USD(R&E)

Future AI Infrastructure Strategic Roadmap

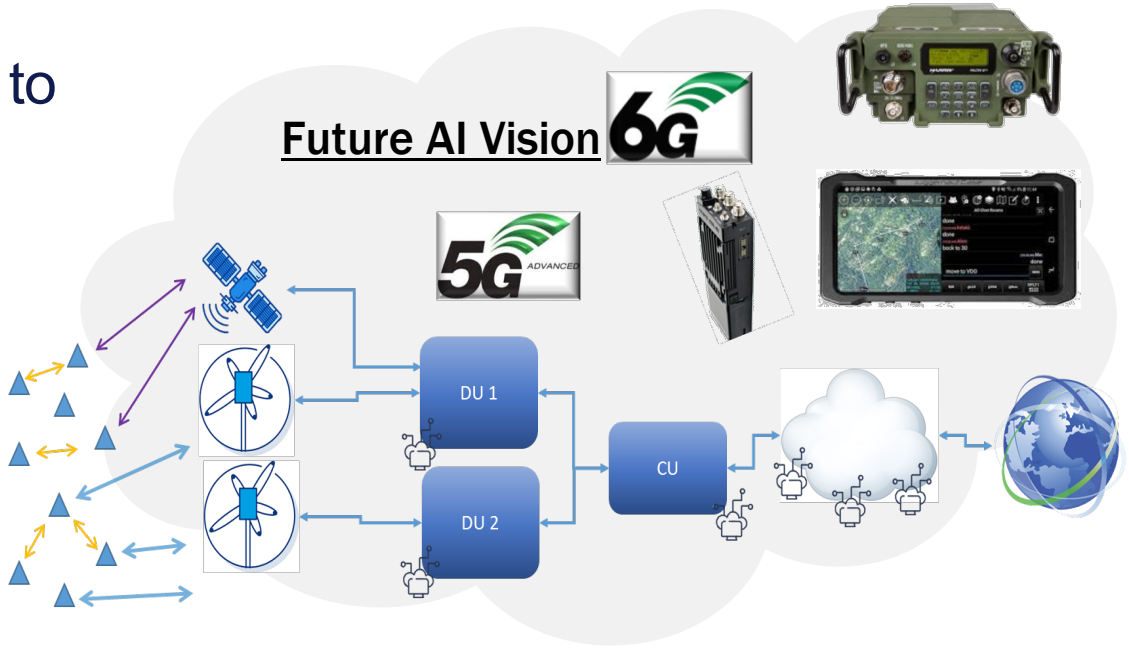
Mr. RJ McIntosh, MBA Data Centers Owners Representative
For the Office of the Under Secretary of Defense for Research and Engineering

Washington, DC 5 March 2025

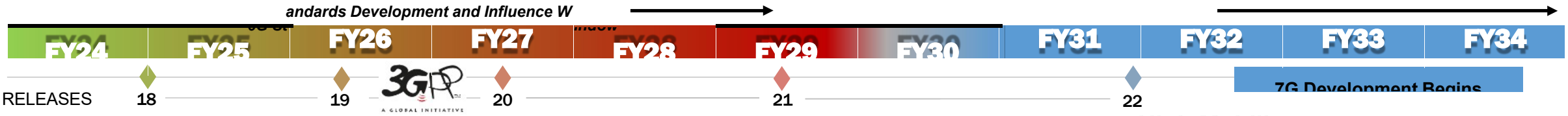
Future AI Infrastructure Problem, Insight and Motivation

- DoD's need for data and networking continues to increase
- Industry has outpaced DoD's AI Infrastructure networking capabilities
- Global industry progress affords DoD the opportunity to influence and leverage significant investments and economies of scale to meet warfighter requirements
  - Industry invests **hundreds of billions of dollars** annually for AI network research and development
- Future AI Infrastructure Focus:
  - Work with commercial co location developers to **Advance** and **Adopt**
  - **Adapt** to DoD and national security need
  - Increase defense utility of commercial developments to spur U.S. leadership through AI Infrastructure **Innovation**

Advancing Access Network (Open RAN) is a key enabler for AI innovation



Engagement with Commercial Industry and Academia to create U.S. AI Capabilities in 6G



COMMERCIAL INDUSTRY

High Data Rates
Enhanced Mobile Broadband (Embb)

Highly Reliable and Responsive
Ultra-Reliable Low Latency Comms (uRLLC)

5G ADVANCED

Massive Connection Density
Massive Machine-type Communications (mMTC)

Enhanced speed and efficiency in specialized services

COMMERCIAL LAUNCH

High Mobility
Expeditionary & Tactical Military Uses

High Data Rates
Enhanced Mobile Broadband (Embb)

Highly Reliable and Responsive
Ultra-Reliable Low Latency Comms (uRLLC)

6G

All-Domain Coverage
Ubiquitous and Instant Access to Information

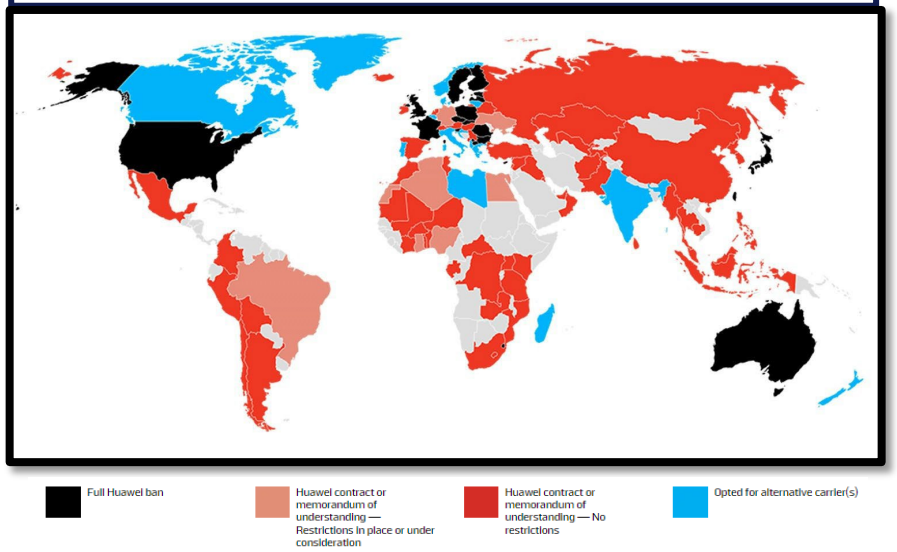
Low Energy & Integrated Sensing
Relevant Situational Awareness

