Regional Forum on Cybersecurity in the Era of Emerging Technologies
&
the Second Meeting of the "Successful Administrative Practices"-2017
Cairo, Egypt 28-29 November 2017

Setting a National Cybersecurity Standard for Telecom Operators

Mohamed ElHarras
CIIP Policies and Strategy, National Telecom Regulatory Authority

Regional Forum on Cybersecurity in the Era of Emerging Technologies
&
the Second Meeting of the "Successful Administrative Practices"-2017
Cairo, Egypt 28-29 November 2017

Setting a National Cybersecurity Standard for Telecom Operators

Mohamed ElHarras
CIIP Policies and Strategy, National Telecom Regulatory Authority

ITUWTDC BUENOS AIRES 2017
9-20 October

CELEBRATING 25YEARS OF ACHIEVEMENTS

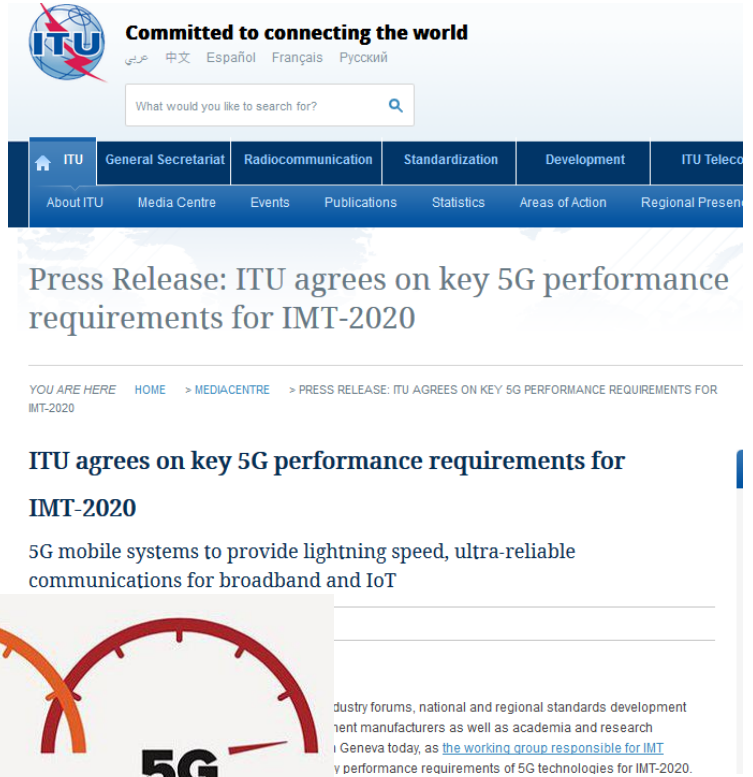
Agenda

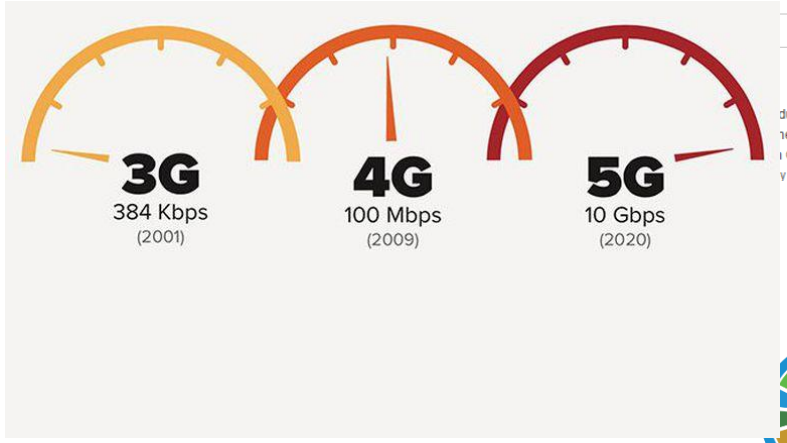
- 5G where it Stands ?
- Threats and Risks of 4/5G
- 4G Implementation Security
- Mobile Operators, a Snapshot
- The Proposed Approach

5G: One Term, Multiple Definitions

The ITU outlined 13 specs that networks will need to meet to call themselves 5G, including:

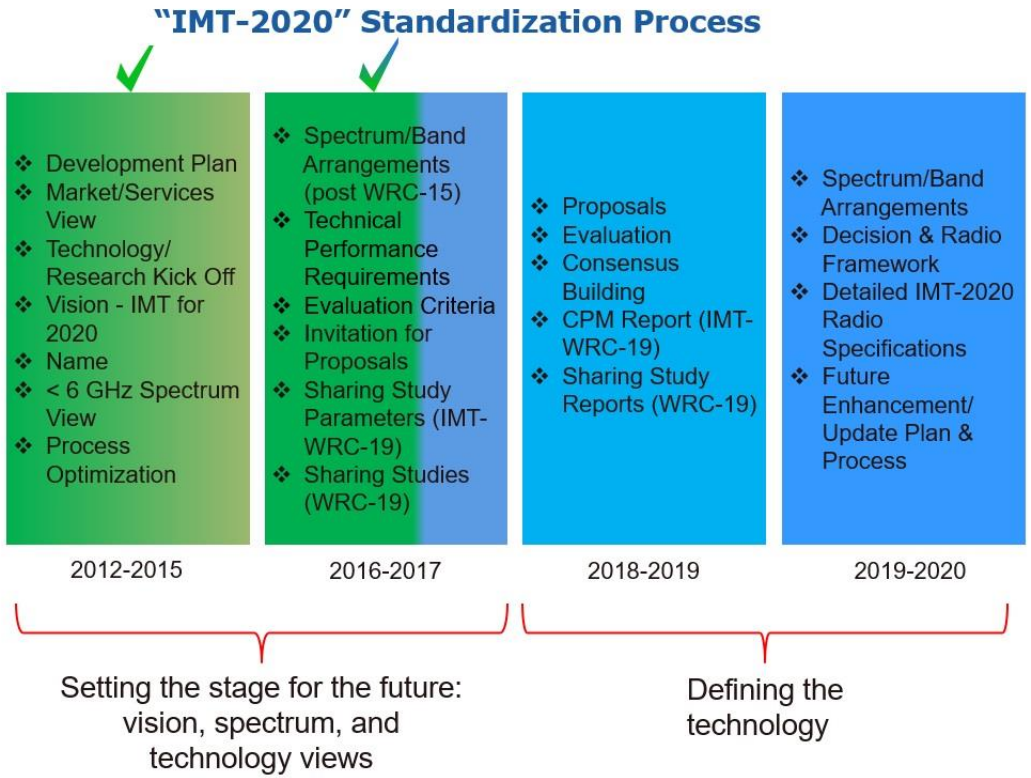
- **20Gbps peak download rate**
- **10Gbps peak upload rate**
- **30bps/Hz peak spectral efficiency downlink**
- **15bps/Hz peak spectral efficiency uplink**
- **100Mbps user experienced download rate**
- **50Mbps user experienced upload rate**





Source: http://www.itu.int/en/mediacentre/Pages/2017-PR04.aspx

5G: The ITU Roadmap



Source: http://www.itu.int/en/mediacentre/Pages/2017-PR04.aspx

5G: Security Risks

- Unauthorized access or usage of assets
- Weak slices isolation and connectivity
- Traffic embezzlement due to recursive/additive virtualization
- Insufficient technology level readiness
- Difficulties to manage vertical SLA and regulation compliance
- Slicing VS Neutrality
- Trust Management Complexity
- Provisions to facilitate change of service provider Domain Lock-in

