CSRIC

Communications Security, Reliability and Interoperability Council

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

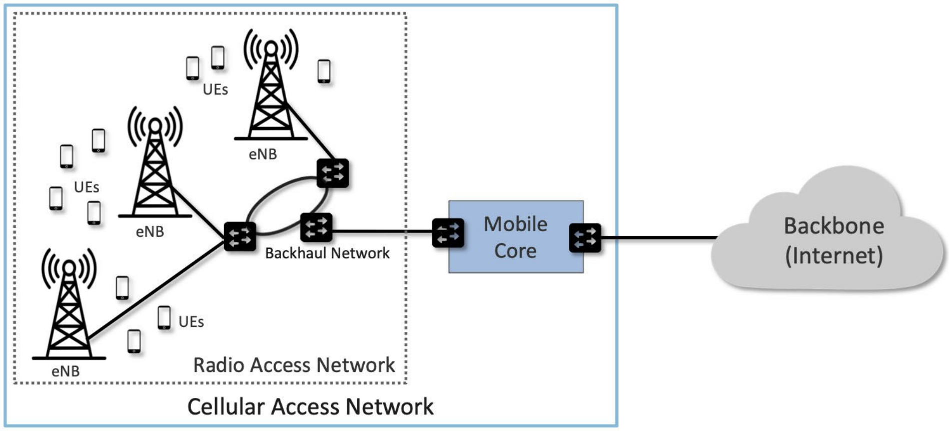
December 18, 2024

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

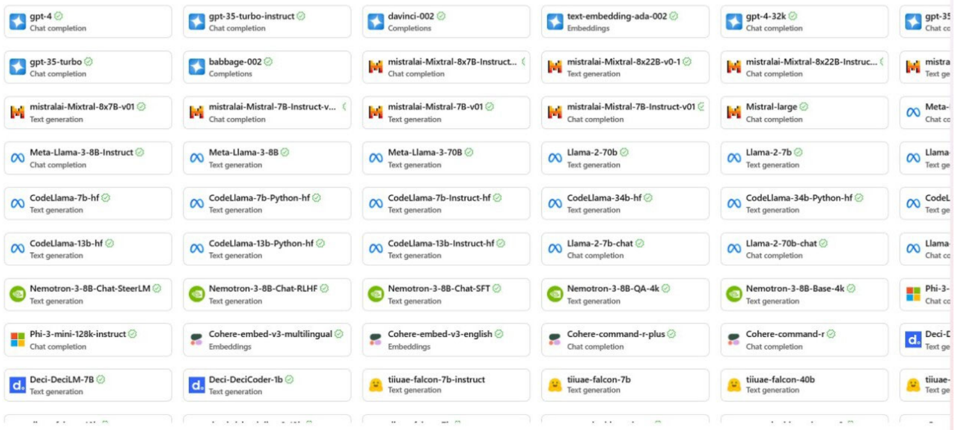
FCC Liaison: Zenji Nakazawa

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/

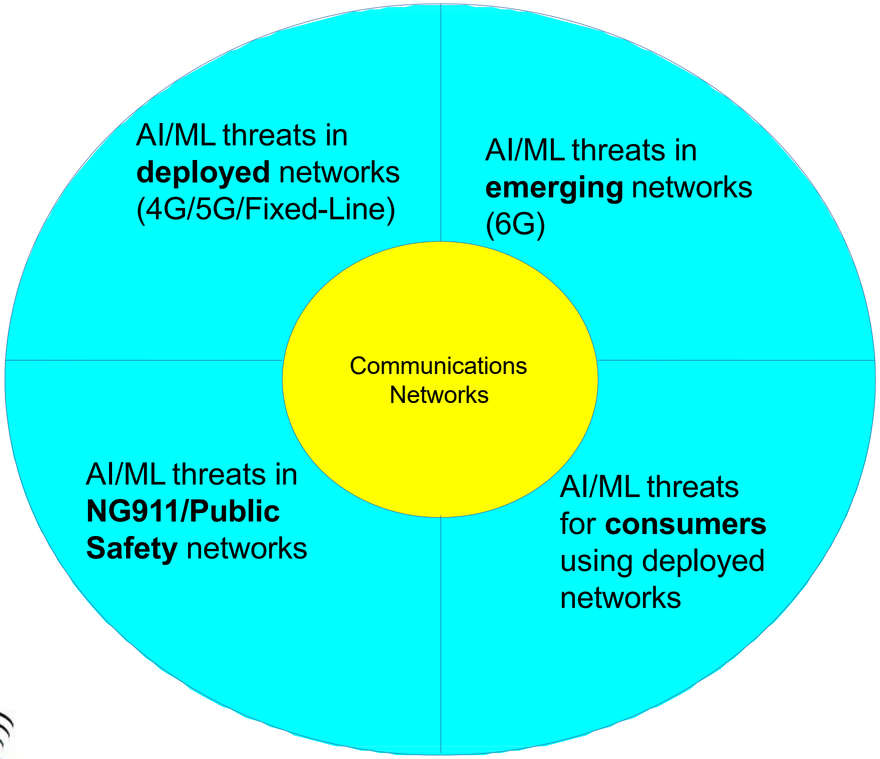


gpt-4 Chat completion	gpt-35-turbo-instruct Chat completion	davinci-002 Completions	text-embedding-ada-002 Embeddings	gpt-4-32k Chat completion	gpt-35 Chat cc
gpt-35-turbo Chat completion	babbage-002 Completions	mistralai-Mixtral-8x7B-Instruct... Chat completion	mistralai-Mixtral-8x22B-v0-1 Text generation	mistralai-Mixtral-8x22B-Instruc... Chat completion	mistra Text ge
mistralai-Mixtral-8x7B-v01 Text generation	mistralai-Mistral-7B-Instruct-v... Chat completion	mistralai-Mistral-7B-v01 Text generation	mistralai-Mistral-7B-Instruct-v01 Chat completion	Mistral-large Chat completion	Meta- Chat cc
Meta-Llama-3-8B-Instruct Chat completion	Meta-Llama-3-8B Text generation	Meta-Llama-3-70B Text generation	Llama-2-70b Text generation	Llama-2-7b Text generation	Llama Text ge
CodeLlama-7b-hf Text generation	CodeLlama-7b-Python-hf Text generation	CodeLlama-7b-Instruct-hf Text generation	CodeLlama-34b-hf Text generation	CodeLlama-34b-Python-hf Text generation	CodeL Text ge
