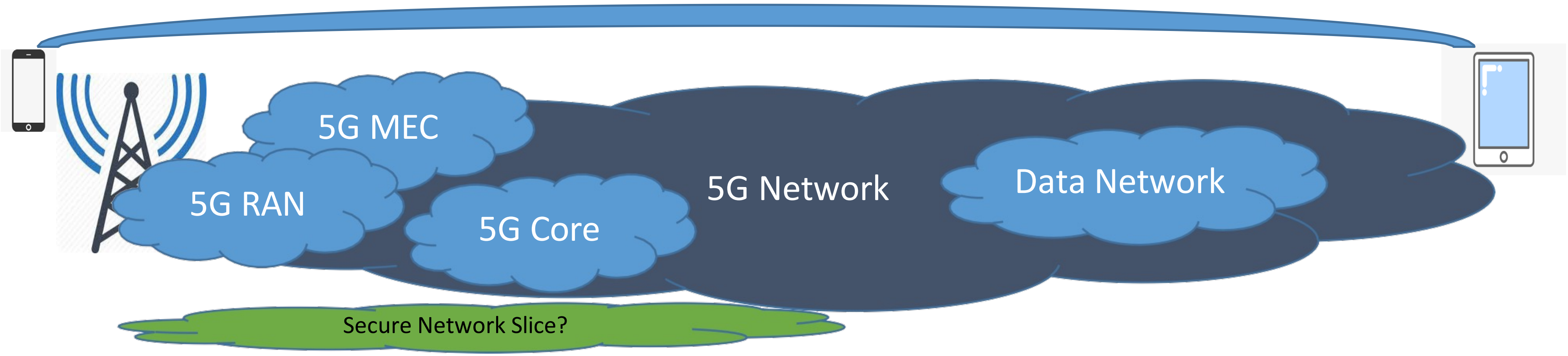
# Securely Operating Through Commercial Infrastructure

## FutureG & 5G Operate Through

Dr. Dan Massey
Director, Operate Through
OUSD (R&E) FutureG & 5G Operate Through

Distribution Statement A: Approved for Public Release, Distribution Unlimited September 2023

# 5G Basics



- **5G Radio Access Network (RAN):** 5G is really all about the physical layer transmission of signals. Beam forming, MIMO, 5G NR, and so forth dramatically improve how signals are transmitted and received.

- **5G Core:** 5G is really all about the core network that takes over once a signal has been received. By enabling and encouraging network function virtualization, 5G dramatically improves how the (often wired) network is constructed and managed.

- **5G Multi-access Edge Computing (MEC):** 5G is really all about pushing computational resources to the edge. By bringing the power of the cloud close the edge, features such as augmented reality/virtual reality benefit from reduced latency and dispersed computations.

# What’s Driving Critical Infrastructure To 5G?

Headlines:
Verizon Wireless Buys Spectrum for $3.6 Billion
AT&T buys spectrum owner for $1.6 billion

- **Spectrum is a Finite (and Valuable!) Shared Resource**
  - ➢ Any type of wireless transmission uses spectrum.
  - ➢ Critical infrastructure competes with rapidly growing users of spectrum.
  - ➢ In general, conflicting use of spectrum results in no useful communication.

- **Massive Investments in 5G Technology**
  - ➢ From IHS Markit 2020 5G Economy Study, commissioned by Qualcomm Technologies, Inc:
    - ▪ Collective investment in R&D and CAPEX by firms that are part of the 5G value chain, within the seven countries examined in the report, will average over $260 billion annually.
    - ▪ The United States and China are expected to lead in 5G CAPEX and R&D, investing a total of $1.3 trillion and $1.7 trillion respectively, over the 15-year time horizon of this study.