Ubiquitous and sustainable access for everyone

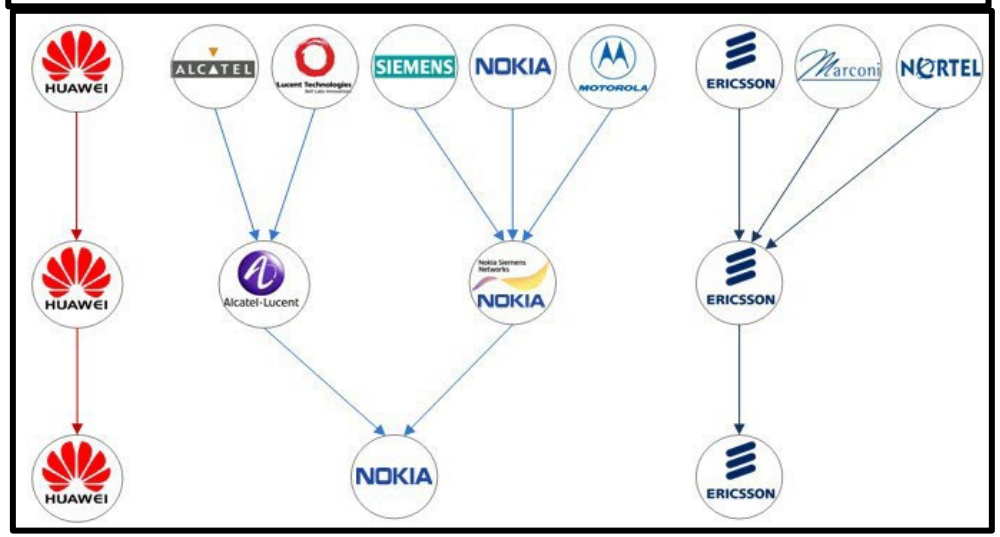
Massive Connection Density
Massive Machine-type Communications (mMTC)

Background and Relevant Political Context

Chinese 5G Global Network Coverage



Telecom industry consolidation over the last 20 years



Source: NetManias, 2023

The last 20 years are marked by the emergence of several strong Chinese state-backed commercial wireless infrastructure equipment providers

a) They leveraged <u>low cost</u> to gain market share
   a) Undercut competitor's pricing by ~30-70% creating market disruption
   b) Lower quality was acceptable for many commercial Mobile Network Operators (MNOs)
b) China committed significant investment in contributing to and influencing the important wireless standards setting forum - <u>3GPP</u>
c) Over time the market saw dramatic improvements in the network performance and capabilities of Chinese products increasing their alure

Key drivers that contributed to significant commercial wireless market consolidation:

(initially 9-10 global providers reduced to 3-4)

a) Fewer choices by MNOs,
b) Many MNOs chose Huawei for low cost
c) Huawei gained significant market share globally
d) China now 'owns' significant global ICT assets.

PRC Impact & Implications

- Through extensive combinations of state-backed investments and control of Chinese industry and academia, the Chinese government invested significantly in developing commercial wireless technologies (i.e., 4G, LTE, 5G, etc.) to gain increasing AI control at the global level over the past 20+ years.
- Chinese-backed companies (e.g., Huawei and ZTE) now 'control' significant commercial wireless infrastructure around the world.
  - These "Untrusted Networks" pose an increasing risk to and hamper the U.S. freedom of movement and operation.
  - Notable Threats: capable of tracking assets & people, surveillance, political influence, establishing 'patterns of life,' network disruptions
- Global Chinese influence is marked by:
  - Control of significant commercial wireless infrastructure globally
    - Despite being pushed out of key EU markets in 2020, Huawei maintains a robust global presence across Asia, Africa, and Latin America.
  - Significant influence over the 3GPP Wireless Standards-setting process
- USG investments in 5G to date have helped. However, more significant investments are necessary to close the gap and regain leadership in this critical technology area. Further recommendations include:
  - Continue to vigorously advance the development of Open Radio Access Networks (RAN)
    - A system that would allow multiple companies to provide different components of a singular 5G network and would aid in developing a rich ecosystem of trusted vendors
  - Increased funding for research and development in FutureG within the DoD, industry, and academia
    - Specifically, to better compete in sixth-generation (6G) technology, which is expected to replace 5G within fifteen years
  - Advancing current and planned efforts in workforce development both domestically and among Allied partners

Future AI Infrastructure Strategic Planning Elements

Drive select commercial AI data centers innovations to meet DoD technical and capability requirements

Cross-Cutting Capabilities

Core framework/ecosystem using tested, open, and secure AI technology within Industry, Academia and DoD

UBIQUITOUS, SECURE AND INSTANT ACCESS

Deliver high availability AI systems with security assurance across all DoD operational settings

RESILIENT AND OPEN COMMERCIAL SOLUTIONS

Leveraging open, standards-based systems with commercial impacts in defense applications

INTEGRATED SENSING AND COMMUNICATION

Leveraging new spectrum and novel signal processing for comprehensive situational awareness and multi-function utility

EXPEDITIONARY AND TACTICAL USE

Innovations enabling commercial network technologies in tactical operations

Joint Task Force AI Infrastructure Workforce Development

Future AI Technology Addresses the Complexity of Future Battlespace

RESILIENT OPEN COMMERCIAL SOLUTIONS

Leveraging open, standards-based systems with commercial impacts to defense applications

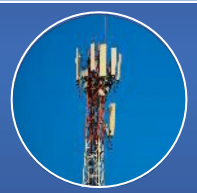
SECURE DOD FG CORE

SPECTRUM SHARING

INTELLIGENT SPECTRUM ACCESS & MANAGEMENT

UBIQUITOUS, SECURE AND INSTANT ACCESS

Improving overall security features of global standards and systems



FG CONNECTED BASES

SMART RESILIENT LOGISTICS

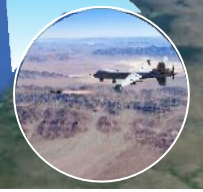
Leveraging USIA and ETU secure comms for logistics

SMART WAREHOUSES PIERSIDE CONNECTIVITY

INTEGRATED SENSING AND COMMUNICATIONS

Enables better overall situational awareness and thus security

AR/VR MAINTENANCE & TRAINING

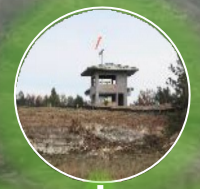


JOINT SENSOR-TO-SHOOTER KILL WEB

RESILIENT & RESPONSIVE LOGISTICS

EXPEDITIONARY AND TACTICAL USE

Providing secure private systems for DoD use



INTEROPERABILITY WITH ALLIES & PARTNERS

Battlespace Control Through Decision Superiority

Future AI Infrastructure Priority Efforts for 2025

OPEN CENTRALIZED UNIT DISTRIBUTED UNIT (OCUDU)