CodeLlama-13b-hf Text generation	CodeLlama-13b-Python-hf Text generation	CodeLlama-13b-Instruct-hf Text generation	Llama-2-7b-chat Chat completion	Llama-2-70b-chat Chat completion	Llama Chat cc
Nemotron-3-8B-Chat-SteerLM Text generation	Nemotron-3-8B-Chat-RLHF Text generation	Nemotron-3-8B-Chat-SFT Text generation	Nemotron-3-8B-QA-4k Text generation	Nemotron-3-8B-Base-4k Text generation	Phi-3- Chat cc
Phi-3-mini-128k-instruct Chat completion	Cohere-embed-v3-multilingual Embeddings	Cohere-embed-v3-english Embeddings	Cohere-command-r-plus Chat completion	Cohere-command-r Chat completion	Deci-D Text ge
Deci-DeciLM-7B Text generation	Deci-DeciCoder-1b Text generation	tiiuae-falcon-7b-instruct Text generation	tiiuae-falcon-7b Text generation	tiiuae-falcon-40b Text generation	tiiuae- Text ge

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


AI/ML threats in **deployed** networks (4G/5G/Fixed-Line)
AI/ML threats in **emerging** networks (6G)
Communications Networks
AI/ML threats in **NG911/Public Safety** networks
AI/ML threats for **consumers** using deployed networks

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*

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*

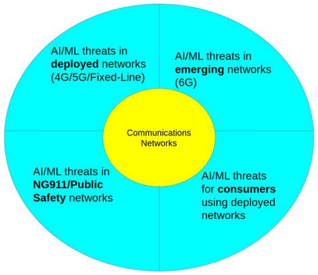
Lei Yu, *Expression Networks LLC*

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

Update since Sep 2024

- 33 members
- 15 alternates
- Weekly meetings after WG was vetted, first one on Oct-03
- 1 interim meeting – Dec-10
- Editor team identified for the first deliverable
- Work is divided into 13 *Technical Areas*