- **5G Enabling Technologies**
  - ➢ From “Key Enabling Technologies of 5G Wireless Mobile Communication” by Sudhir Sharma1, M Deivakani2, K Srinivasa Reddy3, A K Gnanasekar4 and G Aparna:
    - ▪ 5G (fifth generation) is more reliable at a very low cost and provides 10 times more capacity than other generations.
    - ▪ Key enabling technologies used in 5G networks include Device-to-device (D2D) communication, Machine-to-machine (M2M) communication, Millimetre Wave, Quality of Service (QoS), Network Function Virtualization (NFV), Vehicle-to-everything (V2X), Full-Duplex and Green Communication.

# Operate Through Existing Infrastructure

**Build Your Own Infrastructure**

**Operate Through Existing Infrastructure**

*Capability to Build Bridges*

AND

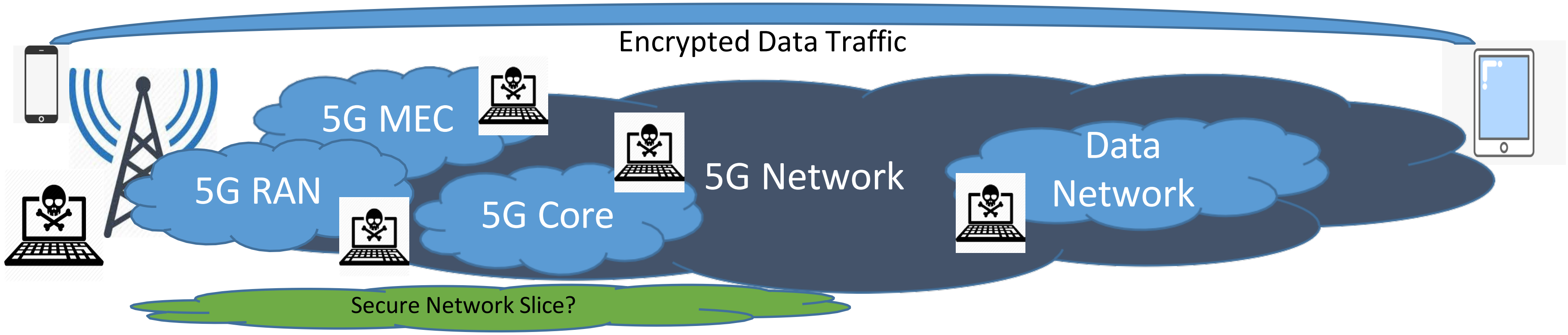
*Make Use of Existing Bridges*

*Capability to Build Comm Infrastructure*

AND

*Make Use of Existing Comm Infrastructure*

# 5G Risks



- **Commercial 5G Networks Lack DoD Suitable Security Assurances:** Commercial 5G adds coverage, Quality of Service, and low cost, but may lack security assurances suitable for DoD missions.

- **Risks From Untrusted Supply Chain Components:** Risks arise from untrusted 5G manufacturers and/or compromised 5G components.

- **Unable to Leverage Indigenous 5G Network Capabilities:** Operating through indigenous 5G networks would benefit DoD missions if security requirements are met.

Distribution Statement A: Approved for Public Release, Distribution Unlimited May 2023

# Security and Resilience: CIA and O

- Classic Confidentiality, Integrity, and Availability:
  - ➢ Confidentiality – encryption, access control, etc..
  - ➢ Integrity – authentication, message integrity, replay attacks, etc..
  - ➢ Availability – denial of service defense, jamming/EW.

- Observability:
  - ➢ Capability to hide in plain sight.
  - ➢ Situational awareness and traffic analysis defense.
  - ➢ Capability to identify and analyze adversary actions.

# Zero Trust & Operate Through

- **Perimeter defense techniques are ineffective for Operate Through**
  - ➢ Perimeter defense aims to keep adversary out of the secure system (castle and moat).
  - ➢ Lack a well-defined perimeter when operating through commercial 5G network.
  - ➢ Underlying network may contain untrusted components.

- **Zero Trust Introduces Key Principles Including**
  - ➢ Continuous authentication and access control.
  - ➢ Push security (e.g. encryption, access control) close to the end systems.
  - ➢ Segmentation (micro-perimeters).
  - ➢ Threat intelligence to drive real-time detection of malfunction or malicious action.

