

Security Challenges for our 5G Connected Society

Silke Holtmanns – January 2024 - 5G Fuse



General Security Challenges

Roaming

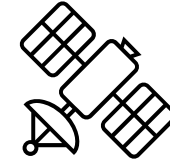


Legacy



Supply chain

Air interface



Satellite usage

Cloud &
Virtualization

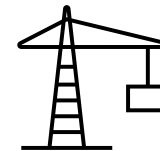
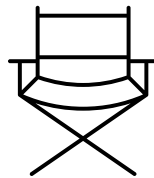


5G

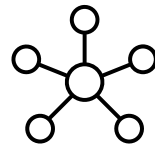


Special use cases

Management &
Orchestration



Third party interfaces &
edge computing



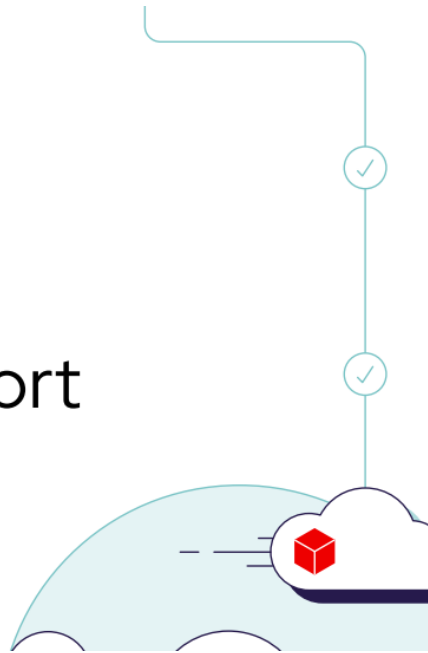
Routing & IT

RedHat Report Key Findings



State of Kubernetes security report

2023



Security incidents are prevalent, impacting all phases of the application development life cycle

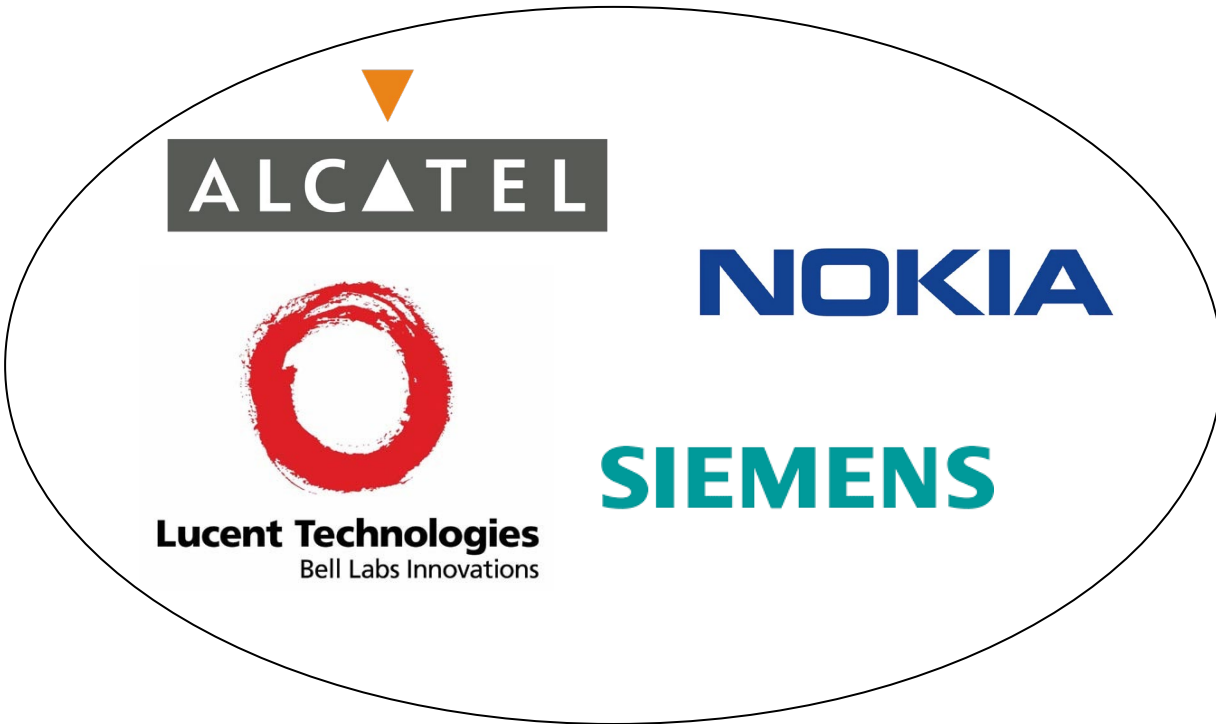
90% of respondents experienced at least one security incident in the last 12 months

Vulnerabilities and misconfigurations are top security concerns with container and Kubernetes environments

More than 50% of respondents are worried about misconfigurations and vulnerabilities, owing to the fact that containers and Kubernetes are highly customizable

Source: <https://www.redhat.com/en/resources/state-kubernetes-security-report-2023>

Why Open RAN Exists? – The Political Side (Market Concentration)



Why Open RAN Exists? – The Technical Side

5G is designed for businesses with many different requirements on:

- Latency
- Amount of devices
- Bandwidth
- Usage patterns
- Mobility patterns
- Different kind of RAN behaviour needed

Intention to create an ecosystem (including RAN apps using AI/ML) that offers for each use case the right solution

