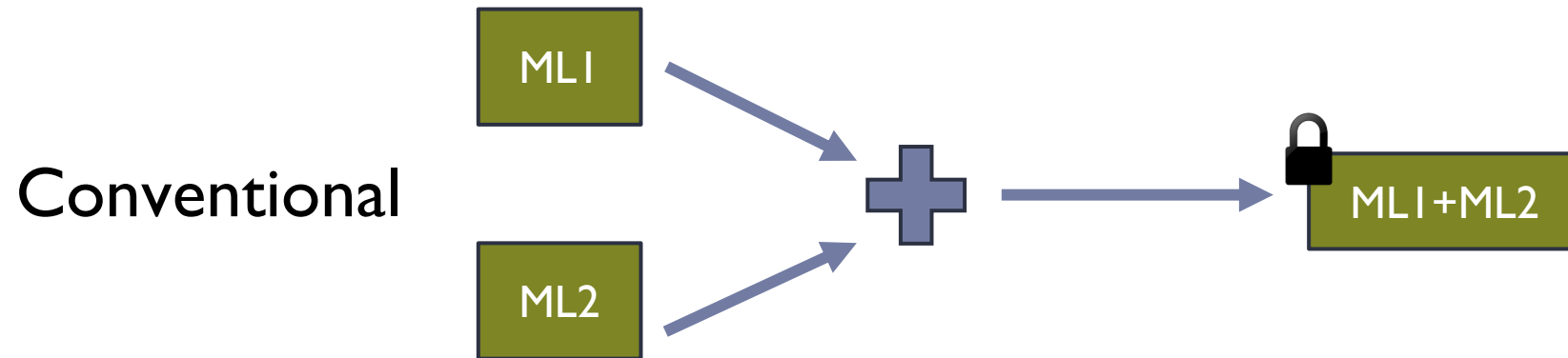
Protection: Encryption of ML models

- ▶ Challenge: ML models are vulnerable during transmission and aggregation by the FL server
- ▶ Conventional solution:
 - ▶ Encryption of ML models
 - ▶ Transmission of the encrypted ML models to the central server
 - ▶ Decryption
 - ▶ Aggregation of the ML models
 - ▶ Encryption of the aggregated model and transmission back to local domains

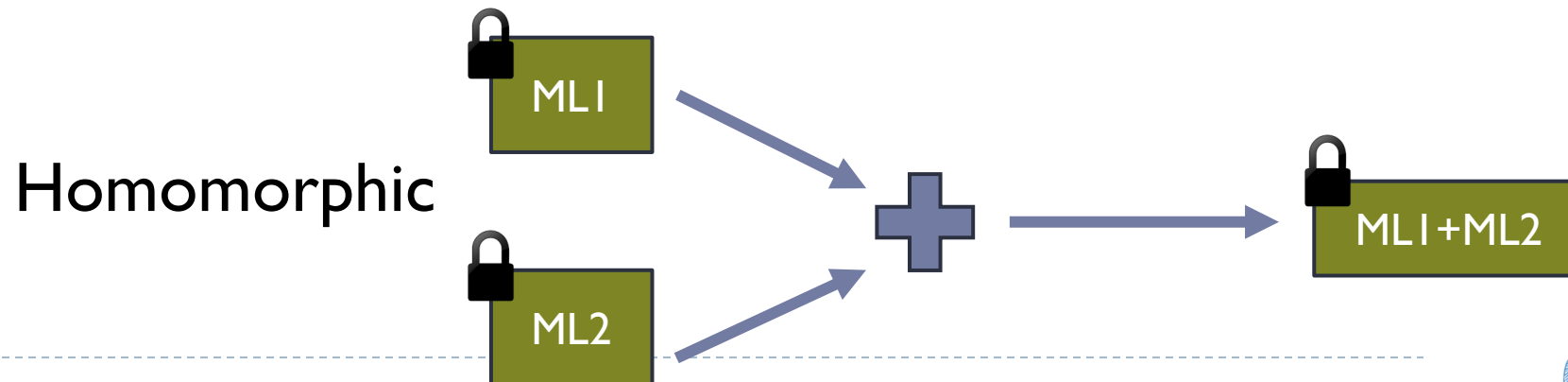


Homomorphic encryption

- ▶ Recently discovered approach that allows basic calculations such as additions and multiplications to be performed on encrypted data

