Working Group 1: Harnessing Artificial Intelligence/Machine Learning to Ensure the Security, Reliability, and Integrity of the Nation's Communications Networks

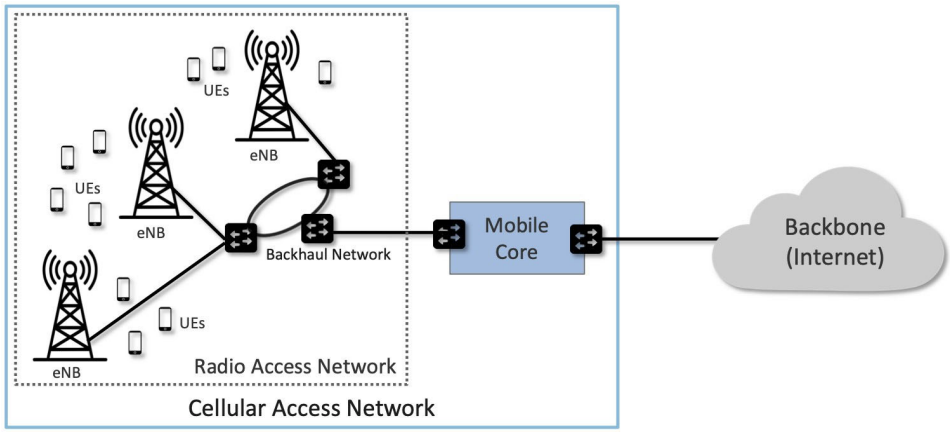
March 19, 2025

Co-Chairs: Vijay K. Gurbani, Vail Systems
Jason Hogg, Microsoft

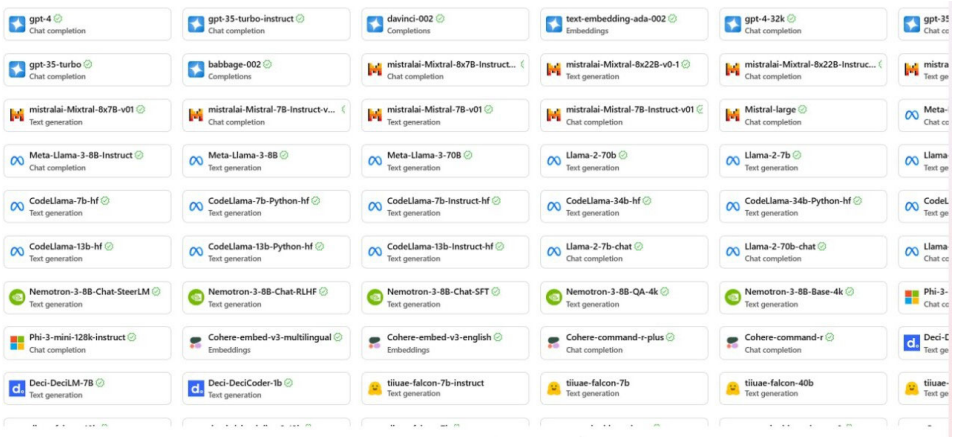
FCC Liaison: Suzon Cameron and Kurian Jacob

Working Group 1 : Background

Fundamental question: How does AI/ML affect the security and reliability of communications networks and how to mitigate the challenges that the technology poses?



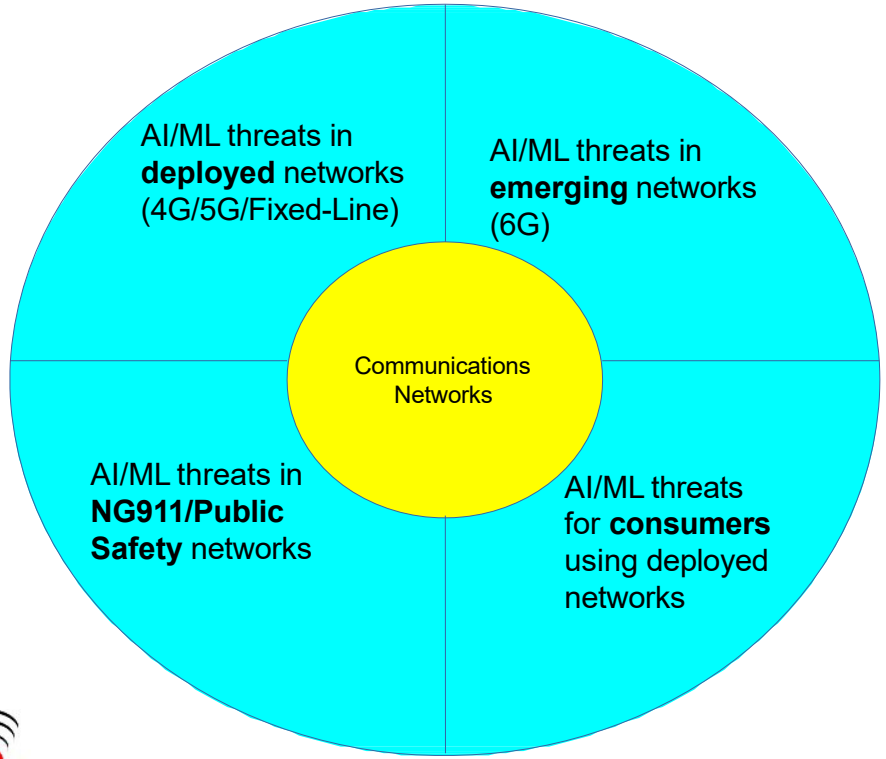
Source: https://5g.systemsapproach.org/



The Challenge(s)

- Communications networks are complex
- AI / ML are being applied across the network
- Different types of AI / ML models
- Rapid rate of development
- How to identify and prioritize relevant threats?
- … without boiling the ocean!

