

# 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.

[Click here to join the Future Networks Technical Community](#) (free for any sponsoring IEEE Society member, and low-cost for non-members), then return to the [INGR page](#) to download full chapters.



International Network Generations Roadmap

Would you like to join an INGR Working Group?

[Click here](#) for contact information for each group.

**Interested in booking a private session with INGR experts for your company? Contact an IEEE Account Manager to discuss an INGR Roadmap Virtual Private Event.**

+1 800 701 4333 (USA/Canada)  
+1 732 981 0060 (worldwide)

[onlinesupport@ieee.org](mailto:onlinesupport@ieee.org)





# IEEE INGR))

**International Network  
Generations Roadmap  
*2023 Edition***

# Security and Privacy



*An IEEE Future Networks Technology Roadmap*  
[futurenetworks.ieee.org/roadmap](http://futurenetworks.ieee.org/roadmap)

## 2 Introduction

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.

Copyright © 2023

# Table of Contents

1.	Introduction .....	8
1.1.	2023 Edition Update .....	10
2.	Working Group Vison .....	11
2.1.	The Big Picture for Security .....	11
2.2.	Vision for a Successful Future Network Industry .....	11
2.3.	Three, Five, and Ten Year Goals .....	11
2.4.	Security's Projected Impact .....	12
2.5.	Scope of Working Group Effort .....	12
2.6.	Linkages and Stakeholders .....	15
2.7.	Working Group Summary of Activities .....	17
3.	Today's Landscape .....	18
3.1.	Current State of Technology and Research .....	18
3.2.	Future Considerations .....	19
4.	Future State (2033) .....	21
4.1.	Reference Architecture .....	21
5.	Foundational Concepts .....	23
5.1.	System Setup and Threat Model .....	23
5.2.	Cybersecurity Frameworks .....	24
5.3.	Cyber Risk Management Framework and Methodology .....	25
5.4.	Emerging Security Frameworks / Approaches / Architectures .....	27
5.4.1.	Zero-Trust (ZT) Security Architecture for NFVi .....	27
6.	Security and Privacy Domains .....	30
6.1.	Management and Orchestration Security .....	30
6.1.1.	Virtualization / Softwarization Security .....	31
6.1.2.	SDN Security .....	33
6.1.3.	Network Slicing Security .....	34
6.2.	Edge Security .....	36
6.3.	Third-Party Security .....	37
6.3.1.	Supply Chain Security .....	37
6.3.2.	Open Source .....	38
6.3.3.	Protocol & Application Programmable Interface (API) Security .....	38
6.3.4.	Device / Hardware Security .....	41
6.4.	Data Privacy and Security .....	42
6.5.	Satellite Security .....	42
6.6.	Virtualized Radio Access Network Security .....	43
6.7.	Massive MIMO Security .....	44
6.8.	mmWave Security .....	45
6.9.	Spectrum Security .....	45
6.10.	Physical Layer Security .....	45
6.10.1.	Physical Layer Security for 6G .....	45

## 4 Introduction

6.11.	AI/ML Security .....	47
6.12.	Cryptography and Post-Quantum Security .....	50
6.12.1.	Post-Quantum Cryptography .....	50
6.12.2.	Quantum Computing as a Threat to Classical Cryptography .....	50
6.12.3.	Ongoing Standardization Efforts.....	50
6.12.4.	Algorithms .....	50
6.12.5.	Practical Deployment Considerations .....	51
6.13.	Block Chain .....	53
6.14.	Security Operations & Incidence Response .....	55
6.14.1.	Security Monitoring and Analytics .....	55
6.14.2.	Predictive / Proactive Security .....	55
6.15.	Digital Forensic Solutions.....	56
6.15.1.	Incident Response (IR).....	56
6.15.2.	IR – Detection and Analysis .....	57
6.15.3.	Containment and Mitigation .....	57
6.15.4.	Recovery and Lessons Learned.....	58
6.15.5.	Offensive Security for 5G/6G .....	58
7.	Security Use-Cases for Various Verticals .....	61
7.1.	Application Security Requirements .....	61
7.2.	Interoperability.....	61
7.3.	Critical Infrastructure Systems Security .....	62
7.3.1.	Smart Grid Use Case.....	62
7.3.2.	U.S. 5G Strategy for National Network and Critical Infrastructure .....	63
7.3.3.	Emergency and First-Responder Networks Security .....	65
7.3.4.	Autonomous Vehicles, V2X Security .....	65
7.4.	Industrial Control Systems (ICS): Industrial IOT-Based SCADA .....	67
7.4.1.	Safety and Security .....	67
7.4.2.	Challenges and Opportunities .....	67
7.4.3.	Categories of Risk in the IIoT .....	69
8.	Standardization Opportunities .....	70
9.	Needs, Challenges, Enablers, and Potential Solutions.....	71
10.	Conclusions and Recommendations .....	76
10.1.	Summary of Conclusions .....	76
10.2.	Working Group Recommendations .....	76
10.3.	Future Work.....	77
11.	Contributor Bios .....	78
12.	References .....	83
13.	Acronyms / Abbreviations .....	85