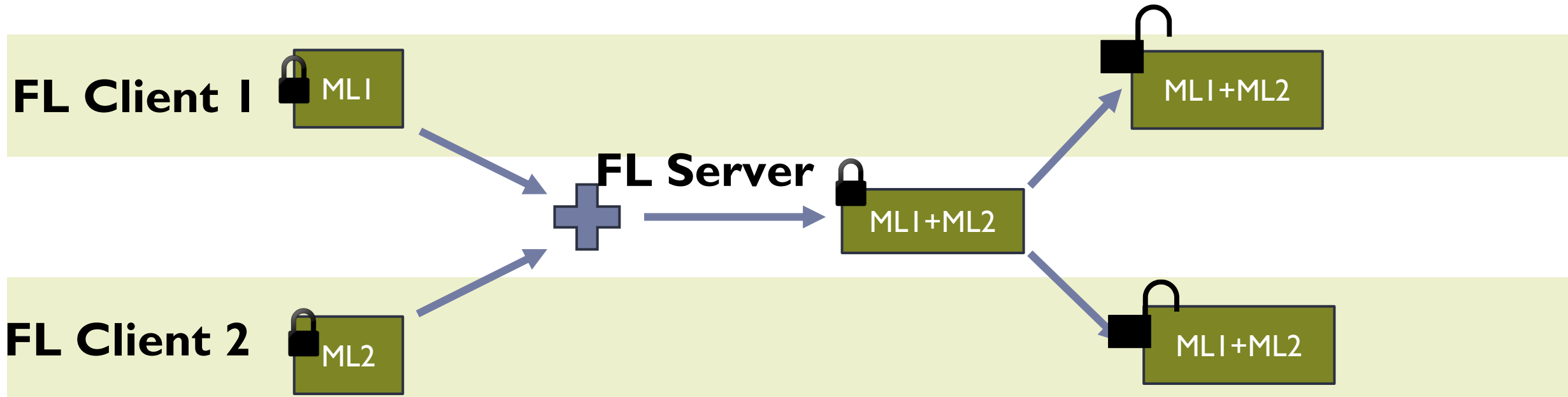


Equivalent to

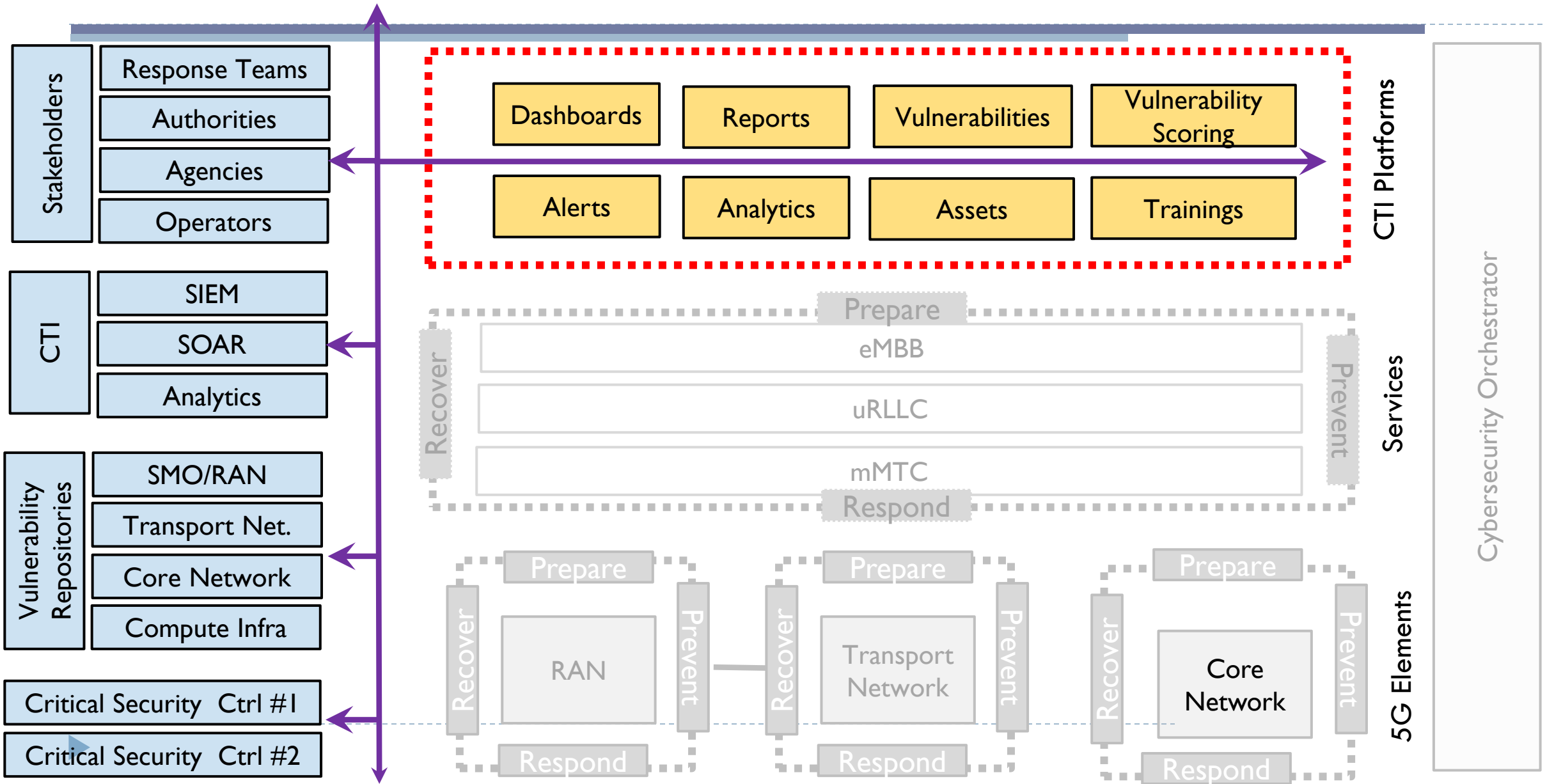


Homomorphic FL

- ▶ **FL Clients:** Homomorphic Encryption of ML models and transmission of the encrypted models to the central server
- ▶ **FL Server:** Homomorphic Aggregation of the ML models
- ▶ **FL Clients:** Decryption of the aggregated ML model