Working Group 1 : Background



Sources of complexity:

1. The technology (AI/ML)
2. The telecommunications network
3. Securing AI/ML

Working Group 1: Members

Co-chairs:
Vijay Gurbani, *Vail Systems*
Jason Hogg, *Microsoft*

Mark D Annas, *City of Riverside, CA*

Praveen Atreya, *Verizon*

Mike Barnes, *Mavenir Systems*

Richard Barron, *The MITRE Corporation*

Chris Bennett, *Motorola Solutions*

Craig Bowman, *Futuri*

Matt Carothers, *Cox Communications*

Christina Chaccour, *Ericsson*

Andrew L Drozd, *ANDRO Computational Solutions*

Luiz Eduardo, *Hewlett-Packard Enterprise*

Bob Everson, *Cisco Systems*

Ben Goldsmith, *DOJ*

Mark Grubb, *CISA*

Ankur Kapoor, *T-Mobile*

Yong Kim, *VeriSign*

Lauren Kravetz, *Intrado Life & Safety*

Salman Marvasti, *Advanced Computer Concepts*

Tim May, *NTIA*

Martin McGrath, *Nokia*

Brian Murray, *Harris County, TX*

Jonathan Petit, *Qualcomm*

Abir Ray, *Expression Networks*

Travis Reutter, *ACA Connects*

Travis Russell, *Oracle Communications*

Peter Santhanam, *IBM*

Narothum Saxena, *UScellular*

Peter Scott, *Public Broadcasting Service*

Rikin Thakker, *NCTA*

David Valdez, *CTIA*

Henry Young, *BSA | The Software Alliance*

Dongsong Zeng, *U.S. Department of Commerce*

Working Group 1: Alternates*

Anmol Agarwal, *Nokia*

Patrick Arsenault, *Intrado Life & Safety, Inc*

Michael Beirne, *CTIA*

Robert Cantu, *NCTA*

Devin Christensen, *CISA*

Sean Donelan, *VeriSign, Inc.*

Narayanan (Nars) Haran, *UScellular*

John Hunter, *T-Mobile*

Jithin Jagannath, *ANDRO Computational Solutions, LLC*

David Marcos, Motorola Solutions

Olga Medina, *BSA | The Software Alliance*

Jennifer L Oberhausen, *Microsoft*

Jim Reno, *Ericsson*

Joseph Smetana, *Vail Systems, Inc.*

Kamakshi Sridhar, *Mavenir Systems, Inc.*

Mourad Takla, *Verizon*

Bill Tortoriello, *ACA Connects*

Lei Yu, *Expression Networks LLC*

* Alternates are not a member of the Working Group and may not vote.

Deliverables

- **Milestones**:

1) Report on the Threats Posed by Artificial Intelligence/Machine Learning Systems to the Security, Reliability and Integrity of Networks and Recommendations on How to Overcome Them, ~~March 2025~~ **June 2025**

2) Report on Recommended Best Practices for the FCC and Industry on the Ethical and Practical Use of Artificial Intelligence/Machine Learning, September 2025

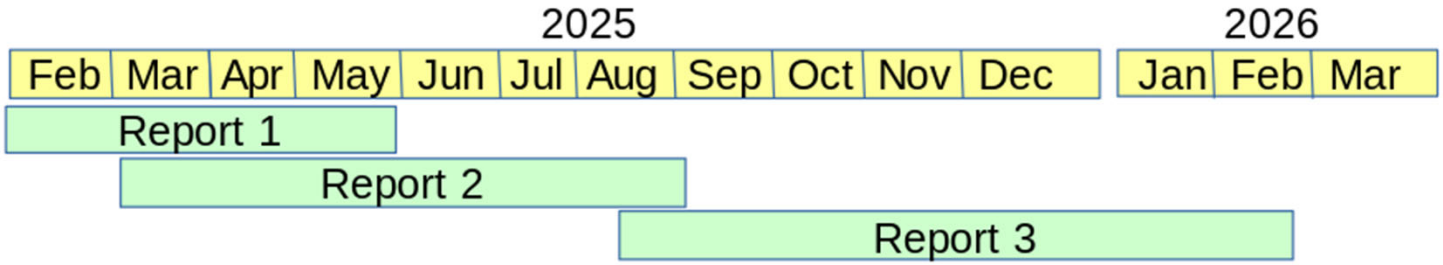
3) Report on Best Practices for the Use of Artificial Intelligence/Machine Learning Systems Specifically Intended for Public Safety Network, March 2026

Updates since Dec 2024

- Jan 29 2025: Formal request to DFO for an extension on Report 1.
- Reduced and consolidated "Techincal Areas" for focus.

