Enabling Secure and Resilient 5G

Dan Elmore, Colonel, USAF (ret)

Director, Critical Infrastructure Security & Resilience

Executive Director, INL Wireless Security Institute

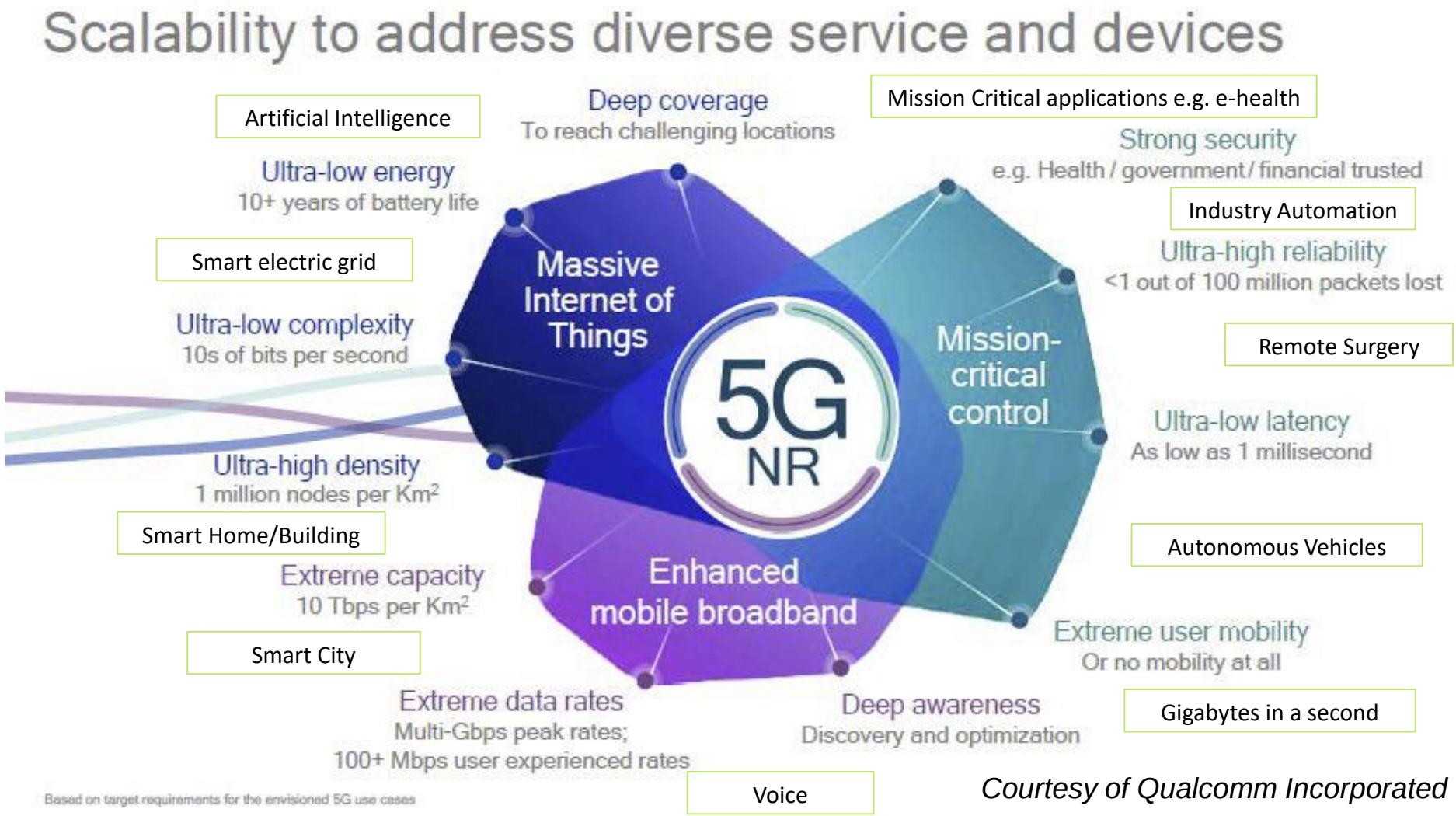
January 2021

Idaho National Laboratory

National 5G Policy Landscape

- **National Strategy to Secure 5G Implementation Plan (Draft), January 6, 2021**
  - Activity 2.1: Risk evaluation of domestic and international suppliers
  - Activity 2.2: Assess threats, vulnerabilities, and risks to 5G infrastructure
  - Activity 2.3: Identify security gaps and threats and strategic partners' supply chains
  - Activity 2.5: Identify/develop/apply security principles for 5G infrastructure
- **National Strategy to Secure 5G, March 2020 and Public Law 116-129, "Secure 5G and Beyond Act of 2020," March 23, 2020**