Technology Area Teams


AI/ML threats in **deployed** networks (4G/5G/Fixed-Line)
AI/ML threats in **emerging** networks (6G)
Communications Networks
AI/ML threats in **NG911/Public Safety** networks
AI/ML threats for **consumers** using deployed networks

Area	Lead	Members
UE Handset	Salman Marvasti	Jonathan Petit
Audio + Speech	Luiz Eduardo	Jonathan Petit, Craig Bowman
UE IoT	Bob Everson	Dongsong Zeng, David Valdez
Business Support Systems	Peter Santhanam	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

Threats for consumers

Threats in deployed networks

Threats in emerging networks

Threats in NG911/Public Safety networks

Technology Area Work Plan

- Each TA is headed by a lead
- Goal of TAs
  - First order goal: Investigate the use of AI/ML in that area and arrive at a set of scenarios to document the risks of AI/ML.
  - High order goal: Take 2-3 scenarios that are representative of the use and risks posed by AI/ML for a further critical analysis.
- The higher-order goal feeds into the first deliverable as recommendations.

High-level Schedule

Target Date	Goal
October 3	Identify Core Technology Focus Areas and Conduct Research
October 31	Develop Report Outline
Nov 1 – Nov 30	Assay Key Technology Area Functions and AI/ML Scenarios
December 13	Build and Fine Tune AI/ML Use Case Portfolios Across Technology Focus Areas
Dec 16 – Jan 14	Deep Analysis of Use Cases and First Draft Writing Period
January 15	Submit First Drafts of Technology Area Segments
Jan 16 – Jan 31	Coalesce Threats and Recommendations
February 7	Complete First Draft - Pens Down
February 26	Final Draft Delivered to DFO Cameron
March 5	Final Draft Transmitted to Council by DFO Cameron
March 19	CSRIC IX Meeting – Report Presentation to Council for Deliberation and Vote

Detailed Team Update

Area	Lead	Members	Scenarios Created (PPT)	Scenarios Peer Reviewed	Detailed Content (Word)	Detail Content Peer Reviewed
UE Handset	Salman Marvasti	Jonathan Petit	12/10/2024	12/12/2024	1/1/2025	1/15/2025
Audio + Speech	Luiz Eduardo	Jonathan Petit, Craig Bowman	COMPLETE			1/15/2025
UE IoT	Bob Everson	Dongsong Zeng, David Valdez	12/13/2024			1/11/2025
Business Support Systems	Peter Santhanam	Travis Russell, Travis Reuter				1/15/2025
Contact center operations	Peter Santhanam	Travis Russell, Travis Reuter				1/15/2025
5G OSS	Praveen Atreya	Abir Ray, Travis Russell, Yong Kim, Henry Young				1/15/2025
5G RAN	Abir Ray	Andrew Drozd, Mike Barnes, Christina Chaccour, Martin McGrath, Richard Baron				1/15/2025
5G Backhaul	Bob Everson	Rob Cantu, Rikin Thakker, Dongsong Zeng				1/15/2025
5G Core	Timothy May	Narothum Saxena, Travis Reutter, Mike Barnes, Christina Chaccour, Martin McGrath, Bob Everson, Praveen Atreya, Travis Russell	12/13/24	By 12/20/24	By 1/8/25	1/15/2025
Network Interconnection	Luiz Eduardo	Salman Marvasti, Travis Reutter, Travis Russell				1/15/2025
Wireline Networks	Robert Cantu	Rikin Thakker, Travis Russell				1/15/2025
6G Networks	Andy Drozd	Christina Chaccour, Martin McGrath, Travis Russell				1/15/2025
Public safety networks	Mark Grubb (?)	Mark Annas, Devin Christensen, Brian Murray, Chris Bennett, Craig Bowman, Peter Scott, Patrick Arsenault, Rob Cantu, Rikin Thakker				1/15/2025

