INL/MIS-24-78352-Revision-0

Empowering Critical Infrastructure Communication with Secure 5G Private Networks

June 2024

Changing the World's Energy Future

Arupjyoti Bhuyan

Idaho National Laboratory

INL is a U.S. Department of Energy National Laboratory operated by Battelle Energy Alliance, LLC

DISCLAIMER

This information was prepared as an account of work sponsored by an agency of the U.S. Government. Neither the U.S. Government nor any agency thereof, nor any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness, of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the U.S. Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the U.S. Government or any agency thereof.

INL/MIS-24-78352-Revision-0

Empowering Critical Infrastructure Communication with Secure 5G Private Networks

Arupjyoti Bhuyan

June 2024

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

Dr. Arupjyoti (Arup) Bhuyan

Directorate Fellow, INL

Director, INL Wireless Security Institute (WSI)

Empowering Critical Infrastructure Communication with Secure 5G Private Networks

Idaho National Laboratory

INL Wireless Security Institute (WSI)

VISION: National Leadership on Wireless Security for Secure Adoption of Advanced Technologies including 5G, Next G/6G, Wi-Fi 6E and related Spectrum

MISSION: Provide best in class security research, assessments, evaluations, engineering support, and technology development to enable government and industry harvest the benefits of advanced wireless technologies

Innovative Research

- Lab directed research on security of advanced technologies and secure spectrum use and sharing
- Externally funded research, analysis, and engineering studies to address national security gaps in secure use of 5G & Future G/6G technologies and spectrum
- Proof of Concept for development and deployment of secure real-world use cases with transformational technologies

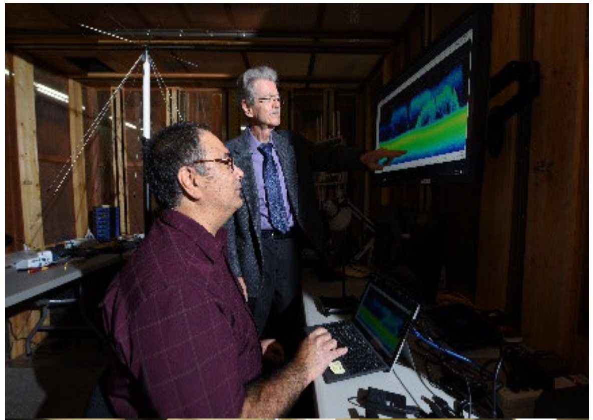
Evaluation & Validation

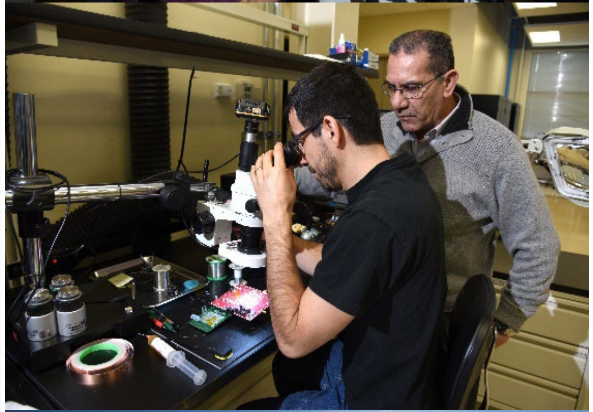
- Effective, accurate, responsive testing and verification
- Advanced Lab based systems for highly efficient and intrusive testing
- Unique Wireless Test Bed (WTB) in outdoor environment providing capability to test real world scenarios at scale
- WTB Spectrum flexibility with NTIA experimental station status

External Collaborations

- Academic and Industry Researchers in US
- Hosting of National Security workshops and Conference Tracks addressing key security topics with participation from US Government, Industry, and Academia
- International collaboration with wireless leaders in US Government partner countries

NOTABLE OUTCOMES: Diversely Funded RDD&D Portfolio supported by WSI as a National Authority on Wireless Security and utilizing resources across INL to exceed customer expectation