- Complex demonstrations
- Security Enhanced WAN
- Secure SDN
- CU-DU OSS Library and Management System
- Virtual container | Virtualization | Virtualization
- High Performance SDR HW (RU) | CU/DU | UE (SDR HW) | OIT (SDR HW)

RESILIENT AND OPEN COMMERCIAL AI SOLUTIONS

UBIQUITOUS, SECURE AND INSTANT ACCESS THROUGH AIDC

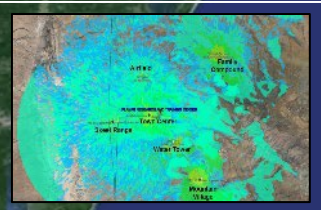
INTEGRATED SENSING AND COMMUNICATION

EXPEDITIONARY AND TACTICAL USE

WORKFORCE DEVELOPMENT

MICROELECTRONICS COMMONS

PLAYAS RESEARCH AND TRAINING CENTER (PRTC) FUTUREG BUILD-OUT



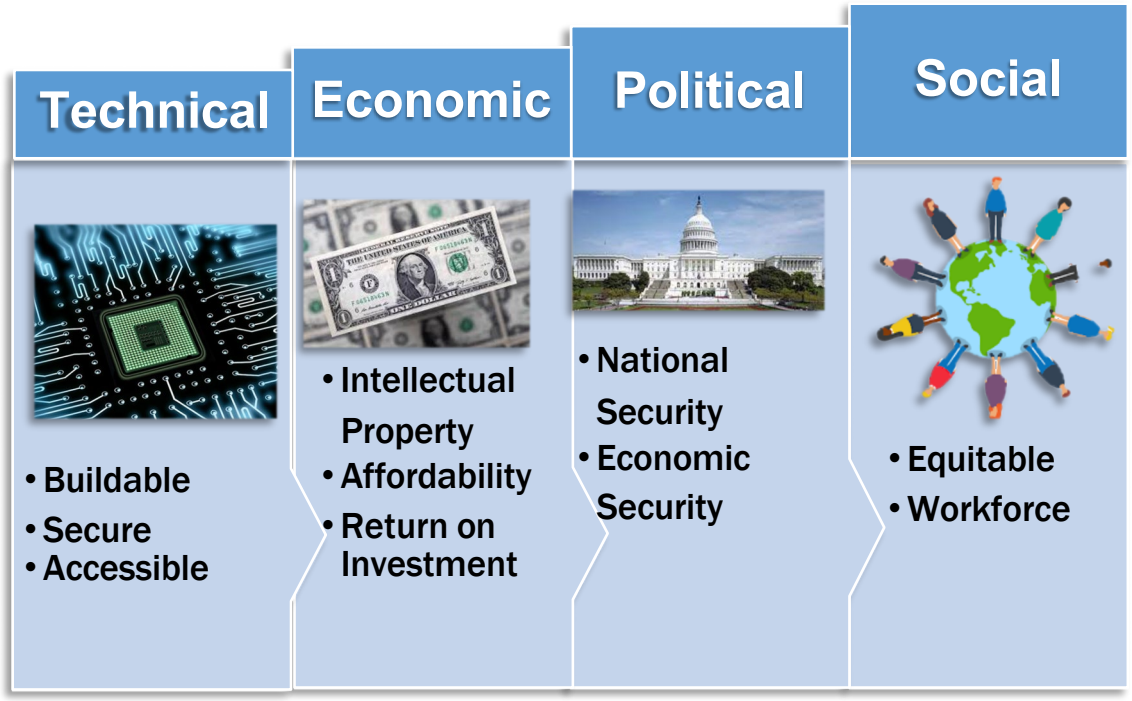
DOD RAN SHARING

RAN SHARING

SMART RESILIENT LOGISTICS USINDOPACOM INTEGRATION

NATO ACT/ LATVIAN RANGE

Resilient and Open AI Commercial Solutions (ROCS)



Elements

- Leverage advances in AI Data Centers hardware, software, and apps
- Support adoption through open competition
- Training and workforce development (Joint Task Forces)
- Privacy enhancing technologies

Projects and Experimentation

- Dynamic Spectrum Management
- Multiple Input, Multiple Output (MIMO) and Radio Access Network (RAN) Spectrum Sharing
- Spectrum Exchange
- Open Centralized Unit Distributed Unit (OCUDU) Initiative
- 5G Challenge & RIC Forum
- 5G Coexistence: Radar 5G Canceller
- Open Programmable Secure (OPS) 5G - with DISA
- Specific Location Investigation for Coexistence of Electromagnetic Systems (SLICES)
- Risk Informed Spectrum Access (RISA)
- Open 6G
- Resilient and Intelligent NextG Systems (RINGS) - with NSF

AI Infrastructure Initiative

Software
Open-source Radio Access Network (RAN) Components

Gov/DoD Users

OCUDU Management
Gov/DoD
Capability Development

Commercial Open-source Manager

Commercial Vendors/Users

Commercial Capability Development

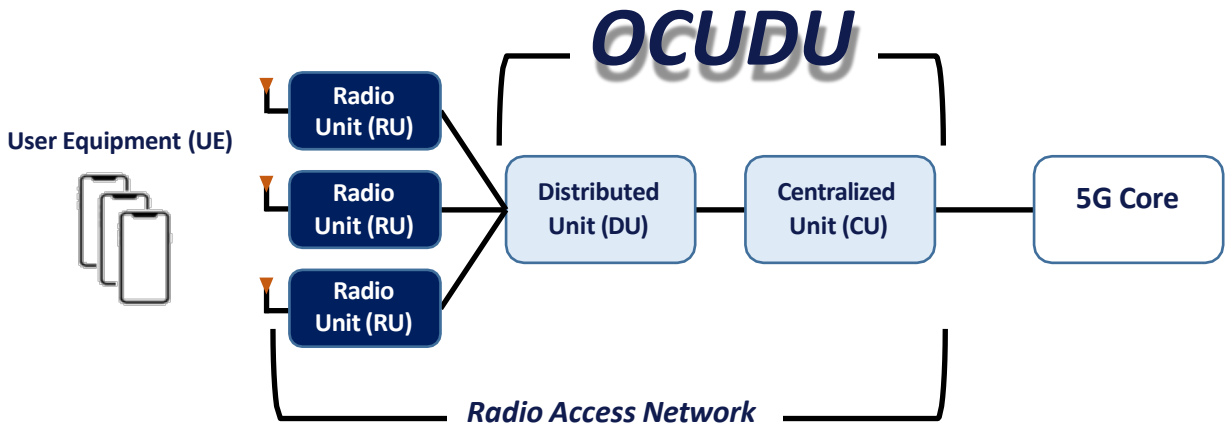
Standards Influence

Virtualization of High-Performance Hardware

Hardware for Base Stations and End Points
Power | Scalability | Security | Spectrum Agility