- **Zero Trust Can Enhance Availability**
  - ➢ Extend zero trust concept to paths as well as devices.
  - ➢ Multi-path routing and dynamic spectrum usage.

***Zero Trust Architecture Promising For Operate Through***

# Operate Through Assumptions

- Critical Infrastructure Will Move to Commercial 5G
  - Includes some (not all) military communication systems.

- Commercial Market Drives 5G Standards and Implementations
  - Critical infrastructure can (and should) engage in standard discussion.
  - Critical infrastructure alone insufficient to drive standards and/or implementations.

- Wide Variety of Security Practices
  - Many security aspects of 5G (3GPP) standards are optional.
  - Operational practices will vary widely.
  - Networks will contain untrusted (and in some cases malicious) equipment.

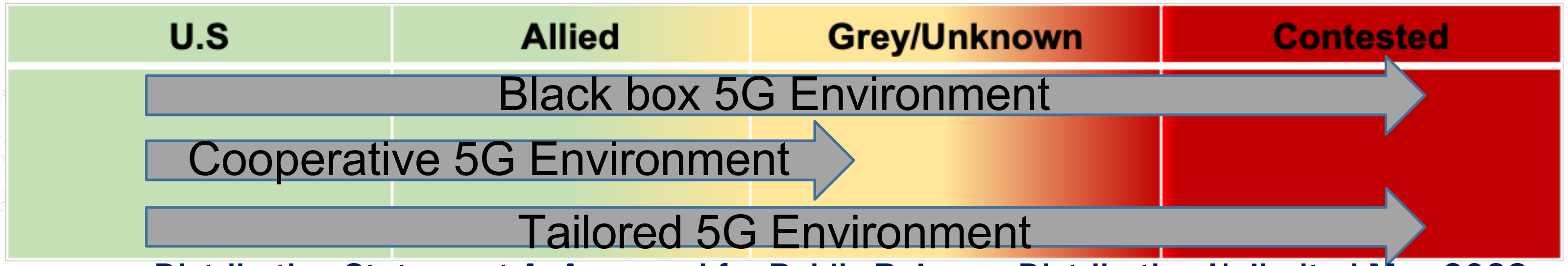
- No Canonical 5G Network
  - Mix of 5G SA and NSA.

# Operate Through Environments

- **“Black Box” 5G Network – Treated as an unreliable bit pipe**
  - ➢ Deploy security at end devices & connect networks via untrusted bit pipe.
  - ➢ Applicable to scenarios where DoD leverages indigenous infrastructure as a user.

- **Cooperative Commercial/Private 5G – Provider will work with DoD on security**
  - ➢ Work with provider to augment some combination of RAN/MEC/CORE.
  - ➢ Work within the commercial environment to the benefit of commercial provider.
  - ➢ Applicable to scenarios where DoD works with indigenous infrastructure as a partner.

- **Security Enhancements for a Tailored Environment**
  - ➢ Full control over code and components.
  - ➢ Introduce changes to the RAN/MEC/CORE without commercial 5G constraints.
  - ➢ Applicable to future scenarios where DoD has developed its own 5G capabilities.



U.S

Allied

Grey/Unknown

Contested

Black box 5G Environment

Cooperative 5G Environment

Tailored 5G Environment

Distribution Statement A: Approved for Public Release, Distribution Unlimited May 2023

# Questions?

Dr. Dan Massey
Director, Operate Through
OUSD (R&E) FutureG & 5G Operate Through

Longmont, CO
23 May 2023

USD(R&E)

# Backup Slides

Dr. Dan Massey
Director, Operate Through
OUSD (R&E) FutureG & 5G Operate Through

Longmont, CO
23 May 2023

Distribution Statement A: Approved for Public Release, Distribution Unlimited May 2023