5G is a transformational technology

Enhanced mobile broadband

Mission-critical services

Massive Internet of Things

5G is foundational to what's next

A unified connectivity fabric for everything

Courtesy of Kabir Kasargod, Qualcomm

Blending Digital with Physical

Courtesy of Kabir Kasargod, Qualcomm

Private 5G Networks in R16

NR-U: New Radio in the Unlicensed Band

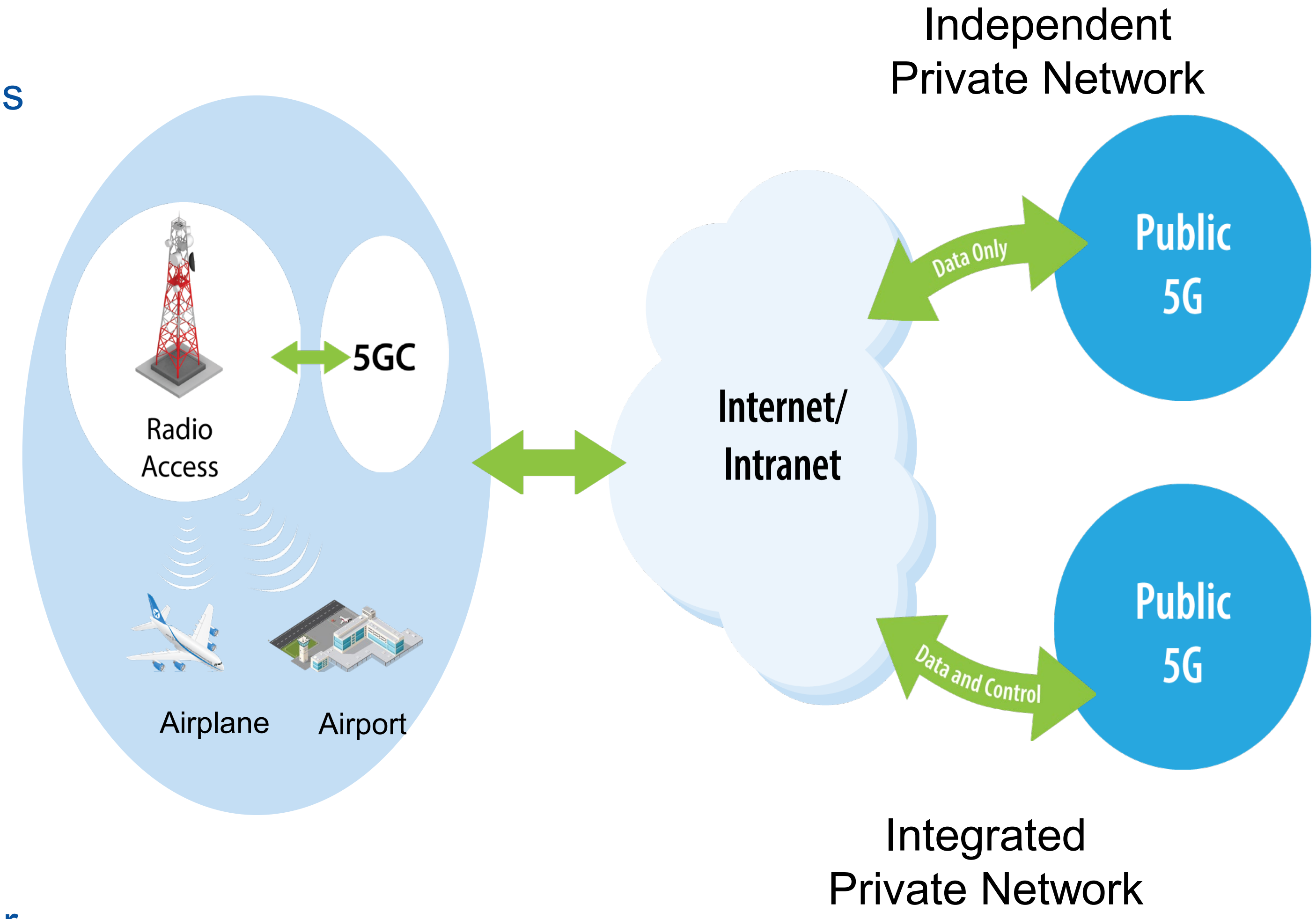
- ✓ Transformation of LTE Licensed Assisted Access (LAA)
- ✓ Standalone mode with **no licensed spectrum**

Network Configurations

- ✓ Isolated and Independent
- ✓ Hybrid - Integrated with public network

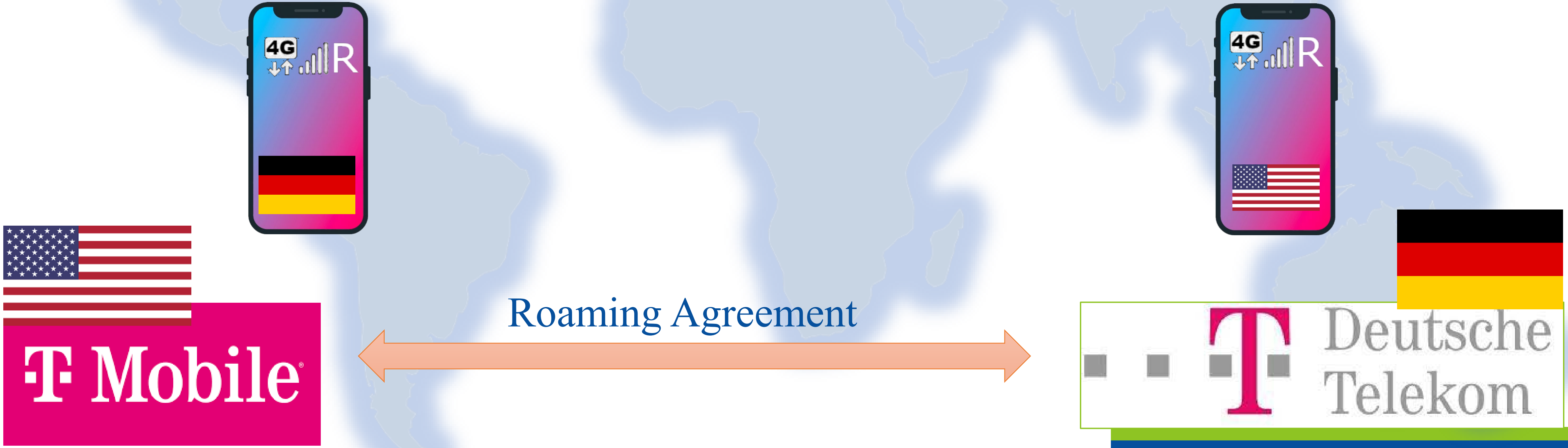
Use cases:

- ✓ Smart Warehouse – DoD 5G Use Case
- ✓ Manufacturing - Industry 4.0
- ✓ CBRS at Dallas Love Field Airport
- ✓ Other use cases: Hospitals, Smart Grid, Nuclear Plants, Mines …..



