OpenRAN – Facts and Fiction in a Changing World…

John W. Strand

www.strandreports.com

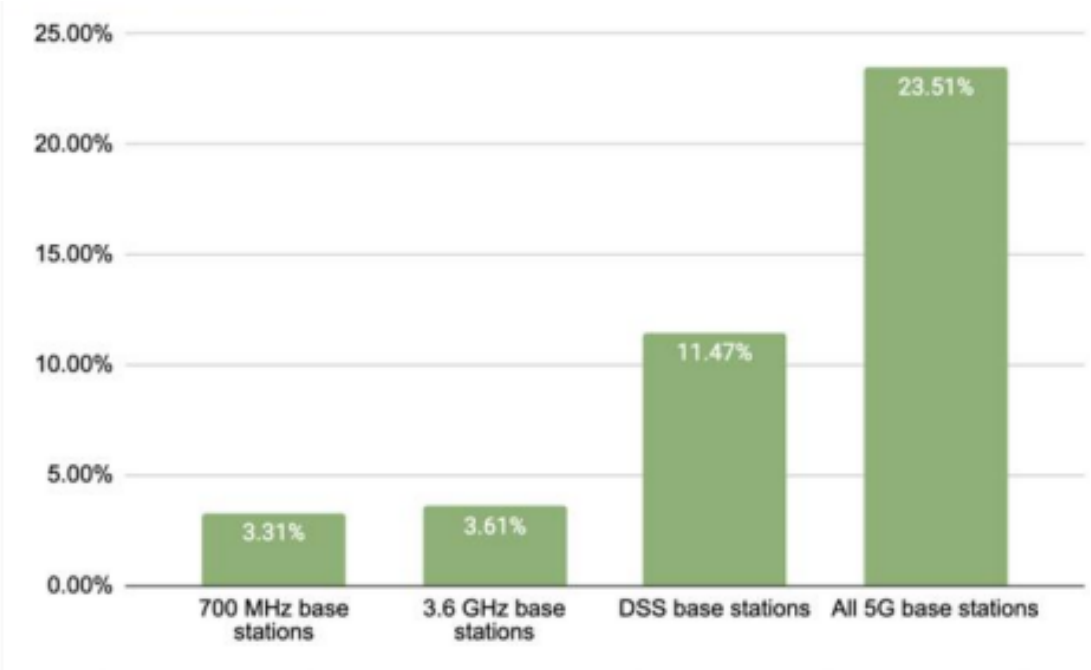
10 OpenRAN questions….

- Can you explain which services are based on RAN that require OpenRAN on a cell site to be implemented?
- Who will develop these OpenRAN-based services?
- Who will sell them?
- What business models underlie these services. Is it for the corporate or consumer market?
- Will these services only be available where the operators have implemented OpenRAN, e.g. outside the big cites?
- If OpenRAN products win market share of 15%, what share of that install base will be OpenRAN in 2025 and 2030?
- Is the vendor diversity not a result of the operators own buy in policy, European operators have bet on Chinese suppliers the last 10 years?
- Is it a problem for OpenRAN that 200 commercial classic 5G networks have been launched by the end of this year. There is only 2 commercial OpenRAN installation?
- Is it a problem that O-RAN Alliance is not a standards development organization like 3GPP and follow WTO Principles for Development of International Standards?
- How are the vendor diversity on that part of the telecom market where Qualcomm, Apple, Google, AWS, Microsoft, Intel etc. dominate?

