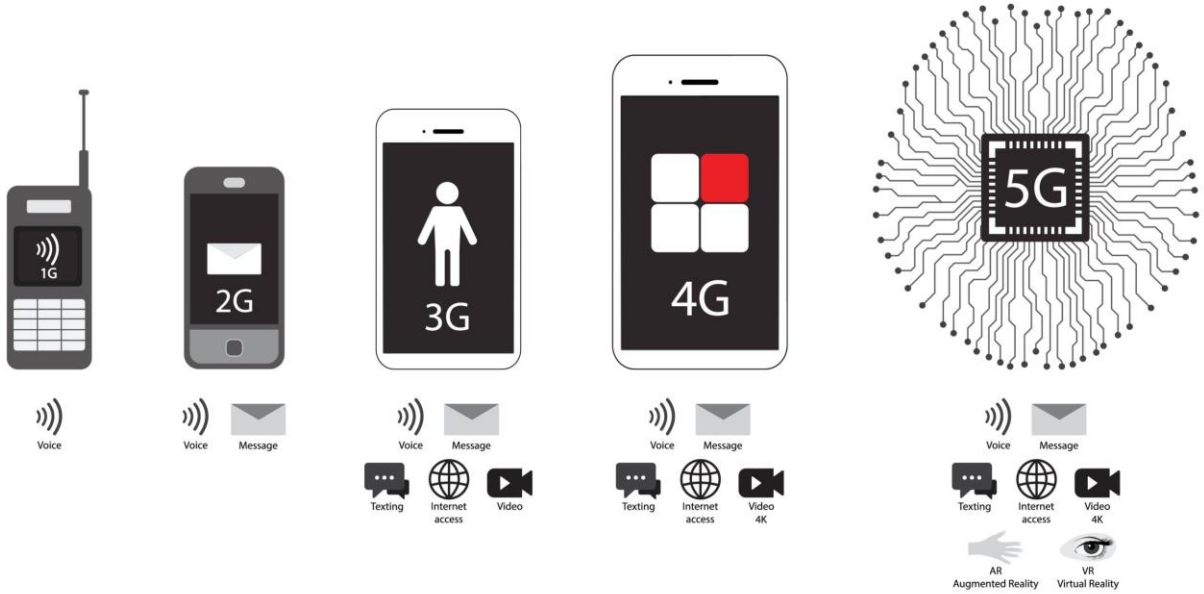
OpenRAN – Facts and Fiction in a Changing World…

Roslyn Layton,
PhD

www.strandreports.com

Mobile networks are a horizontal service and the foundation of the digital society…



On top of these networks we have a series of vertical services. Telecommunications tie things together and send data to the cloud, which is also a horizontal service….

