The bridge to possible

Post-Quantum Security in 5G

Ashish Kundu
Head of Cybersecurity Research
Cisco Research

ACM/IEEE 1st 5G Summit, June 14 ‘22

Space Communication Security (NASA)

If terrorists or hackers illegally listen to, or worse, modify communication content, disaster can occur.

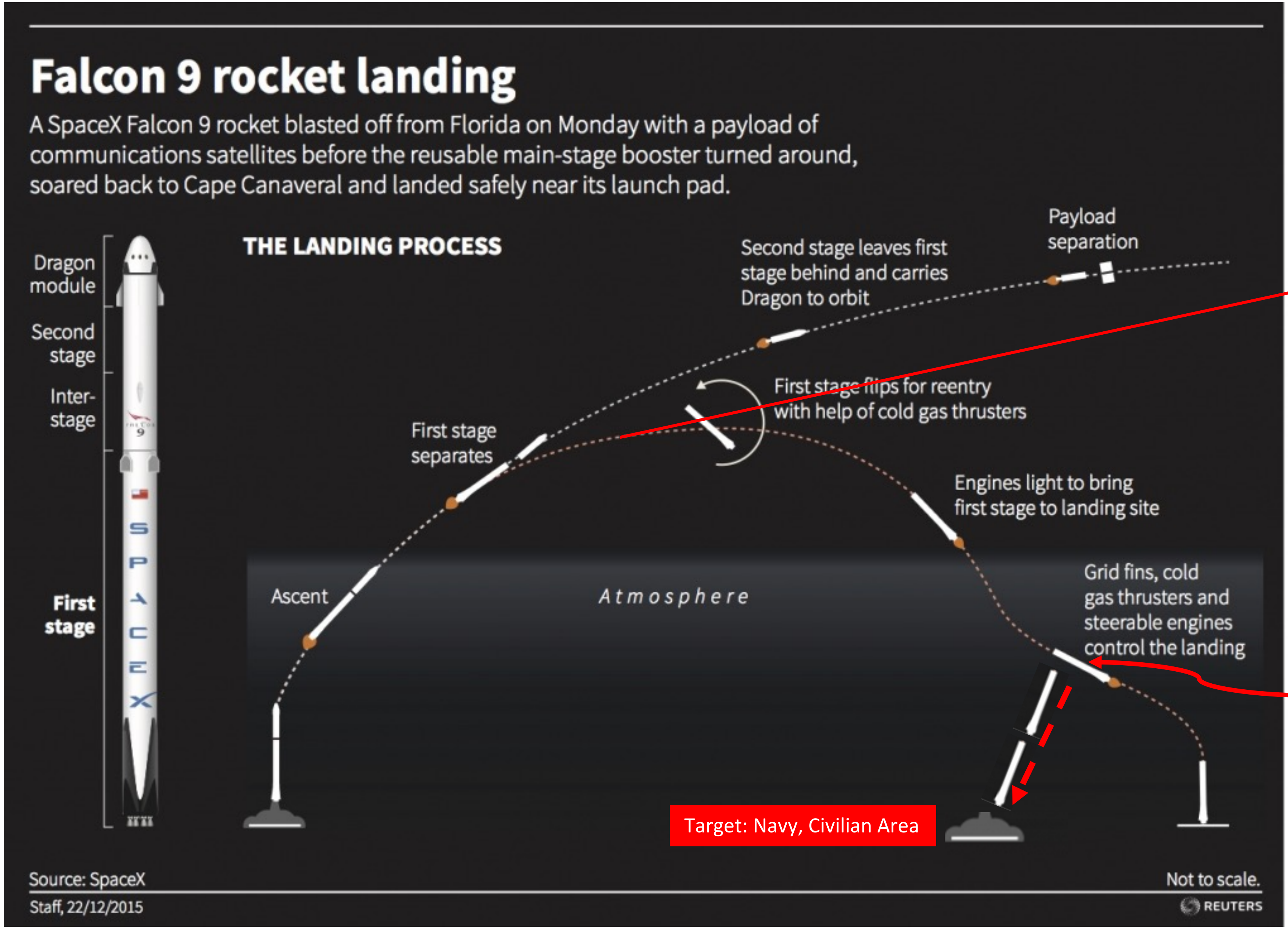
The consequences of a nuclear powered spacecraft under control of a hacker or terrorist could be devastating.

Therefore, all communications to and between spacecraft must be extremely **secure** *and* **reliable**.

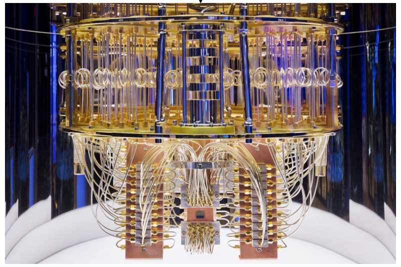
Source: NASA Ames Research Center
https://www.nasa.gov/centers/ames/research/technology-onepagers/secure_space_communication.html

PQC IKE draft here: https://tools.ietf.org/id/draft-tjhai-ipsecme-hybrid-qske-ikev2-03.html