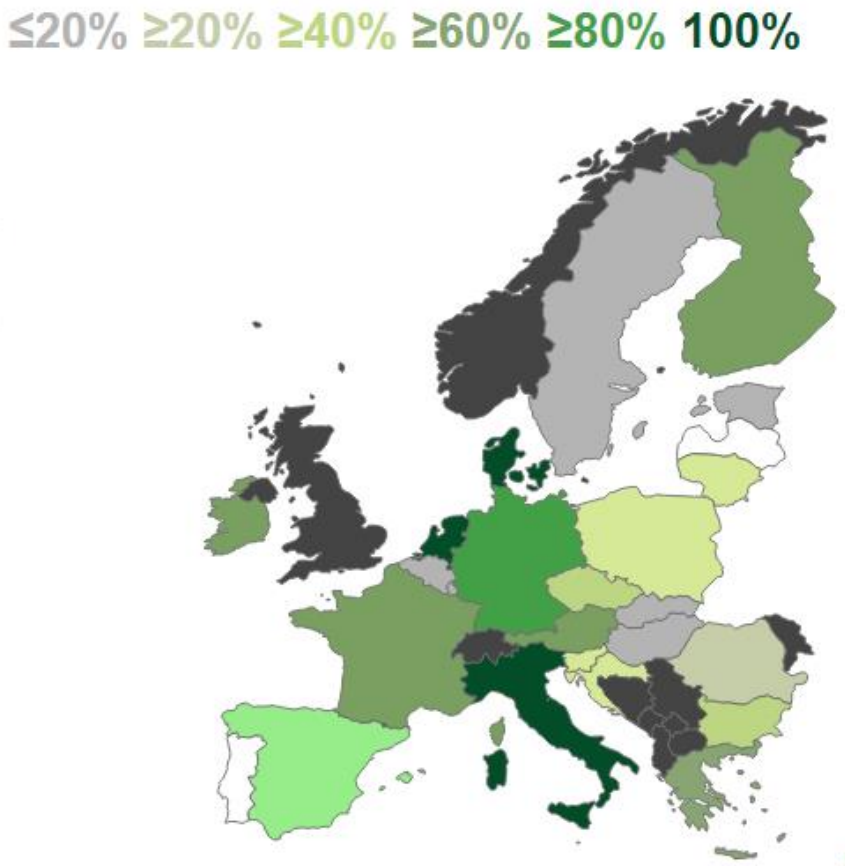
The European tower/radio site market…

- Europe had 672k antennas on 431k sites by end 2021.
- That counts 2G antennas and 3G antennas on the same site for one operator as one antenna.
- For VOD, we estimate 102k antennas excl. VodafoneZiggo; 107.5k if you include
- Germany: DT has 5K antennas 3.5 Ghz, 65K antennas using 2.1 GHz using DSS, TEF 5K antennas 3.5 Ghz and VOD 18K at 6K locations using 1.800 Mhz.
- In Denmark TDC swapped Huawei for Ericsson. 4K sites in 10 months; 90% 5G coverage from day one.