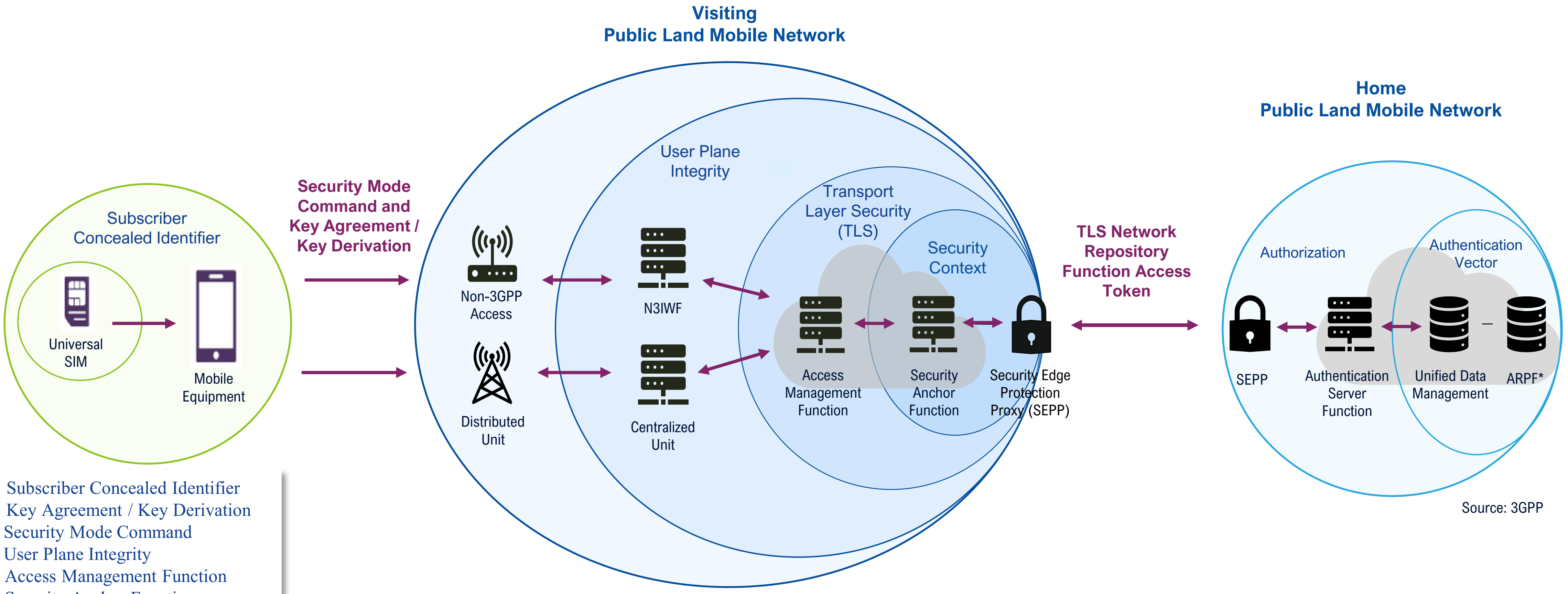
Cellular Roaming Capability

User's ability to continue cellular service outside of its home network service area with pre-arranged provider agreement



Roaming Agreement

5G Security Improvements (3GPP SA3)