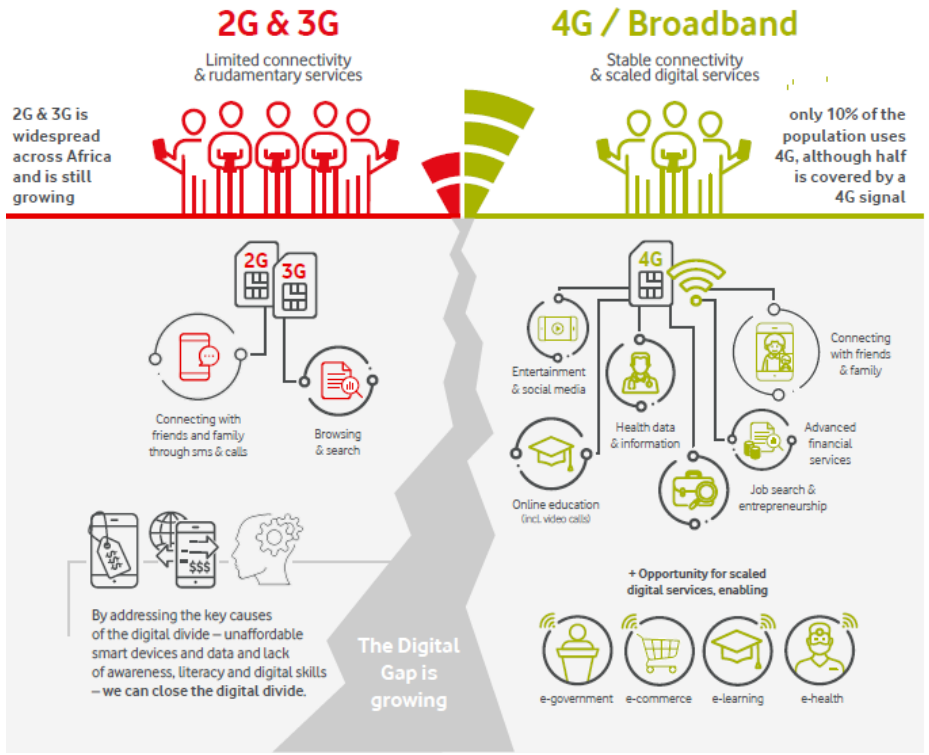
6 OpenRAN studies…

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?
   - Authors are Klement, Felix, Stefan Katzenbeisser, Vincent Ulitzsch, Juliane Krämer, Slawomir Stanczak, Zoran Utkovski, Igor Bjelakovic, and Gerhard Wunder

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?

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?

GSMA predicts that in 2025 there will still be a substantial 2G and 3G penetration in several regions….

2025	2G	3G	2G and 3G
Asia Pacific	7%	14%	21%
Armenia, Azerbaijan, Belarus, Georgia, Kazakhstan, Kyrgyzstan, Moldova, Russia, Tajikistan, Turkmenistan, Ukraine, and Uzbekistan	7%	17%	24%
Europe	1%	7%	8%
Greater China	0%	0%	0%
Latin America	5%	21%	26%
Middle East and North Africa (Algeria, Bahrain, Egypt, Iran, Iraq, Israel, Jordan, Kuwait, Lebanon, Libya, Morocco, Oman, Qatar, Saudi Arabia, Syria, Tunisia, United Arab Emirates and Yemen)	10%	36%	46%
North America	1%	6%	7%
Sub-Saharan Africa	12%	58%	70%

OpenRAN challenge related to IT engineers and system integrators in emerging markets…

- **Small, immature local tech industries.** Industry is already less developed in emerging countries, as is the sophistication for next generation mobile network engineering. IT workers may be in short supply as are the IT firms and system integrators needed to build OpenRAN solutions. This benchmark of network readiness for each country offers scores for technology, people, governance and impact.

- **Brain drains.** Skilled IT workers in emerging markets frequently migrate to developed countries where they can earn more money. MyBroadband's 2019 IT Survey found that 46 percent of IT professionals in South Africa are planning to emigrate or to seek work abroad.

- **Limited IT education:** With some exception, IT education is limited in emerging markets. Education is one critical element to creating a supply of IT workers, which nurtures the larger IT ecosystem. In the developed world, many IT companies partner with universities to support education. These co-operations may be limited, creating a vicious cycle of lack of IT education and lack of IT jobs.

- **A limited installed base.** There are more than 200 commercial 5G networks globally. These are classic 3GPP RAN installations that support 2G, 3G, 4G and 5G on one base station using 3GPP defined equipment. There is only one larger commercial OpenRAN installation, Japan's Rakuten. It has few customers and limited commercial success.

- **Vendor mix complexity**. Moving to an OpenRAN environment requires that mobile operators have the skills and resources to evolve from managing a small handful of equipment vendors to dozens of OpenRAN suppliers with no local or limited regional presence.

- **Small vendors have limited local presence**. When working in a market, customers often require that you have local experiences and local employees or employees in the region. When operating the vital infrastructure of a mobile network, a mobile operatorneeds to know that he has a well-functioning network. Uptime is an important parameter and if technical problems arise, they must be solved quickly.

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.

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.

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. Vendor diversity and/or OpenRAN will not increase security; it will increase complexity
6. You can't distinguish between Core vs. RAN in the network – It is one network.
7. Open-source solutions will not increase security in the network, but will increase the numbers of unknown suppliers (Case: Kubernetes)
8. The value chain will become bigger, longer and more complex.
9. Things will move faster than one realizes.