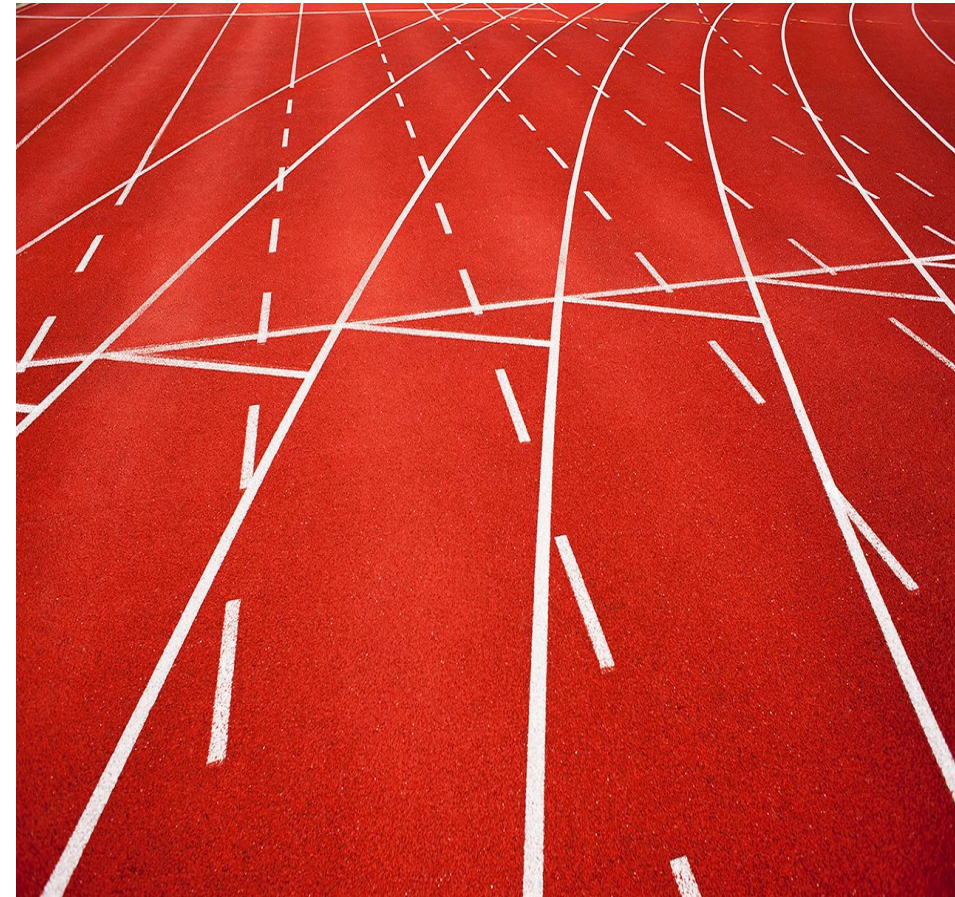


O-RAN Development Under Time Pressure – Fast & Furious

2018 In EU 138 trials of 5G networks in 35 cities

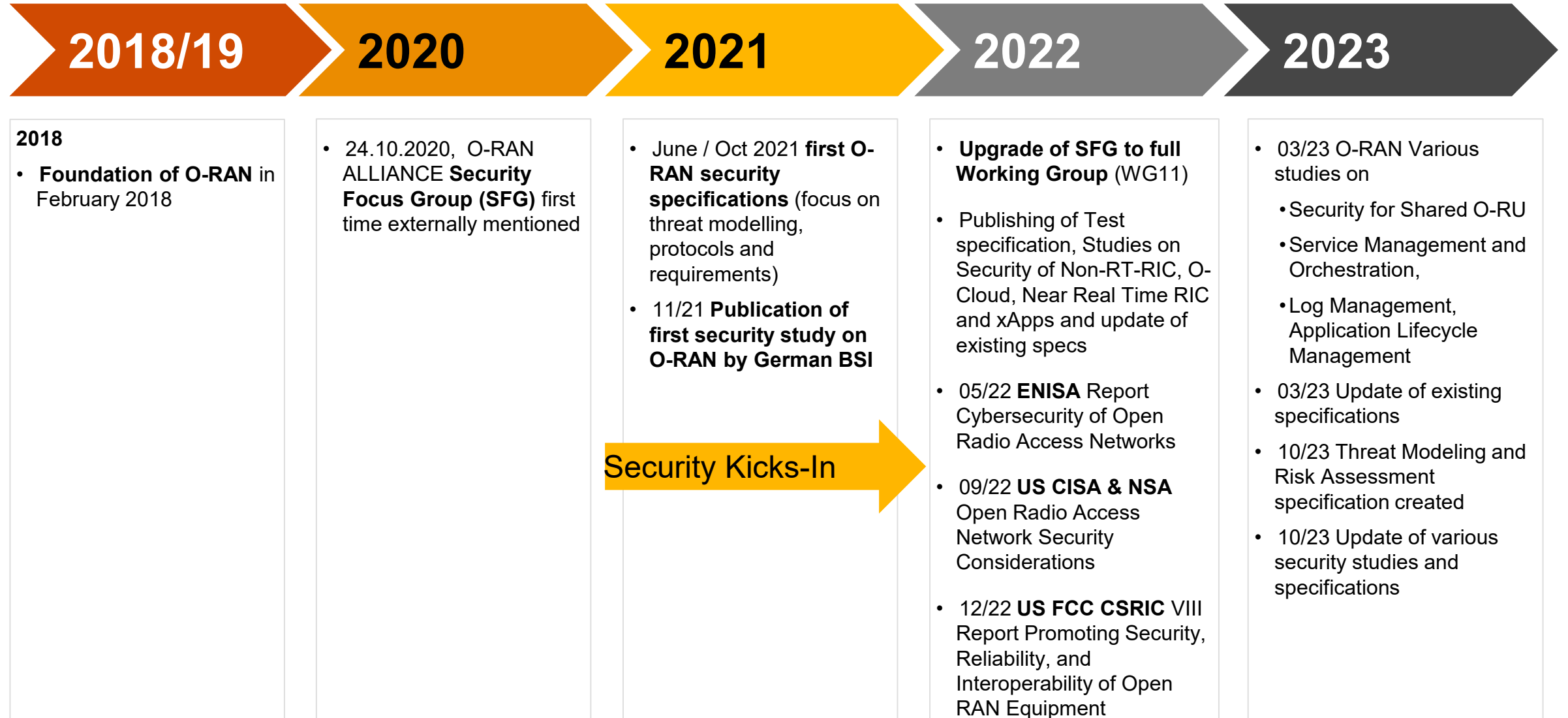
2018 Finnish Operator Elisa Oy launched commercial 5G network

2019/2020 Deployments from U.K.'s Vodafone Group PLC, BT Group-owned EE, France's Orange SA, Germany's Deutsche Telekom AG in 2019 ahead of full commercial service in 2020.



Source: <https://www.spglobal.com/marketintelligence/en/news-insights/trending/ZiQiFaN9Tnrf7Dwf6pQmTw2>

History of O-RAN Security



5G O-RAN Usage by Military

LightReading

Network Tech ▾ Wireless ▾ Software ▾ IT Infrastructure ▾ Digital Transformation ▾ Business ▾ Services ▾

OPEN RAN REGULATORY & POLITICS

US military bases could get private 5G, delighting Dish

The National Defense Authorization Act (NDAA) would allocate \$886 billion in defense spending. It also calls for the US Defense Department to deploy 5G open RAN private wireless networks on military bases.

Mike Dano
December 14, 2023

4 Min Read

LightReading
LIGHT READING HELPS YOU STAY

Source: <https://www.lightreading.com/open-ran/us-military-bases-could-get-private-5g-delighting-dish#close-modal>

5G and Beyond Military Installations and Test Beds in US

5GB Testbeds	Installations
Smart Warehouses	Marine Corps Logistics Base Albany, GA, and Naval Base San Diego, CA
Spectrum sharing between 5G and airborne radar	Hill Air Force Base, UT
Augmented and virtual reality	Joint Base LewisMcChord, WA
Survivable command and control and network enhancement	Nellis Air Force Base, NV
Ship wide and pier connectivity	Naval Base Norfolk, VA
Enhancing aircraft mission readiness	Joint Base Pearl HarborHickam, HI
Augmented reality support of maintenance and training Evaluating DOD's 5G core security experimentation network	Joint Base San Antonio, TX
Spectrum sharing between military communications and 5G	Tinker Air Force Base, OK
Connectivity for forward operating bases and tactical operations centers	Camp Pendleton, CA; Ft. Hood, TX; and Ft. Irwin National Training Center, CA

Source: <https://ieeexplore.ieee.org/document/10210549/>

R. Bajracharya, R. Shrestha, S. A. Hassan, H. Jung and H. Shin, "5G and Beyond Private Military Communication: Trend, Requirements, Challenges and Enablers," in *IEEE Access*, vol. 11, pp. 83996-84012, 2023, doi: 10.1109/ACCESS.2023.3303211

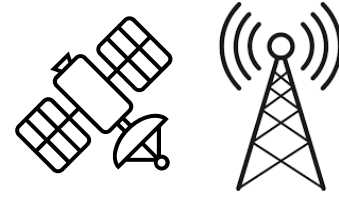
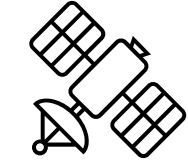
5G in Potential Joint Operations



FIGURE 1. STRATEGIC AND OPERATIONAL MOVEMENT SCENARIOS

Source: NATO CCDCOE, https://ccdcoe.org/uploads/2022/06/Report_Military-Movement-Risks-from-5G-Networks.pdf

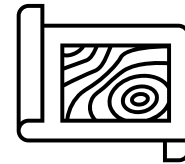
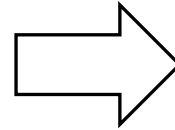
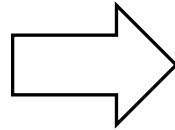
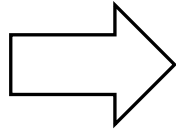
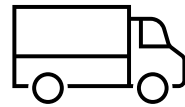
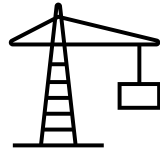
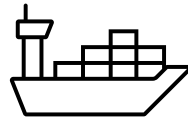
Applications & information residing in home country



Private

Public

Private (own)



