Security in the times of 6G

Ijaz Ahmad,
Senior Scientist, VTT Technical Research Centre of Finland
Adj. Prof. at University of Oulu, Finland

Content

- Security of 5G
  - Security: A brief history of cellular networks
  - New technologies in 5G and related security consequences
- Security in the times of 6G
  - 6G Roadmap
  - What will 6G be?
  - Roadmap of 6G security
- Concluding remarks
- Selected References

Security of 5G

Security: A brief history of cellular networks

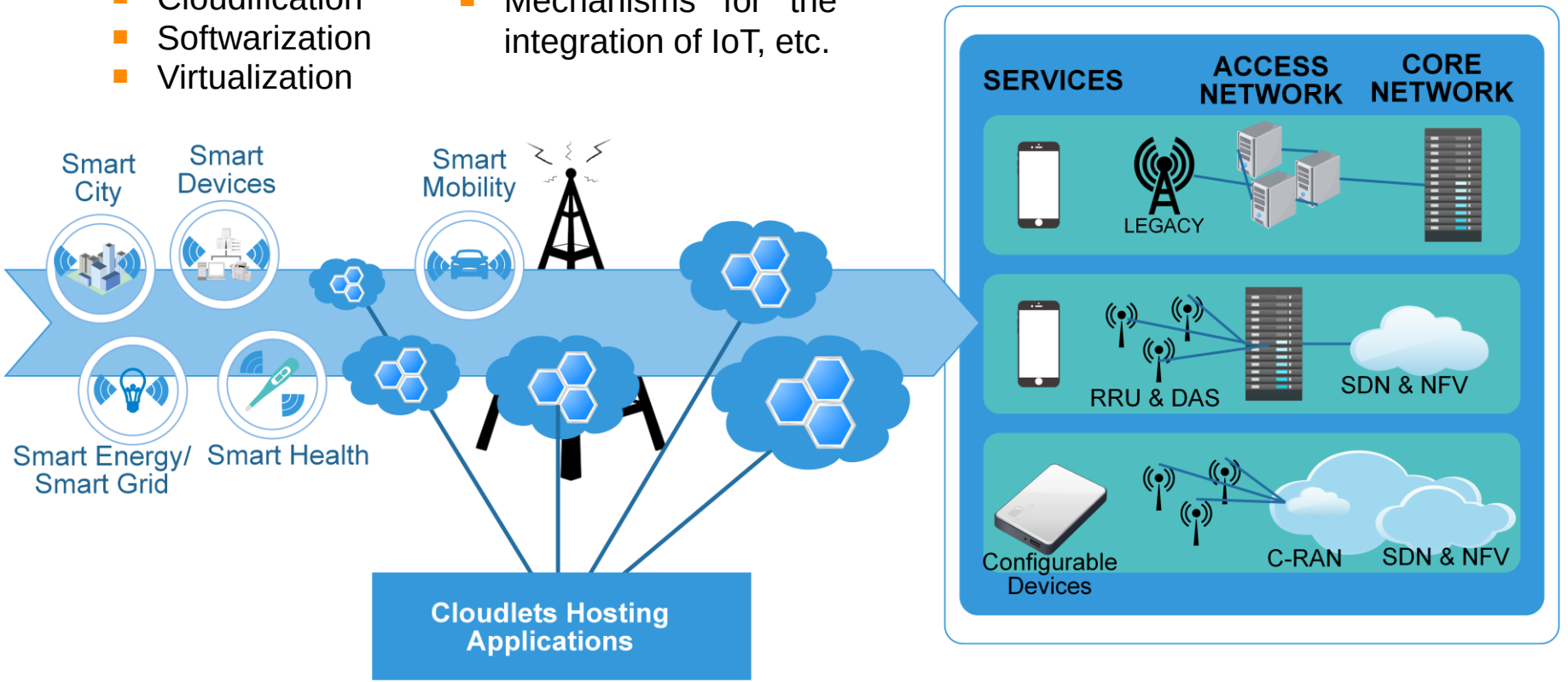
Network	Security Mechanisms	Security Challenges
1G	No explicit security and privacy measures.	Eavesdropping, call interception, and no privacy mechanisms.
2G	Authentication, anonymity and encryption-based protection.	Fake base station, radio link security, one way authentication, and spamming.
3G	Adopted the 2G security, secure access to network, introduced Authentication and Key Agreement (AKA) and two way authentication.	IP traffic security vulnerabilities, encryption keys security, roaming security.
4G	Introduced new encryption (EPS-AKA) and trust mechanisms, encryption keys security, non-3G Partnership Project (3GPP) access security, and integrity protection.	Increased IP traffic induced security, e.g. DoS attacks, data integrity, Base Transceiver Stations (BTS) security, and eavesdroping on long term keys. Not suitable for security of new services and devices, e.g. massive IoT, foreseen in 5G.