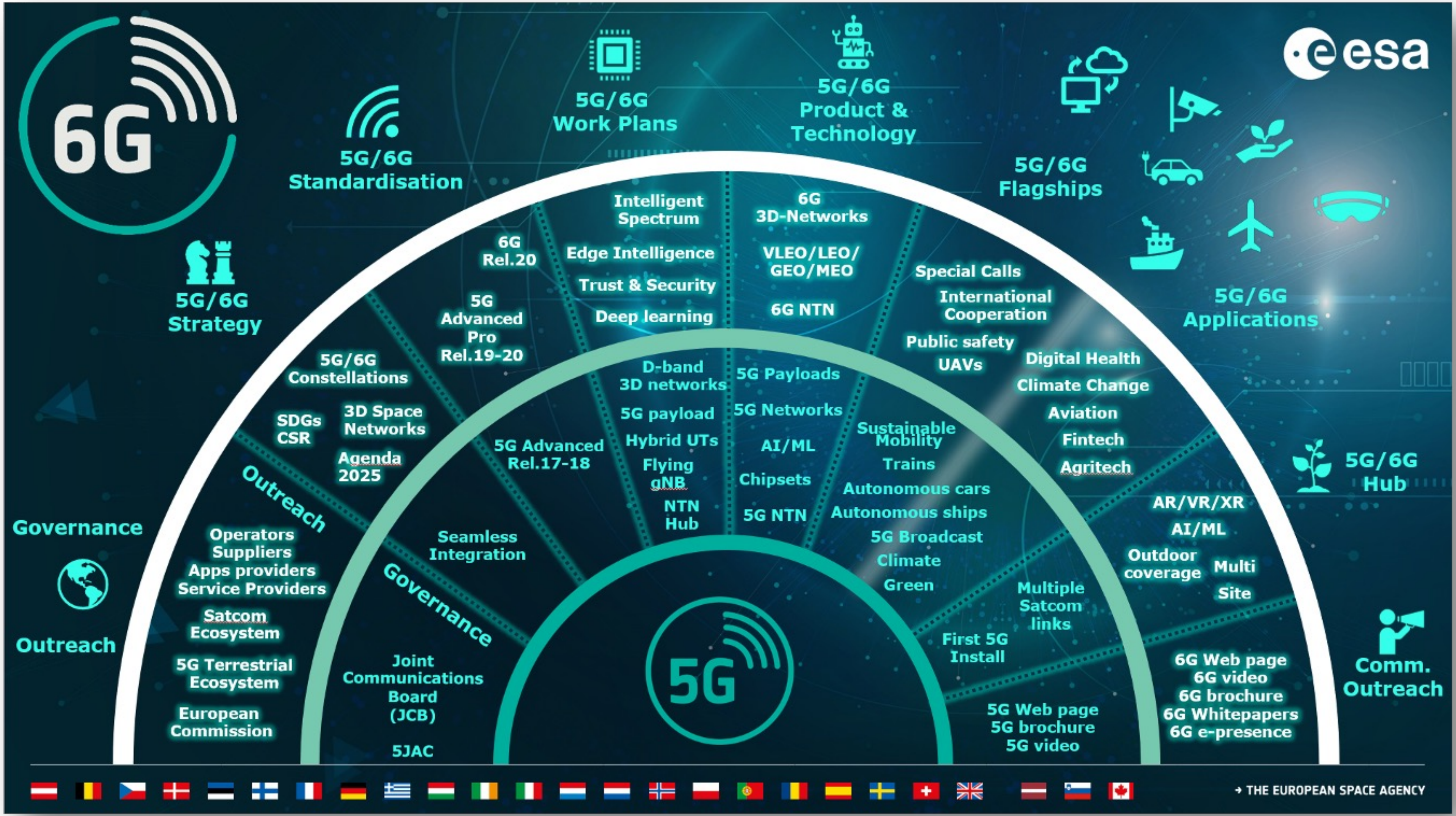
Quantum threat to communication



Encrypted Channel



- Rogue state/entity: break crypto using QC,
- command, capture,
- re-route



6G
5G/6G Standardisation
5G/6G Work Plans
5G/6G Product & Technology
5G/6G Flagships
esa
5G/6G Strategy
5G/6G Applications
5G/6G Hub
Governance
Outreach
Comm. Outreach
Intelligent Spectrum
Edge Intelligence
Trust & Security
Deep learning
6G 3D-Networks
VLEO/LEO/ GEO/MEO
6G NTN
6G Rel.20
5G Advanced Pro Rel.19-20
Special Calls
International Cooperation
Public safety
UAVs
Digital Health
Climate Change
Aviation
Fintech
Agritech
5G/6G Constellations
SDGs CSR
3D Space Networks
Agenda 2025
D-band 3D networks
5G payload
Hybrid UTs
Flying gNB
NTN Hub
5G Payloads
5G Networks
AI/ML
Chipsets
5G NTN
5G Advanced Rel.17-18
Sustainable Mobility
Trains
Autonomous cars
Autonomous ships
5G Broadcast
Climate
Green
AR/VR/XR
AI/ML
Outdoor coverage
Multi Site
Multiple Satcom links
First 5G Install
Outreach
Governance
Operators
Suppliers
Apps providers
Service Providers
Satcom Ecosystem
5G Terrestrial Ecosystem
European Commission
Seamless Integration
Joint Communications Board (JCB)
5JAC
5G
5G Web page
5G brochure
5G video
6G Web page
6G video
6G brochure
6G Whitepapers
6G e-presence
→ THE EUROPEAN SPACE AGENCY

Space, Satellites & 5G

Lockheed Martin partners with satellite start-up Omnispace to build a space-based 5G network

PUBLISHED TUE, MAR 23 2021·8:00 AM EDT | UPDATED TUE, MAR 23 2021·12:47 PM EDT

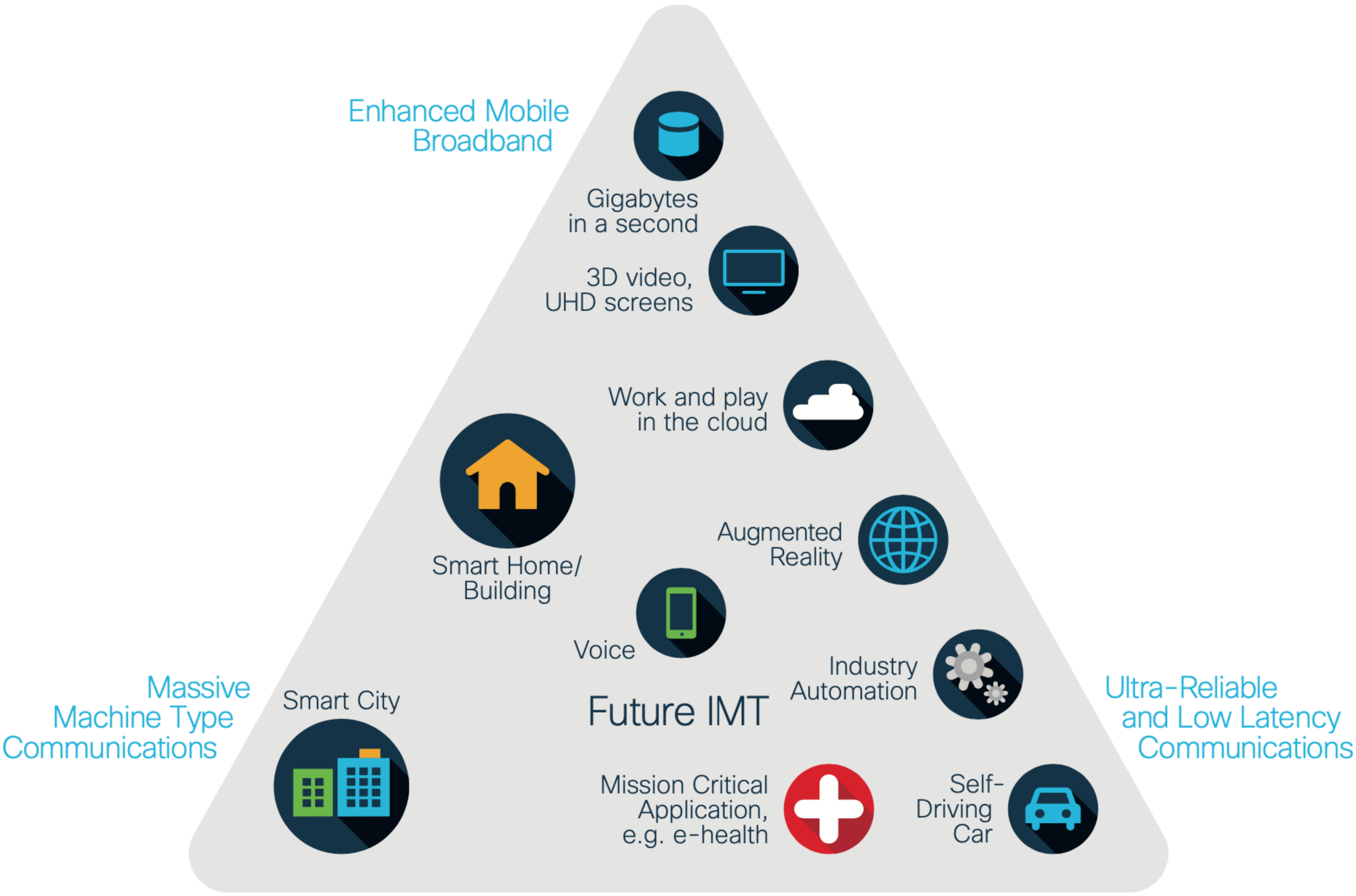
Space Companies Are Investing Big in 5G Technology