Transition for U.S. Production

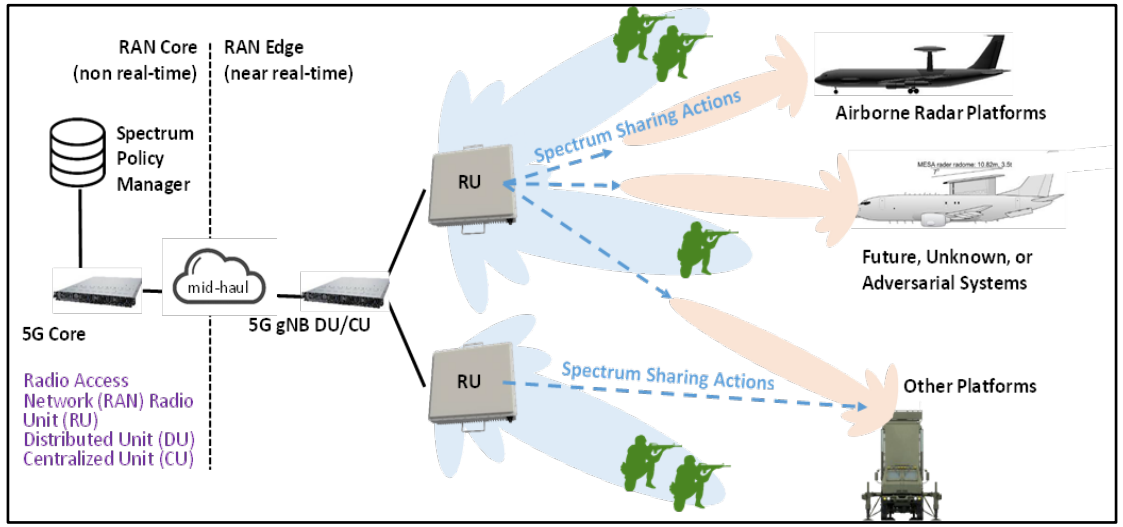
Secure | Transformative | Resilience | Cost Effective
Ubiquitous | Customizable | Transparent | Interoperable



MICROELECTRONICS COMMONS
BRIDGING THE GAP FROM LAB TO FAB

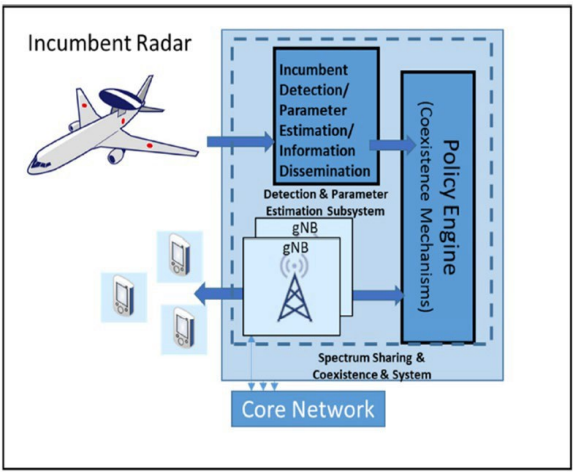
Affecting 6G Standards Through AI Open Source Alternatives – Before it's too late

