



# International Network Generations Roadmap

*-2021 Edition-*

# Security and Privacy



*An IEEE 5G and Beyond Technology Roadmap*  
[futurenetworks.ieee.org/roadmap](https://futurenetworks.ieee.org/roadmap)

Wi-Fi® and Wi-Fi Alliance® are registered trademarks of Wi-Fi Alliance.

The IEEE emblem is a trademark owned by the IEEE.

"IEEE", the IEEE logo, and other IEEE logos and titles (IEEE 802.11™, IEEE P1785™, IEEE P287™, IEEE P1770™, IEEE P149™, IEEE 1720™, etc.) are registered trademarks or service marks of The Institute of Electrical and Electronics Engineers, Incorporated. All other products, company names or other marks appearing on these sites are the trademarks of their respective owners. Nothing contained in these sites should be construed as granting, by implication, estoppel, or otherwise, any license or right to use any trademark displayed on these sites without prior written permission of IEEE or other trademark owners.

This edition of the INGR is dedicated to the memory of Earl McCune Jr., who left us tragically and too soon on 27 May 2020. Earl was a microwave/RF guru, brilliant technologist, major industry/IEEE contributor, global visionary, keen skeptic, and all around fantastic human being. He was a major contributor to the INGR's early work on energy efficiency, millimeter-wave, and hardware. He worked for a technologically advanced yet more energy efficient world, and the contents of the INGR are a tribute to that vision. Rest in peace, Earl!



# Table of Contents

<b>1. Introduction</b>	<b>1</b>
<b>2. Working Group Vision</b>	<b>3</b>
Scope of Working Group Effort	5
Linkages and Stakeholders	7
<b>3. Today's Landscape</b>	<b>9</b>
Current State of Technology and Research	9
<b>4. Future State (2031)</b>	<b>11</b>
Reference Architecture	11
<b>5. Foundational Concepts</b>	<b>12</b>
System Setup and Threat Model	12
Cybersecurity Frameworks	14
Cyber Risk Management Framework and Methodology	15
<b>6. Security and Privacy Domains</b>	<b>16</b>
Management and Orchestration Security	17
Virtualization / Softwarization Security	17
SDN Security	20
Network Slicing Security	21
Edge Security	23
Third Party Security	25
Supply Chain Security	25
Open Source / Application Programmable Interface (API) Security	26
Device / Hardware Security	26
Data Privacy and Security	26
Satellite Security	27
Virtualized Radio Access Network Security	27
Massive MIMO Security	29
mmWave Security	29
Spectrum Security	29
Physical Layer Security	29
Security Monitoring and Analytics	30
Predictive / Proactive Security	31
Digital Forensic Solutions for 5G	31
<b>7. Security Use-Cases for various Verticals</b>	<b>31</b>
Application Security Requirements	31
Critical Infrastructure Systems Security	32
5G and Critical Infrastructure Amalgamation	32
Smart Grid Use Case	32

Emergency and First-Responder Networks Security	35
Autonomous Vehicles, V2X Security	35
<b>AI/ML Security</b>	<b>37</b>
<b>Interoperability</b>	<b>40</b>
<b>Industrial Control Systems (ISC): Industrial IoT Based SCADA</b>	<b>40</b>
<b>Safety and Security</b>	<b>40</b>
<b>Challenges and Opportunities</b>	<b>41</b>
<b>Categories of risk in the IIoT</b>	<b>43</b>
<b>8. Standardization Opportunities</b>	<b>44</b>
<b>9. Needs, Challenges, and Enablers and Potential Solutions</b>	<b>45</b>
<b>Summary</b>	<b>45</b>
<b>10. Conclusions and Recommendations</b>	<b>50</b>
<b>Summary of Conclusions</b>	<b>50</b>
<b>Working Group Recommendations</b>	<b>50</b>
Future Work	51
<b>11. Contributors</b>	<b>52</b>
IEEE ComSoc North America Regional Board, TelNet Management Consulting, Inc.	52
<b>12. References</b>	<b>53</b>
<b>13. Acronyms/abbreviations</b>	<b>55</b>

## Tables

Table 1. Standards Organizations	8
Table 2. Selected 5G threat Scenarios	13
Table 3. Threats for Scada Systems	42
Table 4. Proactive Security for 5G-IoT—Needs, Challenges, Enablers, and Potential Solutions	45
Table 5. AI/ML Security – Needs, Challenges, Enablers and Potential Solutions	47
Table 6. Digital Forensics Solutions for 5G Environments—Needs, Challenges, and Enablers and Potential Solutions	48