Area	Lead	Members
~~UE Handset~~	Salman Marvasti	Jonathan Petit
~~Audio + Speech~~ ~~UE IoT~~ ~~Business Support Systems~~	Luiz Eduardo Bob Everson Peter Santhanam	Jonathan Petit, Craig Bowman Dongsong Zeng, David Valdez Travis Russell, Travis Reuter
~~Contact center operations~~	Peter Santhanam	Travis Russell, Travis Reuter
5G OSS	Praveen Atreya	Abir Ray, Travis Russell, Yong Kim, Henry Young
5G RAN	Abir Ray	Andrew Drozd, Mike Barnes, Christina Chaccour, Martin McGrath, Richard Baron
5G Backhaul	Bob Everson (?)	Rob Cantu, Rikin Thakker, Dongsong Zeng
5G Core	Timothy May	Narothum Saxena, Travis Reutter, Mike Barnes, Christina Chaccour, Martin McGrath, Bob Everson, Praveen Atreya, Travis Russell
Network Interconnection	Luiz Eduardo	Salman Marvasti, Travis Reutter, Travis Russell
Wireline Networks	Robert Cantu	Rikin Thakker, Travis Russell
6G Networks	Andy Drozd	Christina Chaccour, Martin McGrath, Travis Russell
~~Public safety networks~~	Mark Grubb (?)	Mark Annas, Devin Christensen, Brian Murray, Chris Bennett, Craig Bowman, Peter Scott, Patrick Arsenault, Rob Cantu, Rikin Thakker

Updates since Dec 2024



Due dates:

1. Report 1: ~~March 2025~~ June 12, 2025
   Due to DFO: May 23, 2025
2. Report 2: September 2025
   Due to DFO: Aug 11, 2025
3. Report 3: March 2026
   Due to DFO: Feb 28, 2026

Updates since Dec 2024

- Current status of Report 1:
  - All “technical areas” are complete and handed to editors.
  - Editors working on first draft of consolidated report, due on March 21 to WG.
  - Cycle of WG iteration and improvement during March 24 – April 30.
  - Final round of feedback May 1 – May 13.
  - Final report review cycle in WG May 14-May 21.
  - **Handoff Report 1 to DFO May 23.**

Updates since Dec 2024

- Current status of Report 2 (Recommended Best Practices for the FCC and Industry on the Ethical and Practical Use of Artificial Intelligence/Machine Learning):
  - March 6, 13 – Subject Matter Expert Presentations
    - Sam Kaplan, Palo Alto Networks
    - Lei Yu, Expression.ai
    - Sean Kennedy, Nokia Bell Labs
    - Ani Gevorkian, Microsoft
    - Jennifer Oberhausen, Microsoft
- March 20, 27 – Scoping discussions
  - Constrain to telecommunications networks only?
  - Expand to include adjacent industries that use telecommunications?
    - An AI agent makes a 911 call on behalf of its user.

Updates since Dec 2024

- Current status of Report 2 (Recommended Best Practices for the FCC and Industry on the Ethical and Practical Use of Artificial Intelligence/Machine Learning):
  - April, May –Individual teams produce content
  - June, July – Consolidated draft and review cycle(s)
  - **August – Handoff Report 2 to DFO**
- Start of Report 3 (Best Practices for the Use of Artificial Intelligence/Machine Learning Systems Specifically Intended for Public Safety Network), March 2026.

Discussion / Feedback

Thank you!

Working Group # 2:
Ensuring Consumer Access to 911 on All Available Networks As Technology Evolves

March 19, 2025

Co-Chairs: Brandon Abley, Stephen Hayes

FCC Liaison: Gerald English, Ryan Hedgpeth

Deliverables/Schedule

- We have the following milestones:
  1. Report on Recommendations and Best Practices for Connecting Stalled 911 Calls Through Alternative Network Options, **June 2025**
     - Identifying, prioritizing and quickly connecting 911 calls via alternative network options;
     - Reducing latency when utilizing alternative network options and for ameliorating the impact of any significant latency that cannot be avoided;
     - Reducing, or eliminating, any technical limitations currently in place for any, or all, alternate network options.
  2. Report on Recommendations for Preventing Adverse Impacts on PSAPs and NG911 from 911 Calls Made Through Alternative Network Options, **March 2026**
     - Providing PSAPs with actionable, accurate, information, including caller location and source (call type) of call when alternative network options are selected and utilized; and
     - Addressing any impacts, positive or negative, that these alternative network options might have on NG911.

Working Group 2 : Members

Brandon Abley: NENA (Co-chair)
Stephen Hayes: Ericsson (Co-chair)

- Rob Alderfer: Charter Communications
- Jeffrey Bratcher: FirstNet
- Wade Buckner: International Association of Fire Chiefs
- Kirk Burroughs: Apple Inc.
- Victor Burton: Comtech Telecommunications Corp.
- Douglas Campbell: Metropolitan Washington Airports Authority
- Stephen Devine: APCO International
- Stephen Edge: Qualcomm Incorporated
- Craig Fugate: America's Public Television Stations (APTS)
- Mike Gerber: National Weather Service
- Natnael Habtesion: Lumen
- Michael Hayes: Texas 9-1-1 Alliance
- Jeremy Hill: NTIA
- Karima Holmes: CISA
- Mike Hooker: T-Mobile USA
- George Kelemen: (iCERT)
- Lisa Madden: Motorola Solutions
- Christian Militeau: Bandwidth
- Leah Missildine: NASNA
- Peter Musgrove: AT&T
- Jared Owen: NTCA
- Chintan Patel: Verizon
- Tim Schram: NARUC
- Sean Scott: SecuLore
- Christiaan Segura: CTIA
- Dave Sehnert: RapidSOS
- John Snapp: Intrado
- Kelly Springer: ATIS
- Ashley Strickland: Tipton County Emergency Communications District
- Brian Tegtmeyer: U.S. Department of Transportation
- Fabricio Velez: INdigital
- Christy Williams: NCT911