Maritime
Satellite
Communication

Harbor
Country A

Roads
Country B

Deployment Place
Country C

Private Network

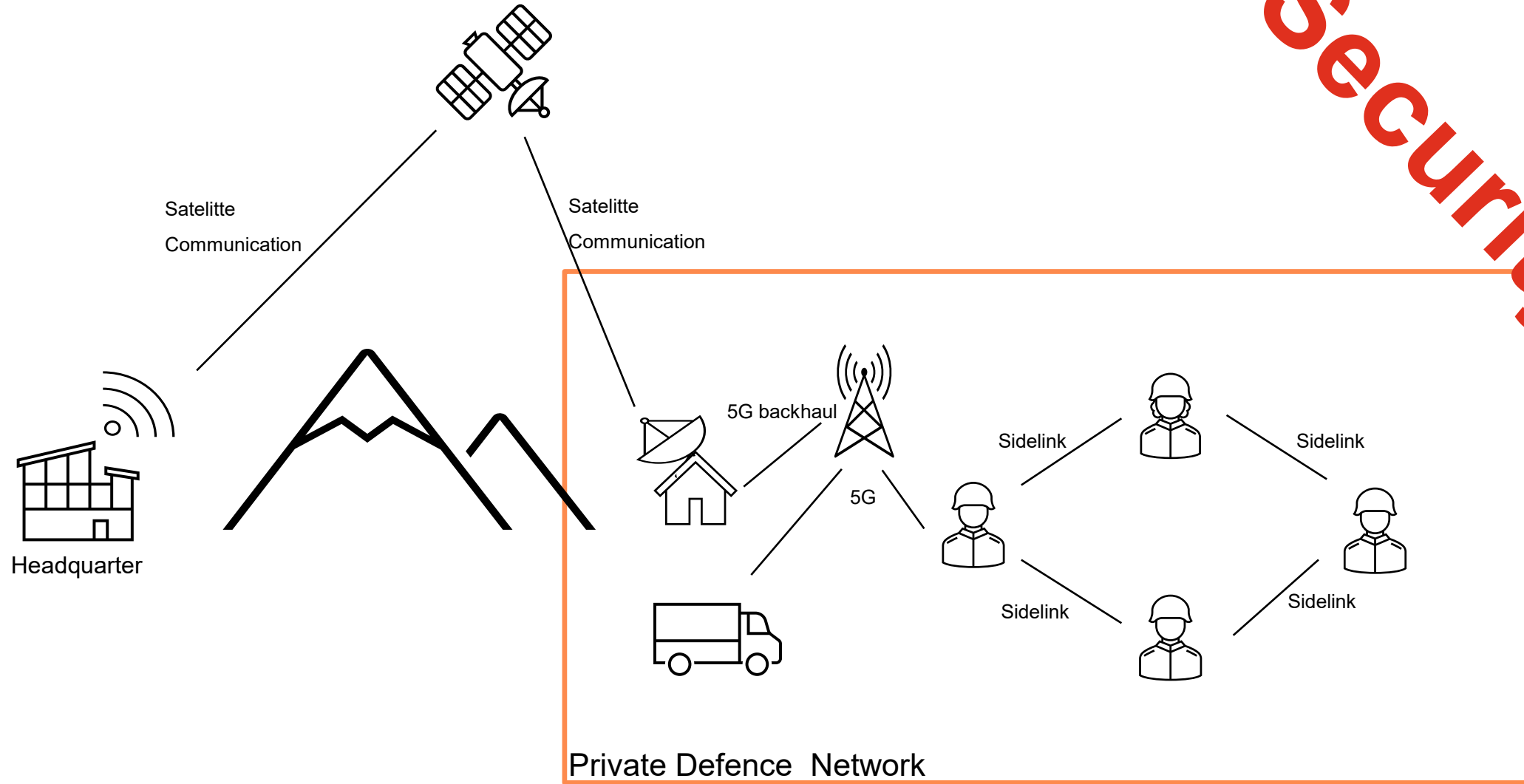
Public Network

Own Network

Movement of Joint Operation Devices

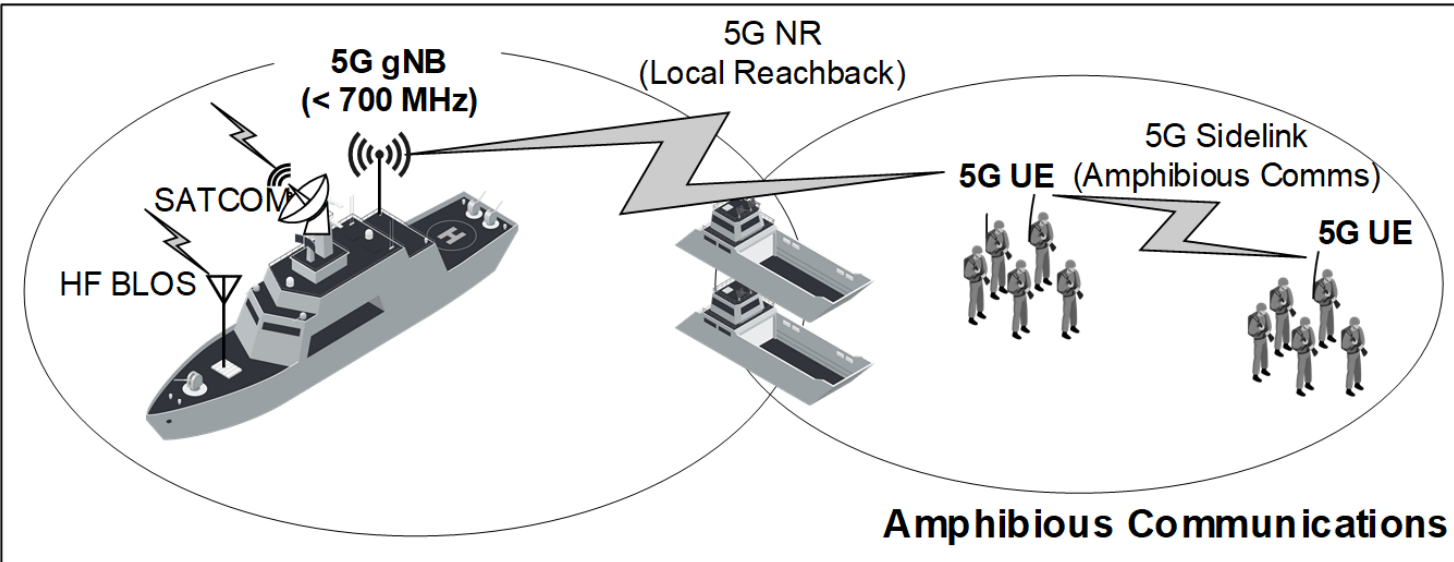
Security?

Direct Communication (Sidelink) Example

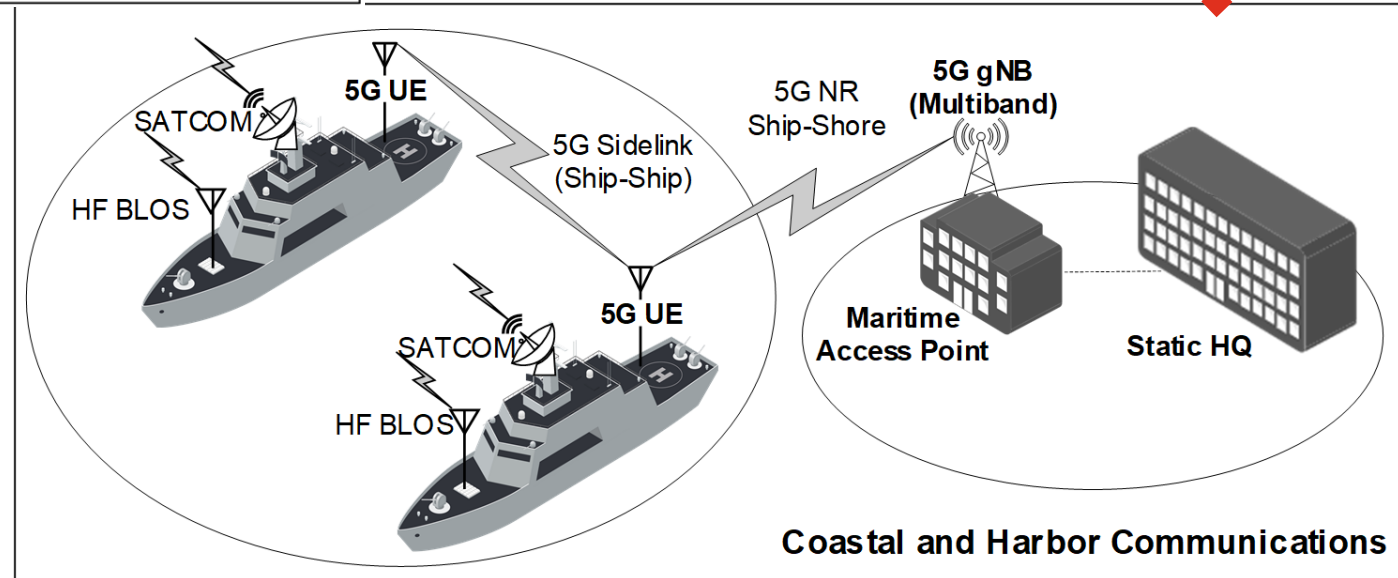


Security?

Military Maritime Scenario with Space Connection



Security?



Source: Luis Bastos; Germano Capela; Alper Koprulu; Gerard Elzinga;
Potential of 5G technologies for military application
<https://ieeexplore.ieee.org/document/9486402>

Mobile Networks are Part of Warfare - Ukraine

Blog | December 16, 2014 | 4 min | [Cathal McDaid](#)

Taking up the Gauntlet – SS7 Attacks in Ukraine

There have been several recent [reports in the media](#) on the results of new research into SS7 network. This interesting [research](#) outlines a series of techniques potential attackers can use to listen in to and read the calls and text messages of others. An obvious question for those of us in the telecom security industry is whether the threat is real and what we should do to address it. In considering an answer, we can look at a little-reported incident that occurred in Ukrainian Mobile networks earlier this year.

Last May, a report was issued by the Ukrainian Telecom Regulator (NKRZI[1]). This document, which went essentially unreported by the press outside of Ukraine & Russia, contains the result of the investigation of the NKRZI, assisted by the Ukrainian Security Service (SBU), into telecom network activity over several days in MTS Ukraine. The key findings of this report were that over a 3 day period in April 2014, a number of Ukrainian mobile subscribers were affected by suspicious/custom SS7[2] packets from telecom network elements with Russian addresses, causing their location and potentially the contents of their phone calls to be obtained.