- Wireless networks have been prone to security threats, such as:
  - 1G: prone to illegal cloning and masquerading.
  - 2G: prone to message spamming and unwanted broadcasting.
  - 3G: open to Internet security vulnerabilities.
  - 4G: further migrated Internet security threats with increased speed.
  - 5G: can open our lives to security vulnerabilities in the form of IoT, critical infrastructures, health, and even our private lives:-privacy.

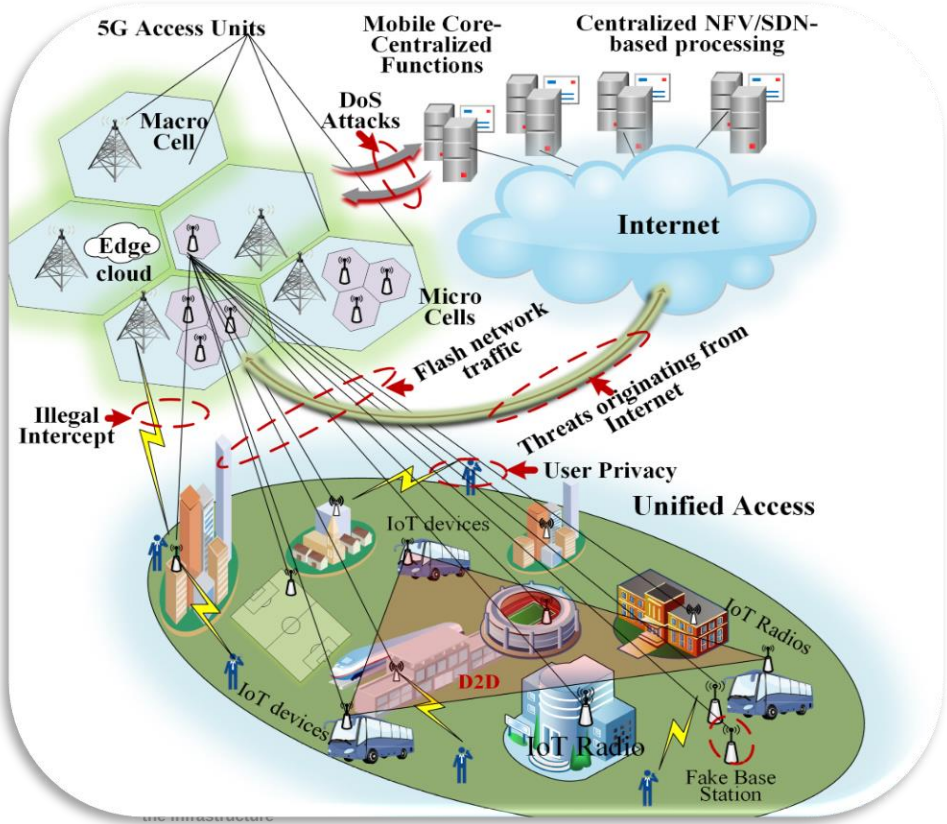
New technologies introduced in 5G

- Cloudification
- Softwarization
- Virtualization

- Mechanisms for the integration of IoT, etc.