AI Spectrum Management

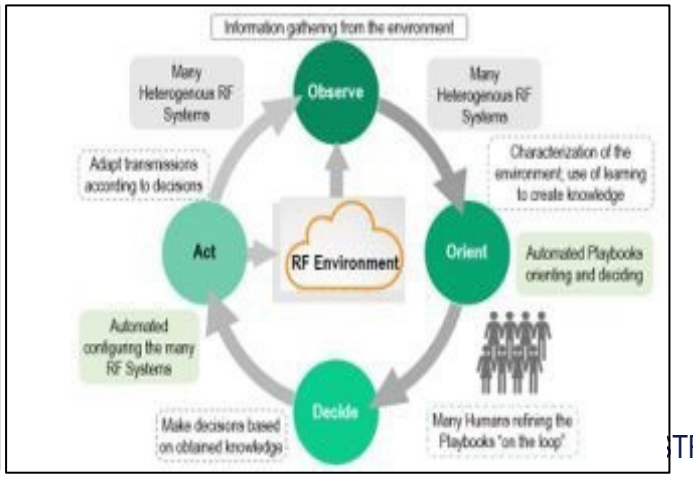


MIMO and RAN Spectrum Sharing

Dynamic Spectrum Management

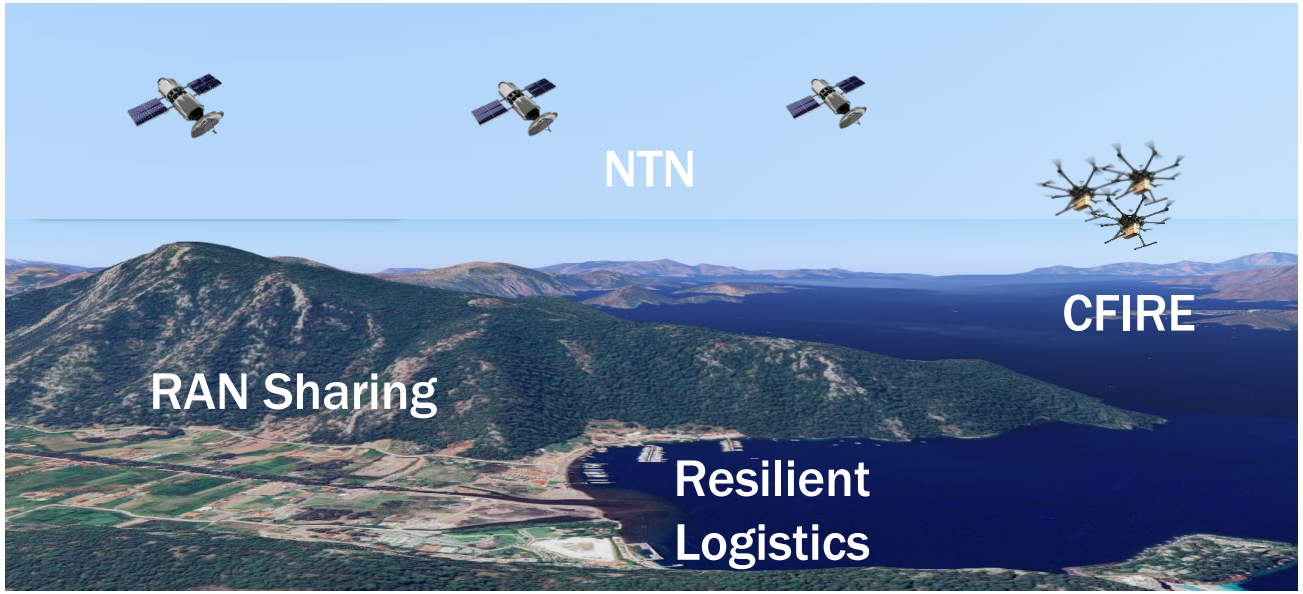


Spectrum Exchange



- **Objective**: Challenges to spectrum management continue to grow with the rise of innovative new technologies. Spectrum has traditionally been allocated based on licensing. Increased spectrum demand has created numerous conflicts in unlicensed and shared spectrum bands creating both economic and security challenges.
- **Relevance:** By adopting select AI Data Center Ecosystem Research and develop technologies for deconfliction, sharing, and management of impacts to 6G site deployment locations
- **Warfighter Impact**:
  - Conduct applied research to:
    - Plan, sense, and deconflict spectrum
    - Enable spectrum sharing
    - Develop spectrum management tools
  - Transition applied research to higher TRL funding sources for ultimate inclusion as part of the DoD reference architecture
  - Ultimately spectrum management becomes an automated function of the RAN Intelligent Controller (RIC).

Ubiquitous, Secure and Instant Access (USIA)



AI Elements

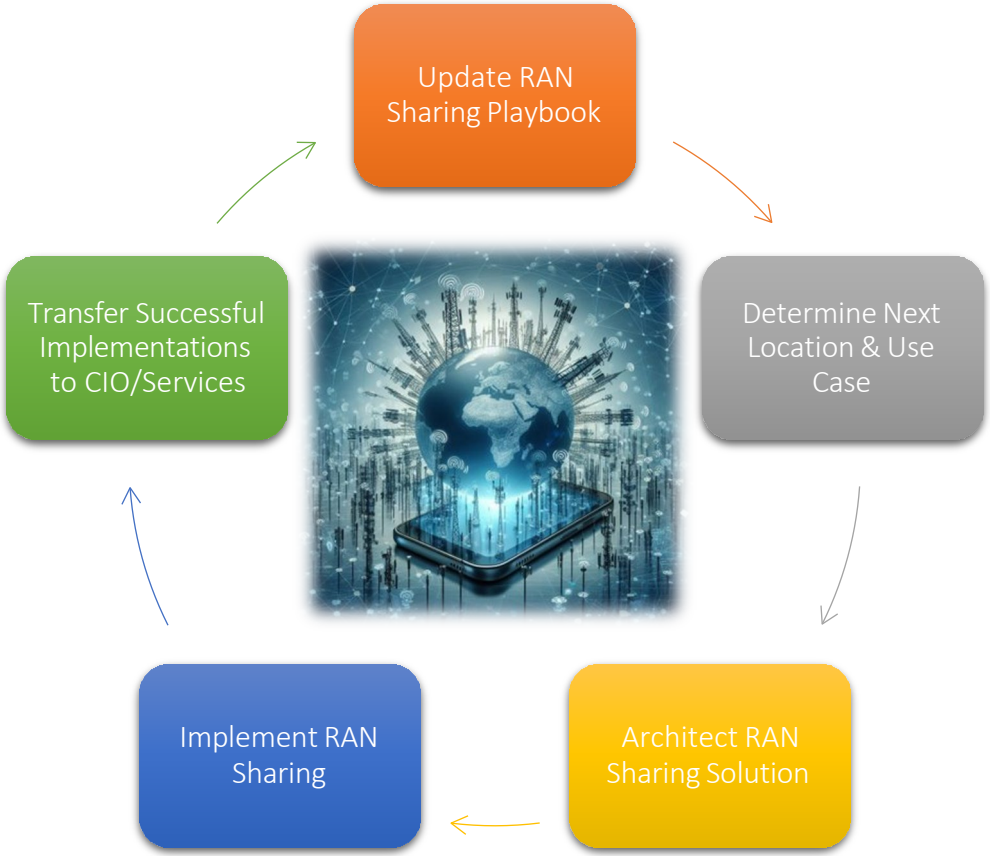
- Cloud-native, Tactical Edge apps
- Non-terrestrial Networking (NTN)
- Integrated Access and Backhaul (IAB)
- New sensors, data, devices, environments & processing
- Increases in AI network availability
- Reduction in latency

Projects and Experimentation

- Idaho National Laboratory 5G Attack Vectors & Testbed
- U.S. DOE Data Center Owners Representative Engagement
- Secure Transit over Untrusted Networks (STUN)
- Resilient Unified Gateway (RUG)
- Security Enhanced Open Radio Access Networks (SE-RAN)
- DISA engagement for IT flows of responsibilities