## Tables

Table 1. Standards Organizations .....	16
--	----

Table 2. Selected 5G Threat Scenarios .....	24
Table 3. Mapping of Protocols and Network Functions .....	39
Table 4. HTTPv2 Vulnerability and its Effect of NS/EP Users (SBA Control Plane).....	39
Table 5. GTP Vulnerability and Its Effect on NS/EP Users (User Plane) .....	40
Table 6. API Vulnerability and its Effect on NS/EP Users (I).....	41
Table 7. API Vulnerability and its Effect on Users (II) .....	41
Table 8. Threats for SCADA Systems.....	69
Table 9. Proactive Security for 5G-IoT — Needs, Challenges, Enablers, and Potential Solutions .....	71
Table 10. AI/ML Security – Needs, Challenges, Enablers, and Potential Solutions .....	73
Table 11. Digital Forensics Solutions for 5G Environments—Needs, Challenges, Enablers, and Potential Solutions .....	74

## Figures

Figure 1. Key Dimensions of 5G/6G Networks (Source: 5G Lab German) <sup>[4]</sup> .....	9
Figure 2. Security Perspective .....	10
Figure 3. Key Pillars of Future Networks Security.....	13
Figure 4. 3GPP Security Architecture .....	21
Figure 5. 5G/6G Threat Model .....	23
Figure 6. NIST CSF Framework 2.0 <sup>[12]</sup> .....	25
Figure 7. Risk Assessment Process <sup>[13]</sup> .....	26
Figure 8. Generic Risk Model with Key Factors <sup>[13]</sup> .....	26
Figure 9. Comparison between CNF and VNF Virtualized Stack .....	27
Figure 10. Zero Trust Access <sup>[14]</sup> .....	28
Figure 11. Core Zero-Trust Logical Components <sup>[14]</sup> .....	28
Figure 12. Reference Zero-Trust Architecture for Cloud Native Application .....	29
Figure 13. 6G Security Pillars.....	30
Figure 14. Potential Security Issues with Virtualization.....	32
Figure 15. SDN Security - Select Cyber Risk Scenarios and Potential Mitigations .....	34
Figure 16. Network Slicing Security .....	35
Figure 17. Network Slicing Security – Select Risk Scenarios and Potential Mitigations .....	35
Figure 18. Mobile Edge Security Context .....	36
Figure 19. Mobile Edge Security - Select Cyber Risk Scenarios and Potential Mitigations .....	37
Figure 20. GEO (Geosynchronous Orbit), HEO (Highly Elliptical Orbit), MEO (Medium Earth Orbit), LEO (Low Earth Orbit), and HAP (High Altitude Platforms) <sup>[14]</sup> .....	42
Figure 21. O-RAN Architecture .....	43
Figure 22. Cloud RAN Security - Select Cyber Risk Scenarios and Potential Mitigations .....	44
Figure 23. Architecture of the Machine Learning Function Orchestrator <sup>[17]</sup> .....	48
Figure 25. Store and Share Data Securely .....	54
Figure 26. Proactive 5G Security .....	56
Figure 27. Critical Infrastructure Inter-Dependencies <sup>[1]</sup> .....	63
Figure 28. First Responder Use Case on Orchestration .....	65
Figure 29. IoT Security Solution .....	68

## 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 fulfill 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 5G systems (physical, network, and application) as well as different parts of the E2E 5G architecture including a risk management framework that considers 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 a cross-collaboration effort within IEEE FNI, the security working group also looks into the security issues associated with other roadmap working groups.