The ‘attacks’ outlined in the document involved SS7 packets being sent between the mobile operators. Without going into specific details, what occurred is a series of SS7 packets were received by MTS Ukraine’s SS7 network which modified control information stored in network switches for a number of MTS Ukraine mobile users. In doing so, when one of the affected mobile subscribers tried to ring someone else, their call would be forwarded to a physical land line number in St. Petersburg, Russia, without their knowledge – in effect the **call has been intercepted**. There is an additional further step

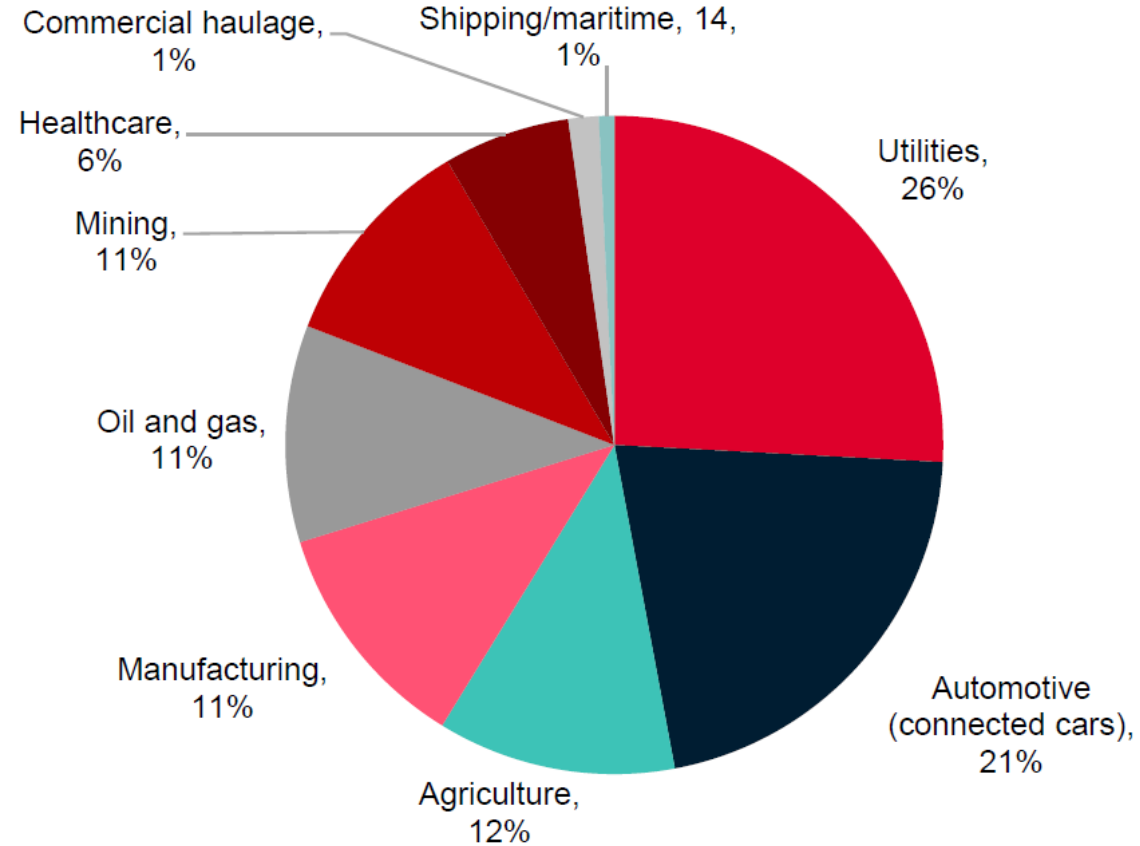


Key Performance Indicators of Military Communication Systems

Indicator	Priority Value
Priority	High: Battlefield real-time confrontations Medium: Training activities Low: Logistics devices
Availability	99.9999%
Delay	< < 1
User rate	peak rate can approach 20 Gbps
Reliability	Weapon strike: 99.999% C2: 99.9% Service support: 99%
Mobility	High: > 200 km/h Medium: 2 ~ 200 km/h Low: < 2 km/h
User density	High: > 10 ⁴ per km ² Medium: 100 ~ 10 ⁴ per km ² Low: < 100 per km ²
Security	High: Classified Medium: Secretive Low: Unsecured
Energy efficiency	High: Weapon sensors Medium: Battlefield scenario Low: Remote operations

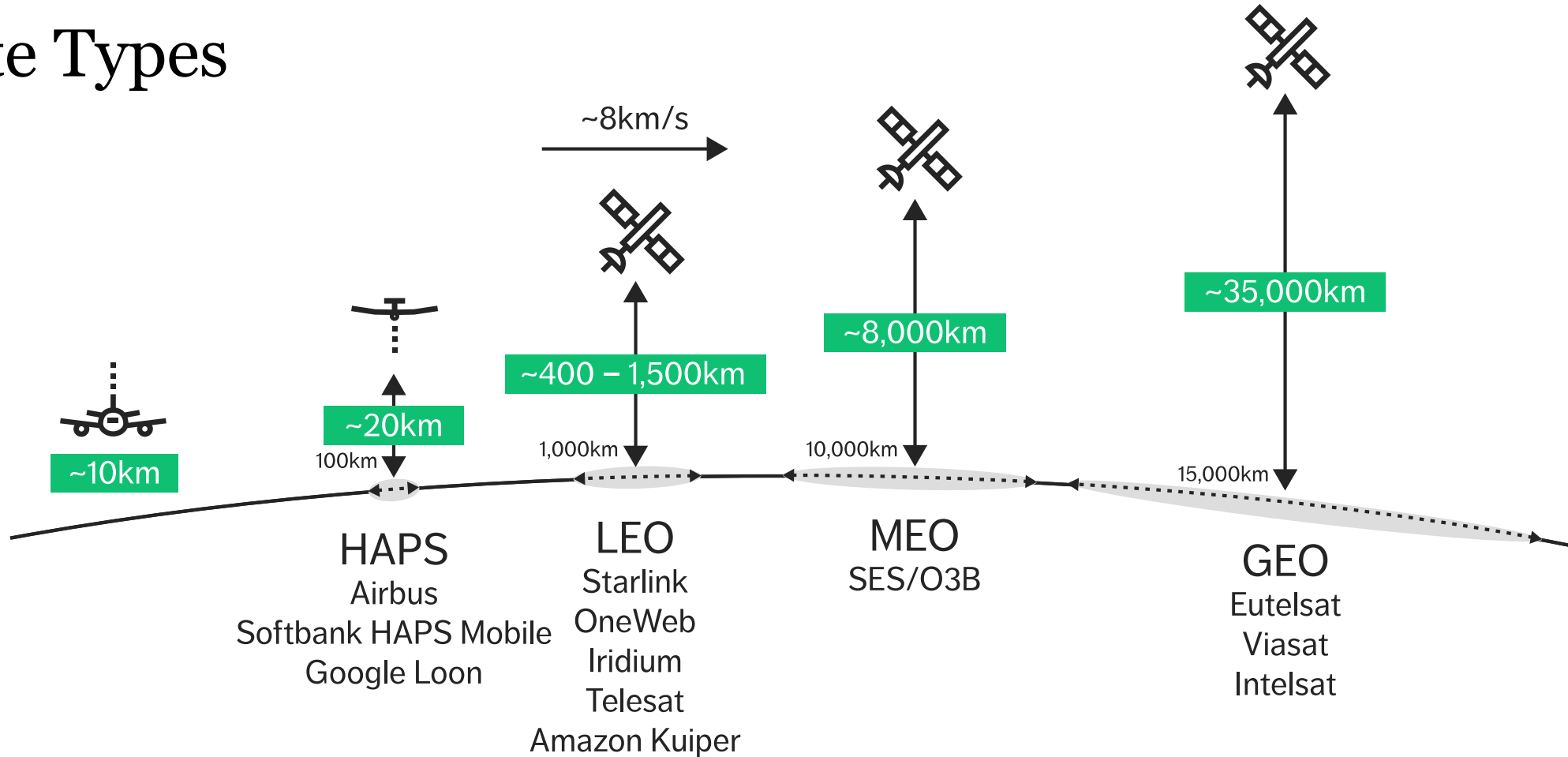
Source: <https://ieeexplore.ieee.org/document/10210549/>
R. Bajracharya, R. Shrestha, S. A. Hassan, H. Jung and H. Shin, "5G and Beyond Private Military Communication: Trend, Requirements, Challenges and Enablers," in *IEEE Access*, vol. 11, pp. 83996-84012, 2023, doi: 10.1109/ACCESS.2023.3303211

Figure 7: 1.9 billion devices (8% of the IoT market) across nine sectors are addressable for D2D satellite by 2035



Source: <https://data.gsmaintelligence.com/research/research/research-2022/satellite-2-0-going-direct-to-device>