Working Group 2 : Alternates*

- Waqas Ahmed, *CISA*
- Terri Brooks, *T-Mobile*
- Paul Brown, *Lumen*
- John Chiaramonte, *ICERT*
- Kate Elkins, *NHTSA*
- April Heinze, *NENA*
- Ryan Jensen, *ATIS*
- Lalit Kotecha, *Verizon*
- James B Ramsay, *NARUC*
- Praveen Srivastava, *Charter Communications*

* Alternates are not a member of the Working Group and may not vote.

Work Status on Deliverable #1 (June 2025)

- Work progressing on the document (Currently on rev 13)
- Weekly meetings to progress the document
- Structure of the document stable and most of the early sections are done
- Work currently focused on the analysis section of the report
- Responsibilities have been allocated and are being integrated into the document
- Each new alternate access (satellite, private networks, wifi, sidelink, etc.) presents unique challenges and configurations with respect to network selection – triggering lively discussions
  - Capabilities, limitations, and availability of different access technologies
  - Device capabilities with respect to different accesses
  - Network configurations and capabilities
  - User behavior and perceptions
- Work on track to meet June timeframe

Presentations

- Already Presented:
  - 2025-03-05: NTN Overview (T-Mobile)
  - 2025-03-12: Calls from Different Devices on CPE (Intrado)
- Upcoming:
  - 2025-04-02: E911 over Sidelink (Qualcomm)
  - Date tbd: Emergency services over Satellite (AT&T)

Discussion / Feedback

Thank you!

Working Group #3 :
Preparing for 6G Security and Reliability

March 19, 2025

Co-Chairs: Brian Daly (AT&T), George Woodward (Rural Wireless Association, Inc.)

FCC Liaison: Jeffrey Goldthorp

Working Group #3 Charter & Tasks Review

- The Chairwoman of the FCC directs CSRIC IX to examine and address security and reliability risks unique to emerging 6G networks and services.
- CSRIC IX will develop a plan for the development and deployment of reliable and security 6G networks and services that minimize privacy risks.
- 6G networks are at least seven years from commercial deployment, but wireless technology moves at such a brisk pace that the Commission is compelled to seek early recommendations from stakeholders that will lead to more secure and reliable 6G networks and services.
- 6G is expected to result in orders of magnitude improvements in network speed and latency, enabling capabilities that cause distinctions between the physical and cyber worlds to fade.
- CSRIC IX will make an early foray into examining and addressing potential security and reliability risks in emerging 6G networks and service.

Milestone: Report on Potential Security and Reliability Risks in 6G and Recommendations for Mitigation, December 2025

Working Group #3: Members

Alexandra Blasgen	Consumer Technology Association
Leonid Burakovsky	Palo Alto Networks
Afeite Dadja	CTIA
Robert Dew	Cybersecurity and Infrastructure Security Agency
Paul Eisler	USTelecom – The Broadband Association
Robert Gazda	InterDigital
Anu Jagannath	ANDRO
Puneet Jain	Intel
Virendra Kumar	Qualcomm
Michael Lijenstram	Ericsson
Jason Livingood	Comcast
Martin McGrath	Nokia
Susan Miller	ATIS
Douglas Montgomery	NIST
Harish Negalaguli	Motorola Solutions
Anthony Petrovich	Mavenir Systems, Inc.
Abir Ray	Expression Networks LLC
Michael Regan	Telecommunications Industry Association
Travis Russell	Oracle Communications
Yousif Targali	Verizon
Peter Thermos	Palindrome Technologies
Jean C. Trakinat	T-Mobile USA
Douglas Varney	USCellular

Co-Chairs:

Brian Daly	AT&T
George Woodward	Rural Wireless Association, Inc.
Jeffrey Goldthorp	FCC Liaison

Working Group #3: Alternates*

Anmol Agarwal, *Nokia*
Colin Andrews, *TIA*
J. David Grossman, *CTA*
Taylor Hartley, *Ericsson*
Abhijeet Kolekar, *Intel Corporation*
Andrezj Osinski, *CISA*
Justin Perkins, *CTIA*
Michael Salmon, *Verizon*
Gregory Schumacher, *ATIS*
Kathleen S Thompson, *USTelecom*