Disclaimer: in this document we use 5G to refer to future networks including evolution such as B5G, 6G, etc.

### **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.

## CONTRIBUTORS

Ashutosh Dutta	John's Hopkins University / Applied Physics Lab, Security Working Group Co-Chair
Eman Hammad	Texas A&M University, Security Working Group Co-Chair
Michael Enright	Quantum Dimension, Inc.
Fawzi Behmann	IEEE ComSoc North America Regional Board, TelNet Management Consulting, Inc.
Arsenia Chorti	ENSEA, CNRS
Ahmad Cheema	Shared Services Canada
Kassi Kadio	Shared Services Canada
Julia Urbina-Pineda	IEEE HKN Member and CyberIIoT CEO
Khaled Alam	Rogers Communications (Formerly)
Ahmed Limam	Higher Institute of Engineering and Technology (ESPRIT)
Fred Chu	University of California, Los Angeles
John Lester	Our Lady of Fatima University Valenzuela, Philippines
Jong-Geun Park	Seoul National University of Science and Technology
Joseph Bio-Ukeme	Carleton University
Sanjay S Pawar	Usha Mittal University of Technology
Roslyn Layton	Aalborg University
Prakash Ramchandran	Intel
Kingsley Okonkwo	Chevron
Lyndon Ong	Ciena
Marc Emmelmann	Fraunhofer FOKUS
Omneya Issa	Department of National Defence, Canada
Rajakumar Arul	Amrita Vishwa Vidyapeetham
Sireen Malik	T-Mobile
Sivarama Krishnan	National Library of Medicine
Suresh Sugumar	Intel Corporation
Tk Lala	ZecureZ Consulting Company
Baw Chng	Bawman LLC
Bharat Rawal	Gannon University
Taha Sajid	Comcast
Haobo Lai	Haobo Lai Associates
Glaucio Carvalho	Brock University
Matthew Borst	IEEE Future Networks Initiative
Brad Kloza	IEEE Future Networks Initiative

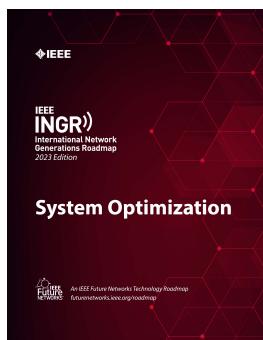
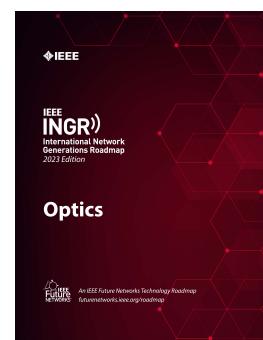
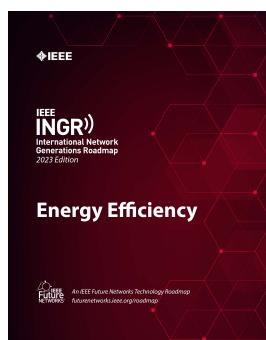
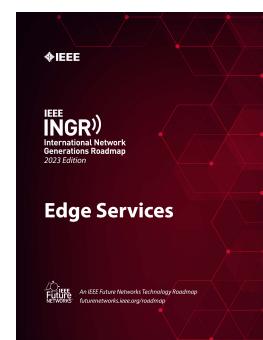
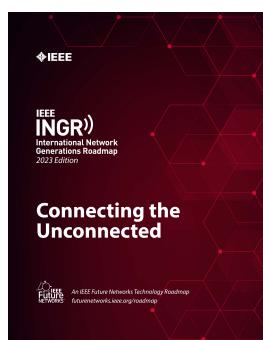
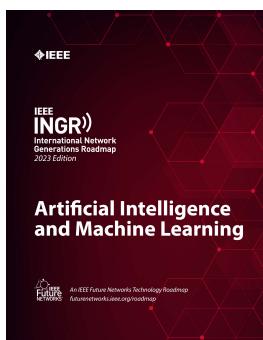
Want to read the full chapter?

Accessing full INGR chapters is easy and affordable.

## Step 1. [Click here to join Future Networks](#)

(free for any sponsoring IEEE Society member, and low-cost for non-members)

## Step 2. Return to the [INGR page](#) to download full chapters.



**14 chapters available!**