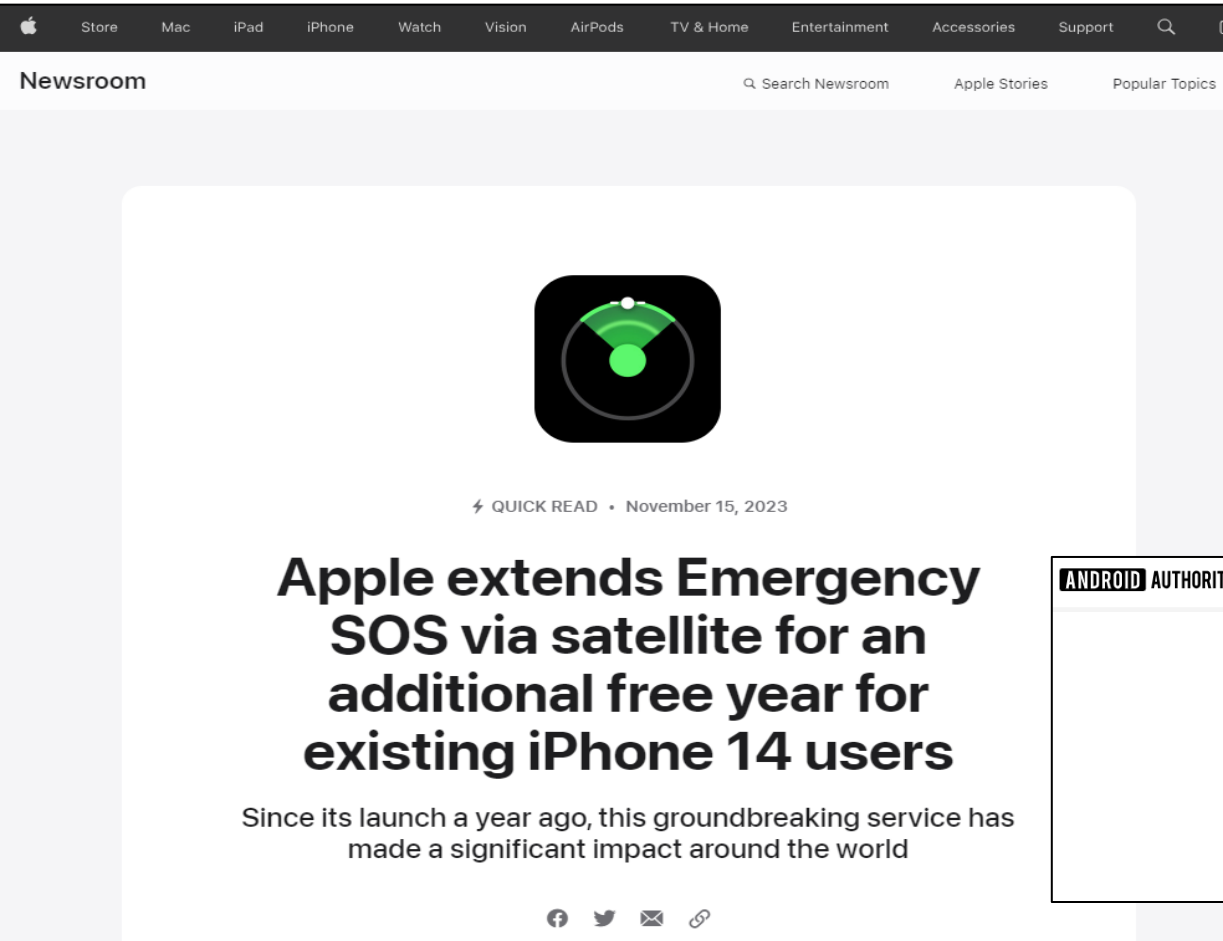
Satellite Types



Source: Ericsson Technology Review article, Using 3GPP technology for satellite communication


<https://www.ericsson.com/en/reports-and-papers/ericsson-technology-review/articles/3gpp-satellite-communication>

Device Support



The screenshot shows the Apple Newsroom website. At the top, there is a navigation bar with links for Store, Mac, iPad, iPhone, Watch, Vision, AirPods, TV & Home, Entertainment, Accessories, and Support. Below this is a search bar and links for Search Newsroom, Apple Stories, and Popular Topics. The main content area features a large green Wi-Fi icon with a satellite symbol inside. Below the icon, it says "QUICK READ • November 15, 2023". The headline reads "Apple extends Emergency SOS via satellite for an additional free year for existing iPhone 14 users". A sub-headline below the headline states "Since its launch a year ago, this groundbreaking service has made a significant impact around the world". At the bottom of the article, there are social media sharing icons for Facebook, Twitter, Email, and a link icon.

Newsroom Search Newsroom Apple Stories Popular Topics

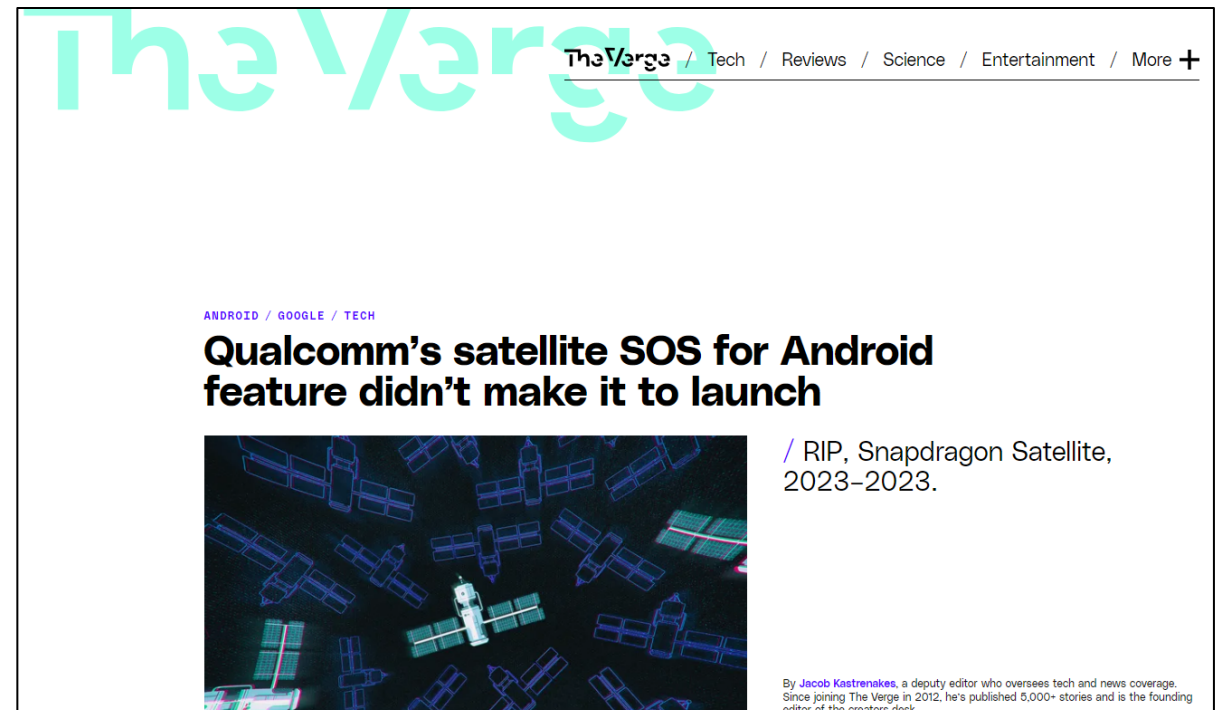


⚡ QUICK READ • November 15, 2023

Apple extends Emergency SOS via satellite for an additional free year for existing iPhone 14 users

Since its launch a year ago, this groundbreaking service has made a significant impact around the world

Facebook Twitter Email Link

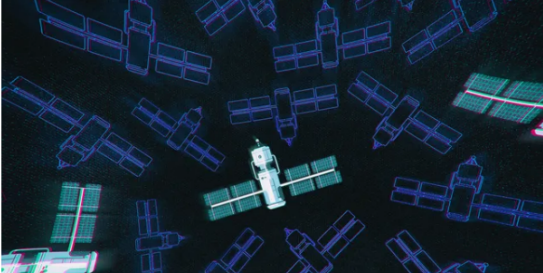


The screenshot shows the The Verge website. The top navigation bar includes "The Verge" logo and links for Tech, Reviews, Science, Entertainment, and More. The main article headline is "Qualcomm's satellite SOS for Android feature didn't make it to launch". Above the headline, it says "ANDROID / GOOGLE / TECH". Below the headline is a photograph of several satellites in space. To the right of the photo, there is a sub-headline: "/ RIP, Snapdragon Satellite, 2023-2023." Below the photo, there is a byline: "By Jacob Kastrenakes, a deputy editor who oversees tech and news coverage. Since joining The Verge in 2012, he's published 5,000+ stories and is the founding editor of the creator desk."

The Verge Tech / Reviews / Science / Entertainment / More +

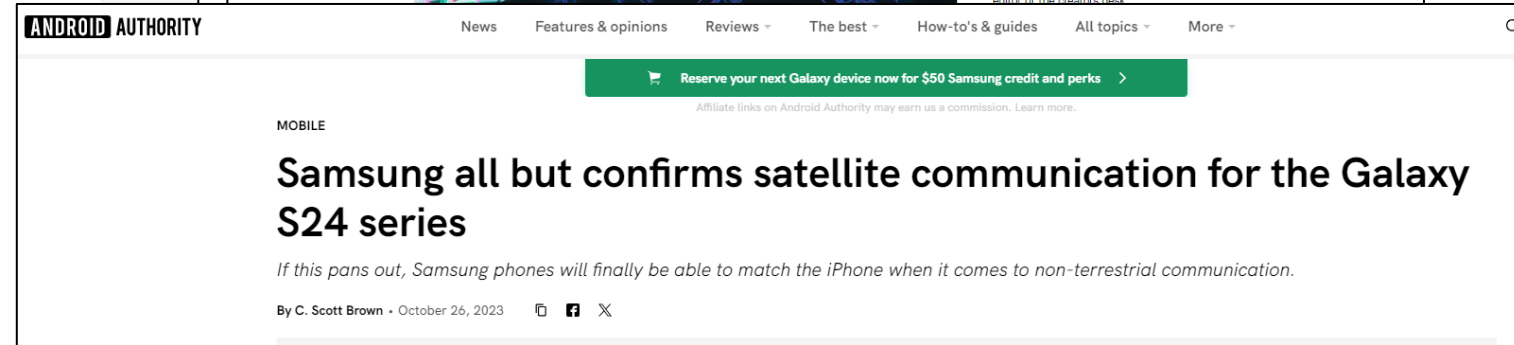
ANDROID / GOOGLE / TECH

Qualcomm's satellite SOS for Android feature didn't make it to launch



/ RIP, Snapdragon Satellite, 2023-2023.