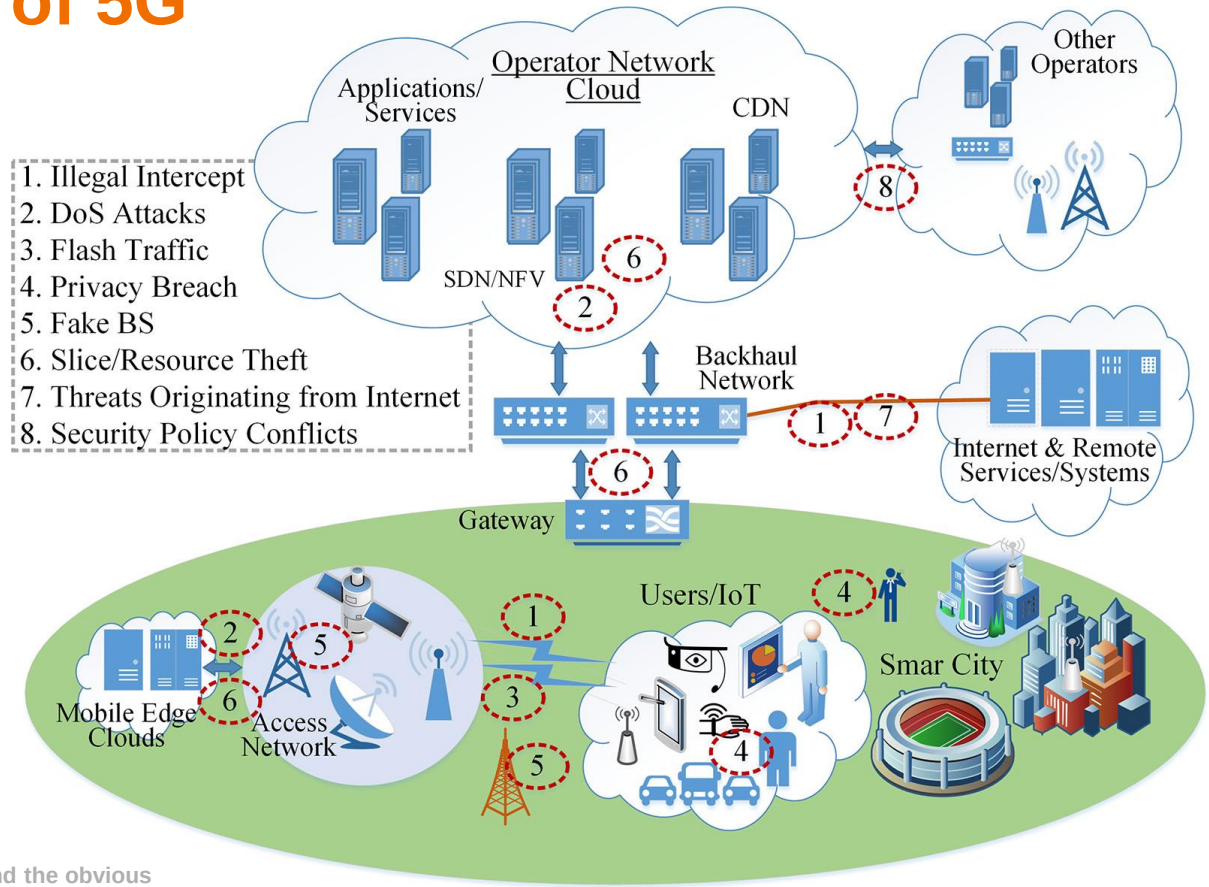


Resulting security challenges



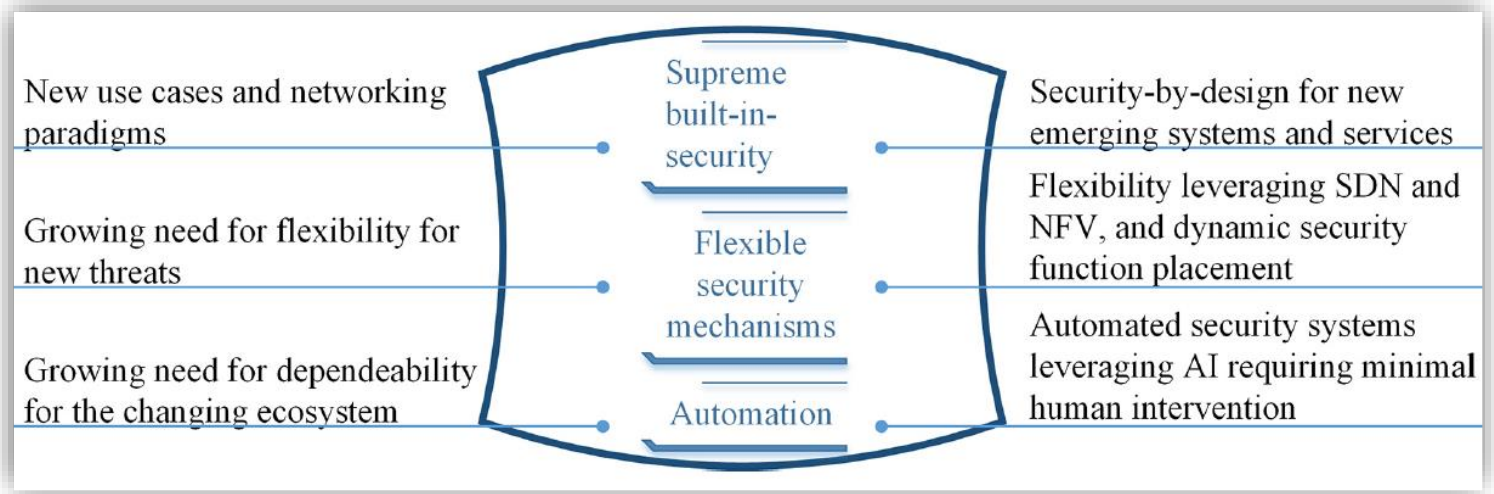
- Clouds: Maintaining important network control entities, user information in shared environments.
- SDN: Centralized control, open interfaces & third-party applications, control channel fingerprinting, and data plane dependability.
- Virtualization: Slice creation/sharing, VNF configurations, and hypervisor's centralized control.
- IoT: Flash network traffic or signaling storms, fingerprinting a compromised node (firmware implementation).