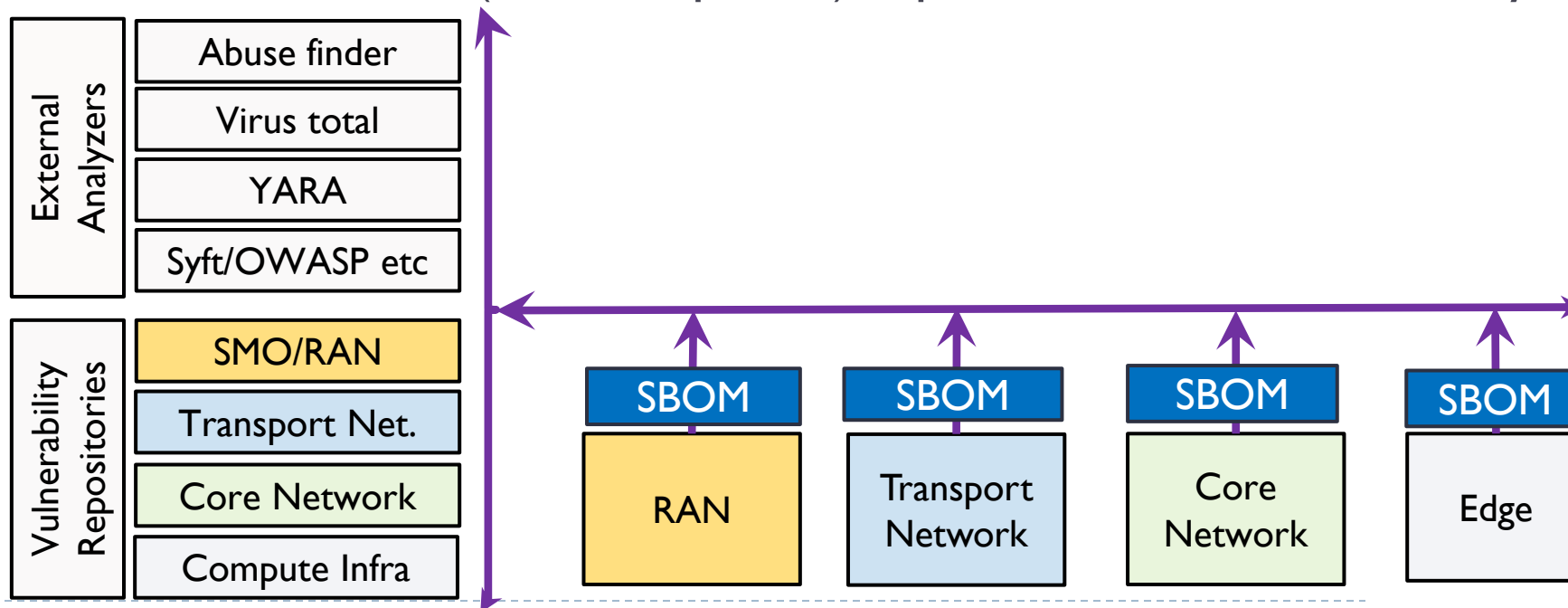
Cyberthreat intelligence sharing



Information Sharing