The Current Landscape

The Dissolve of Political Borders

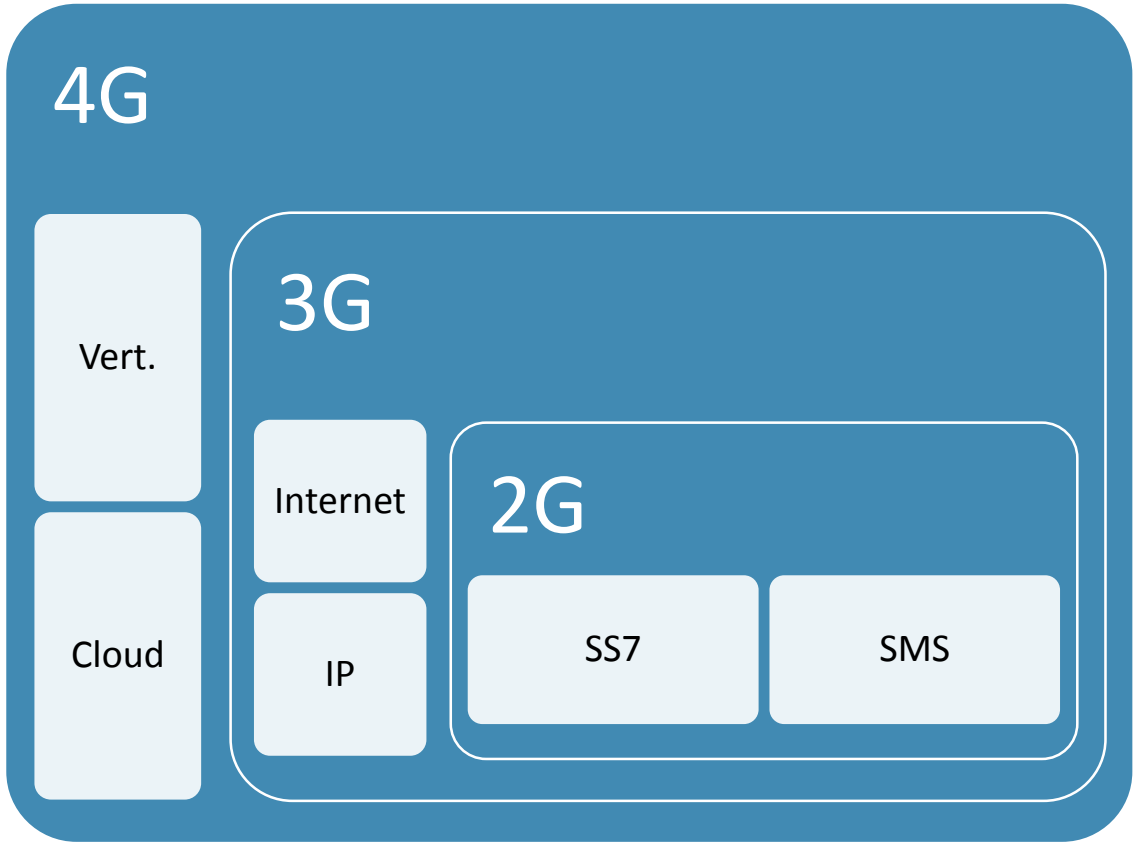
Being a critical infrastructure, mobile operators might be subject to various kinds of threats

The Mobile Operators Snapshot

- Heterogeneous Environment
- Complex interconnectivity
- Legacy vs. modern architecture
- Low-usage services (MMS)

The Modus Operandi

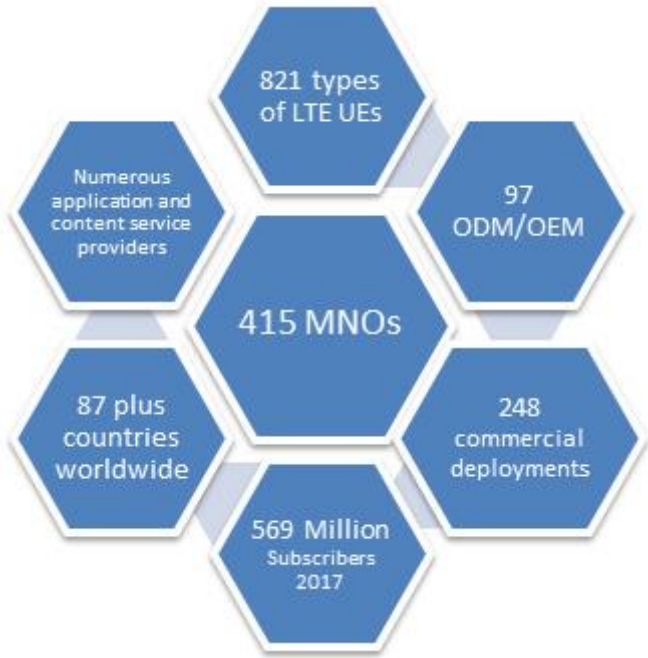
- Security vs. Business Operation Competence
- Security Team is not empowered
- Declining Mobile Operators Revenues
- Global Economic Pressures