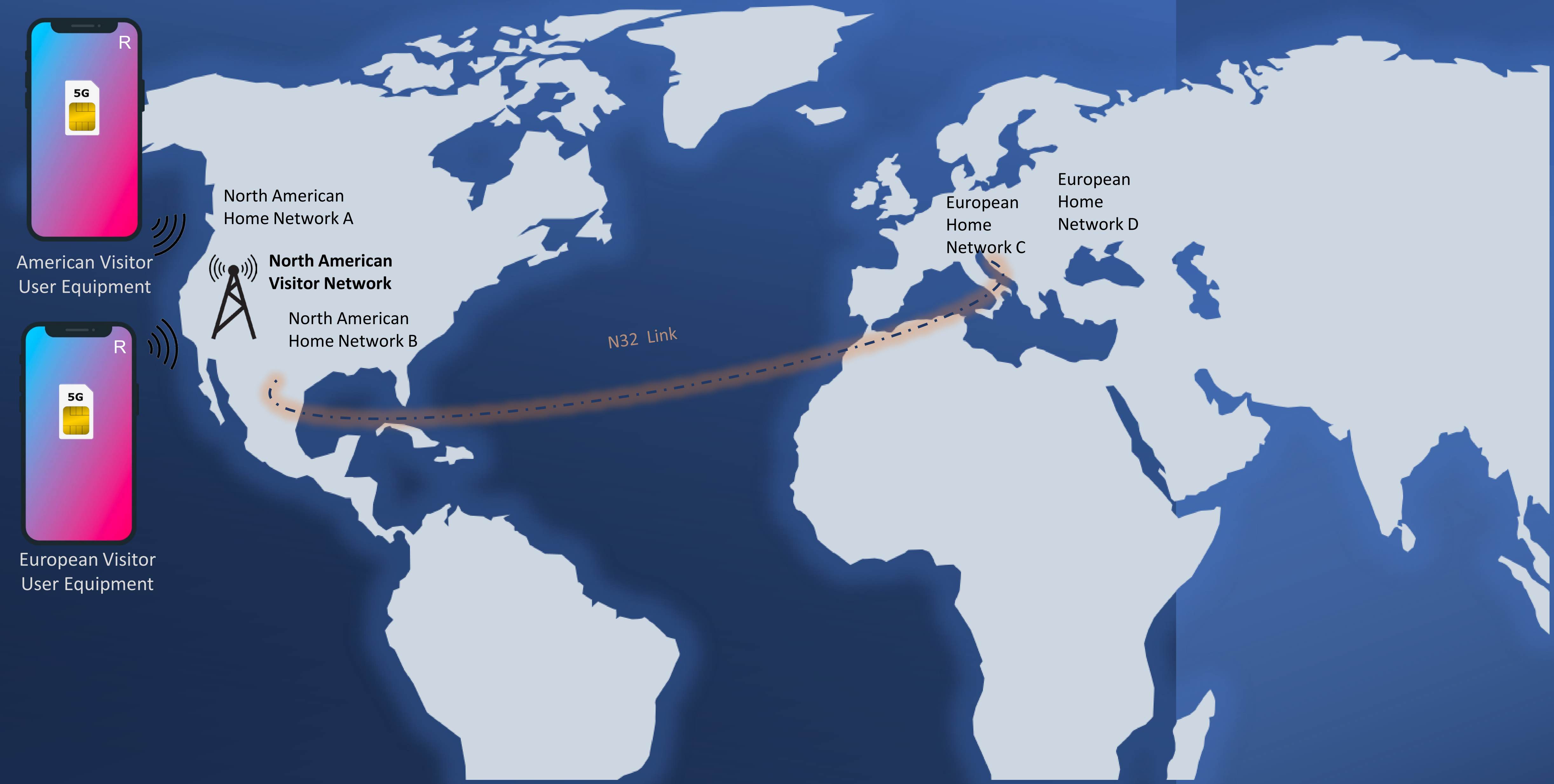


Visiting
Public Land Mobile Network
Home
Public Land Mobile Network
Subscriber Concealed Identifier
Universal SIM
Mobile Equipment
Security Mode Command and Key Agreement / Key Derivation
Non-3GPP Access
Distributed Unit
User Plane Integrity
TLS
N3IWF
Centralized Unit
Transport Layer Security (TLS)
Security Context
Access Management Function
Security Anchor Function
Security Edge Protection Proxy (SEPP)
TLS Network Repository Function Access Token
Authorization
Authentication Vector
SEPP
Authentication Server Function
Unified Data Management
ARPF*

Source: 3GPP

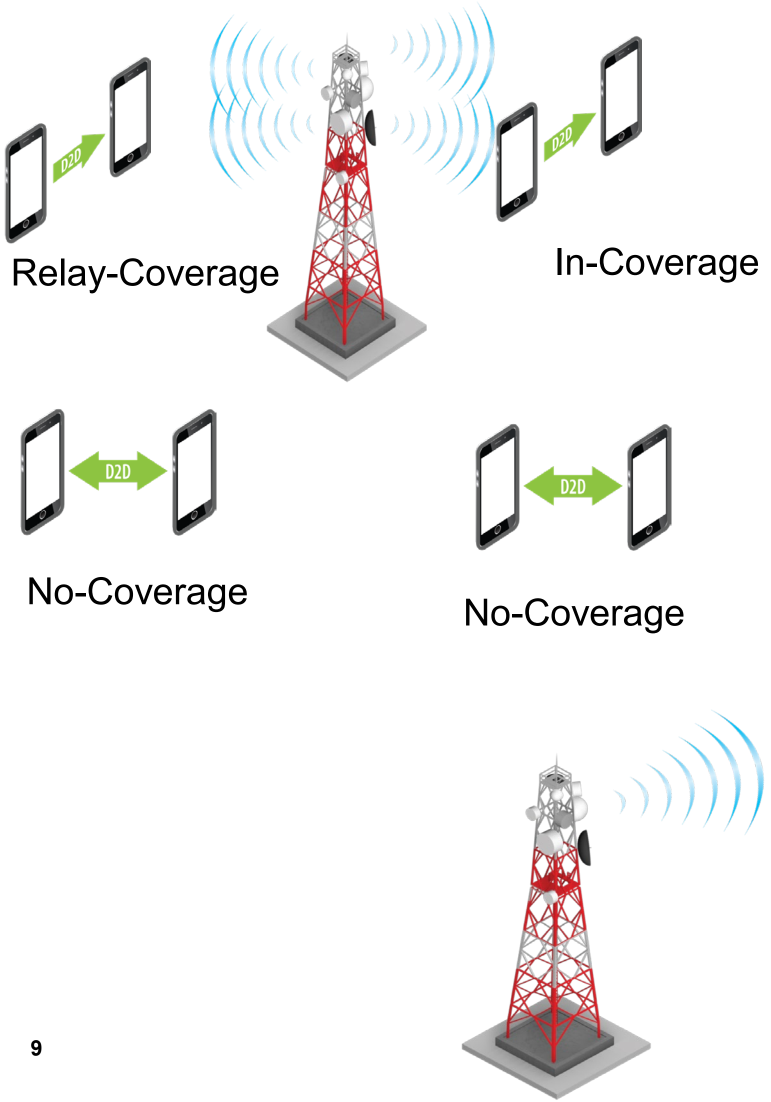
SUCI	Subscriber Concealed Identifier
Ka/Kd	Key Agreement / Key Derivation
SMC	Security Mode Command
UPI	User Plane Integrity
AMF	Access Management Function
SEAF	Security Anchor Function
TLS	Transport Layer Security
SEPP	Security Edge Protection Proxy
Auth	Authorization
AV	Authentication Vector
UDM	Unified Data Management
ARPF	Authentication Credential Repository and Processing Function
NRF	Network Repository Function