By Elizabeth Howell published October 20, 2019

Satellite internet is going to be a big thing.

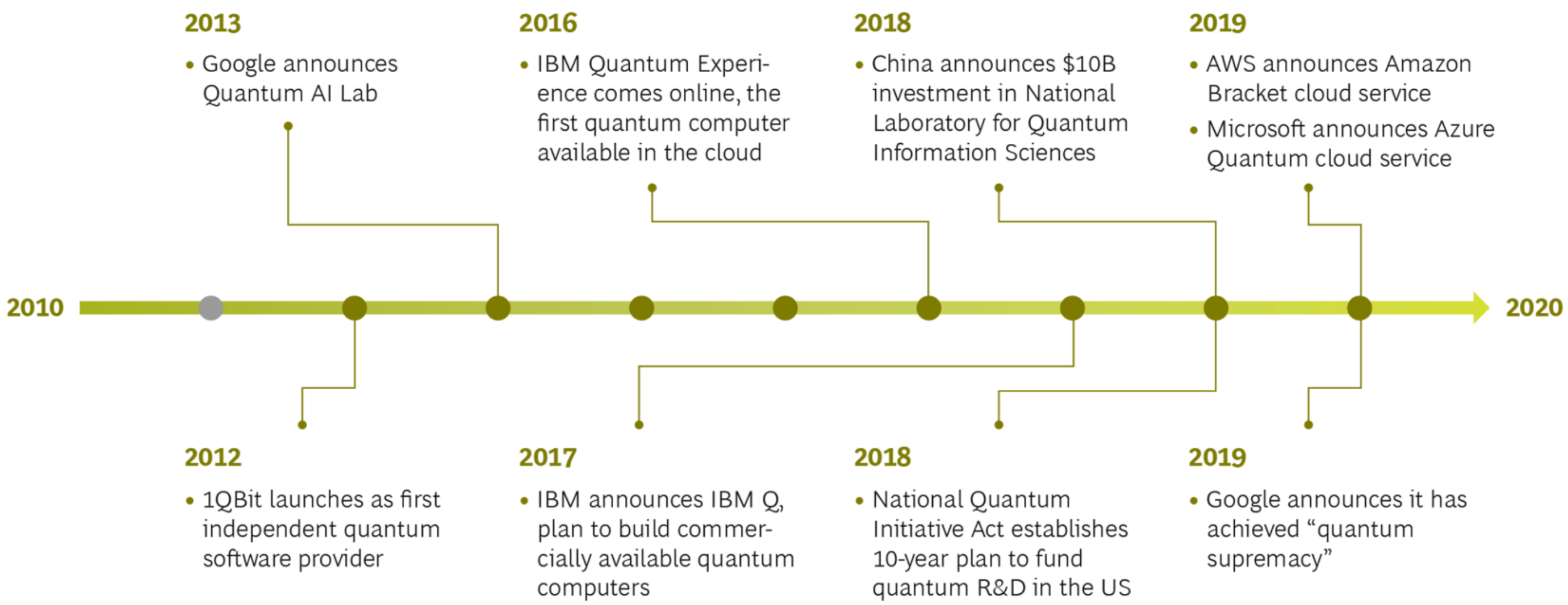
Lockheed Martin And Omnispace Explore Space-Based 5G Global Network

5G satellite hybrid connectivity would bolster terrestrial mobility


Enhanced Mobile Broadband
Gigabytes in a second
3D video, UHD screens
Work and play in the cloud
Smart Home/ Building
Augmented Reality
Voice
Industry Automation
Massive Machine Type Communications
Smart City
Future IMT
Ultra-Reliable and Low Latency Communications
Mission Critical Application, e.g. e-health
Self-Driving Car