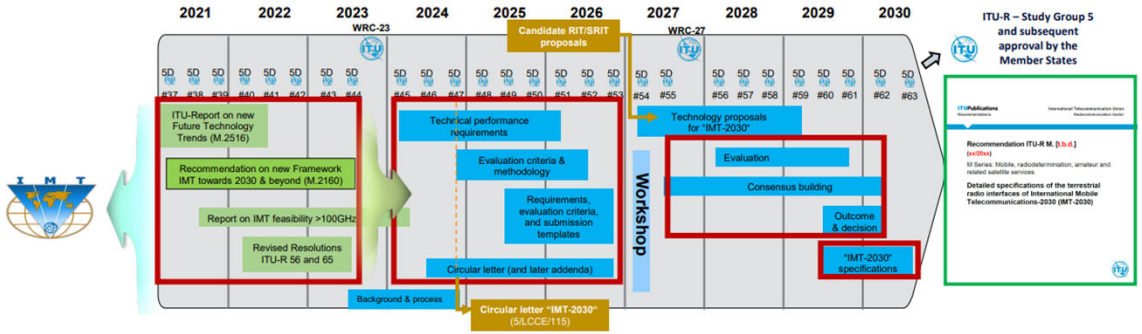
* Alternates are not a member of the Working Group and may not vote.

Working Group #3 Status

- Bi-weekly virtual meetings have continued
- Subject Matter Experts invited for presentation to the working group:
  - 6G Threat Analysis
  - 6G Sensing and Security
  - “Security first” Approach to 6G
  - Post Quantum Cryptography as it applies to 5G and 6G mobile Networks
- Working group deliverable is in progress

Understand 6G Timelines, Use Cases, Architecture and Features

ITU-R Timeline and Process

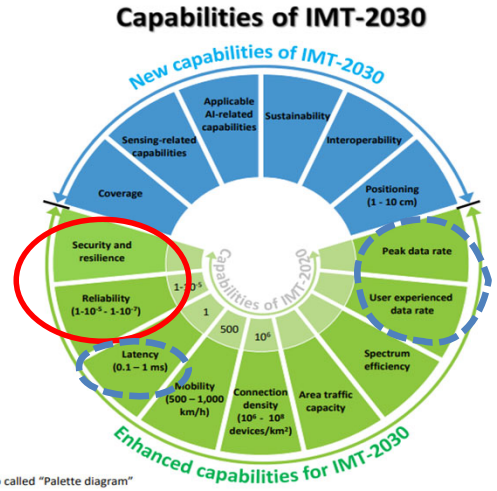


Note 1: WP 5D #59 will additionally organize a workshop involving the Proponents and registered Independent Evaluation Groups (IEGs) to support the evaluation process

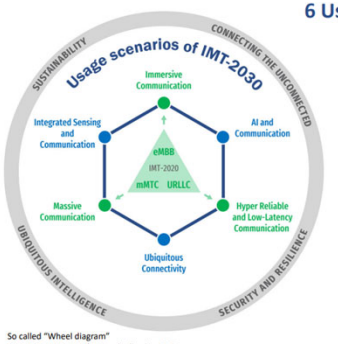
Note 2: While not expected to change, details may be adjusted if warranted. Content of deliverables to be defined by responsible WP 5D groups

Framework → **Requirements and Evaluation criteria** → **Evaluation and Consensus building** → **Specification** → **Approval**

Capabilities of IMT-2030



So called "Palette diagram"



So called "Wheel diagram"
Source: Document 5/131 and edited in SG 5

6 Usage scenarios

Extension from IMT-2020 (5G)

- eMBB → Immersive Communication
- mMTC → Massive Communication
- URLLC → HRLLC (Hyper Reliable & Low-Latency Communication)

New

- Ubiquitous Connectivity
- AI and Communication
- Integrated Sensing and Communication

4 Overarching aspects:

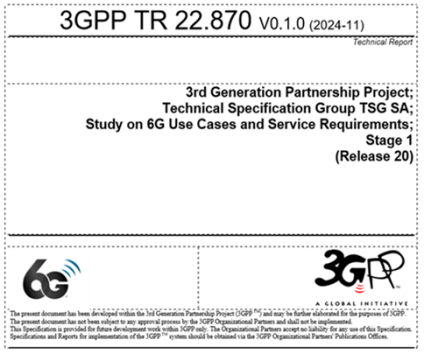
act as design principles commonly applicable to all usage scenarios

Sustainability, Connecting the unconnected, Ubiquitous intelligence, Security/resilience

CSRIC
Communications Security, Reliability and Interoperability Council

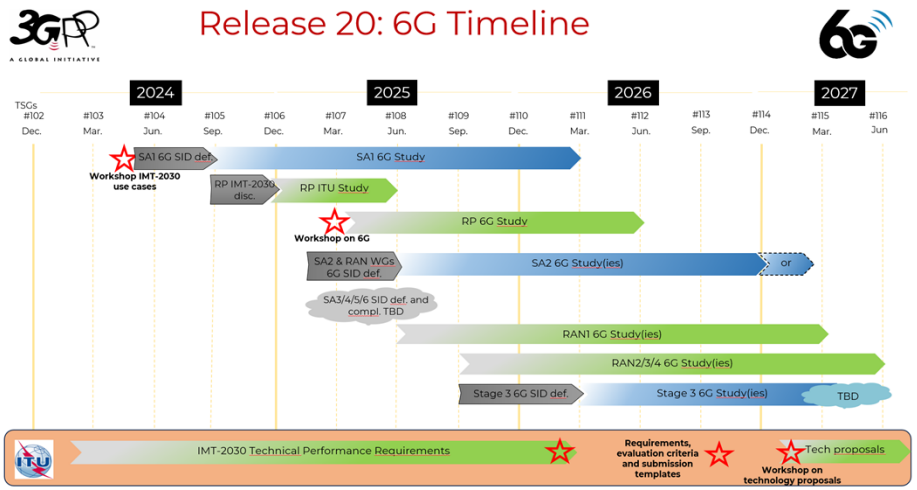
Understand 6G Timelines, Use Cases, Architecture and Features