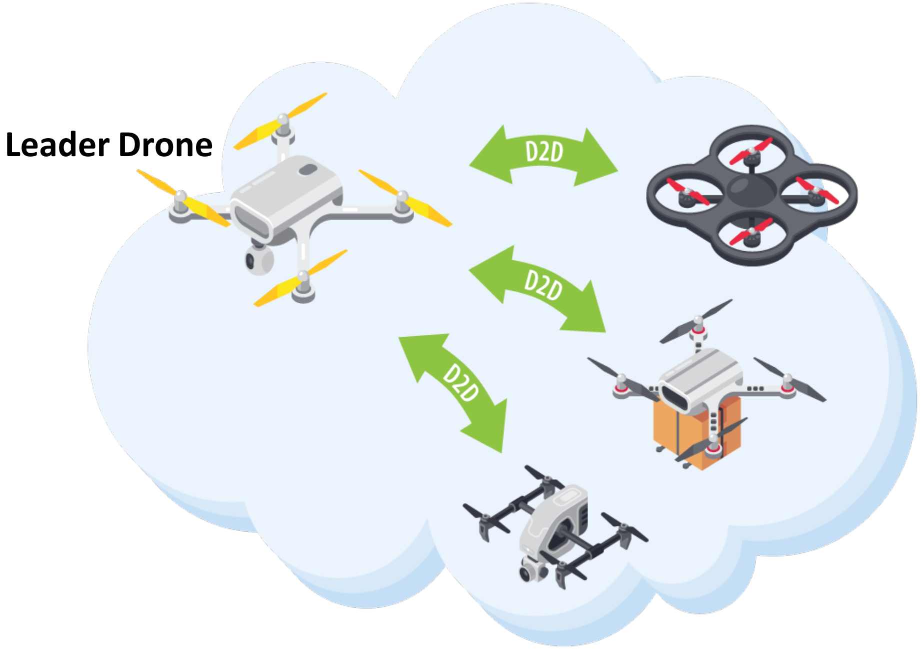
5G Simultaneous Roaming among Multiple Partner Networks



Courtesy of Scott Jeffery, INL Wireless Security Researcher

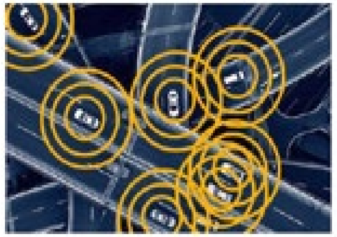
5G Side link: Device to Device (D2D) in R17





Swarm of Drones

(Group of Vehicles, Medical Equipment)



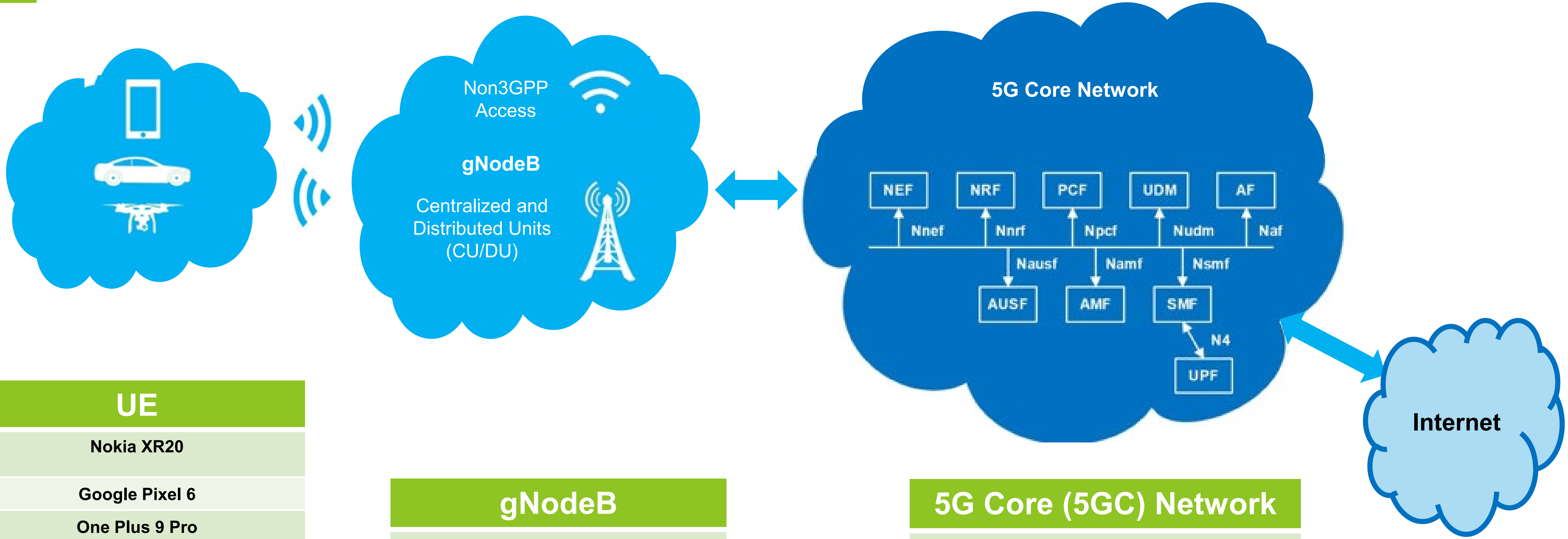
Extended sensing

Passing on environment data to other vehicles who are not within sensor distance

Platooning

Forming groups dynamically and reducing vehicle distance

INL’s 5G Private Network for Security Assessment



UE
Nokia XR20
Google Pixel 6
One Plus 9 Pro
Motorola Edge 20 Pro Nemo Outdoor 5G
Apple iPhone
Samsung S21/S22