Example Analysis (1): RAN Energy Savings

No	Use case	What is the AI doing?	What is the threat?	How to mitigate?
1	Energy Saving	Energy Efficiency (EE) system in RAN optimizes power consumption across network elements while maintaining Quality of Service (QoS). • Collects real-time traffic patterns and network performance metrics • Predicts traffic loads and required capacity • Dynamically adjusts power states of radio elements • Controls sleep modes and carrier shutdowns • Manages multiple-input multiple-output (MIMO) configurations	a) Data Poisoning Attacks • Adversaries could inject manipulated traffic pattern data during model training • Impact: Models could make incorrect predictions leading to: • Unnecessary power-downs during high traffic periods • Excessive power consumption during low-demand periods • Service disruptions due to misconfigured sleep modes b) Model Evasion Attacks Attackers might craft adversarial inputs to fool the traffic prediction models • Example: Injecting specific traffic patterns that trigger unnecessary power-saving modes • Impact: Service degradation in specific geographic areas • Increased power consumption due to frequent mode switching • Customer experience deterioration	Mitigation Strategies a) Data Protection • Implement robust validation for training data sources • Deploy anomaly detection for real-time telemetry Establish data integrity checks for historical records b) Model Security • Regular retraining with validated data sets • Implementation of model validation frameworks Monitoring of model prediction patterns for anomalies c) Operational Controls • Rate limiting on power state changes • Multi-factor validation for significant configuration changes Geographic correlation checks for power optimization decisions d) Architectural Safeguards • Distributed model deployment with local validation • Hierarchical decision-making with oversight • Fallback mechanisms for suspicious behavior

Example Analysis (2): BSS

No	Use case	What is the AI doing?	What is the risk?	How to mitigate?
5 (TM Forum)	Lead Generation for Enterprise Markets: Enhances the ability of sales teams to identify high-potential leads, particularly in the SME sector, driving revenue growth.	*GenAI application* Analyzes market data and customer behavior to provide actionable sales insights.	The system may produce wrong recommendations.	- Quantify the system performance with proper benchmarks. - Make sure proper trust attributes (e.g. source attribution and explainability, etc.) are produced with the recommendation. - Include learning mechanisms to improve the performance over time.
6 (TM Forum)	Publishing BSS Knowledge for Business Users: Facilitates access to relevant business information, enhancing decision-making and operational efficiency.	*GenAI application.* Synthesize and publish BSS knowledge for business users.	The system may produce wrong/inappropriate information.	- Quantify the system performance with proper benchmarks. - Make sure proper trust attributes (e.g. source attribution, explainability, etc.) are produced with the recommendation. - Include learning mechanisms to improve the performance over time.
7 (TM Forum)	Intelligent Field Operation Assistance: Optimizes field operations, reducing costs and improving service delivery through quicker fault detection and resolution.	*Agents based Mixture of Experts AI application.* Provides real-time support and decision-making tools for field maintenance engineers (FMEs), enhancing operational efficiency.	- Complex application needing significant investment - The system may produce wrong recommendations.	- Quantify the system performance with proper benchmarks. - Make sure proper trust attributes (e.g. source attribution, explainability, etc.) are produced with the recommendation. - Include learning mechanisms to improve the performance over time.

Discussion / Feedback

Thank you!

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

December 18, 2024

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.

CSRIC Communications Security, Reliability and Interoperability Council

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
- Steve Watkins: Cox Communications
- Christy Williams: NCT911

Working Group 2 : Alternates*

- Waqas Ahmed, *CISA*
- Terri Brooks, *T-Mobile*
- 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

- Work is proceeding at a good clip
- Entire report 1 and 2 outlined
- 5-10% of report 1 is already drafted
- Contributions in progress for ~30% of the full report
- The group meets weekly; meetings are energetic and effective
- Meetings paused through December to accommodate holidays

Report 1 Content (Heading level 1 only)

- Technical Background
- Backup Networks Available for 9-1-1
- Prioritization of Backup network Options
- 9-1-1 Alternate Access Scenarios
- Intelligent Network Selection
- Limitations in use of Backup Networks
- Callbacks
- Class of Service and Method Tokens
- Information Delivered to PSAPs

* ~50 subheadings not shown here

Next Steps

- Review current outstanding contributions to text
- Continue drafting document sections assigned to authors
- Build on work from CSRIC VIII report on WiFi for 9-1-1
- Invite experts to consult on new technologies and backup access methods
- Workgroup generally has sufficient expertise to complete the work, but some ultra-specialist input is needed from private sector partners