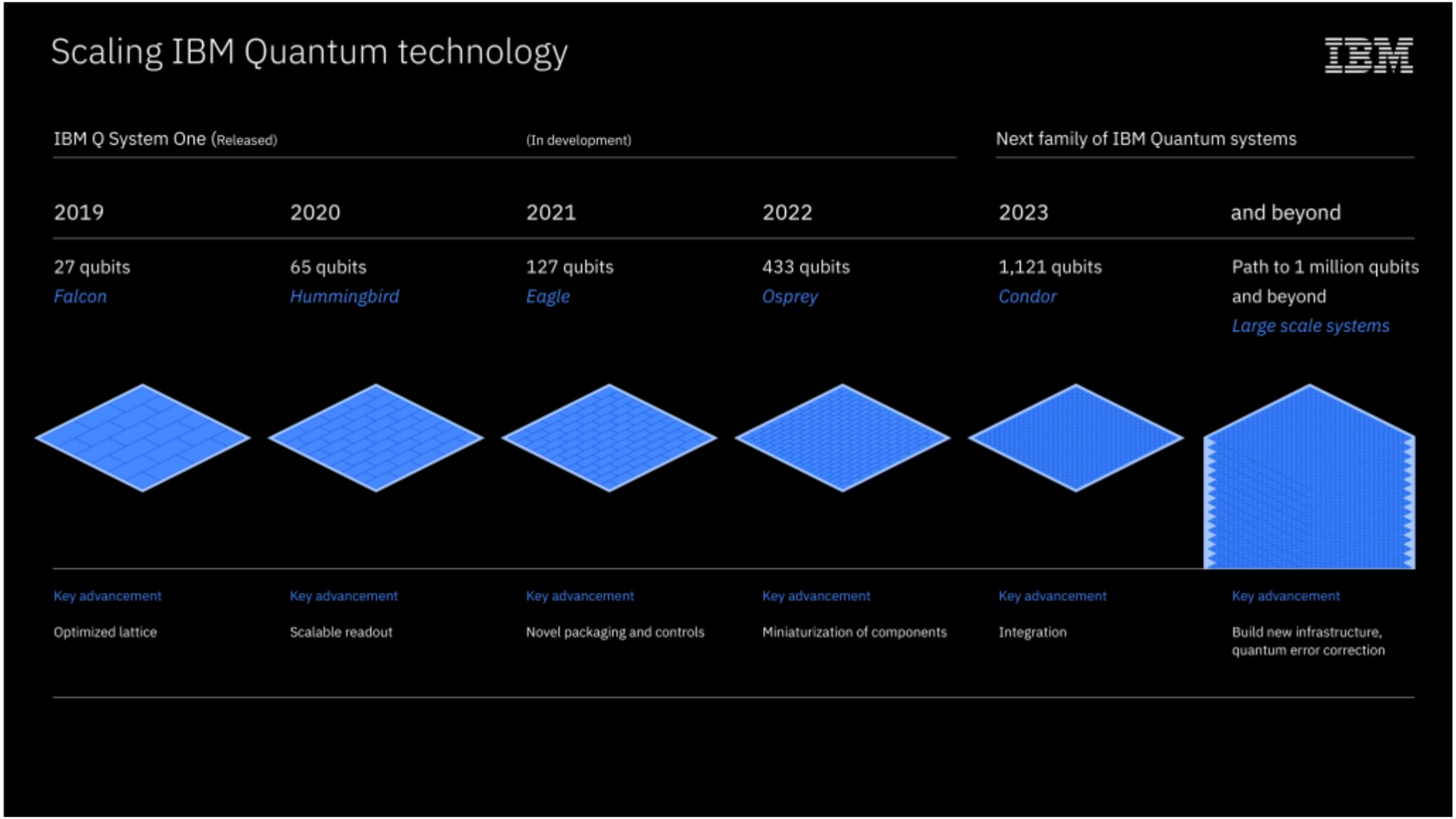
Source: ITU

Progress of quantum computing



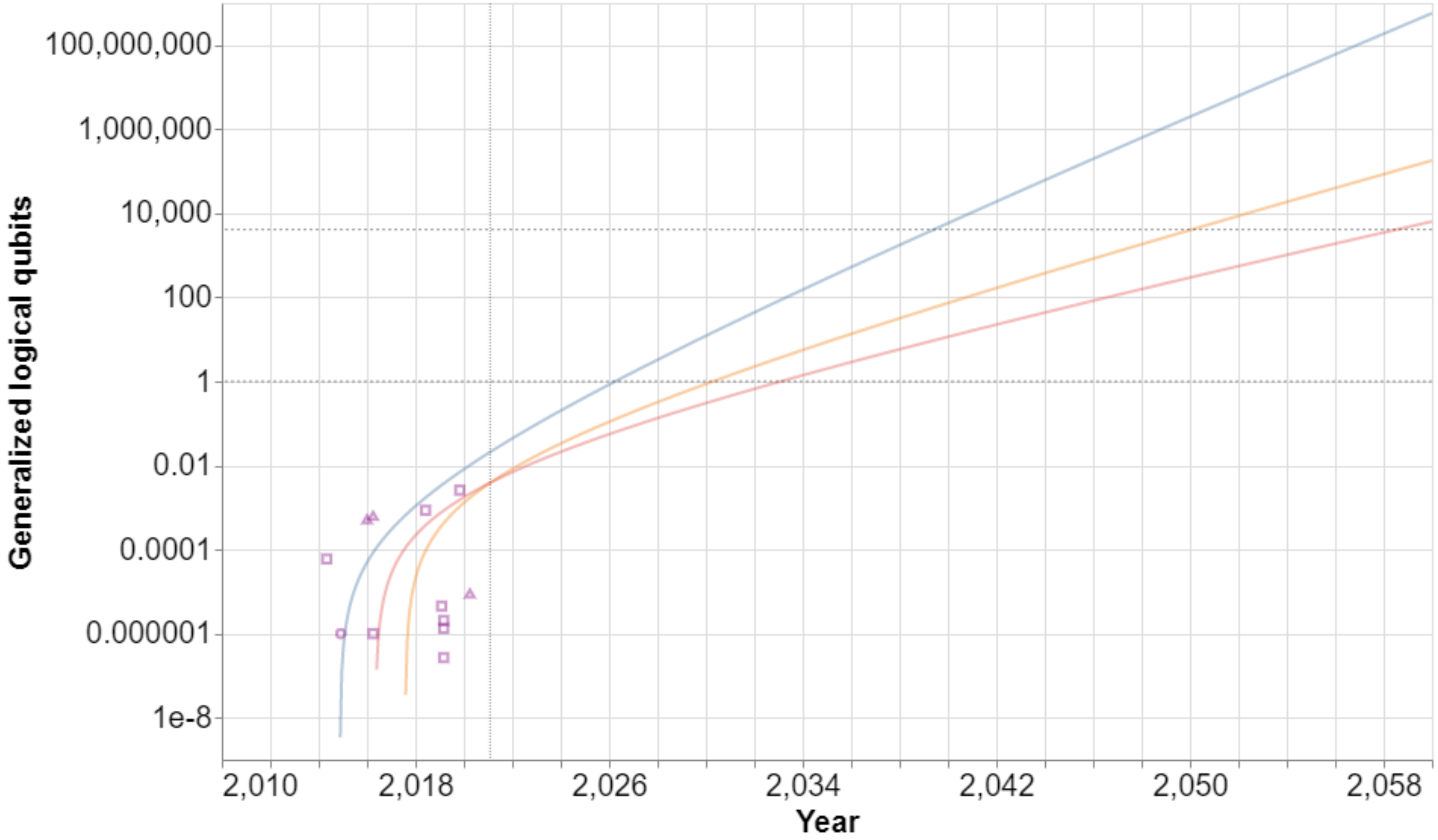
Sources: Industry interviews, desk research, Crunchbase, BCG analysis.