gNodeB
Nokia gNodeB
RadiSys gNodeB

5G Core (5GC) Network
Open5gs
Open5GCore
Free5GC

Unique National Security Infrastructure and Capabilities

INTEGRATION
RELIABILITY
SECURITY
RESILIENCE
Controls
Communications
Cyber

Electric Grid Test Bed

Commercial Feeds,
Test Loops/Spurs

Water Security Test Bed

Municipal Water System

Radiological Ranges

First Responder Training

Specific Manufacturing

Quality Product

Wireless Test Bed

Agile Spectrum

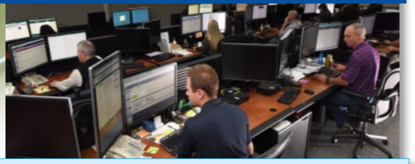
National Security Test Range

~20k TNT, VA Center

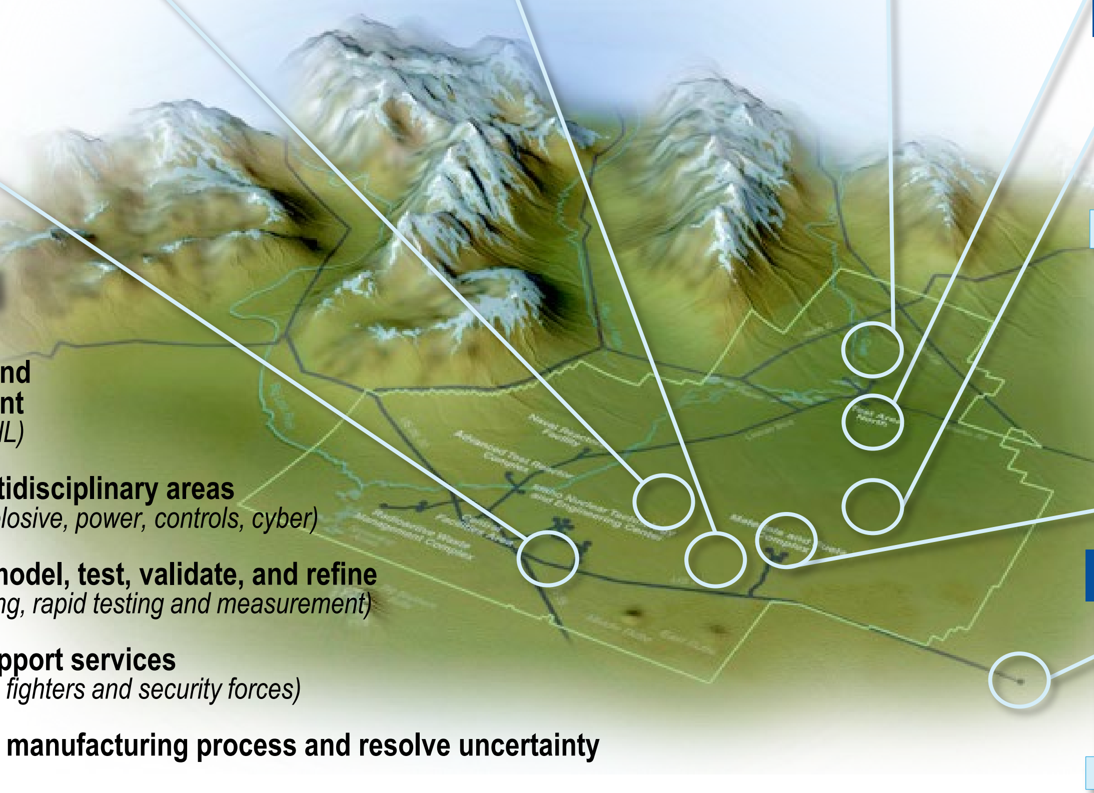
Nuclear Materials R&D

Electro-refining, SNM for Test/R&D

Research and Education Campus



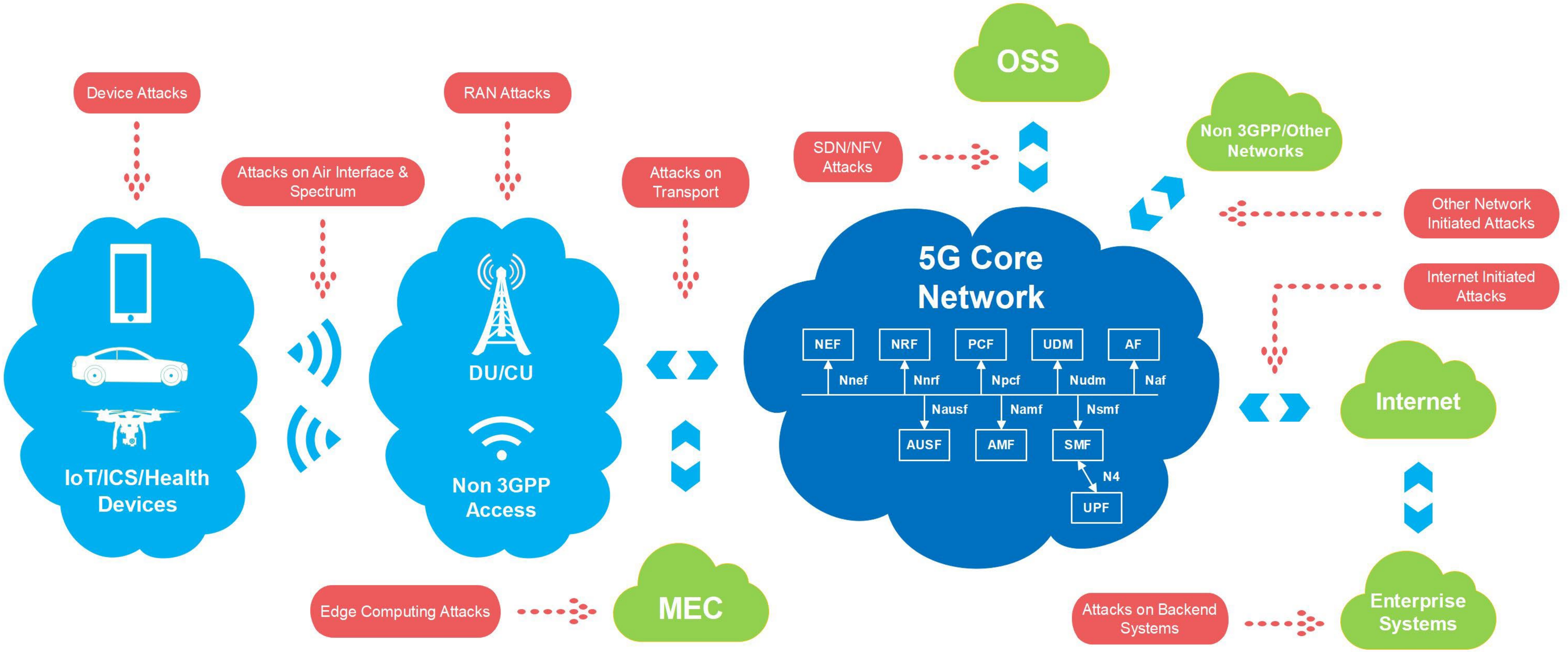
Controls & Energy Security Labs


Naval Reactors Facility
Advanced Test Reactor Complex
Idaho Nuclear Technology and Engineering Center
Materials and Fuels Complex
Test Area North
Radioactive Waste Management Complex