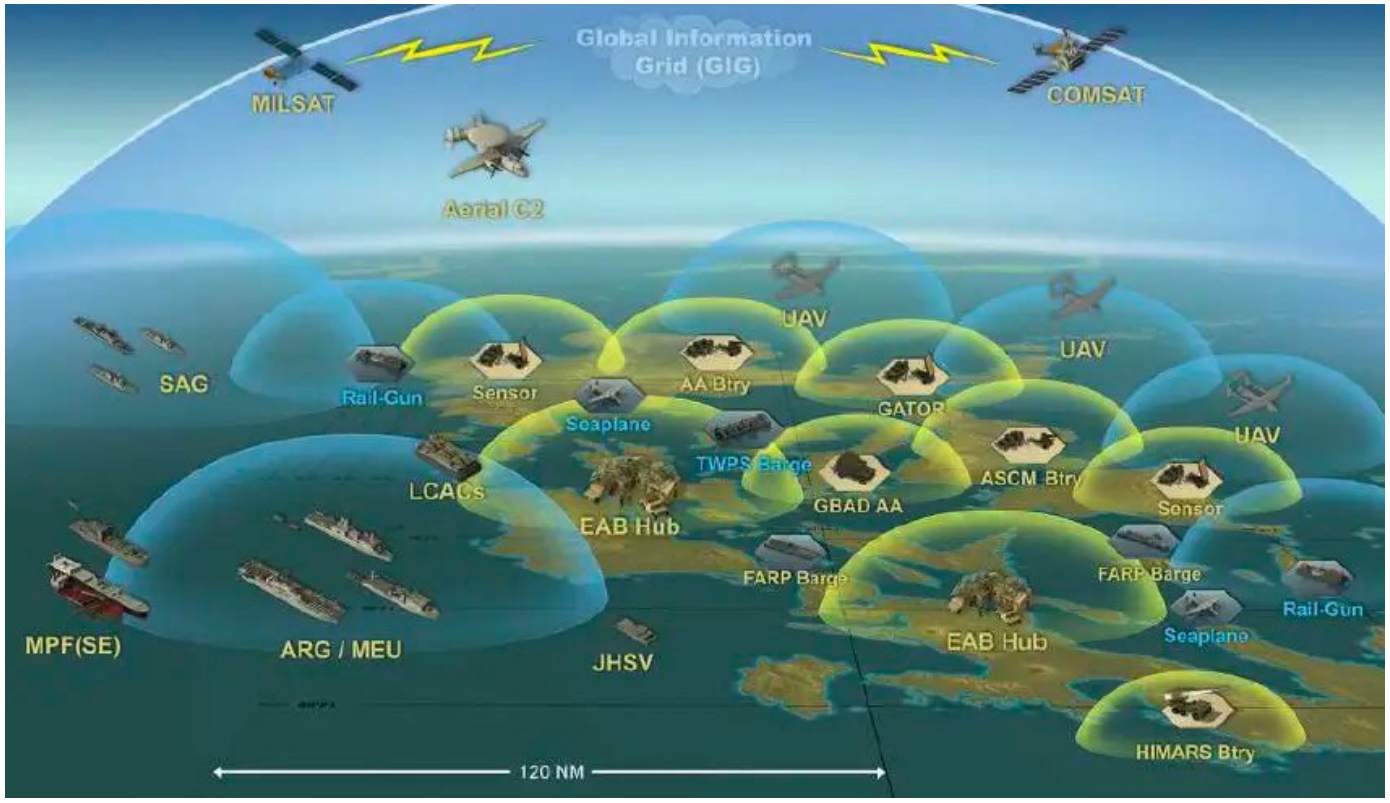
AI Access Network (RAN) Sharing

Ubiquitous, Secure and Instant Access (USIA)



- **Objective:** Identify, develop, test, and demonstrate agile AI Data Centers capabilities for operationally relevant RAN Sharing solutions in DoD global areas of interest.
- **Future AI Relevance**: The RAN Sharing project explores current and developing RAN architectures across the globe to determine the most technically optimal and secure way to quickly access existing capabilities for DoD operational use. Project objectives will result in a RAN Sharing playbook and global roadmap as a plug and play implementation guide.
- **Warfighter Impact**: The RAN Sharing project will greatly enhance the warfighters' ability to quickly communicate and share data across the area of operations using existing and readily accessible 5G technological. Based on the warfighters operational needs and what applications are used, the impact of this capability can span across all warfighting functions with security protocols previously unavailable with legacy RAN options. The security of communication and data flow can be scaled to fit the environment and end user. This puts an operational viable end user device in every warfighter's hands.

Expeditionary and Tactical Use (ETU)



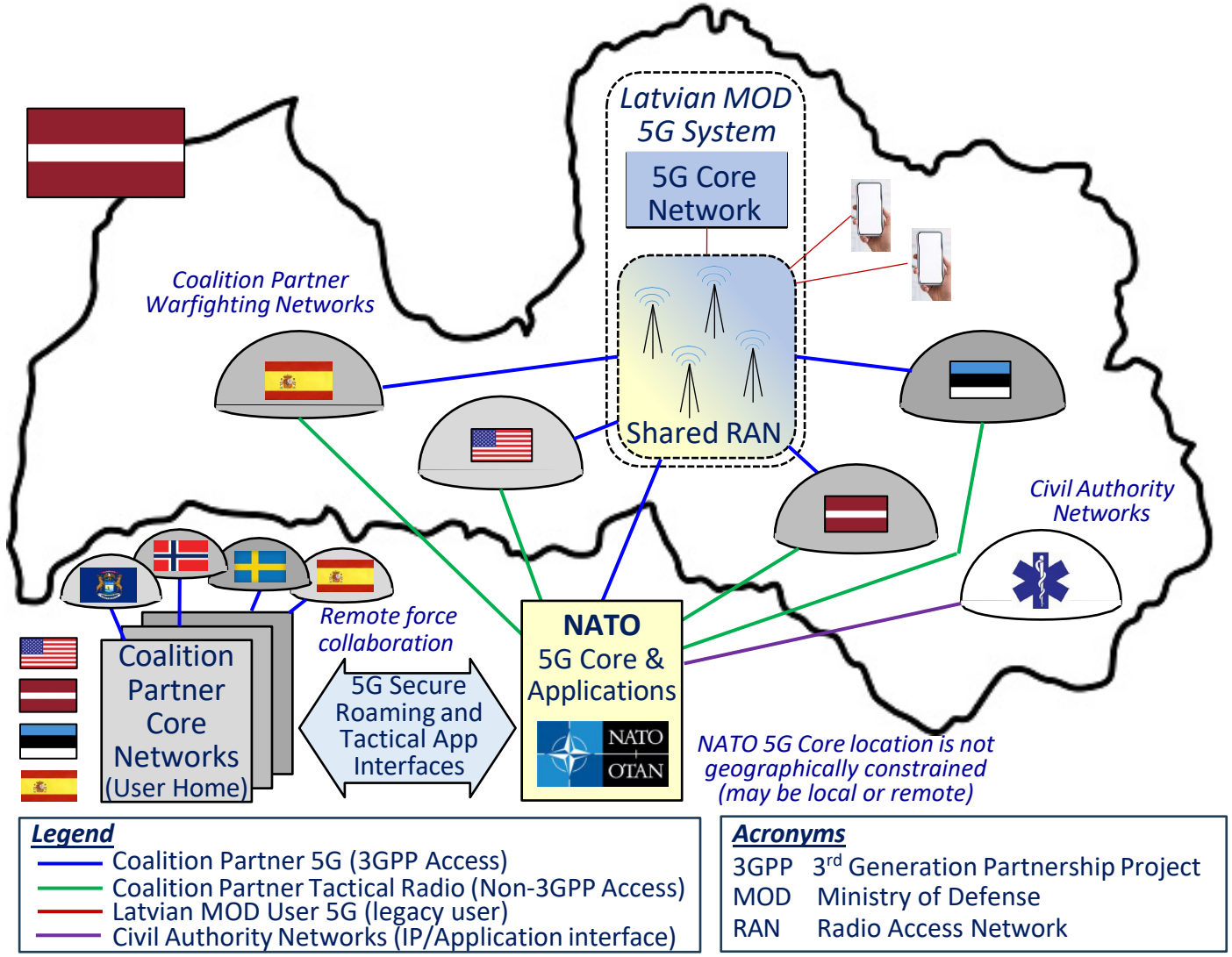
Elements

- Waveform resilience for tactical and expeditionary environments
- Simplified network deployment, management, and orchestration
- Heterogenous network integration for Partner Force interoperability