 https://www.bcg.com/publications/2021/building-quantum-advantage/



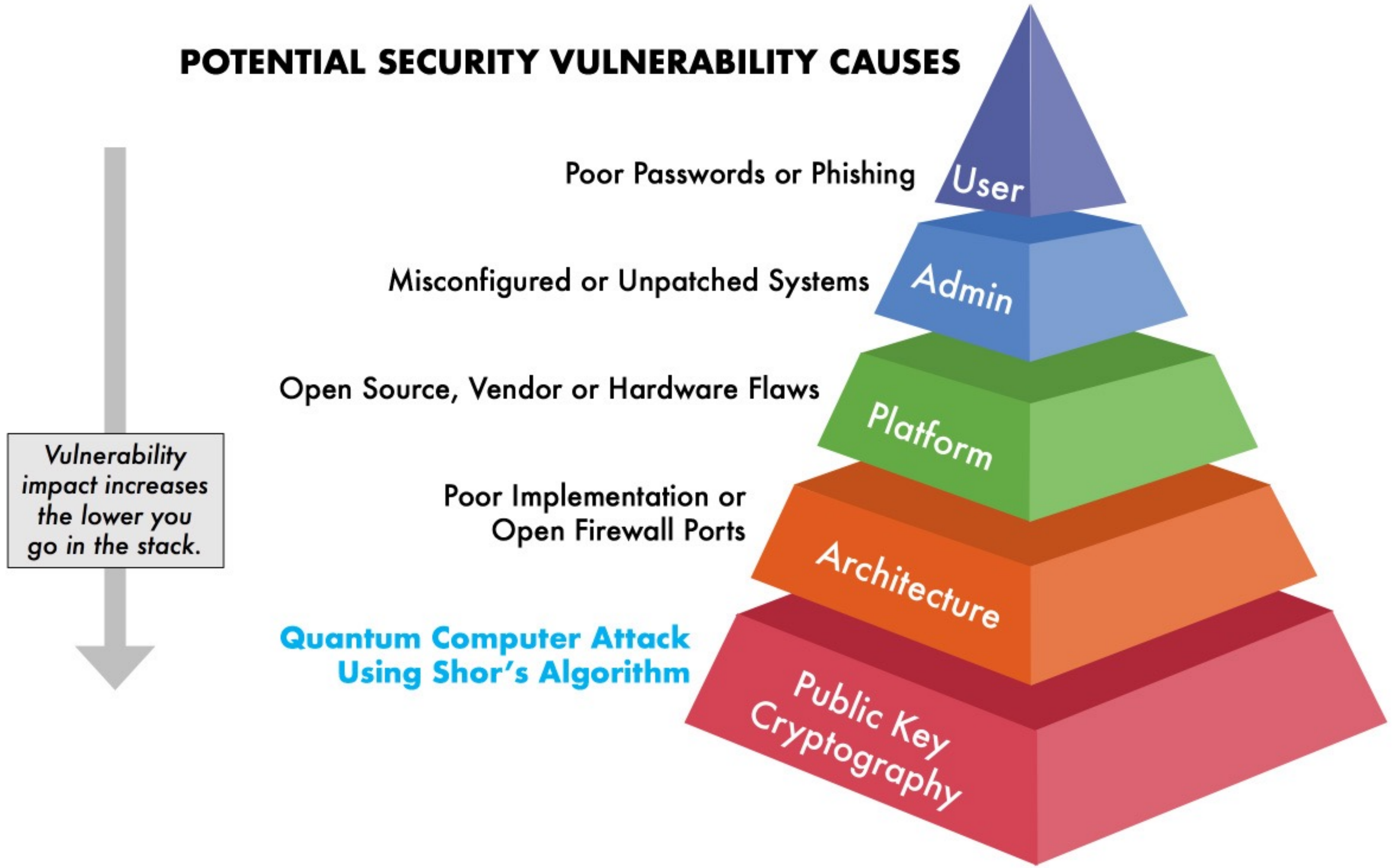
IBM's planned 1,121-qubit "Condor" quantum processor, slated for 2023, could be the company's first truly useful quantum computer for businesses.