- ✓ **Full-scale real-world testing and demonstrations for deployment** *(designed, built and operated by INL)*
- ✓ **Integrated testing across multidisciplinary areas** *(radiological, physical security, explosive, power, controls, cyber)*
- ✓ **Rapid development through model, test, validate, and refine** *(high fidelity, effects-based modeling, rapid testing and measurement)*
- ✓ **Access to the full range of support services** *(lineman, engineers, rad techs, fire fighters and security forces)*
- ✓ **Ability to develop prototypes, manufacturing process and resolve uncertainty**

Uniquely configured for 5G use case evaluation

5G Network & Attack Surfaces

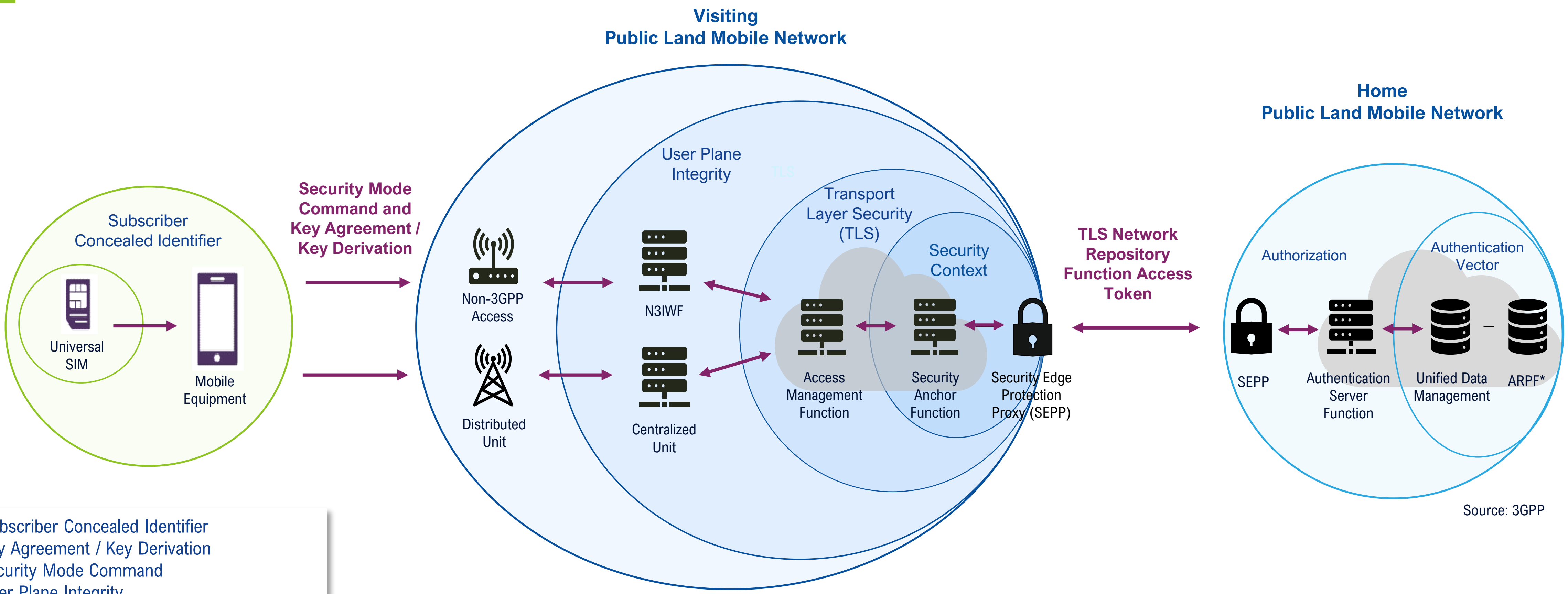


IoT: Internet of Things
ICS: Industrial Control System

MEC: Multi-access Edge Computing

SDN: Software Defined Networking
NFV: Network Function Virtualization
OSS: Operational Support System

5G Security Improvements (3GPP SA3)



Source: 3GPP

SUCI	Subscriber Concealed Identifier
Ka/Kd	Key Agreement / Key Derivation
SMC	Security Mode Command
UPI	User Plane Integrity
AMF	Access Management Function
SEAF	Security Anchor Function
TLS	Transport Layer Security
SEPP	Security Edge Protection Proxy
Auth	Authorization
AV	Authentication Vector
UDM	Unified Data Management
ARPF	Authentication Credential Repository and Processing Function
NRF	Network Repository Function

Needed 5G Security for Mission Critical Communication

- Optional 3GPP security procedures*
  - ✓ User plane encryption
  - ✓ Integrity Protection for user data
- 5G Network Slicing for customized security policy
  - ✓ Secondary authentication
  - ✓ Authentication, Authorization and Accounting Server (AAA-S)
- 5G Network Configurations
  - ✓ Certificate management
  - ✓ Encryption scheme (avoidance of Null Encryption)
- Application layer solutions – Security Apps
- AI/ML based solutions for detection and mitigation of attacks including zero-day attacks