Security of 5G



Security of 5G

- Modular, technology and service-based solutions, mainly driven by the 3GPP.
- It can be claimed that 5G, as a connectivity infrastructure, is the most secure compared to the previous generations.



Security in the times of 6G

Roadmap of 6G

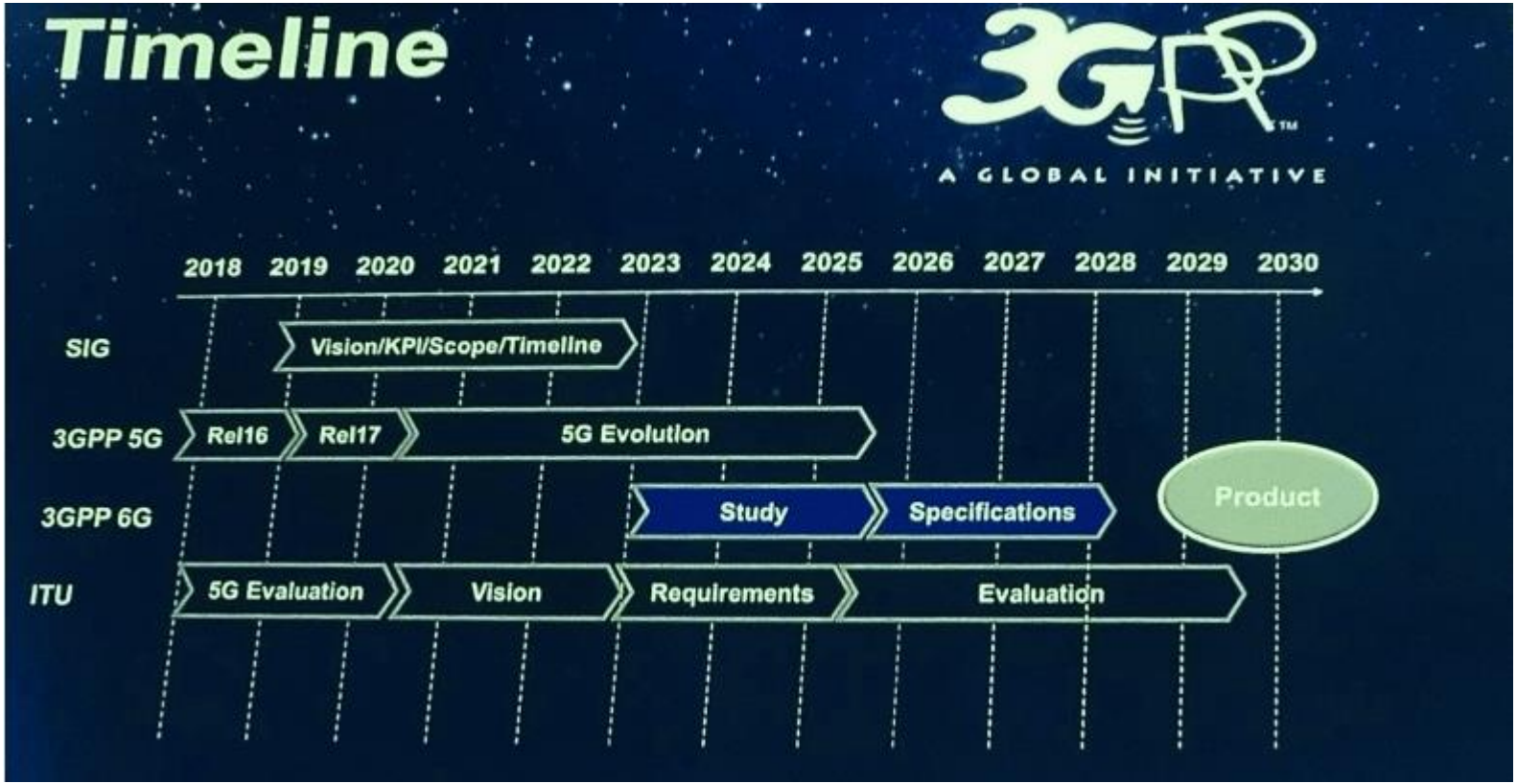


Figure source: 3GPP

What will be 6G?

- 6G should
  - contribute to an efficient, human-friendly and sustainable society through ever-present intelligent communication,
  - enable new applications (XR, industrial systems connectivity) through new technologies (terahertz).
- 6G needs
  - to be highly distributed and decentralized in nature, much like a mesh of self-organized autonomous networks working in unison.
  - each self-organizing autonomous network will have network control in its own physical vicinity.
  - therefore, have localized security policies, procedures, and technologies to maintain the independent working status of the local network.