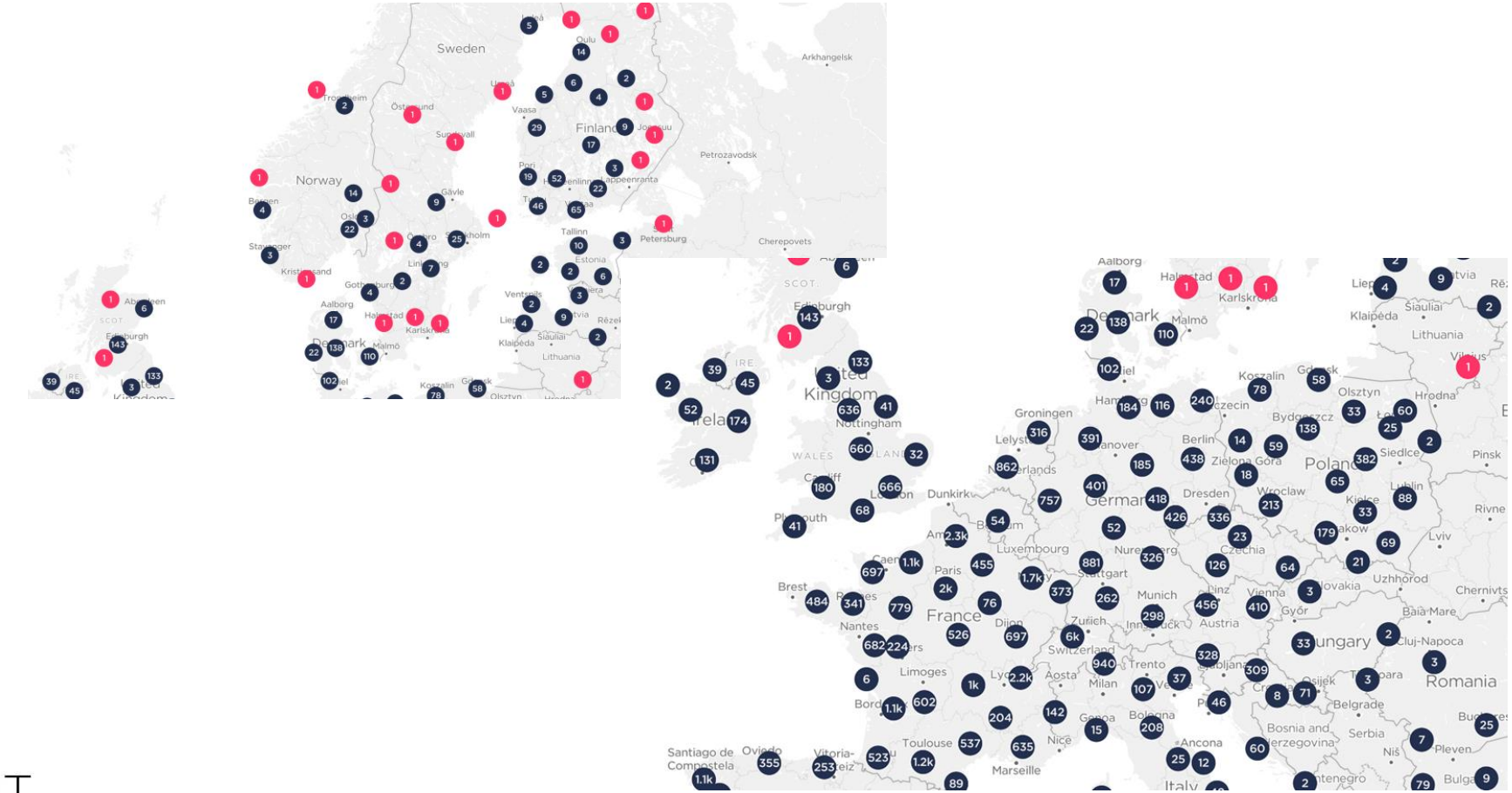
A total of 147,380 5G base stations (23.5% of the 4G sites), covering 64% of the population by end 2021 in EU27…..



Source: https://5gobservatory.eu/



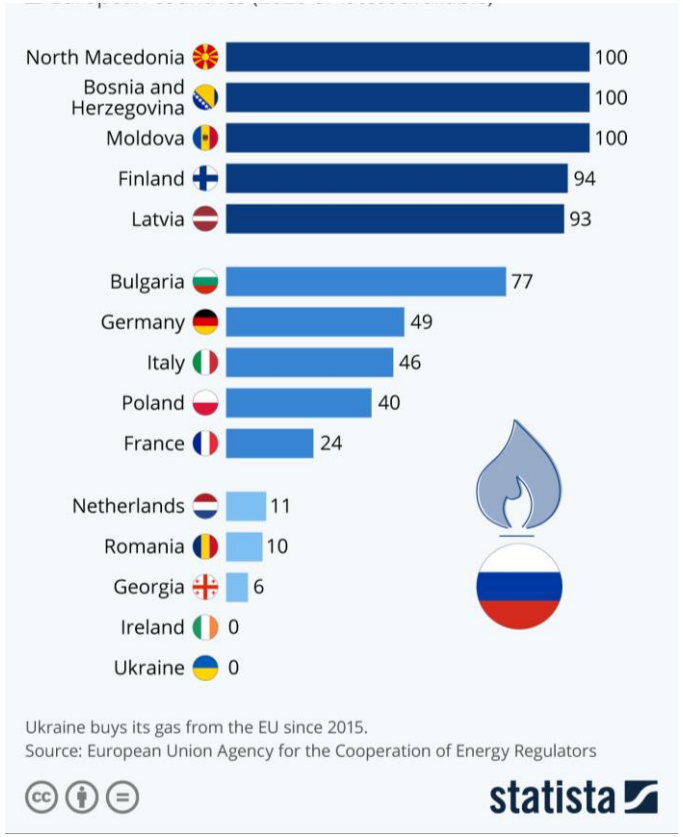
Regions: Ookla 5G Map tracks 5G rollouts…



STRAND CONSULT

WORKSHOPS
STRATEGIC REPORTS
ANALYSES
WHITE PAPERS
RESEARCH NOTES

Which European Countries Depend on Russian Gas?