* Reference: CSRIC Report on RECOMMENDATIONS FOR IDENTIFYING OPTIONAL SECURITY FEATURES THAT CAN DIMINISH THE EFFECTIVENESS OF 5G SECURITY

3GPP Network Data Analytic Function (NWDAF)

The NWDAF provides analytics to 5GC NFs and OAM (3GPP TS 23.288, TS 29.520 in Release 17)

- DCCF: Data Collection and co-ordinating function
- MFAF: Messaging Framework Adaptor Function
- ADRF: Analytics Data Repository Function
- AnLF: Analytics logical function - performs inference, derives analytics information (i.e. derives statistics and/or predictions)
- MTLF: Model Training logical function trains Machine Learning (ML) models and exposes new training services (e.g. providing trained ML model)
- OAuth2 protocol is used with Network Repository Function (NRF) as authorization server

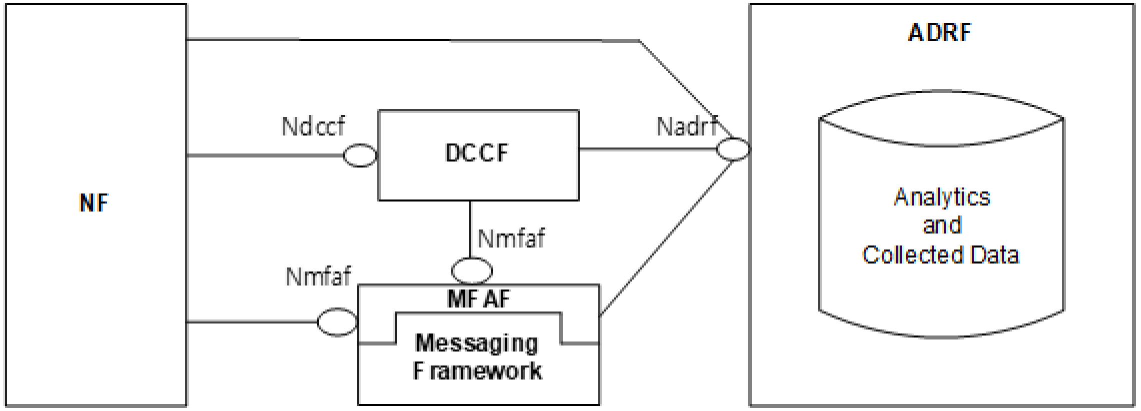
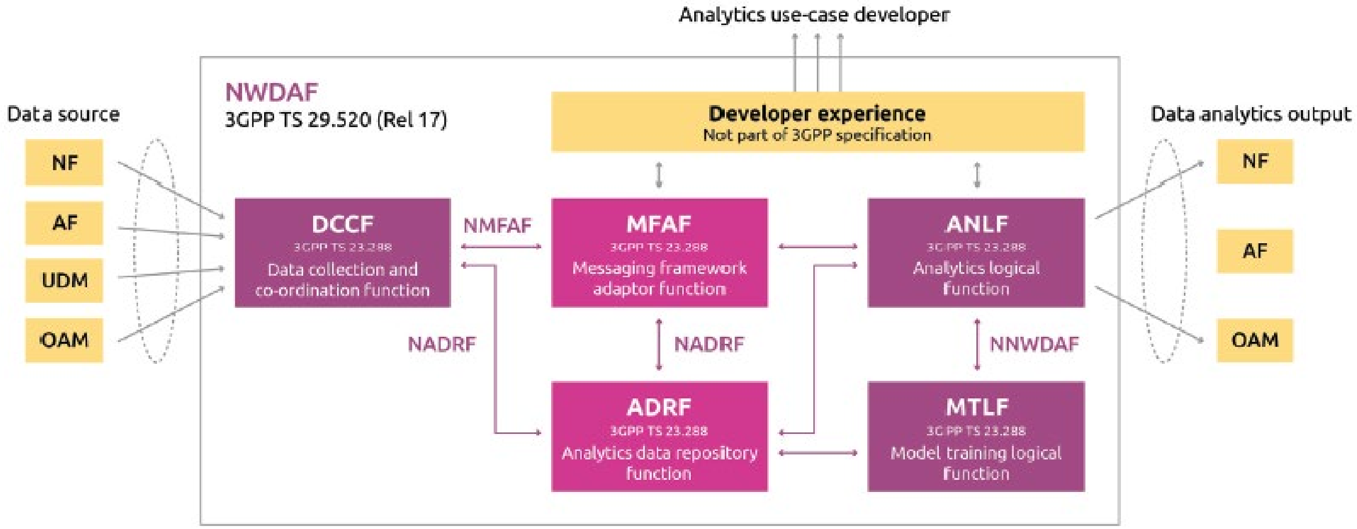

NF
Ndccf
DCCF
Nadrf
Nmfaf
Nmfaf
MF AF
Messaging Framework
ADRF
Analytics and Collected Data

Figure 4.2.1-1: Data storage architecture for Analytics and Collected Data

TS 23.288


Analytics use-case developer

Data source
NF
AF
UDM
OAM

NWDAF
3GPP TS 29.520 (Rel 17)

Developer experience
Not part of 3GPP specification

DCCF
3GPP TS 23.288
Data collection and co-ordination function

NMFAF

MFAF
3GPP TS 23.288
Messaging framework adaptor function

ANLF
3GPP TS 23.288
Analytics logical function

NADRF
NADRF
NNWDAF

ADRF
3GPP TS 23.288
Analytics data repository function

MTLF
3GPP TS 23.288
Model training logical function

Data analytics output
NF
AF
OAM

From Capgemini Engineering NWDAF component-level architecture – source 3GPP

arupjyoti.bhuyan@inl.gov

630-803-9111 (cell)

INL

Idaho National Laboratory