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

December 18, 2024

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
Puneet Jain	Intel
Anu Jagannath	ANDRO Computational Solutions, LLC
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

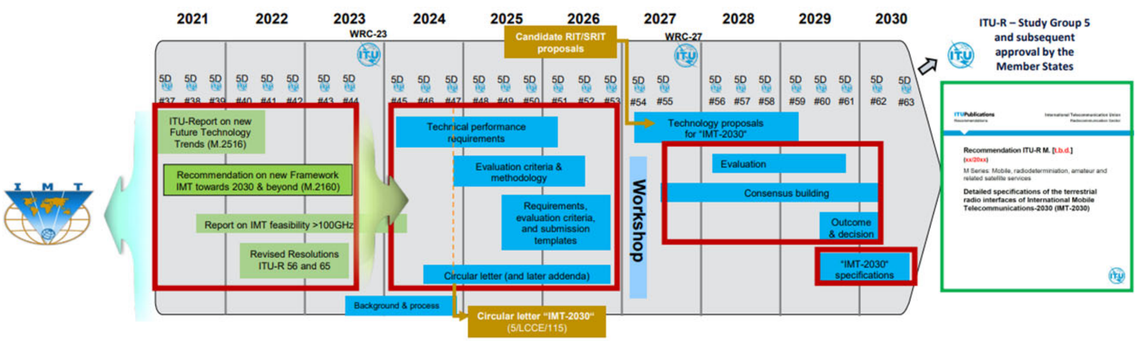
- Bi-weekly virtual meetings are being held
- Subject Matter Experts invited for presentation to the working group:
  - 6G Threat Analysis
  - Considerations of the threat vectors in 6G and mitigations such as zero trust
  - 6G Sensing and Security
- Draft outline developed for the working group deliverable

Draft Outline - Potential Security and Reliability Risks in 6G and Recommendations for Mitigation

- Section 1- Understand 6G Timelines, Use Cases, Architecture and Features
- Section 2 - Define the 6G Threat Landscape- Identify Potential Threats
- Section 3. Analyze Threats
- Section 4 - Identify Vulnerabilities
- Section 5 - Evaluate Impact and Likelihood
- Section 6 - Evaluate Existing Controls
- Section 7 - Develop Mitigation Strategies
- Section 8 - Continuous Monitoring and Updating
- Section 9 – Reliability and Resiliency
- Section 10 - Collaboration and Standardization
- Section 11. Advisements and Recommendations

Understand 6G Timelines, Use Cases, Architecture and Features

ITU-R Timeline and Process

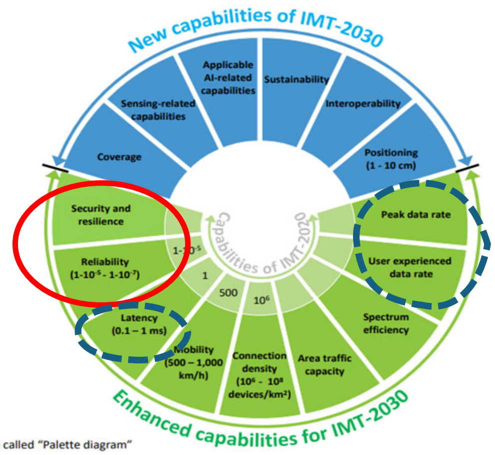

2021
2022
2023
2024
2025
2026
2027
2028
2029
2030
WRC-23
WRC-27
Candidate RIT/SRIT proposals
5D #37 #38 #39 #40 #41 #42 #43 #44 #45 #46 #47 #48 #49 #50 #51 #52 #53 #54 #55 #56 #57 #58 #59 #60 #61 #62 #63
ITU-Report on new Future Technology Trends (M.2516)
Recommendation on new Framework IMT towards 2030 & beyond (M.2160)
Report on IMT feasibility >100GHz
Revised Resolutions ITU-R 56 and 65
Background & process
Technical performance requirements
Evaluation criteria & methodology
Requirements, evaluation criteria, and submission templates
Circular letter (and later addenda)
Circular letter "IMT-2030" (5/LCCE/115)
Workshop
Technology proposals for "IMT-2030"
Evaluation
Consensus building
Outcome & decision
"IMT-2030" specifications
ITU-R – Study Group 5 and subsequent approval by the Member States
ITUPublications
Recommendation ITU-R M. [t.b.d.]
(xx/20xx)
M Series: Mobile, radiodetermination, amateur and related satellite services
Detailed specifications of the terrestrial radio interfaces of International Mobile Telecommunications-2030 (IMT-2030)