## Figures

Figure 1. Key dimensions of 5G Networks, courtesy of 5G Lab Germany [4].	2
Figure 2. 5G & Beyond: Security Perspective, the progress of the 5G and beyond revolution may well be hindered if security issues are not tackled early on while the systems are being designed, standardized and deployed.	3
Figure 3. 3GPP security architecture	11
Figure 4. 5G Threat Model	12
Figure 5. NIST CSF Framework [12].	15
Figure 6. Risk assessment process [13].	16
Figure 7. Generic risk model with key factors [13].	16
Figure 8. 5G Security Pillars	17
Figure 9. Potential security issues with virtualization	18
Figure 10. SDN Security - Select Cyber Risk Scenarios and Potential Mitigations	20
Figure 11. Network Slicing Security	22
Figure 12. Network Slicing Security – Select Risk Scenarios and Potential Mitigations	22
Figure 13. Mobile Edge Security Context	24
Figure 14. Mobile Edge Security - Select Cyber Risk Scenarios and Potential Mitigations	24
Figure 15. GEO (Geosynchronous Orbit), HEO (Highly Elliptical Orbit), MEO (Medium Earth Orbit), LEO (Low Earth Orbit), and HAP (High Altitude Platforms) [14].	27
Figure 16. O-RAN Architecture	28
Figure 17. Cloud RAN Security - Select Cyber Risk Scenarios and Potential Mitigations	28
Figure 18. Proactive 5G security	31
Figure 19. Critical Infrastructure Inter-dependencies [1].	33
Figure 20. First Responder Use Case on Orchestration	35
Figure 21. Architecture of the Machine Learning Function Orchestrator [15].	38
Figure 22. IoT security Solution.	42
Figure 23. IIoT based Scada Risk by Threats	44



## ABSTRACT

The digital transformation brought on by 5G is redefining current models of end-to-end (E2E) connectivity and service reliability to include security-by-design principles necessary to enable 5G to achieve its promise. 5G trustworthiness highlights the importance of embedding security capabilities from the very beginning while the 5G architecture is being defined and standardized. Security requirements need to overlay and permeate through the different layers of 5G systems (physical, network, and application) as well as different parts of an E2E 5G architecture within a risk-management framework that takes into account the evolving security-threats landscape. 5G presents a typical use-case of wireless communication and computer networking convergence, where 5G fundamental building blocks include components such as Software Defined Networks (SDN), Network Functions Virtualization (NFV) and the edge cloud. This convergence extends many of the security challenges and opportunities applicable to SDN/NFV and cloud to 5G networks. Thus, 5G security needs to consider additional security requirements (compared to previous generations) such as SDN controller security, hypervisor security, orchestrator security, cloud security, edge security, etc. At the same time, 5G networks offer security improvement opportunities that should be considered. Here, 5G architectural flexibility, programmability and complexity can be harnessed to improve resilience and reliability.

The working group scope fundamentally addresses the following:

- 5G security considerations need to overlay and permeate through the different layers of the 5G systems (physical, network, and application) as well as different parts of an E2E 5G architecture including a risk management framework that takes into account the evolving security threats landscape.
- 5G exemplifies a use-case of heterogeneous access and computer networking convergence, which extends a unique set of security challenges and opportunities (e.g. related to SDN/NFV and edge cloud, etc.) to 5G networks. Similarly, 5G networks by design offer potential security benefits and opportunities through harnessing the architecture flexibility, programmability and complexity to improve its resilience and reliability.
- The IEEE FNI security WG's roadmap framework follows a taxonomic structure, differentiating the 5G functional pillars and corresponding cybersecurity risks. As part of cross collaboration, the security working group will also look into the security issues associated with other roadmap working groups within the IEEE Future Network Initiative.

Key words:

5G Cybersecurity, security, privacy, data protection, reliability, resilience, mMTC, URLLC, SDN/NFV, cyber risk assessment and management, threat scenarios, cyber attacks, security controls, mitigation, defense.

This file is a free sample of this chapter.  
The full chapter is available exclusively to signed-in participants of the [IEEE Future Networks Community](#).