  - Develop strategy and implementation plan to accelerate adoption of 5G
  - Assess cybersecurity, economic, national security risks as 5G is developed and deployed
- **"R&D Priorities for American Leadership in Wireless Communications" (OSTP, May 2019)**
  - Pursue spectrum flexibility & agility to use multiple bands and waveforms
  - Improve near real-time spectrum awareness
  - Increase spectrum efficiency and effectiveness through secure sharing
- **2019 Defense Science Board (DSB) Task Force**
  - "Create test beds for exploring innovative use cases"
  - "Establish evidence-based positions on key features, security, and safety"
  - "Accelerate mmWave technology development and transition"

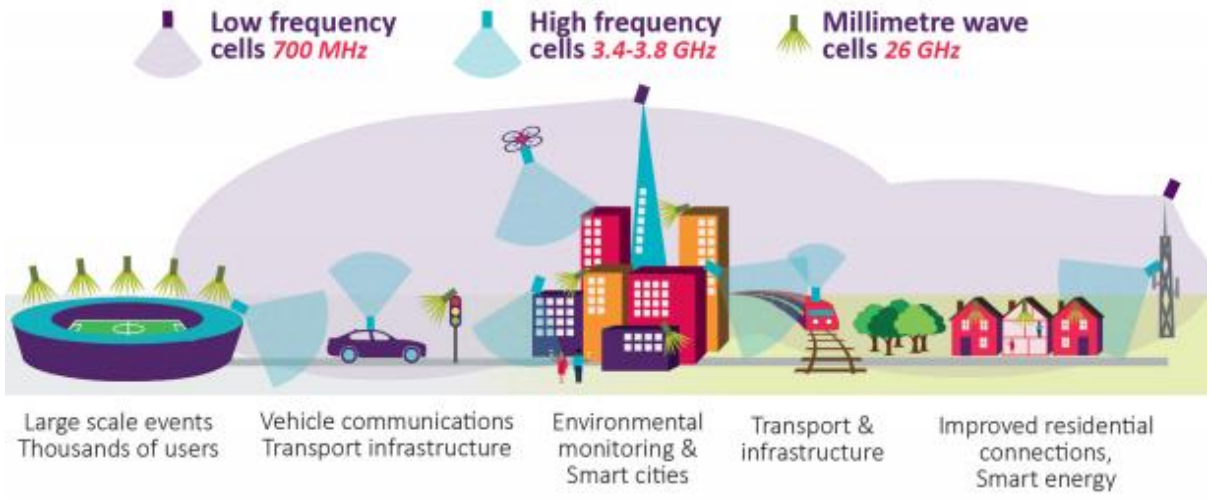
Why is 5G Getting National Policy Attention