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

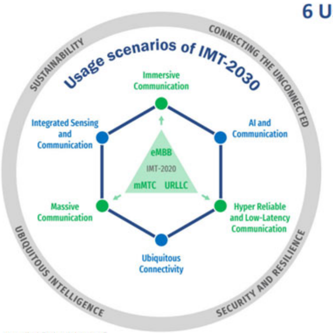
Note 2: While not expected to change, details may be adjusted if warranted. Content of deliverables to be defined by responsible WP 5D groups

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

Capabilities of IMT-2030


New capabilities of IMT-2030
Coverage
Sensing-related capabilities
Applicable AI-related capabilities
Sustainability
Interoperability
Positioning (1 - 10 cm)
Security and resilience
Reliability (1-10⁻⁵ - 1-10⁻⁷)
Latency (0.1 – 1 ms)
Mobility (500 – 1,000 km/h)
Connection density (10⁶ - 10⁸ devices/km²)
Area traffic capacity
Spectrum efficiency
User experienced data rate
Peak data rate
Capabilities of IMT-2020
1-10⁻⁵
1
500
10⁶
Enhanced capabilities for 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

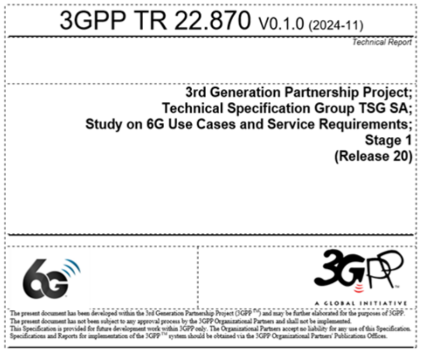
4 Overarching aspects:

act as design principles commonly applicable to all usage scenarios

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

Understand 6G Timelines, Use Cases, Architecture and Features

- Rel-20 SA1 6G study has started
- Rel-20 content to be decided in 1H2025
- Release 20 content defined in two steps with 5G Advanced and 6G work staggered and decisions made separately
- 3GPP workshop on 6G to be held in March 2025
  - Vision & Priorities for the Next Generation
  - RAN, System Architecture, Core Network & Protocols
- Rel-21 will have the specification work on 6G and the TSG RAN IMT-2030 submission



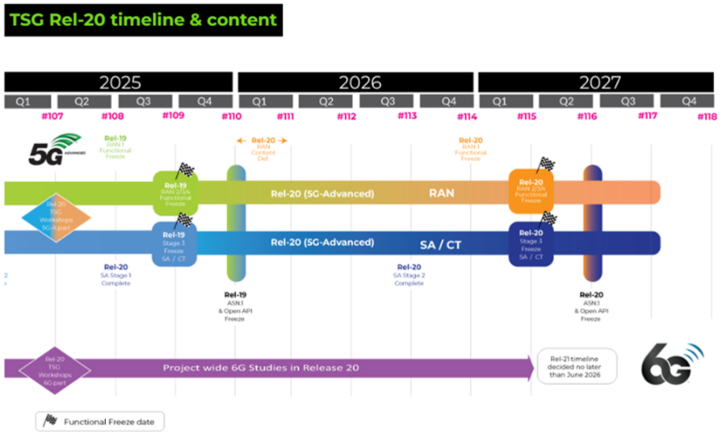
3GPP TR 22.870 V0.1.0 (2024-11)

Technical Report

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

A GLOBAL INITIATIVE

The present document has been developed within the 3rd Generation Partnership Project (3GPP TM) and may be further elaborated for the purposes of 3GPP.
The present document has not been subject to any approval process by the 3GPP Organizational Partners and shall not be implemented.
This Specification is provided for future development work within 3GPP only. The Organizational Partners accept no liability for any use of this Specification.
Specifications and Reports for implementation of the 3GPP TM system should be obtained via the 3GPP Organizational Partners' Publications Offices.