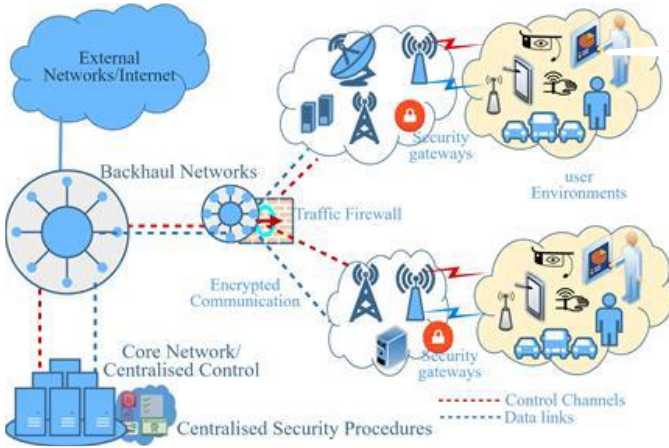
What will be 6G?...

- However, there are several limitations in the existing or evolving architectures:
  - The existing systems, such as the 3GPP-based network architecture is highly centralized,
  - It will be challenging to meet the strict requirement of future services, such as latency (physical limitations, such as speed of microwave),

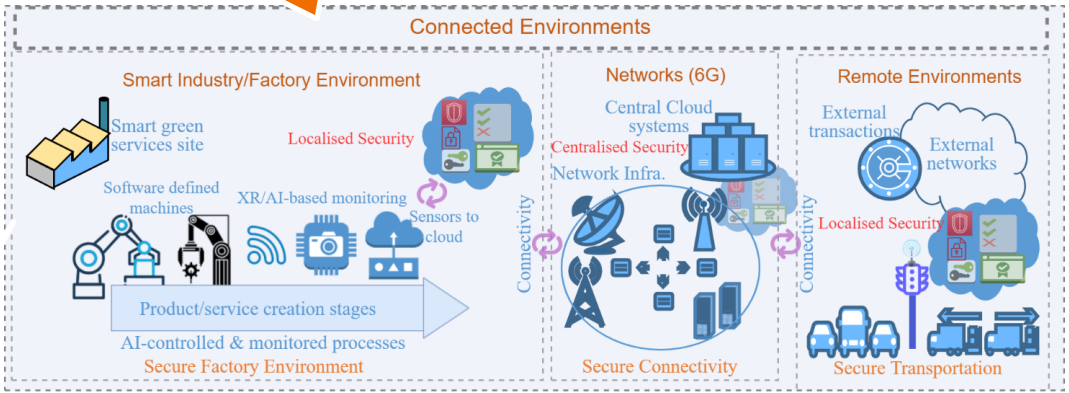
$$t = \frac{50km}{c} = \frac{50 \times 3}{3.0 \times 10^8 m/s} \approx 0.17ms$$

  - There is a need of sustainable solutions, see, the 5G new radio consumes less energy per gigabyte compared to the 4G standards, but the increased number of devices use a combined high amount of energy.
- Hence, distributed and decentralized, and sustainable network control and security policies, procedures, and technologies must be developed.