Europe is at risk: Share of Chinese Vendors in 102 Mobile Networks in Europe …..dawn of the post Huawei era

Reality today:

With a large European install base of critical equipment made by Chinese government suppliers, the CCP can exert influence, if not shut down networks.

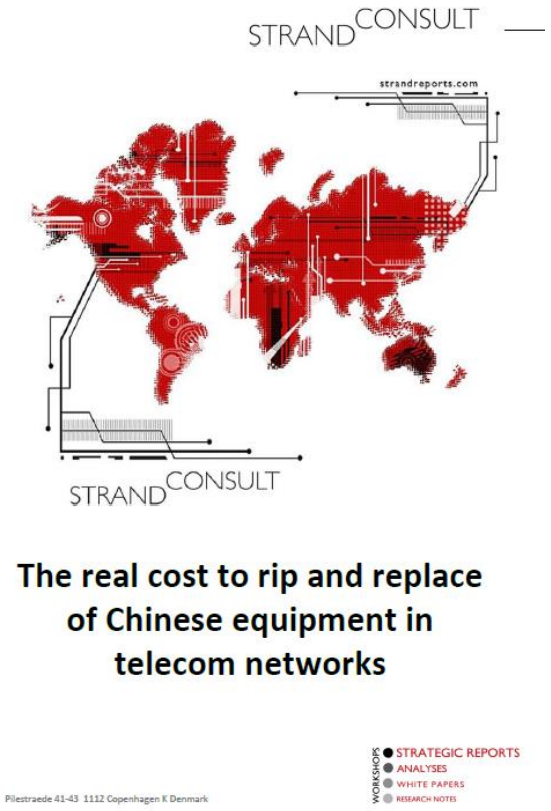
Outlook for tomorrow:

Long term development to post Huawei era.

Even knowing the risks, some European operators chose Huawei for 5G

Strand Consult: June 2020

The real cost to rip and replace Chinese equipment from telecom networks….



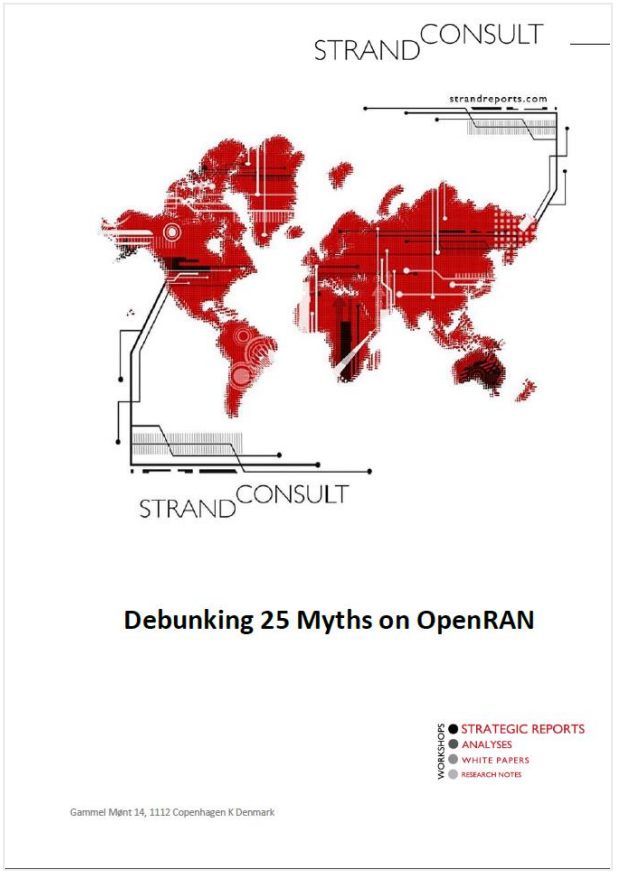
To evaluate the impact of restricting Huawei equipment from networks, one must include the fact that operators must upgrade their networks if they want 5G, regardless of whether they use Huawei. That is to say that there is a sunk cost to network upgrades which must be subtracted from the total cost of using Huawei. Most of Europe's networks are already 3-5 years old and are ready to be replaced.

In any case, 70–80 percent of the existing RAN equipment must be replaced, regardless of the political decision or the choice of vendor.