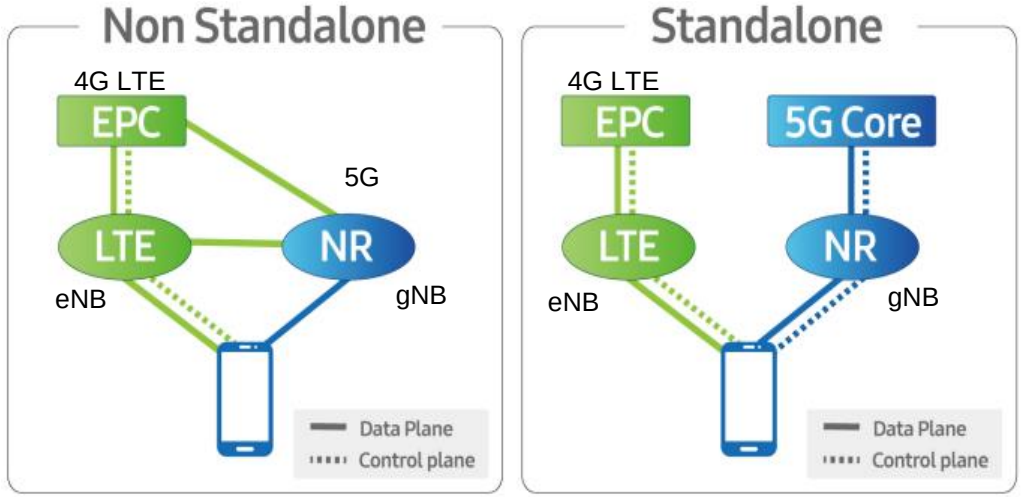
Courtesy of Qualcomm Incorporated

Where is 5G Heading – Challenges Moving Forward

5G Frequency Ranges and Use Cases:



5G Deployment Scenarios:



5G NSA (Non Standalone)

5G SA (Standalone)

US started with fixed, 5G NR (NSA)

- 5G Non-Standalone radios (NSA)
  - 5G radio heads
  - Using 4G core infrastructure
  - 4G legacy security challenges

National Needs:

- Reallocated and unlicensed spectrum
- Spectrum sharing
- Secure 5G devices and networks
- Secure supply chain
- Zero trust security techniques
- 5G test and evaluation capacity

5G Capability but New National Security Challenges

"The communication sector is an integral component of the US economy and our national security, underlying the operations of all business, public safety and government." Christopher Krebs, DHS Director of Cybersecurity and Infrastructure Security, 14 May 2019 Senate Judiciary Hearing on 5G

New key capabilities with 5G

- 5G enabled IoT[1] and industrial IoT, connected health, vehicles (V2X), UAS/Drone (A2X), etc.
- 5G NR (New Radio); use of unlicensed and shared spectrum
- 5G Core (5GC) introduces Service Based Architecture (SBA)
- Beam based Air Interface for sub-6 GHz and mmWave
- Edge computing, SDN[2] and NFV[3]

New Security Challenges

- Secure operation of large number of devices, vehicles, UAS/Drones; authentication and identification
- Increase in illegal and disruptive use of spectrum sharing
- Increase in attack surface – need to secure increased number of interfaces
- Adapting wireless security to beam based directional transmission, increase in mmWave base station density
- Secure operation of edge connectivity, SDN, and NFV

[1] Internet of Things, [2] Software Defined Networking, [3] Network Function Virtualization

Going Forward:

Accelerating 5G Security and Resilience

- **Form Strong Public-Private Partnerships**
  - Provide focus on most needed capability and policy gaps facing 5G deployment
  - Add visibility to help investments in critical gap areas, spanning the “valley of death”
  - Synergize efforts at all phases from basic research to commercial adoption
  - Continue strong university collaboration on 5G security research
- **Establish Trusted 5G Evaluation Platforms**
  - Identify and characterize wireless security issues that will validate effect and lead to creation of effective solutions
  - Validate in both virtual and full–scale situations
  - Provide stressed and extreme condition wireless network testing
  - Tame the “Wild West” of user and edge devices
  - Holistic, application-specific evaluation
- **Closely Coordinate Approaches to Critical Limitations**
  - International challenges to system security and data protection
  - Identify the “critical assets” in 5G networks and create a set of disruptive tactics and intrusion tests (“red teaming”) to ensure needed mitigations are in place
  - Concepts helping rural and underserved areas