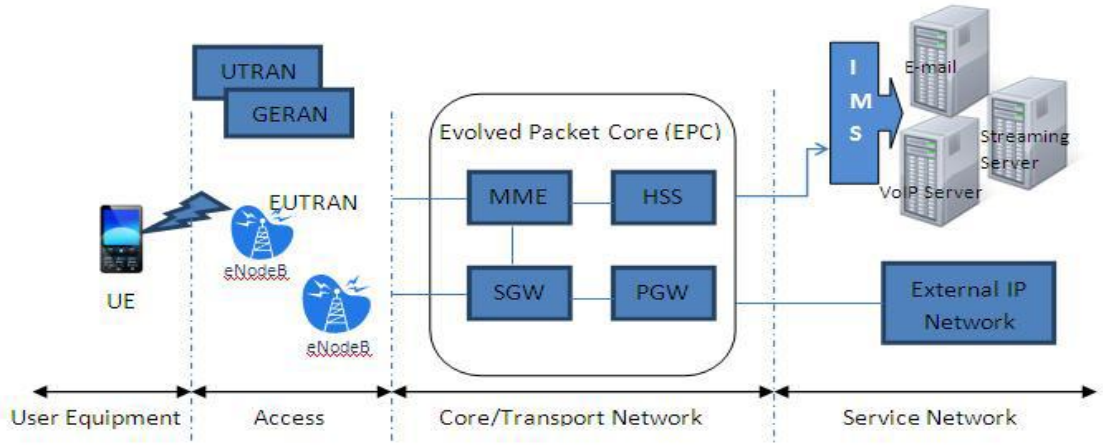


Unforeseen threats due to interdependencies plus the known risks of each generation

4G: The ECO System

- Distributed network and open architecture
- Decentralized accountability for security
- Complex business models (IS/Service sharing)
- Minimizing security spend