- SA1 6G study on use cases and service requirements was approved at TSG SA#105 (SP-241391). The 6G RAN Study (part I: ITU focused) was approved at TSG RAN#106 (RP-243327)
- Technical studies on the 6G radio interface and 6G core network architecture within the RAN and SA Working Group to start in June 2025.
- Release 21 will be the official start of normative 6G work and is expected to produce the first formal 6G technical specifications, aligning with IMT-2030 submission requirements.
- The Release 21 timeline is expected to be finalized no later than June 2026, with ASN.1/OpenAPI freezes projected no earlier than March 2029.


3GPP TR 22.870 V0.1.0 (2024-11)

Technical Report

3rd Generation Partnership Project;
Technical Specification Group TSG SA;
Study on 6G Use Cases and Service Requirements;
Stage 1
(Release 20)



3GPP 6G Workshop

3GPP 6G Workshop was held March 10-11, 2025, in Incheon, Korea

- Opportunity for 3GPP members to present their vision & priorities for next generation radio technology, system architecture, core network and protocols.
- 1,676 **registrations**, 748 **in-person** registrants
- 219 input **contributions** from **operators**, **vendors**, **academia**, **and MRPs**
- Discussions covering **radio**, **core network**, **protocols**, **and more**

6G Security & Resilience Goals

- Increased security, integrity, and privacy are required from day one, incorporating zero trust principles and post-quantum security measures.
- Designing networks that are robust and can withstand various events, including operational errors, heavy traffic, and disasters.

Can threat modeling be used to identify threats to 6G?

Threat Modeling Overview

- **Definition:**
  - **Structured representation of information impacting application security.**
  - **Views the application and its environment through a security lens.**
- **Process:**
  - **Captures, organizes, and analyzes security-related information.**
  - **Enables informed decision-making about application security risks.**
- **Outcomes:**
  - **Produces a threat model.**
  - **Generates a prioritized list of security improvements for concept, requirements, design, or implementation.**

The need for threat mitigations can be identified in one of two ways:

- **After an attack and damage has occurred (reactive)**
- **Before an attack and damage can occur (predictive) – identify likely attacks and associated risks**

3GPP TR 33.926 Security Assurance Specification (SCAS) threats and critical assets in 3GPP network product classes defines a generic set of threats for SCAS verification.

- **STRIDE - Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege.**

Threat Modeling: What can this WG do to address 6G security and privacy risks and the 6G threat landscape?

For 6G, a comprehensive and multi-faceted threat modeling approach would be ideal to address the complex and evolving security requirements of next-generation mobile networks.

When CSRIC addressed a similar question about 5G threats and mitigations, 5G security was already well defined and developed, and CSRIC recommendations focused on what optional security capabilities 5G networks should implement as a best practice.

The challenge - 6G security (standards) will not be at this stage for several years.

- **Threat models dependent on a system architecture por data flows, which have not been developed for 6G.**

What should be the focus on the working group?

- **Select a set of 6G services and use one or more of the threat modeling methods which aren't dependent on system architectures or data flows – attack trees, CVSS, PnG, security cards, hTMM**
- **Select the same set of 6G services and develop negative use cases as an input to future 6G threat modeling**
- **Not focus on 6G architecture, rather cover emerging security directions that are expected to be reaching widespread deployment during the 6G timespan such as Zero Trust and Quantum Safe Cryptography. The coverage can be on the aspects that should be designed into 6G from the start (and not included in 5G or made optional due to legacy 5G network impacts (bolt on))**
- **Focus on negative use case development and threat modeling processes as recommendations for improving 6G security development**
- **Others??**

Integrated Sensing & Communications (ISaC)

- **Sensing: Gather a mapping of the environment, determine the location, speed, and direction of passive “non-connected” objects**
- **Integrated sensing: Sensing functionality as an integrated part of the communication network**
- **ISaC is a potential feature to develop as an add-on for 5G or as part of 6G**

Monitoring UAV activities, tracking hostile drones., e.g., around restricted zones such as airports, infrastructure, possibly even nation-wide.

Sensing for UAVs: ISAC can enable UAVs to operate in all conditions by augmenting onboard sensors with network-based sensing capabilities.

ISAC's integrated positioning and sensing in smart factory halls add a layer of visibility by sensing all objects on the factory floor or in a warehouse.