In the last 3 years mobile operators have bought radio access network (RAN) equipment for $8.75 billion (about $2.9 billion annually). Forty percent of this equipment has been purchased from Huawei and ZTE. A conservative estimate suggests that replacing the Huawei and ZTE equipment purchased since 2016 (which "probably" can be upgraded to 5G) will cost $3.5 billion. This amount compares to 14 months of total European radio access network (RAN) purchases, a small number both for Europe and the world.

At year-end 2017, 85 percent of the population in Europe (465 million people) subscribed to mobile services. The actual cost to replace the Chinese equipment is $3.5 billion for the non-upgradeable equipment. The cost is equal to a "one-time cost" of $7 or €6.5 per mobile subscriber.

Debunking 25 Myths of OpenRAN….

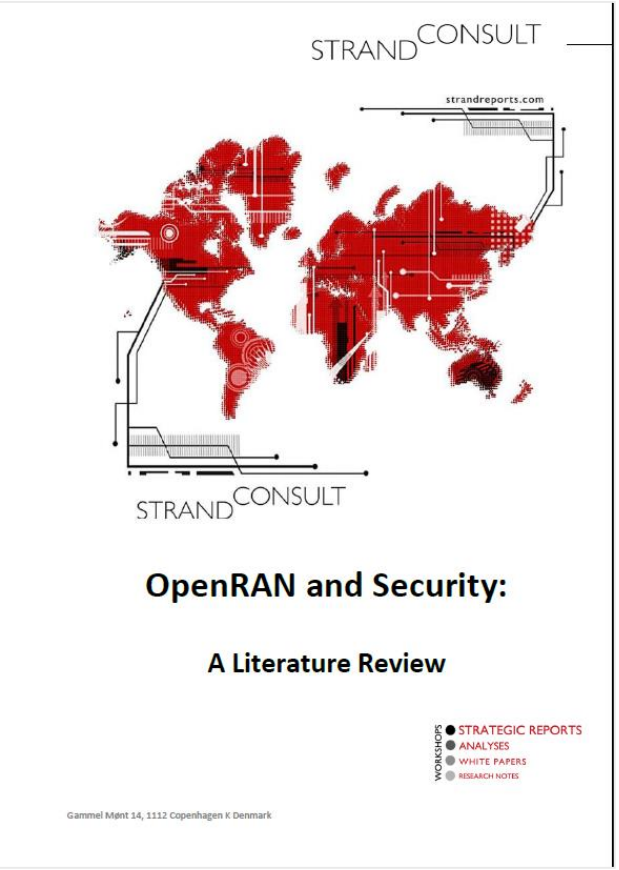


- Lack of objectivity and/or empirical support
- Preconceived notions, assumptions, and assertions about theeconomics of infrastructure, competition, and innovation
- Little to no discussion of the infrastructure value chain beyond the large infrastructure equipment providers
- Ignorance or failure to disclose that OpenRAN is not a technical standard. The O-RAN Alliance develops technical specifications for 4G and 5G RAN internal functions and interface, not for 2G and 3G. The O-RAN Alliance is not a standards development organization (SDOs) like the 3GPP.
- Ignorance or failure to disclose that OpenRAN only supports 4G and 5G and therefore it is not a 1:1 commercial alternative for 5G networks. Moreover OpenRAN does not support 2G and 3G, the prevailing network generation in many developing countries, and yet OpenRAN is reported as a solution for developing countries.
- Ignorance or failure to disclose that 182 commercial 5G networks have been launched globally. These are classic RAN installations that support 2, 3, 4 and 5G in one base station. There is only 1 commercial OpenRAN installation, Rakuten in Japan.
- Ignorance or failure to disclose how small expectations are for the OpenRAN install base by 2025 and 2030 compared to the entire market. This is likely just 1 percent in 2025 and under 3 percent in 2030.
- Ignorance or failure to disclose the role of Chinese vendors in OpenRAN ecosystem and their leading role in OpenRAN governance and specification setting