and exposure: Pre-deployment

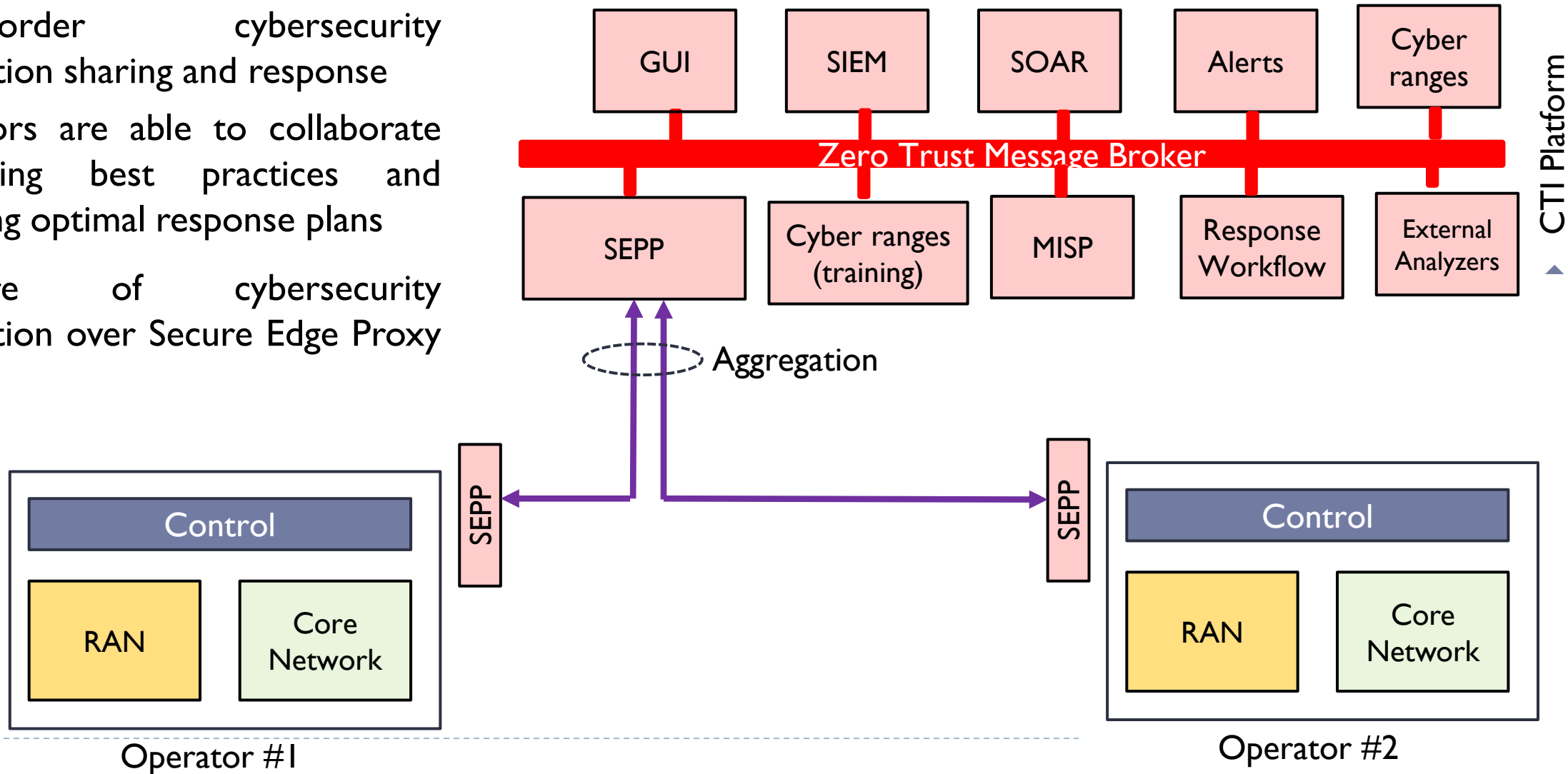
▶ Secure design lifecycle:

- ▶ Identify and document vulnerabilities and components contained in the product before this is deployed in operational environment
- ▶ Create a Software Bill of Material (SBOM) for every building block which is scanned against threats available in local (domain specific) repositories or external analyzers



Information Sharing and exposure

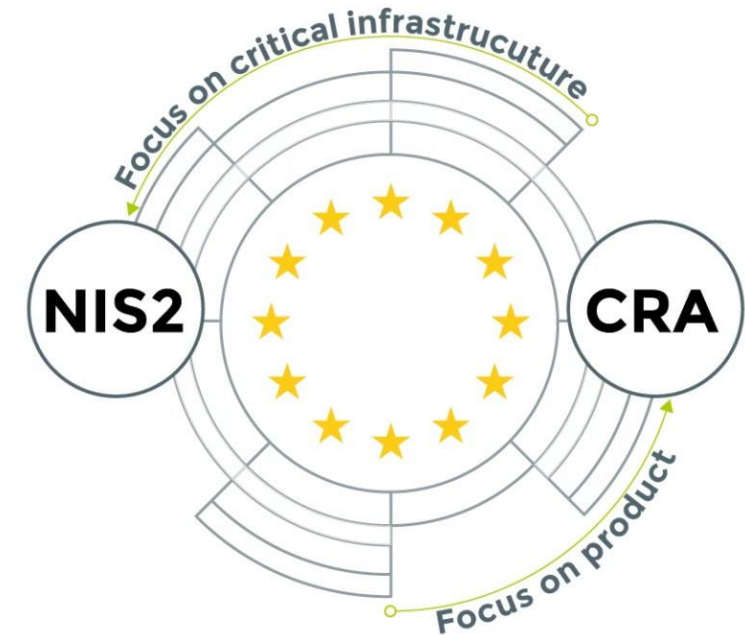
- ▶ Cross-border cybersecurity information sharing and response
- ▶ Operators are able to collaborate exchanging best practices and deploying optimal response plans
- ▶ Exposure of cybersecurity information over Secure Edge Proxy (SEPP)



Legislation I

▶ Cybersecurity Resilience Act (CRA)

- ▶ ensure that manufacturers improve security of products with digital elements from the design and development phase and throughout the entire life cycle
- ▶ ensure a coherent cybersecurity framework, facilitating compliance for hardware and software producers
- ▶ enhance transparency of security properties of products with digital elements
- ▶ enable businesses and consumers to use securely products with digital elements



The CRA entered into force on December 10, 2024, and its main obligations will apply from December 11, 2027.



Legislation II

- ▶ Network and Information Systems 2 (NIS2) Directive: Requires the adoption of technologies and processes implementing the full range of DevSecOps assisting to:
 - ▶ detect and quantify risks and threats affecting infrastructure components and network services
 - ▶ supporting security and resilience in the digital supply chain
 - ▶ integrate security incident management systems with external vulnerability repositories and analyzers improving system's capability to detect threats
 - ▶ ensure that the full cybersecurity workflow process (from detection to prevention and response) is tracked and executed within predefined time thresholds
 - ▶ support vulnerable reporting generation and sharing - integrating AI models
 - ▶ perform technical training enabling businesses across all sectors and consumers to use products with digital elements securely
 - ▶ adopt dashboards and simple Human Interfaces enhanced with visual analytics tracking security KPIs
 - ▶ coordinate with authorities relying on common format for reporting and scoring



Since 18 October 2024 NIS2 has been a legal security requirement throughout EU states.



Conclusions

- ▶ Migration from 5G to 6G brings amazing technology advancements and capabilities
- ▶ These often come at the expense of increased Attack Surface across a multiplicity of domains of the very complex 6G ecosystem
- ▶ Zero Trust Networking is proposed as a suitable framework to address security challenges
- ▶ In this context a variety of threats can be identified and addressed to minimise both occurrence and impact of possible attacks
- ▶ Cyber Threat Intelligence Sharing is proposed to better prepare against potential threats/attacks
- ▶ EU legislation is also addressing security related issues through CRA and NIS2 directive



Thank you!



Acknowledgments

- ▶ Associate Professor:
 - ▶ Markos Anastasopoulos
- ▶ Post doctoral Researchers:
 - ▶ Victoria Alevizaki
 - ▶ Alexandros Manolopoulos
- ▶ PhD Students:
 - ▶ Petros Georgiadis
 - ▶ Ilias Floudas
 - ▶ Ioanna Mesogiti