By Jacob Kastrenakes, a deputy editor who oversees tech and news coverage. Since joining The Verge in 2012, he's published 5,000+ stories and is the founding editor of the creator desk.



The screenshot shows the Android Authority website. The top navigation bar includes "ANDROID AUTHORITY" logo and links for News, Features & opinions, Reviews, The best, How-to's & guides, All topics, and More. Below the navigation bar is a green banner that says "Reserve your next Galaxy device now for \$50 Samsung credit and perks". Below the banner, it says "Affiliate links on Android Authority may earn us a commission. Learn more." The main article headline is "Samsung all but confirms satellite communication for the Galaxy S24 series". Above the headline, it says "MOBILE". Below the headline is a sub-headline: "If this pans out, Samsung phones will finally be able to match the iPhone when it comes to non-terrestrial communication." Below the sub-headline, there is a byline: "By C. Scott Brown • October 26, 2023" and social media sharing icons for Facebook, Twitter, and X.

ANDROID AUTHORITY News Features & opinions Reviews The best How-to's & guides All topics More

Reserve your next Galaxy device now for \$50 Samsung credit and perks

Affiliate links on Android Authority may earn us a commission. Learn more.

MOBILE

Samsung all but confirms satellite communication for the Galaxy S24 series

If this pans out, Samsung phones will finally be able to match the iPhone when it comes to non-terrestrial communication.

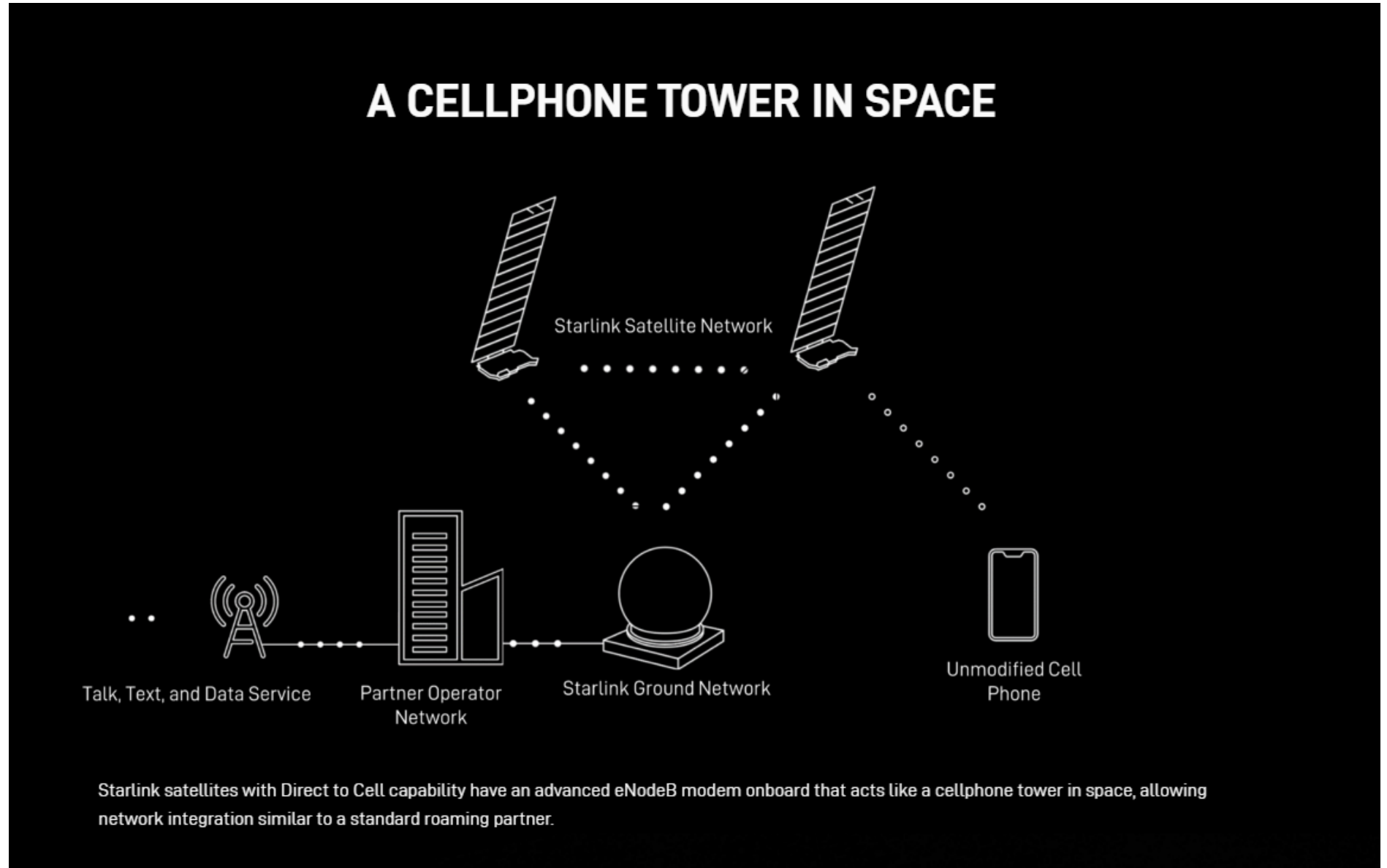
By C. Scott Brown • October 26, 2023 Facebook Twitter X

Sources: <https://www.apple.com/newsroom/2023/11/apple-extends-emergency-sos-via-satellite-for-an-additional-free-year/>

<https://www.theverge.com/2023/11/10/23955416/qualcomm-snapdragon-satellite-shut-down-emergency-sos-iridium>

<https://www.androidauthority.com/samsung-galaxy-s24-satellite-3379711/>

Direct to Cell (4G Approach) – Example Starlink




Using Mobile Phones with Satelittes - 2024

MOBILE WORLD LIVE

5G+ RAN Vendors Operators Big Tech Devices AI & Cloud Network Tech Regulation More : Events v

LYNK GLOBAL NETWORK TECH STARLINK JANUARY 3, 2024

First Starlink sat-to-phone birds leave launchpad



BY CHRIS DONKIN

SHARE [f](#) [in](#) [X](#) [@](#)

SpaceX launched six Starlink satellites with the capability to provide mobile coverage directly to standard smartphones, a service the company asserts will improve global connectivity and help eliminate dead zones.


T-Mobile Our story v Responsibility v Newsroom v Investors v Careers v Sup

First SpaceX Satellites Launch for Breakthrough Direct to Cell Service with T-Mobile

January 03, 2024

Major step forward in companies' vision to create truly universal coverage by pairing SpaceX's Starlink satellite technology with T-Mobile's industry-leading network

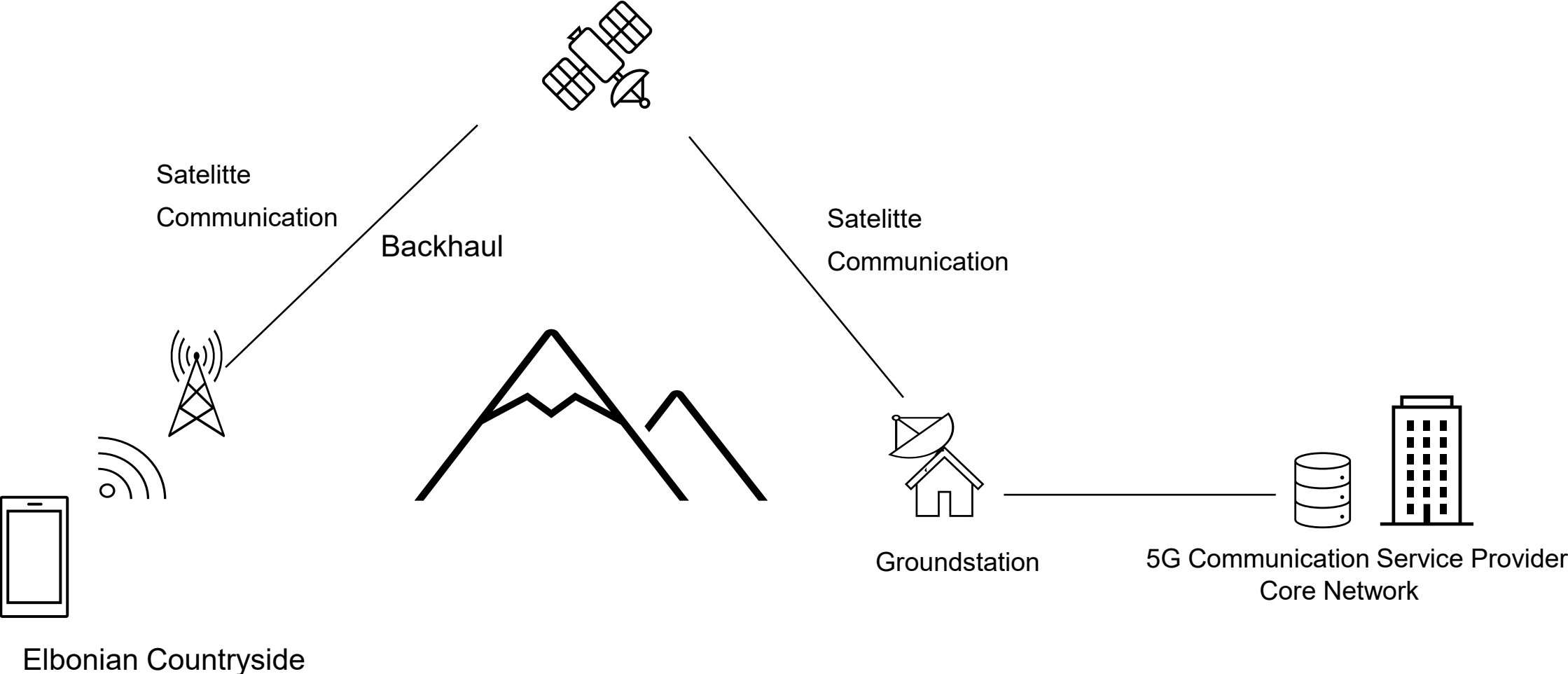
Five international partners have joined T-Mobile and SpaceX on their quest for global connectivity