Projects and Experimentation

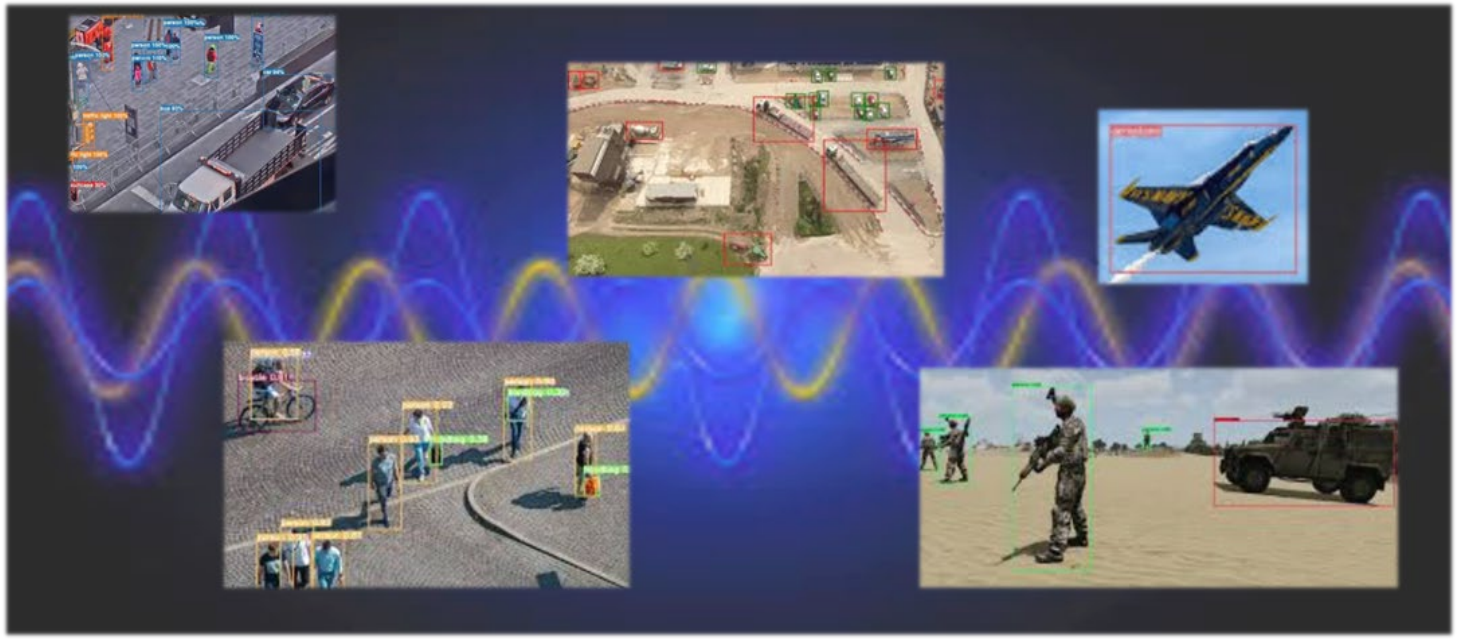
- Physical Layer Leverage
- Army - Tactical Mobility
- USMC - Expeditionary Advanced Base Operations
- Secure Multi-hop Sidelink
- Open Source Tactical Edge Network Testbed
- International Stand Alone Roaming
- Distributed Squad Beamforming – LPx
- Reconfigurable Tactical Open Radio Access Networks
- High-Risk Infrastructure Avoidance

Scalable Interoperable Resilient (SIR)



- **Objective:** Employ standard AI capabilities to provide a scalable, interoperable, and resilient warfighting network for NATO
- **Future Relevance:** Leverages capabilities that enable secure roaming, RAN Sharing, and internetworking between a core and a heterogeneous group of tactical radios to position NATO as a service provider
- **Warfighter Impact:**
  - **Scalability**—Use host nation RAN Sharing with a NATO core and secure roaming to maximize coverage and rapidly achieve shared situational awareness
  - **Interoperability**—Supports information exchange among NATO allies using their organic tactical radios and commercial mobile devices
  - **Resilient Communications**—Provides the warfighter with options to employ the best waveform(s) (tactical, 5G, or both) for each phase of the mission

Integrated Sensing and Communications (ISaC)



Projects and Experimentation

- Intelligent Reflecting Surfaces (IRS)
- Force Protection Surveillance System (FPSS)
- Nellis Air Force Base
- Playas Research & Training Center (PRTC)

Future Projects

- Object Detection / Sensing
- Radar for communications
- Spectrum Co-existence

Elements

- AI infrastructure (co-location centers, towers, waveforms)
- Sensors
- AI-based identification

Smart Resilient Logistics (SRL)