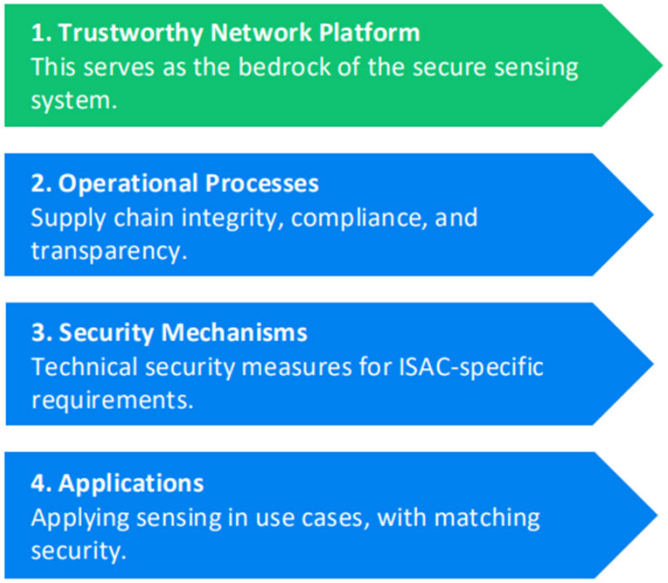
This visibility can be used for autonomous mobile robot collision avoidance, potentially eliminating the need for security cages.

ISAC can complement sensors onboard vehicles that increase safety for the transport and automotive sectors.

The transition to automated systems working as copilots or autopilots requires accurate information on the surrounding environment.

Building a Secure Sensing (ISaC) System

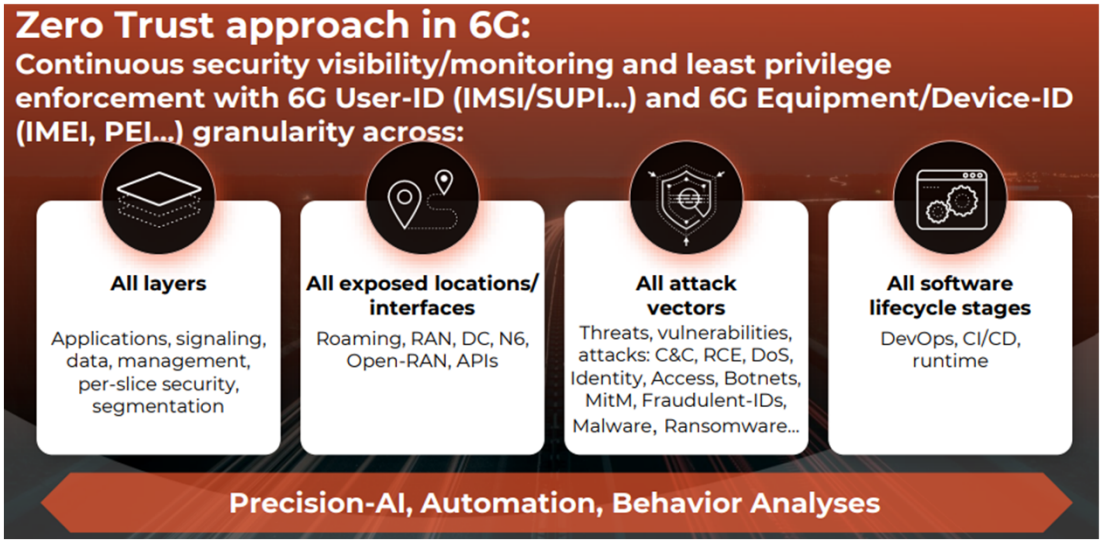
- **Framework of 4 layers:**
  - **Ensure that the network is inherently designed to support security, privacy, reliability, availability, and robustness.**
  - **A secure foundation offering end-to-end reliability, resilience against threats, and adherence to privacy-by-design principles.**
  - **Implementation of strong supply chain controls to prevent vulnerabilities.**
  - **Enforce access controls and authorization mechanisms.**
  - **Protect sensing information at rest, in transit and use.**
  - **Apply privacy-enhancing technologies (PETs) to secure sensitive data during sensing.**
  - **Ensure data provenance and integrity to validate the authenticity and source of collected data.**
  - **Deploy sensing technology in scenarios where it adds measurable value (e.g., environmental monitoring, critical infrastructure).**
  - **Address specific security and privacy needs for each use case, ensuring trust and compliance**



New features such as ISaC may add new needs, threats, solutions, and considerations.

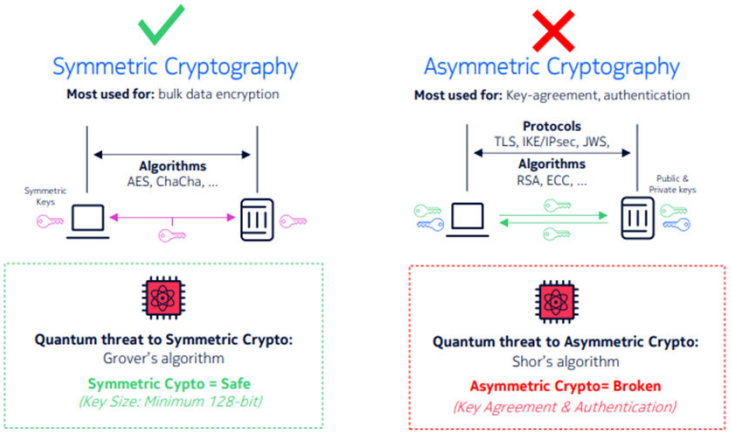
6G Security: A New Approach is Needed

- **“Security-First” approach in 6G**
  - Complement the existing focus on improvements in speeds, latency, coverage, and other connectivity elements.
- **6G should adopt a Zero Trust from the very beginning:**
  - In the 6G Service Requirements
  - In the 6G Reference Architecture