T-Mobile **SPACEX**

GO FOR LAUNCH

Satellite Backhaul




Extending Coverage - Backhaul

MOBILE WORLD LIVE Search news, topics, companies and more...

5G+ RAN Vendors Operators Big Tech Devices AI & Cloud Network Tech Regulation More :

EUROPE NETWORK TECH SUB-SAHARAN AFRICA VODAFONE SEPTEMBER 5, 2023

Vodafone seals satellite deal with Project Kuiper



BY HANA ANANDIRA

SHARE [f](#) [in](#) [X](#) [@](#)

Vodafone Group teamed with Amazon's broadband satellite service **Project Kuiper** to extend connectivity in Europe and Africa, part of a mission to bring 4G and 5G services to underserved communities.

ASIA PACIFIC RELIANCE OCTOBER 27, 2023

Jio pledges affordable satellite broadband across India



Reliance Jio unveiled satellite communications play JioSpaceFiber, a service it claims will be capable of delivering gigabit-level broadband to the most remote parts of India.

Communication in Space Tracks

Legacy Mobile Satellite Services (MSS)

- Aims to integrate legacy MSS technologies into new smartphones using MSS spectrum

Examples:

Apple iPhone 14, Globalstat, Huawei Mate 50, Bei Dou, Qualcomm Snapdragon (Iridium)

Long-Term Evolution (LTE) 4G Usage

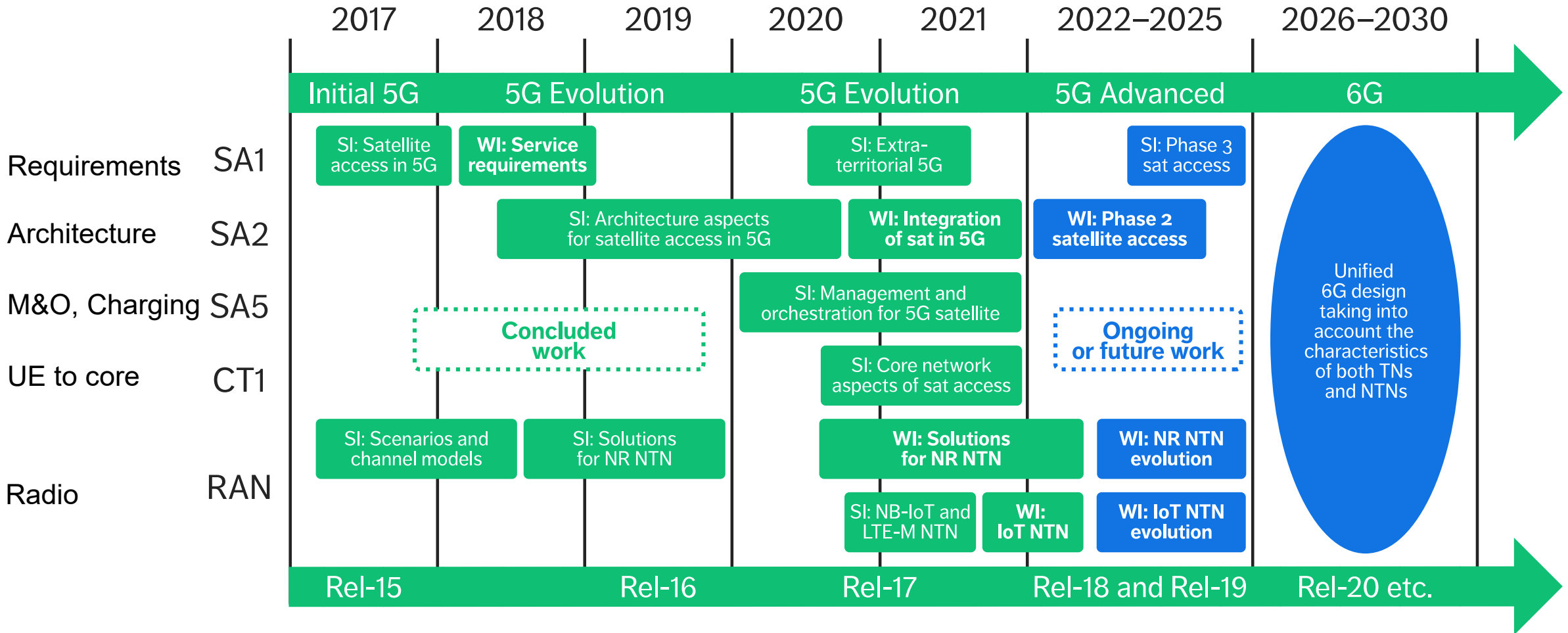
- Basically puts a 4G base station (eNB) onto the satellite (LEO)
- Requires a cooperation with a communication service provider
- Can be used with normal LTE phones
- Called Direct-to-Cell

Example: Starlink

5G Non-Terrestrial Network (NTN)

- Phones support features to support NTN (frequency / Doppler shift, mobility, RTT, no HARQ)
- Requires location
- Transparent and regenerative architecture
- Focus on LEO

NTN - Status 3GPP



Source: Ericsson Technology Review article, Using 3GPP technology for satellite communication

<https://www.ericsson.com/en/reports-and-papers/ericsson-technology-review/articles/3gpp-satellite-communication>

Fresh from the Oven

TSG SA Meeting #102

SP-231790

December 11 – 15, 2023, Edinburgh, Scotland

Source: SA WG3

Title: New SID on Study on Security Aspects of 5G Satellite Access

Phase 3

Document for: Approval

Agenda Item: 6.1.3

3GPP TSG-SA3 Meeting #113

S3-235103

Chicago, USA, 6 - 11 November 2023

(revision of S3-234570)

Source: CATT, Nokia, Xiaomi, CAICT, China Mobile, China Unicom, ZTE, Deutsche Telekom, Thales, China Telecommunications, Samsung, Sectra Communications

Title: New SID on Study on Security Aspects of 5G Satellite Access

Phase 3

Document for: Approval

Agenda Item: 6.3

3GPP™ Work Item Description

Information on Work Items can be found at <http://www.3gpp.org/Work-Items>
See also the 3GPP Working Procedures, article 39 and the TSG Working Methods in 3GPP TR 21.900