6 OpenRAN studies…

1. Cybersecurity of Open Radio Access Networks
   - Published by EU
2. Open-RAN Risikoanalyse
   - Published by Bundesamt für Sicherheit in der Informationstechnik
3. Open RAN Security in 5G
   - Published by Open RAN Policy Coalition
4. The O-RAN Alliance Tackles Security Challenges on All O-RAN Interfaces and Components
   - Published by The O-Ran Alliance Security Task Group
5. Security Threat Analysis and Treatment Strategy for ORAN
   - Published at he 2022 24th International Conference on Advanced Communication Technology
6. Open or not open: Are conventional radio access networks more secure and trustworthy than Open-RAN?
   - Authers are Klement, Felix, Stefan Katzenbeisser, Vincent Ulitzsch, Juliane Krämer, Slawomir Stanczak, Zoran Utkovski, Igor Bjelakovic, and Gerhard Wunder

OpenRAN and Security: Key Findings



1. 3GPP has developed the 5G standard with major innovations in security including but not limited (1) DDoS) (2) stronger encryption, (3) Security protocols for roaming, (4) “zero trust” enhancements for core network architectures (5) APIs which require verification (6) cloud security, and (7) network slicing. ***An important question is whether and to what degree OpenRAN includes these elements and/or other elements.***

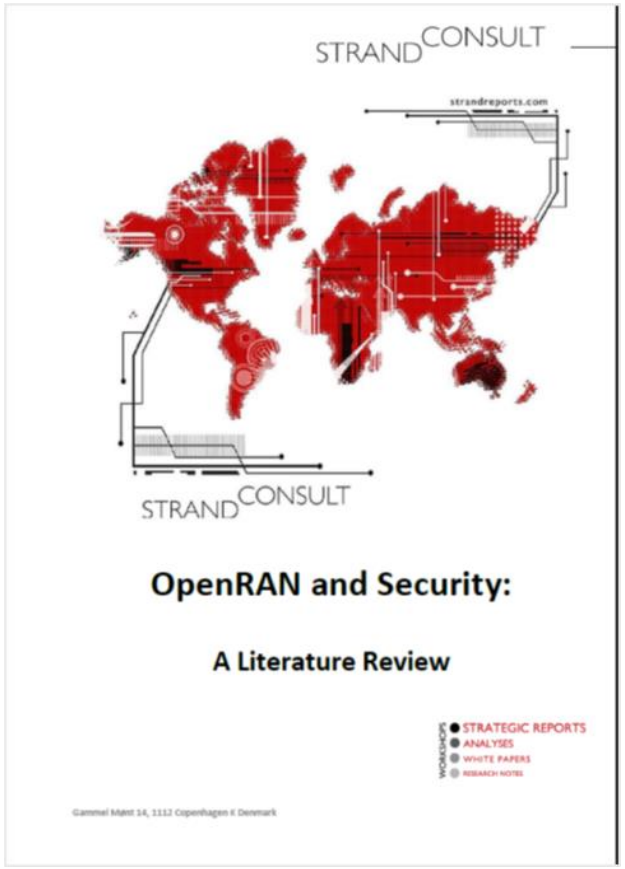
2. There are no “net new” security benefits with OpenRAN. It has no unique security standards or capabilities which are not already present with existing 5G RAN technologies.

3. Open-source software, whether in OpenRAN or classic RAN, does not necessarily make a network more secure.

4. OpenRAN presents significant new risks because of the introduction of multiple vendors, components, and interfaces each with different grades of security, quality, and product development. While OpenRAN potentially offers some benefits such as reducing dependency on some suppliers, it comes with costs, tradeoffs, and exposure to a new set of risks and dependencies.

5. A frame of reference is important with any new product or service where security risks are significant. In this way, OpenRAN security could be examined with the framework like that of automobile, for example the European New Car Assessment Programme (Euro NCAP).

OpenRAN and Security: Key Findings (2)



6. The most significant document on OpenRAN security to date was recently published by the European Union in concert with the security authorities of the 27 member states and the EU's Cyber Security agency ENISA.