# CI Operating Through Commercial Infrastructure

- **Energy Sector**
  - ➢ Control systems moving online for sensing and automated control, improved efficiency, added resilience to failures, new generation capabilities (microgrids), and support for new loads on the network (fast charging).
  - ➢ 5G Project: funding the National Renewable Energy Lab to evaluate feasibility of replacing fixed wired connectivity with low latency 5G networks.
- **Transportation Sector**
  - ➢ Vehicle to Everything (V2X) moving from bespoke system to 5G based commercial infrastructure.
  - ➢ 5G Project: funding DoT Volpe Center to assess commercial vehicle V2X development.
- **Dams Sector**
  - ➢ Monitoring systems moving online to identify issues and vulnerabilities, mitigate threats, and rapidly adapt in the event of natural (or man made) disasters.
  - ➢ 5G Project: funding U.S. Corp of Engineers to develop monitoring and mitigation system that operates over commercial wireless networks.

**Could/should the military operate on commercial networks?**

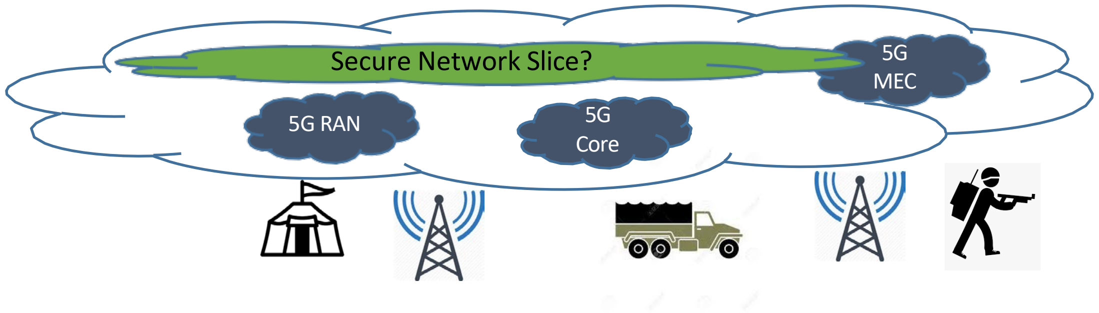
# ENISA Threat Framework

- Evaluate Security Efficacy Across Four Categories:
  - Confidentiality, Integrity, Availability, and Observability.

- ENISA (European Union Agency for Cybersecurity) Framework Defines Threats and Categories They May Impact.

| Threats | Potential Impact On |
|---|---|
| **Manipulation of network configuration / data forging** | Integrity, Availability, Observability, |
| **Exploitation of software, hardware vulnerabilities** | Confidentiality, Integrity, Availability, Observability, |
| **Denial of service (DoS)** | Availability |
| **Malicious code/software** | Confidentiality, Integrity, Availability, Observability, |
| **Abuse of remote access to the network** | Integrity, Observability, |
| **Abuse of information leakage** | Confidentiality, Integrity, Observability, |
| **Abuse of authentication** | Confidentiality, Integrity, Availability, Observability |

# Secure Network Slicing



- **Overall Objectives:**
  - ➢ Increase security, preserve performance.

- **Possible Solutions:**
  - ➢ Request network slice from 5G network.
  - ➢ Network slice provides specialized service on top of existing 5G network.
  - ➢ Networking slicing anticipated to be a standard service in 5G.
  - ➢ Network slicing typically used for performance metrics:
    - ▪ Provide higher bandwidth to devices using the slice.
    - ▪ Provide low latency to devices using the slice.

- **Secure Network Slicing Questions:**
  - ➢ Can a slice provide added security instead of performance?

# Example Lessons Learned (?) On Separation

- (Lack of) Wisdom In Putting Both Infotainment system and Vehicle Control on Same Network Segment?
  - Cybersecurity 101: Separation of Duties, Isolation, and Segmentation.
  - Vehicle networks evolved over time.
  - Frequently see references to vehicle network limitations.

- (Lack of) Wisdom in Putting Infotainment and Vehicular Control on Same 5G Network?
  - Rely on the same 5G network for passengers streaming videos and V2V or V2I signaling?
  - Network will evolve over time.
  - Cost and efficiency of building out a separate network?