**Title: Study on Security Aspects of 5G Satellite Access
Phase 3**

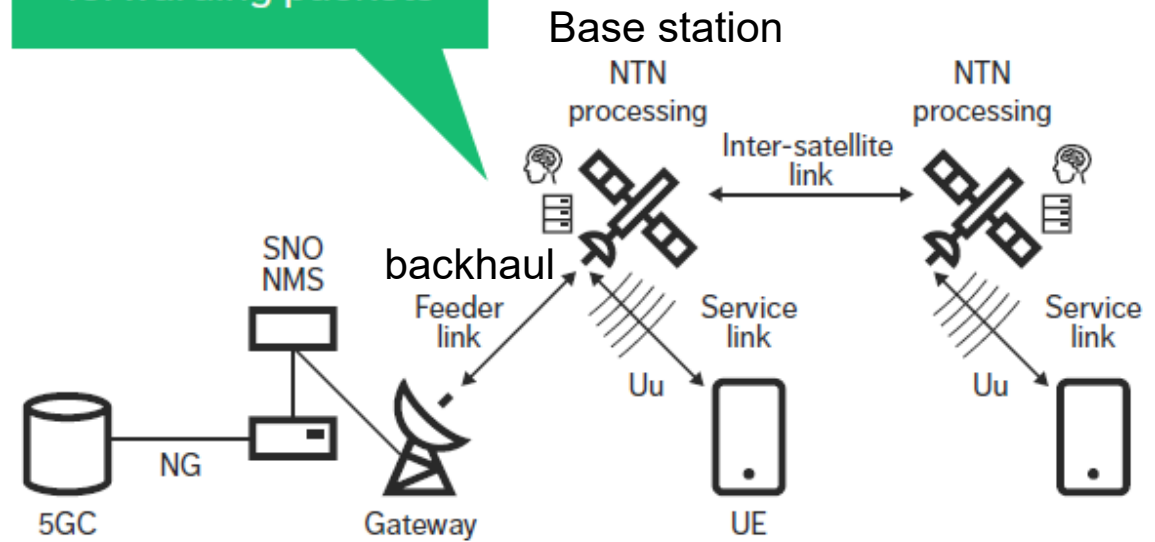
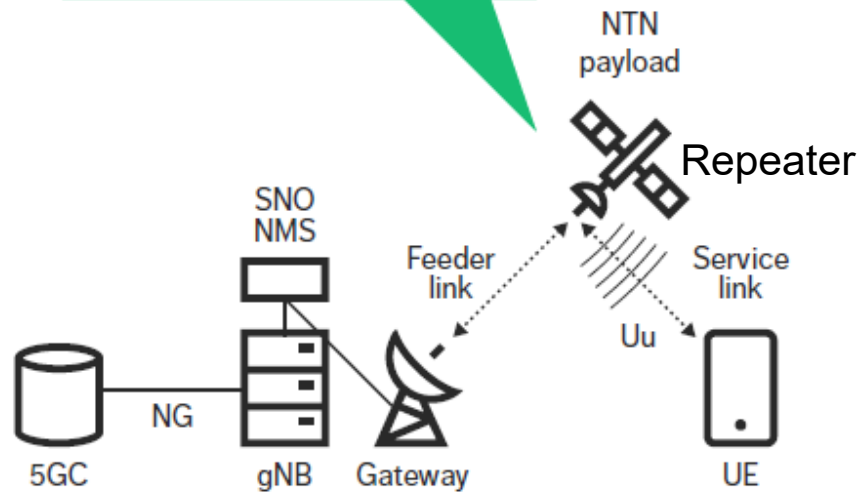
5G NTN – Enhanced 5G Phones

Transparent payload

Regenerative payload

RF operations only
(not capable of
decoding packets)

Capable of decoding,
processing and
forwarding packets



Security Challenges for Space - GPS

The screenshot shows a news article from ERR.ee. The main headline is "Estonia also affected by end-of-year GPS systems jamming". Below the headline is a map of the Baltic Sea region with color-coded areas indicating the level of GPS interference. A legend indicates: Green for 0-20%, Yellow for 20-50%, Orange for 50-80%, and Red for 80-100%. The article text states that Estonia experienced GPS jamming on December 31, 2023, and that Russia is suspected of being the source. It also mentions that other countries in the region, including Finland, Latvia, Poland, Sweden, and Russia, were also affected.

January 2024

Source: <https://news.err.ee/1609210817/estonia-also-affected-by-end-of-year-gps-systems-jamming>
<https://yle.fi/a/74-20067383><https://thebarentsobserver.com/en/life-and-public/2023/11/finland-suspects-russia-jams-gps-signals-essential-weather-balloons>
<https://www.reuters.com/article/idUSKCN1QZ1WM/>

The screenshot shows a news article from Yle. The main headline is "Agency confirms GPS jamming in Finland on NYE". The article text states that according to Traficom's aviation chief Jari Pöntinen, the disturbances did not affect flight safety because planes are outfitted with alternative navigation systems. The article is dated January 2023.

The screenshot shows a Reuters article from 2018. The main headline is "Norway says it proved Russian GPS interference during NATO exercises". The article text states that Oslo (Reuters) - Norway has electronic proof that Russian forces disrupted global positioning system (GPS) signals during recent NATO war games, and has demanded an explanation from its eastern neighbor, the Nordic country's defense minister said on Monday. It also mentions that both Finland and Norway said in November that Russia may have intentionally disrupted GPS signals before and during Western military exercises, which also affected the navigation of civilian air traffic in the Arctic.

The Barents Observer

Finland suspects Russia jams GPS signals vital for weather balloons

Tracking data for balloons released by the Finnish Meteorological Institute in Sodankylä have been lost several times, jeopardizing weather forecasts for northern regions.

[Read in Russian | Чумамь по-русски](#)

By **Thomas Nilsen**

November 2023



November 22, 2023

ADVERTISEMENT

Security Challenges for Space – Modems, Terminals, Dishes, Software

CYBERSCOOP Topics ▾ Special Reports Events Podcasts Videos Insights

THREATS

Satellite hack on eve of Ukraine war was a coordinated, multi-pronged assault

The satellite hack that took the world by storm was more complex than initially thought, according to a Viasat executive.

BY [CHRISTIAN VASQUEZ](#) AND [ELIAS GROLL](#) • AUGUST 10, 2023

The Register

Starlink satellite dish cracked on stage at Black Hat

Once the modchip plans are live, you can, too

By [Jessica Lyons Hardcastle](#) Fri 12 Aug 2022 | 22:40 UTC

BLACK HAT A security researcher has shown how to, with physical access at least, fully take over a Starlink satellite terminal using a homemade modchip.

Lennert Wouters, a researcher at the KU Leuven University in Belgium, walked through his methodology during a talk at Black Hat in Las Vegas this week.

threatpost Podcasts / Malware / Vulnerabilities / InfoSec Insiders / Webinars

High-Severity Cisco DoS Flaw Plagues Small-Business Switches Black Hat 2020:

Black Hat 2020: Satellite Comms Globally Open to \$300 Eavesdropping Hack

Space Odyssey: An Experimental Software Security Analysis of Satellites

Johannes Willbold*, Moritz Schloegel*‡, Manuel Vögele*, Maximilian Gerhardt*, Thorsten Holz‡, Ali Abbasi‡

*Ruhr University Bochum, *firstname.lastname@rub.de*
‡CISPA Helmholtz Center for Information Security, *lastname@cispa.de*

Source: <https://cyberscoop.com/viasat-ka-sat-hack-black-hat/>
<https://threatpost.com/black-hat-satellite-comms-eavesdropping-hack/158146/>
https://www.theregister.com/2022/08/12/starlink_terminal_hack_black_hat/
<https://jwillbold.com/paper/willbold2023spaceodyssey.pdf>

Security Challenges for Space – NTN Networks

- **Telecommunication legacy protection (core, O-RAN, MEC/edge)**
- **Telecommunication roaming protection**
- **Parameter protection that would allow DoS e.g., unavailable period, maximum time offset, QoS etc**
- **Jamming protection**
- **Updating algorithms & protocols**
- **Protection of new APIs**



The screenshot shows a research report page with the following content:

- Navigation:** RESEARCH NEWS ABOUT (with a search icon)
- Breadcrumbs:** Research > Transparency and Accountability
- Title:** Finding You
- Subtitle:** The Network Effect of Telecommunications Vulnerabilities for Location Disclosure
- Authors:** By Gary Miller and Christopher Parsons
- Date:** October 26, 2023
- Action:** Download this report
- Table of Contents:**
 - Introductions
 - 1. Roaming, SIMs, and Services 101
 - 2. Geolocation Attacks Against Telecommunications Networks
 - 3. Case Studies and Statistics
 - 4. Incentives Enabling Geolocation Attacks
 - 5. Geolocation Tracking in 5G Networks and Unimplemented Defensive Measures
 - 6. Conclusion

Evolution Steps

- **Strife towards a Zero Trust Architecture**
- **Find ways to "manage" legacy security risk through suitable firewalls and threat intelligence**
- **Further research into jamming protection e.g., through beamforming, frequency agility & magic and slicing isolation levels**
- **Bring in the toughest security requirements e.g., distributed architecture, interoperability, multi-domain (sea, land, air, space)**
- **Involvement of business customers into the design process**
- **Hands-on testing**
- **Certification & Validation (specs are only recommendations for usage)**
- **Post quantumn crypto preparation**

Questions?

Silke.Holtmanns@pwc.com

PS: This report was just published on Monday after the conference, but is very closely related and recommended reading
https://info.enea.com/tracking_on_the_battlefield_report

pwc.fi

This publication has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, PricewaterhouseCoopers Oy, its members, employees and agents do not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.

© 2024 PricewaterhouseCoopers Oy. All rights reserved. Not for further distribution without the permission of PwC. "PwC" refers to the network of member firms of PricewaterhouseCoopers International Limited (PwCIL), or, as the context requires, individual member firms of the PwC network. Each member firm is a separate legal entity and does not act as agent of PwCIL or any other member firm. PwCIL does not provide any services to clients. PwCIL is not responsible or liable for the acts or omissions of any of its member firms nor can it control the exercise of their professional judgment or bind them in any way. No member firm is responsible or liable for the acts or omissions of any other member firm nor can it control the exercise of another member firm's professional judgment or bind another member firm or PwCIL in any way.