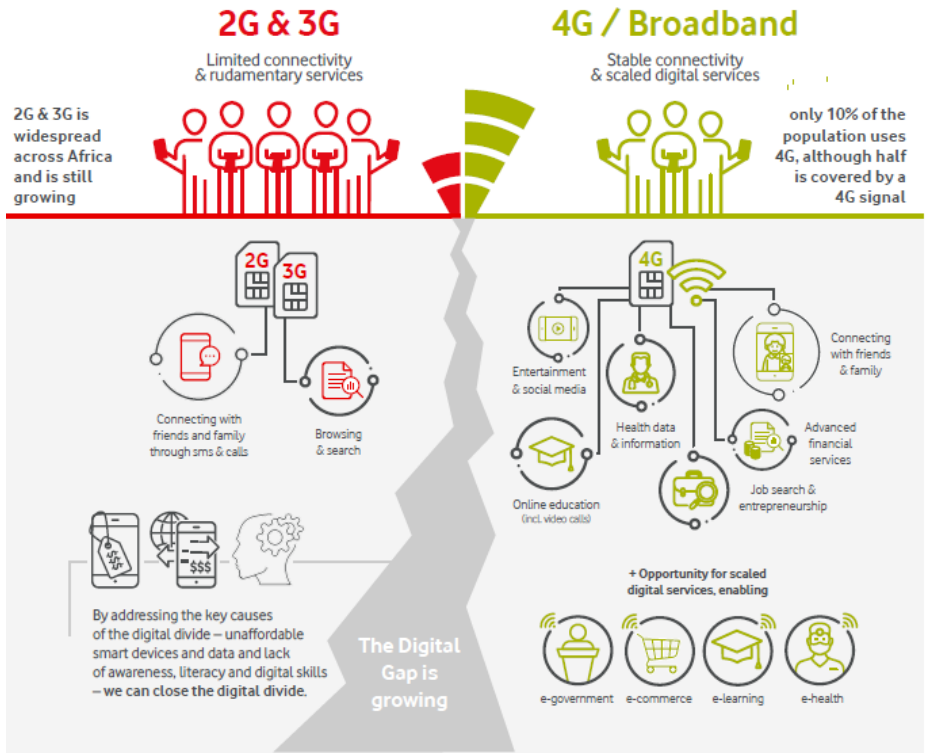
7. Security reports on OpenRAN have not appeared yet from the US, UK, India or Japan, though officials from these countries have touted OpenRAN. Reportedly the US government has Open RAN security assessments underway.

8. The report "OpenRAN and Security: A Literature Review" includes an extended discussion on technical security associated with technology produced by Chinese firms. This section covers malicious hardware, software and components, data theft and exfiltration, and unethical and illegal business practices.

9. It is not clear how OpenRAN security will overcome supply chain risk. The supply security elements of 5G are important but are not necessarily secured through standardization. Network operators must rip and replace equipment from Huawei and ZTE because of security risk. OpenRAN proponents have not yet addressed this key security conundrum, the assertion that OpenRAN can reduce reliance on Chinese vendors while its is in part designed and produced by Chinese vendors.

10. The report also documents that US trade associations and government officials have touted OpenRAN and its security benefits without providing empirical evidence or technical demonstrations.

Case: 4G in Africa 2022….



Case: Vodafone: A lifeline, not a luxury Accelerating 4G access in Sub-Saharan Africa

In sub-Saharan Africa, only 10% of the population is using 4G, although 50% is covered by a 4G signal.

By 2025 there will still be a substantial 2G and 3G penetration in several regions. In Latin America GSMA predicts 21 percent 3G phones and 5 percent 2G phones in 2025 totaling 26 percent of the market.

According to GSMA, there will be over 1 billion 2G and 3G customers by 2025 who do not have a phone that supports 4G or 5G / OpenRAN?

5G mobile networks and security - Please remember…

1. 5G is an evolution: We are at the beginning.
2. The cloud will have a central role in the future – it is like a App store
3. Artificial Intelligence (AI) will be built into all solutions and services.
4. Technical checks cannot ensure security if the vendor is malicious
5. It is not expensive to replace old Chinese infrastructure with non-Chinese infrastructure.
6. Vendor diversity and/or OpenRAN will not increase security; it will increase complexity
7. You can't distinguish between Core vs. RAN in the network – It is one network.
8. Open-source solutions will not increase security in the network, but will increase the numbers of unknown suppliers (Case: Kubernetes)
9. The value chain will become bigger, longer and more complex.
10. Things will move faster than one realizes.

Is OpenRAN is too little, too late to make a difference? If OpenRAN gets the success, it will account for less than 1% of the 5G sites in 2025; and 3% in 2030……

For more info, go to StrandConsult.dk