Post Quantum Cryptography

- **The threat: Cryptographic Relevant Quantum Computers (CRQCs) break widely-used asymmetric cryptography ("public key cryptography")**
  - **Symmetric crypto ("secret key cryptography") solutions are still considered safe, however**
- **Asymmetric Cryptography used extensively in mobile network infrastructure/devices today**
- **Asymmetric Cryptography currently used in 5G expected to be also leveraged in 6G**
- **Goal - secure against both quantum and classical computers and deployable without drastic changes to existing communication protocols and networks.**

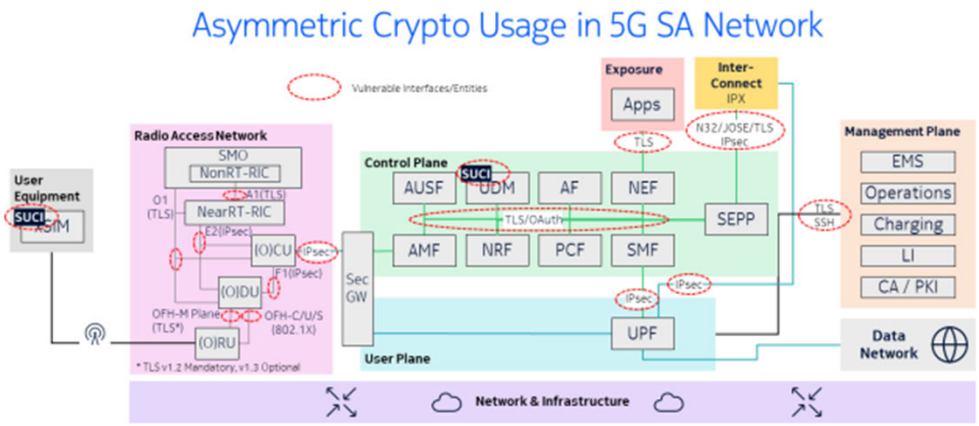


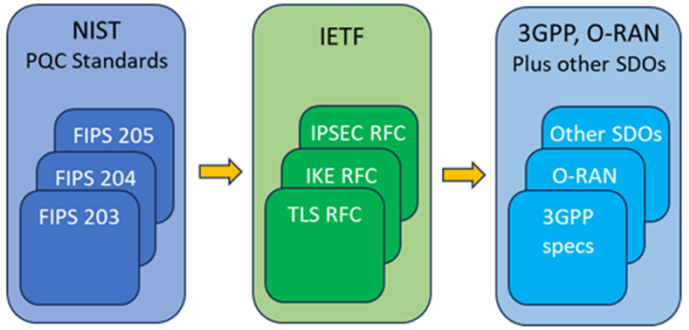
Quantum Security Threats

- **Harvest-Now, Decrypt-Later (HNDL):**
  - **Attackers capture encrypted data today to decrypt it once a Cryptographically Relevant Quantum Computer (CRQC) is available.**
  - **Significant threat for long-term confidential data.**
- **Quantum Decryption:**
  - **Decryption by a CRQC may take time but can eventually intercept and decrypt communications.**
  - **Attackers gain access to sensitive information without detection.**
- **Quantum-Impersonation Attack:**
  - **Adversaries use quantum capabilities to exploit public key cryptographic systems.**
  - **Allows impersonation of legitimate users, enabling unauthorized actions like signing documents or deceptive communications.**
- **Quantum Man-in-the-Middle (QMITM):**
  - **Similar to classical MITM, but with CRQC, attackers can tamper with or alter messages between two parties.**
- **Side-Channel Attacks:**
  - **Exploit indirect information (timing, power consumption, electromagnetic emissions).**
  - **Threat to both classical and Post-Quantum Cryptography (PQC) algorithms.**

Post Quantum Cryptography & Mobile systems

- **Security Protocols vulnerable include:**
  - **TLS, IPsec, N32, OAuth, X.509, PKI, JWS, JWE…**
- **SUPI privacy protection broken**
  - **HN Private/Public Key pair generated using Asymmetric Key Agreeme Crypto (e.g. ECDHE)**
- **There is Standards work addressing the Quantum Computer Threat**
  - **NIST PQC Standardization Program**
  - **IETF making strong progress in adoption of NIST PQC standards**
- **3GPP is expected to undertake first PQC studies in 6G Rel20 and define normative specifications in 6G Rel21**
- **O-RAN Alliance PQC plans undecided but crypto inventor study ongoing**
- **ATIS report - Preparing 5G for the Quantum Era: An Analysis of 3GPP Architecture and the Transition to Quantum-Resistant Cryptography**
- **5G Americas paper "Post Quantum Computing Security"**
- **GSMA Post-Quantum Telco Network Task Force & Post Quantum Telco Network Impact Assessment Whitepaper**





Deliverables/Schedule

- Virtual meetings scheduled on a bi-weekly basis.
  - Continue subject matter expert presentations on specific topics or research areas are scheduled
  - ATIS workspace set up for document management and collaboration
- **Deliverable**: Report on Potential Security and Reliability Risks in 6G and Recommendations for Mitigation.
- **Deliverable Schedule**: December 2025

Discussion / Feedback

Thank you!