Projects and Experimentation

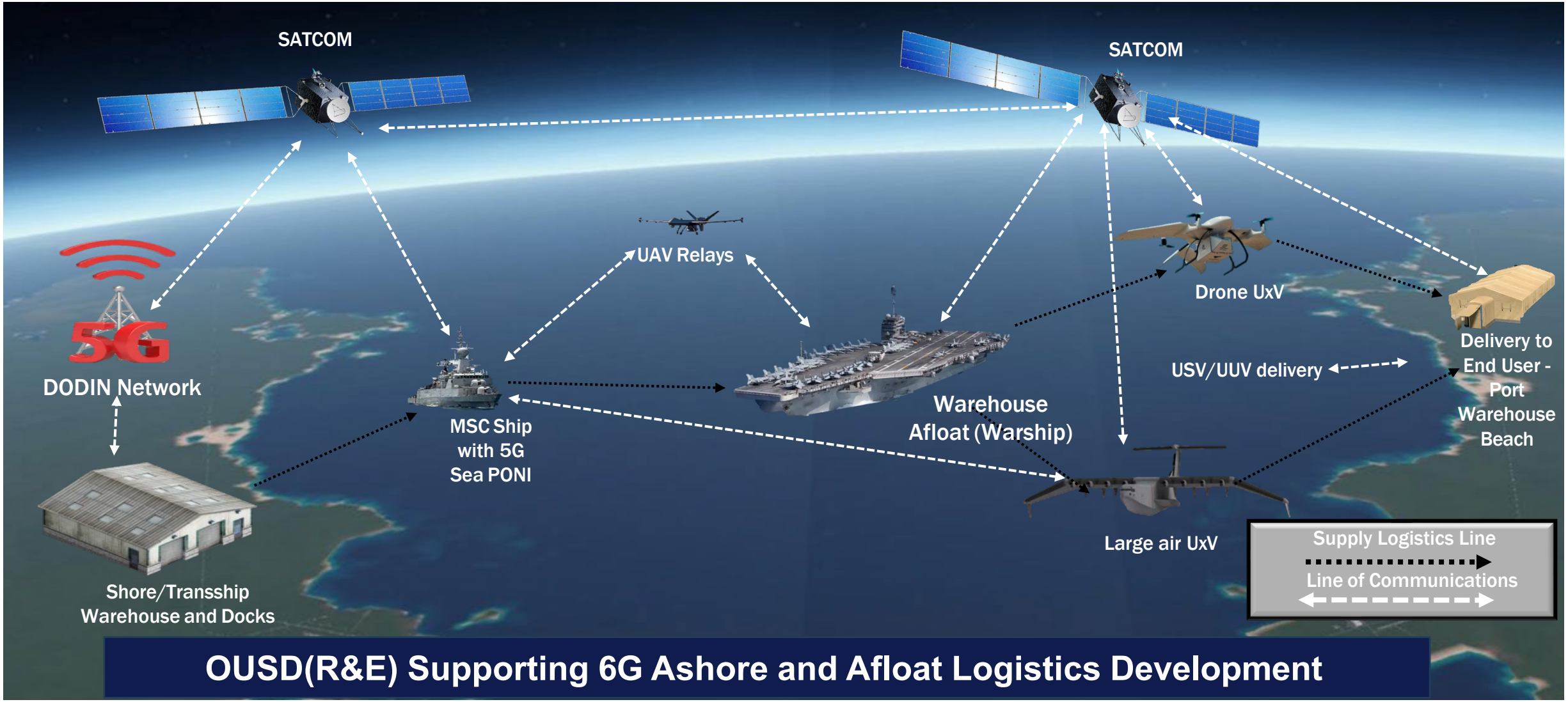
- Guaranteed Architecture for Physical Security (GAPS) - with DARPA & DISA
- Squad Networked Lethality (SNL)
- Naval Base Coronado Smart Warehouse
- Marine Corps Logistics Base Albany Smart Warehouse
- Joint Base Pearl Harbor-Hickham / Naval Air Station Whidbey Island "Flight Line of the Future Modernization"
- Naval Station Norfolk Pier-Side 5G Installation

Elements

- Collaborate with other DoD agencies on unified logistics strategy
  - Extend smart warehousing to legacy DoD warehouses
  - Improve AI EDGE capabilities regional
  - Logistics common operating picture
  - Data analytics to support predictive logistics
  - Command and Control (C2) of AI logistics with data analytics provide reactive logistics to redirect material solutions as needed
- Promote unmanned delivery systems

INDOPACOM Integration

Smart Resilient Logistics (SRL)



OUSD(R&E) Supporting 6G Ashore and Afloat Logistics Development

Workforce Development

Problem

A profound skills gap exists in the telecommunications industry workforce due to technology advancement and vast new investment running into a general lack of available training and education.

Workforce Development Approach

Explore, adopt, and advance new workforce development engagement models that establish national defense requirements as a compelling career purpose and marketable skills for a new generation of American workers.

Opportunities actively being pursued in 2025

Michigan Air National Guard (Battle Creek, MI)
- Workforce development trial that promotes hands-on work with 5G Hardware in open-air experiments
- Michigan's State Partnership Program is with Latvia creates opportunities to work directly with NATO partner forces
- Objective: accelerating development of a smarter, high-tech workforce both in and out of uniform
- Focus: Tactics Techniques & Procedures (TTP) development for 5G/FutureG tactical use

Naval Post-Graduate School (NPS)
- Funds an active-duty workforce program
- Objective: transform episodic 5G research into sustained and intentional development of open source 5G/FutureG expertise
- Focus: plan, deploy, operate, and maintain 5G/FutureG networks in expeditionary and tactical environments
- Education Level: Masters/PhD

FutureG Service Academy Internship Program
- Design, develop, and fund an internship program for senior cadets and midshipmen at the United States Service Academies
- Create hands-on experience with FutureG technology to address technical military problems
- Allows FutureG programs to leverage their labor and expertise and provide continuing champions
- 4 to 8-week summer phase working full-time, in person with FutureG program managers
- Future officers can continue their research part-time as their "senior capstone" project
- To date, worked with 11 cadets and midshipmen from all three service academies
- Received outstanding after-action reviews for the value of the experience

Science, Mathematics, and Research for Transformation (SMART) https://www.smartscholarship.org/smart/
- Leverage the current DoD scholarship-for-service program
- The largest education and workforce development initiative under the DoD STEM Program
- Scholarship recipients receive hands-on experience at one of over 200 DoD facilities during their internships
- Transition to knowledgeable early career professionals

Microelectronics (ME) Commons 5G/6G Hub Work

- **CHIPS Act supports the creation of ME Commons**
  - Regional "AI Hubs" mission: expand the nation's global leadership in microelectronics
  - 5G/6G Technology is a major focus and is a primary technology area at 4 of the 8 Hubs.

- **Future Support to ME Commons**
  - Principal Director for Future, Dr. Thomas Rondeau, serves as the Primary Advisor to 5G/6G Hubs
  - Applied Research: Applied research in 5G/6G prototyping to inform lab-to-fab developments
  - Transition Paths: FutureG-ME Commons collaboration enhances capabilities to the Warfighter

Active collaboration between the Future Office and ME Commons to meet DoD mobile wireless goals

Highlights of Future AI Infrastructure Roadmap

- Military data and network requirements are outpacing DoD capabilities
- The rapid pace of global commercial AI Data Center technology development presents unique teaming (Public Private Partnerships) opportunities
- **OUSD(R&E)'s FutureG Office is:**
  - Driving **innovation** in relevant technical areas for DoD
  - **Incentivizing** the pace and direction of U.S.-based commercial wireless development
  - **Changing the landscape** of DoD-commercial relationships to drive market-based competition, rapid innovation cycles, and secure networking

Future AI will advance, adopt, adapt, and innovate on commercial technologies to advance national security objectives


UNDER SECRETARY OF DEFENSE FOR RESEARCH AND ENGINEERING
USD R&E
DEPARTMENT OF DEFENSE