 https://fortune.com/2020/09/15/ibm-quantum-computer-1-million-qubits-by-2030/

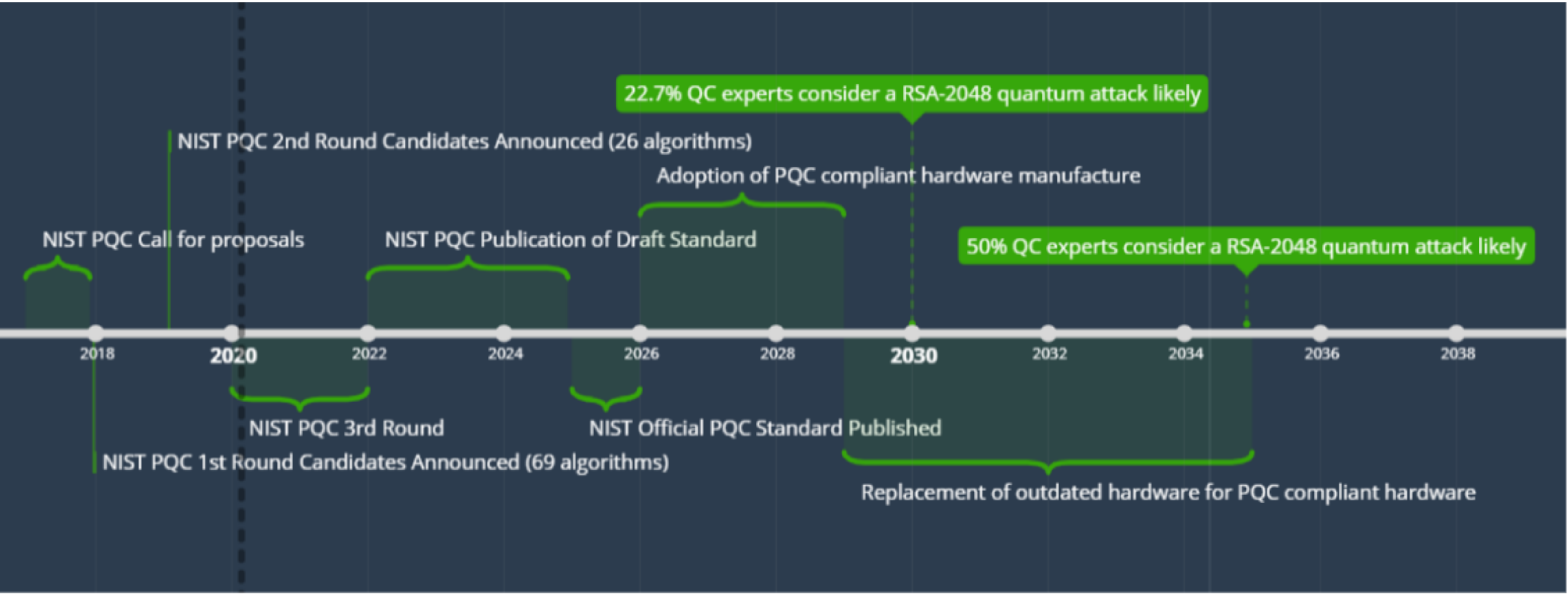


https://blog.jessriedel.com/2020/09/15/quantum-computing-timelines/

Risk along the Computing Stack



Source: https://www.isara.com/blog-posts/quantum-computing-security-breaches.html



https://blog.jessriedel.com/2020/09/15/quantum-computing-timelines/

The Quantum Threat – Qubits vs Bits

TABLE 4.1 Literature-Reported Estimates of Quantum Resilience for Current Cryptosystems, under Various Assumptions of Error Rates and Error-Correcting Codes

Cryptosystem	Category	Key Size	Security Parameter	Quantum Algorithm Expected to Defeat Cryptosystem	# Logical Qubits Required	# Physical Qubits Required[a]	Time Required to Break System[b]	Quantum-Resilient Replacement Strategies
AES-GCM[c]	Symmetric encryption	128 192 256	128 192 256	Grover's algorithm	2,953 4,449 6,681	4.61×10^6 1.68×10^7 3.36×10^7	2.61×10^{12} years 1.97×10^{22} years 2.29×10^{32} years	
RSA[d]	Asymmetric encryption	1024 2048 4096	80 112 128	Shor's algorithm	2,050 4,098 8,194	8.05×10^6 8.56×10^6 1.12×10^7	3.58 hours 28.63 hours 229 hours	Move to NIST-selected PQC algorithm when available
ECC Discrete-log problem[e-g]	Asymmetric encryption	256 384 521	128 192 256	Shor's algorithm	2,330 3,484 4,719	8.56×10^6 9.05×10^6 1.13×10^6	10.5 hours 37.67 hours 55 hours	Move to NIST-selected PQC algorithm when available
SHA256[h]	Bitcoin mining	N/A	72	Grover's Algorithm	2,403	2.23×10^6	1.8×10^4 years	
PBKDF2 with 10,000 iterations[i]	Password hashing	N/A	66	Grover's algorithm	2,403	2.23×10^6	2.3×10^7 years	Move away from password-based authentication

Source: Quantum Computing: Progress and Prospects, Grumbling & Horowitz, National Academic Press, 2019