INL's Focus on Accelerating Secure 5G Deployment

- **Launched INL Wireless Security Institute (WSI) Fall, 2019 to**
  - Focus secure and resilient wireless research efforts needed to protect the nation's critical infrastructure (5G and beyond)
  - Lead collaboration (internal and external) on research for wireless and spectrum security and resiliency with national impact
  - Create a national forum for government labs, agencies, academic and industry researchers
- **Second wireless security workshop** in November 2020 with an invited group of wireless security researchers and leaders across the country (300 total registrants)
- **Formed WSI External Advisory Board**
  - Completed first board meeting last week (20/22 Jan)

Through research partnerships, recognized leadership, and differentiating capabilities, INL is becoming a catalyst for discovery and the preferred provider for wireless security and resilience research and evaluation.

VISION

Advance 5G National Leadership and Accelerate the Secure Adoption of 5G and Beyond Technology

MISSION

Provide best in class policy and decision data, security evaluation, engineering support, and technology development enabling government and industry to maximize the benefits of 5G and beyond technology

Wireless Security Applied R&D

Conduct R&D addressing critical national wireless security gaps

Spectrum Innovation

Develop needed spectrum sharing techniques and devices

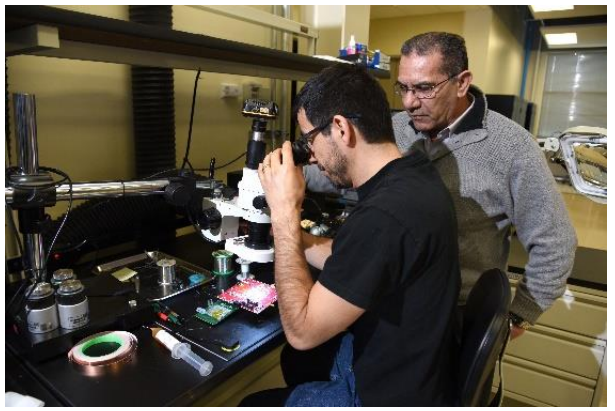
Next Generation Wireless Test Bed

Effective, accurate, responsive testing at scale

END STATE

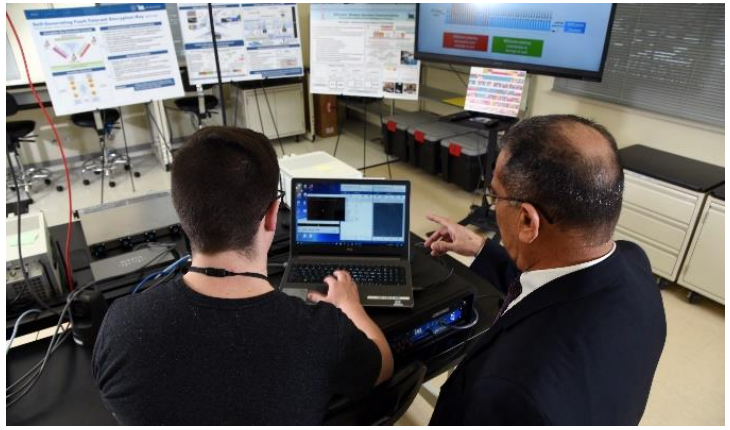
Broad, Diversely Funded RDD&D Portfolio

INL Established as National Authority on Wireless Security



INL's Unique Wireless Range Aligned with National 5G Needs

- **Isolated Location and Agile Spectrum Management**
  - NTIA approved wireless experimental station
  - Low RF Noise Floor
  - 890 square miles
- **Commercial-Scale Cellular Networks**
  - 4G, 3G, 2G
  - Four Network Operations Centers
  - *New: 5G security assessment program*
- **Industry and Scientific Expertise**
  - Full RF spectrum and protocols
  - Power grid, control systems cybersecurity
  - Design, software, and hardware