Roadmap of 6G security



From centralized to decentralized security



Towards 6G

Sustainable **6G** Security Architecture

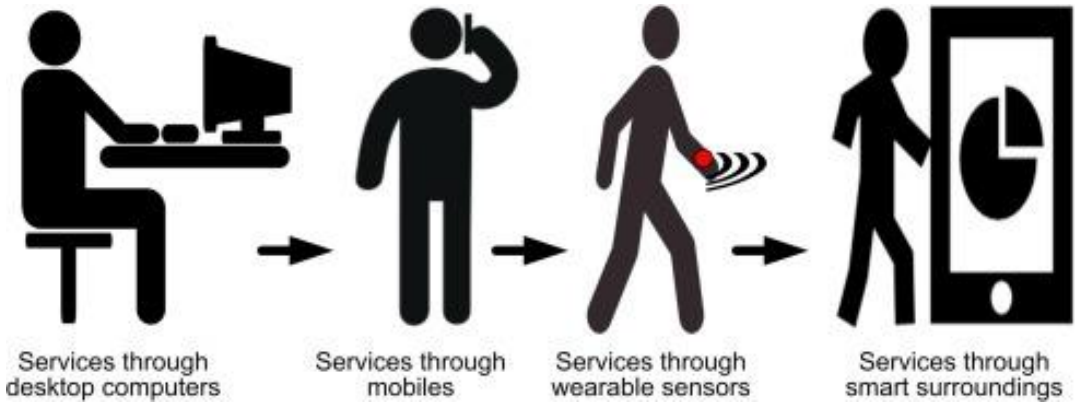
Resource-efficient in memory, processing, bandwidth:~ energy

Security of 6G

- The security architecture should be
  - Distributed in nature to meet the requirements, e.g., latency, of future services, such as authentication of moving vehicles, industrial systems,
  - Secure the network from the threats of AI, including inadvertent weaknesses and threats, such as using non-integrity verified data,
  - Secure all resources from the threats posed by quantum computing.
- Security systems need to be sustainable
  - Emerging solutions based on AI will consume huge amounts of computing, memory, transceiver, spectrum, and energy resources,
  - Distributed ledger technologies (DLTs) provide opportunity for security in untrusted environments, however, use huge amounts of resources,
  - Centralization cost resources, e.g., time and spectrum.

Concluding remarks

- 6G will provide ubiquitous connectivity with ubiquitous security that needs;
  - the definition of omni-present security, that require
  - the defintion of distributed security architecture, which
  - must be sustainable by design, that require
  - the difinition of sustainable security, and KPIs and KVIs for sustainable security.
- Hence, the immediate and most interesting research challenge we are facing is defining the potential security architecture that will fullfill the above needs.



Important References

1. I. Ahmad, S. Shahabuddin, T. Kumar, J. Okwuibe, A. Gurtov and M. Ylianttila, "Security for 5G and Beyond," in *IEEE Communications Surveys & Tutorials*, vol. 21, no. 4, pp. 3682-3722, Fourthquarter 2019. Link
2. I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila and A. Gurtov, "Overview of 5G Security Challenges and Solutions," in *IEEE Communications Standards Magazine*, vol. 2, no. 1, pp. 36-43, MARCH 2018. Link
3. Liyanage, Madhusanka, Ahmad, Ijaz, et al., eds. *A Comprehensive Guide to 5G Security*. John Wiley & Sons, 2018.
4. Porambage, P., Gür, G., Osorio, D. P. M., Liyanage, M., Gurtov, A., & Ylianttila, M. (2021). The roadmap to 6G security and privacy. *IEEE Open Journal of the Communications Society*, *2*, 1094-1122.
5. Nguyen, Van-Linh, Po-Ching Lin, Bo-Chao Cheng, Ren-Hung Hwang, and Ying-Dar Lin. "Security and privacy for 6G: A survey on prospective technologies and challenges." *IEEE Communications Surveys & Tutorials* 23, no. 4 (2021): 2384-2428.
6. Wang, Minghao, Tianqing Zhu, Tao Zhang, Jun Zhang, Shui Yu, and Wanlei Zhou. "Security and privacy in 6G networks: New areas and new challenges." *Digital Communications and Networks* 6, no. 3 (2020): 281-291.

Questions?

Thank you!

beyond

the obvious

Ijaz Ahmad
Ijaz.ahmad@vtt.fi
+358 404865746

@VTTFinland
@your_account

www.vtt.fi