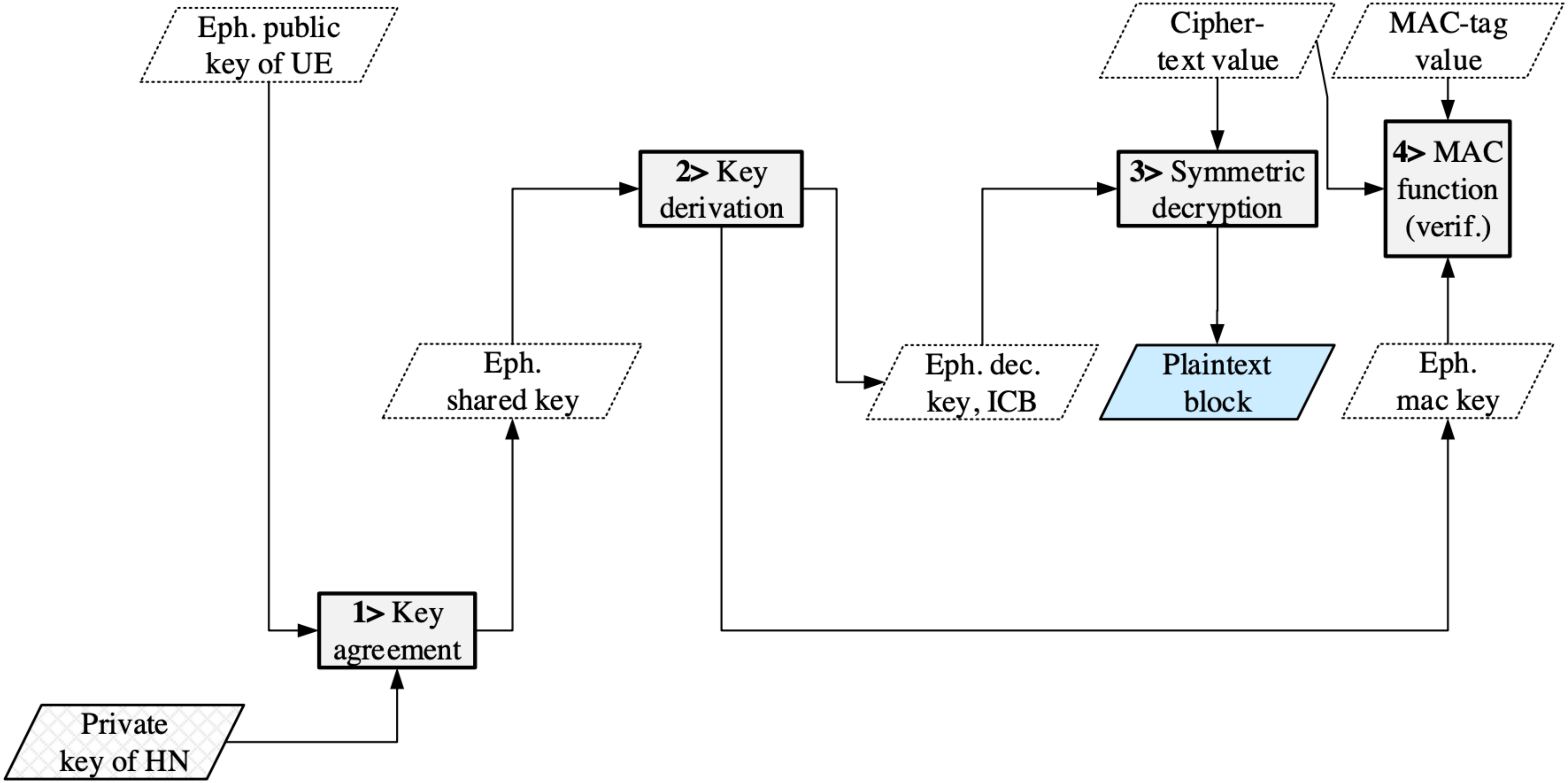
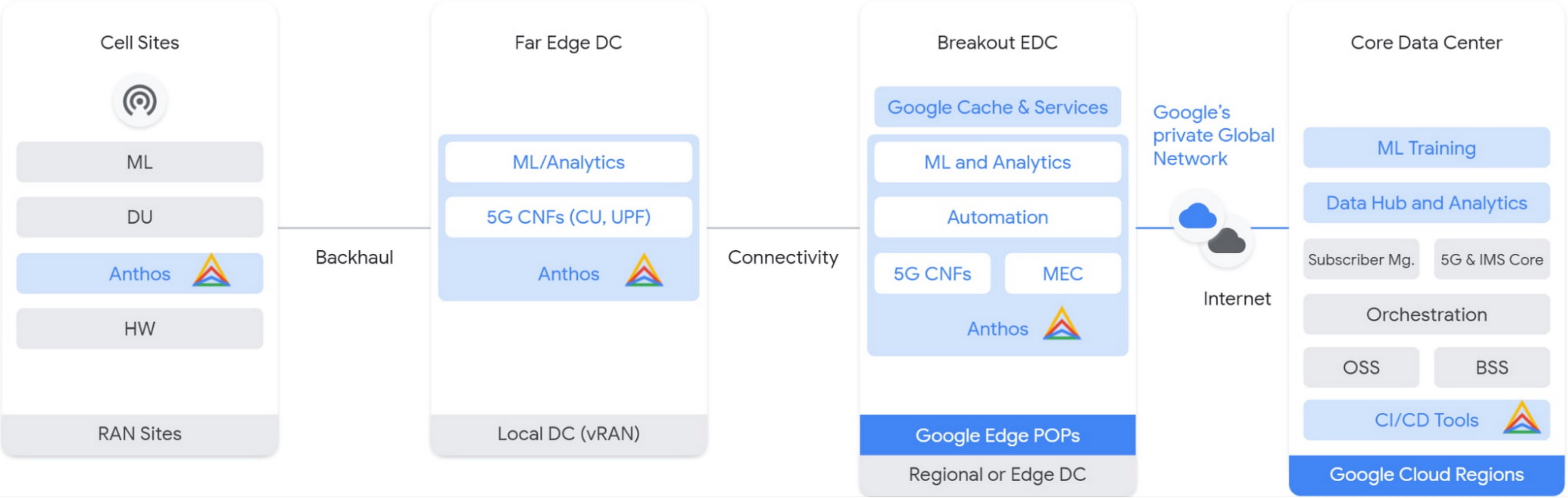
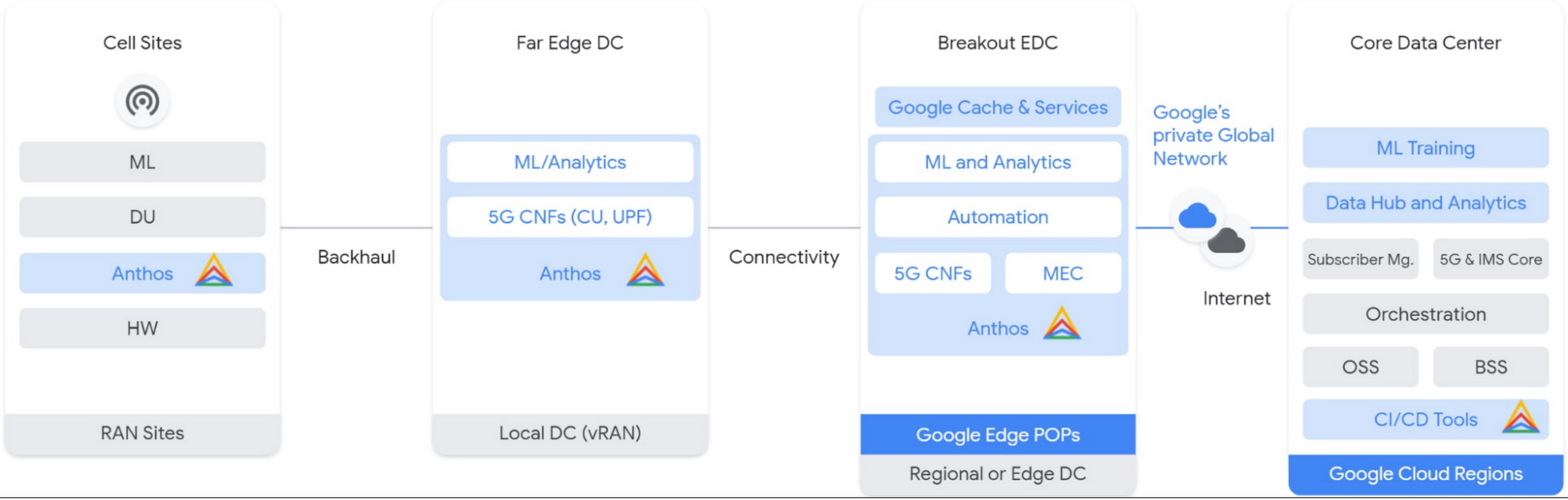


Figure C.3.3-1: Decryption based on ECIES at home network



https://cloud.google.com/blog/topics/telecommunications/how-csps-can-use-cloud-networks-to-deliver-5g