TSG Rel-20 timeline & content
2025
2026
2027
Q1
Q2
Q3
Q4
Q1
Q2
Q3
Q4
Q1
Q2
Q3
Q4
#107
#108
#109
#110
#111
#112
#113
#114
#115
#116
#117
#118
5G ADVANCED
Rel-19 RAN 1 Functional Freeze
Rel-20 RAN Content Def.
Rel-20 RAN 1 Functional Freeze
Rel-19 RAN 2/3/4 Functional Freeze
Rel-20 (5G-Advanced)
RAN
Rel-20 RAN 2/3/4 Functional Freeze
Rel-20 TSG Workshops 5G-A part
Rel-19 Stage 3 Freeze SA / CT
Rel-20 (5G-Advanced)
SA / CT
Rel-20 Stage 3 Freeze SA / CT
Rel-20 SA Stage 1 Complete
Rel-20 SA Stage 2 Complete
Rel-19 ASN.1 & Open API Freeze
Rel-20 ASN.1 & Open API Freeze
Rel-20 TSG Workshops 6G part
Project wide 6G Studies in Release 20
Rel-21 timeline decided no later than June 2026
6G
Functional Freeze date

Understand 6G Timelines, Use Cases, Architecture and Features

- **Very Early** Insights into the 3GPP SA1 Study related to the WG charter:
  - **Network Security for 6G**
    - It is expected that cellular networks become "more secure" with each subsequent generation
    - Networks are becoming more complex, with 6G also seeming to be a convergence of disparate technologies (e.g., information, operation, communication), complicating the ecosystem with their differences in approaches, threats, disciplines, and capabilities
    - The mobile communication ecosystem needs to enhance security and privacy, embracing new security paradigms, techniques, and leveraging evolving security technologies
    - It is expected that cloud deployments will play an even more important role in 6G
    - 6G network must provide trust and security mechanisms for secure access to and communication with network elements
  - **Quantum-resistant security**
    - Quantum computing technology poses significant threats to some classical cryptography
    - 6G system should provide security protection for communication against the potential attacks posed by quantum computing

Understand 6G Timelines, Use Cases, Architecture and Features

- **Very Early** Insights into the 3GPP SA1 Study related to the WG charter:
  - **False Base Station Attack Mitigation**
    - False Base Station (FBS) attacks and its potential to cause active and passive impacts are an alarming concern worldwide
    - Increasing the level of security between the radio network entities and the UE during the initial network selection procedure, may be possible to prevent false Base Station at earlier stages of communication establishment
    - Subject to operator policy and regulatory requirements, the 6G system should support a means for a UE to be able to distinguish a false base station from an authentic base station
  - **Resilient positioning in satellite networks**
    - Dependency on GNSS results in major threats and risks, in case of unavailability or disruption of GNSS (jamming, spoofing or obstructions)
    - 6G system with satellite access may provide positioning service with 3GPP technologies, independently of non-3GPP positioning technologies (e.g. GNSS)

Understand 6G Timelines, Use Cases, Architecture and Features

- **Very Early** Insights into the 3GPP SA1 Study related to the WG charter:
  - **Disaster Relief**
    - Resiliency when the terrestrial network is down, and "terrestrial" mobile service is not available in the area
    - Look for alternative available network(s) in the area, such as satellite access and HAPS based access networks
    - Public warning service (i.e., Wireless Emergency Alerts) to the impacted area
  - **AI**
    - APIs to allow authorized third parties to retrieve availability information about computational resources
    - Monitoring and reporting of computational resource usage in the operator managed data network
  - **Other possible use cases with security implications:**
    - Immersive Communication
    - Integrated Sensing and Communication
    - Low-altitude UAV supervision

Deliverables/Schedule

- Virtual meetings scheduled on a bi-weekly basis.
  - Subject matter expert presentations on specific topics or research areas are scheduled
  - ATIS workspace set up for document management and collaboration
- 2-day face-to-face meeting (with virtual option) scheduled in January (Alpharetta, GA)
- **Deliverable**: Report on Potential Security and Reliability Risks in 6G and Recommendations for Mitigation.
- **Deliverable Schedule**: December 2025

Thank you!