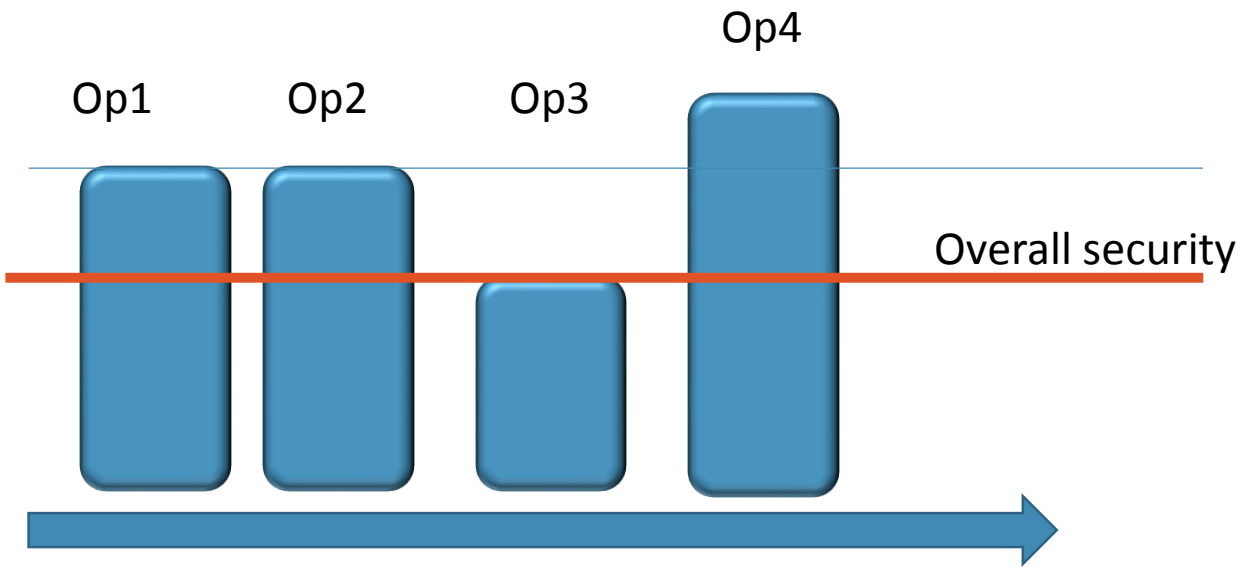


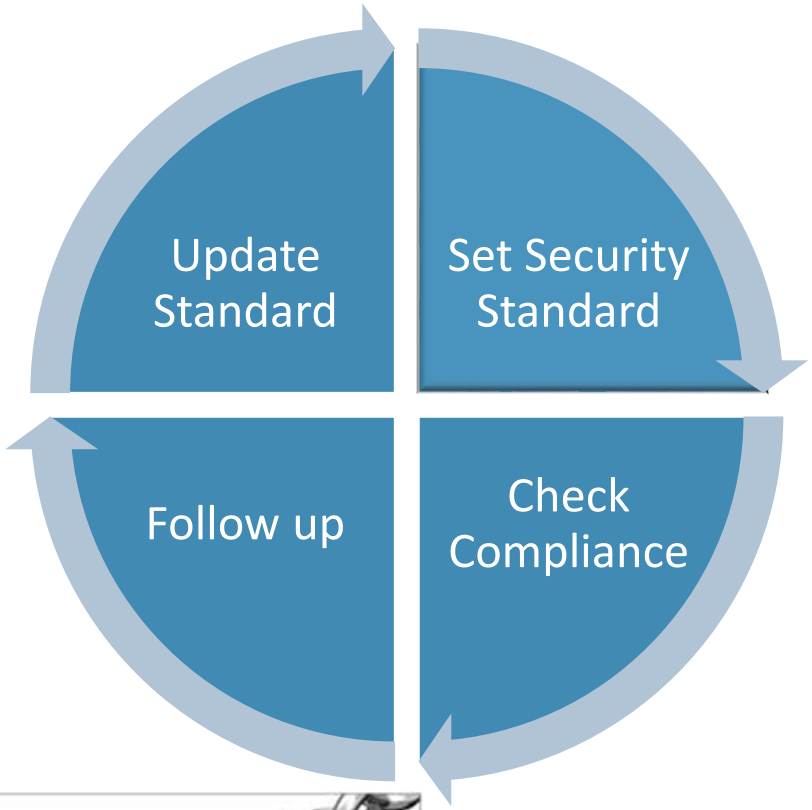


Source: https://www.csiac.org/journal-article/4g-lte-security-for-mobile-network-operators/

One Approach, Different Networks

- **Multiple operators with different 4G implementations.**
- **Different corporate cultures, business objectives and processes.**
- **The national overall networks security is at the lowest score of the group.**





The Approach

- A recognized standard should be adopted (NIST, ENISA , ..etc.)
- Auditing on the standard
- Partnership with mobile operators
- Legal / Regulatory continuous update for concurrency (weak point)
- Emergency plans and measures
- Program for awareness (user, operator)
- Technical program to transfer know-how of LTE security (radio testing, equipment type approval for security, ..etc.)
- Promoting best practices among operators
- Efforts coordination through regulations
- Improve sustainability measures (BCP/ DR)

Image: https://www.itgovernance.co.uk/blog/three-pillars-of-cyber-security/

4G/5G: Possible Good Practices for Security

Preventive (General)

- Interoperability standards
- Security audits with remediation commitments
- Strong partner agreement
- Security Budget

Preventive (Access Network)

- Physical security
- Network monitoring, IPS systems
- Authentication, , authorization, encryption
- Security Architecture

Preventive (UE)

- Subscriber education
- Industry security standards & controls on UE
- Antivirus
- Strong authentication, authorization, OS encryption

Preventive (Transport)

- Security Architecture: VPNs, VLANs
- Encryption, IKE/ IPSec
- Network monitoring, management and load balancing

4G/5G: Possible Best Practices for Security

Preventive (Service Network)

- Border Security
- Enable security protocols
- Strong authentication
- Implement Security Gateways

References

- Daksha Bhasker, “4G LTE Security for Mobile Network Operators”, Journal of Cyber Security and Information Systems, Vol 1 Issue 4, 2016
- Jeffrey Cichonski et al, “Guide to LTE Security “, NIST Special Publication Draft 800-187, 2016
- E. Belmekki, N. Bouaouda, B. Raouyane and M. Bellafkih, "IP Multimedia Subsystem: Security Evaluation," *Journal of Theoretical and Applied Information Technology,* vol. 51, no. 1, 2013.
- H. J. W. Z. Chuanxiong Guo, "Smart-Phone Attacks and Defenses," Microsoft Research.

Thank You