Quntum Threats



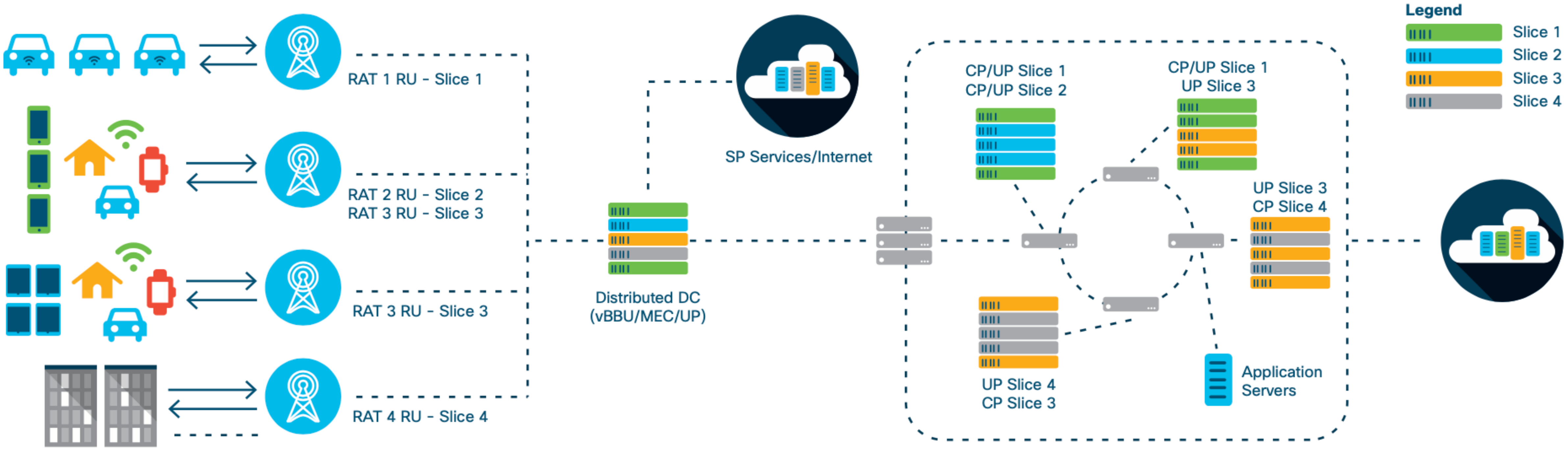
Device Trust, Endpoint

RAN unsafe crypto

Quantum unsafe cryptography implementation, usage

Deploying and operating cloud-based 5G networks, Jan 24 2022, https://cloud.google.com/blog/topics/telecommunications/how-csps-can-use-cloud-networks-to-deliver-5g

5G Threat Surface



Device Threats
Malware
Sensor Susceptibility
TFTP MitM attacks
Bots DDoS
Firmware Hacks
Device Tampering

Air Interface Threats
MitM attack
Jamming

RAN Threats
MEC Server Vulnerability
Rogue Nodes

Backhaul Threats
DDoS attacks
CP/UP Sniffing
MEC Backhaul sniff

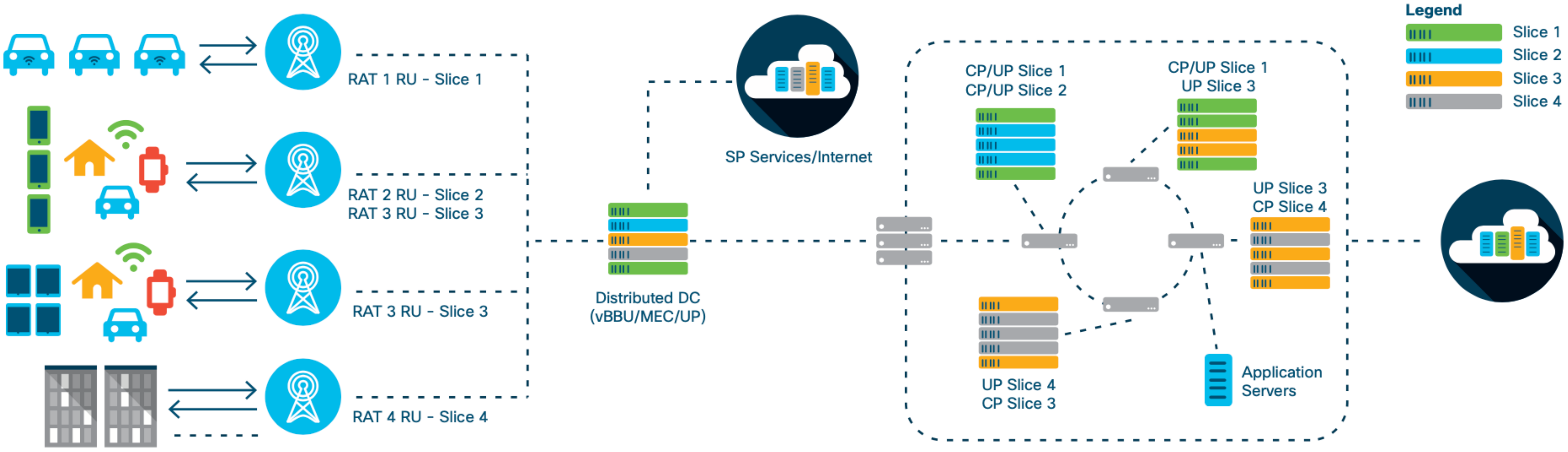
5G Packet Core & OAM Threats
Virtualization
Network Slice security
API vulnerabilities
IoT Core integration
Roaming Partner vulnerabilities
DDoS & DoS attacks
Improper Access Control

SGI/N6 & External Roaming Threats
IoT Core integration
VAS integration
App server vulnerabilities
Application vulnerabilities
API vulnerabilities

[1] 5G Security innovation with Cisco, White paper, 2018

5G Threat Surface

Quntum Threats



Device Threats
Malware
Sensor Susceptibility
TFTP MitM attacks
Bots DDoS
Firmware Hacks
Device Tampering

Air Interface Threats
MitM attack
Jamming

RAN Threats
MEC Server Vulnerability
Rogue Nodes

Backhaul Threats
DDoS attacks
CP/UP Sniffing
MEC Backhaul sniff

5G Packet Core & OAM Threats
Virtualization
Network Slice security
API vulnerabilities
IoT Core integration
Roaming Partner vulnerabilities
DDoS & DoS attacks
Improper Access Control

SGI/N6 & External Roaming Threats
IoT Core integration
VAS integration
App server vulnerabilities
Application vulnerabilities
API vulnerabilities

Device Trust, Endpoint

RAN unsafe crypto

Quantum unsafe cryptography implementation, usage

[1] 5G Security innovation with Cisco, White paper, 2018