INL's Wireless Test Bed and State-of-the-Art Wireless Research Labs
Support Acceleration of 5G thru R&D, Deployment, Evaluation and Test

Isolated, Reconfigurable, Multidisciplinary, High-Fidelity Environment

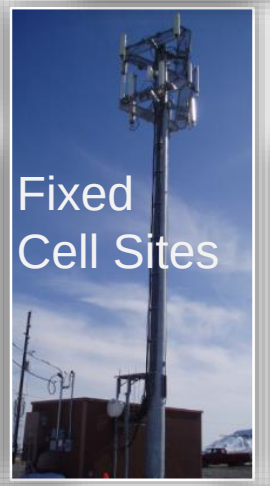
INL Range

Monitoring Equipment

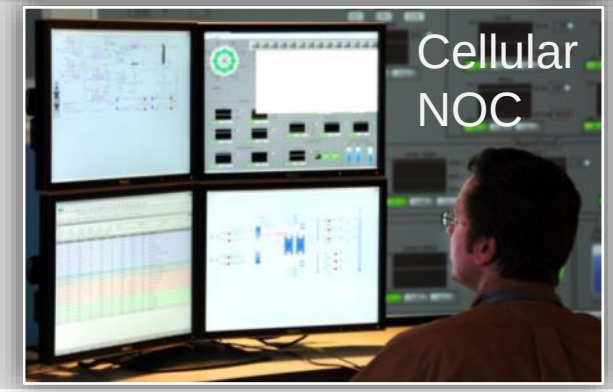
Multiple Test Sites

PSTN Simulator

Call Generator



Idaho Falls



ABORATORY

Ongoing Wireless Security Institute R&D Activities

- **WSComm enables flexible spectrum sharing with robust underlay channel**
  - Improves spectrum sharing, spectrum monitoring, and interference mitigation
  - Multiple US patents and 2012 R&D 100 Award
- **Underlay Communication Channel for Massive Machine-type Communications (mMTC) for 5G and Beyond Applications (LDRD)**
  - Faster link set-up speed using Cyclic Prefixed Direct Sequence Spread Spectrum as data control underlay channel
- **Wireless RF Signal Identification and Protocol Reverse Engineering (WiFIRE)**
  - Monitor frequency power usage, type of signaling, and information passed
  - 2019 R&D 100 Award and a Idaho Innovation Award Finalist
- **Detection of Drones Connected with Commercial Cellular**
  - Identifying network signatures generated by Cellular drones
- **CyPhy (Cyber Secure Physical Layer in 5G mmWave) (LDRD)**
  - Enhancing security of 5G mmWave communications in the presence of unauthorized devices and intruders
- **Innovative Secure 5G mmWave Cellular Network for Operating Drones/UAS (LDRD)**
  - Secure communications for control of Drone Swarms with increased spectral efficiency and reliability
- **Secure mmWave Spectrum Sharing with Autonomous Beam Scheduling (LDRD)**
  - Improve spectral efficiency, throughput, and security of spectrum sharing
- **5G and LTE Security Assessments and Exploitation**
  - Identify security vulnerabilities and scenarios that can exploit them

Wireless Security Research and Engineering Expertise Based on Industry Experience

- **50+ technical experts in wireless communications**
  - Cellular, Telecommunications, IP, HF, all TS/SCI-cleared
- **Expertise from major wireless and telecommunication companies**
  - AT&T, T-Mobile, Nokia, Lockheed Martin, Boeing, Motorola, Hughes, L-3 Com, EG&G, Nextel, and Radix
- **Experienced in design, testing, installation, configuration, maintenance and operations of next generation cellular communications systems**

Idaho National Laboratory