5G SECURITY CHALLENGES

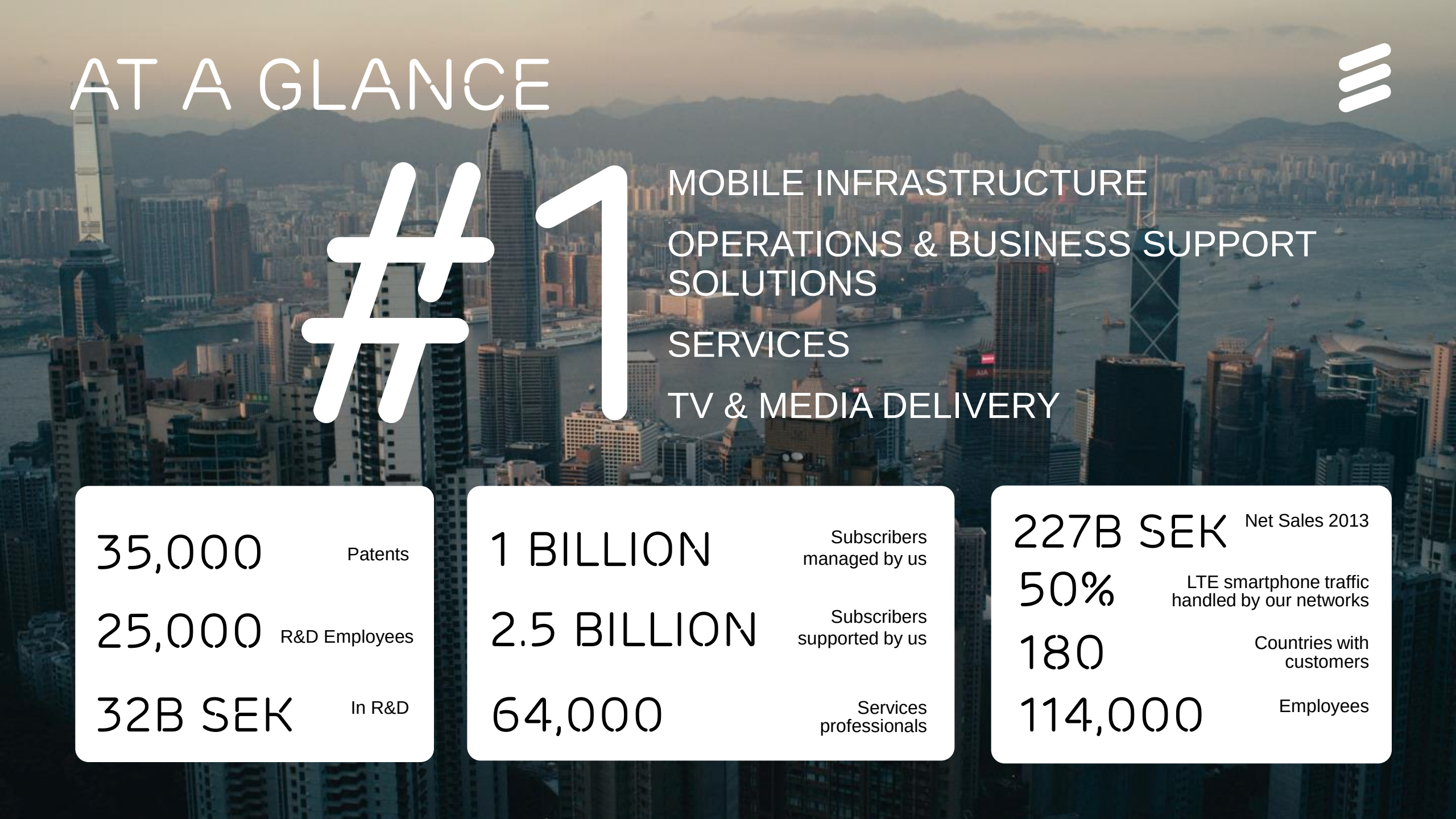
KTH ACCESS-FORCES CPS WORKSHOP

Mats Näslund, Ericsson Research and KTH/CSC
Oct 27, 2015

CONTENTS

- Part I: Background
  - Mobile network evolution
  - Mobile network security – history
  - What is 5G and what does it imply for security?
  -
- Part II: Some challenges

AT A GLANCE



#1

MOBILE INFRASTRUCTURE

OPERATIONS & BUSINESS SUPPORT SOLUTIONS

SERVICES

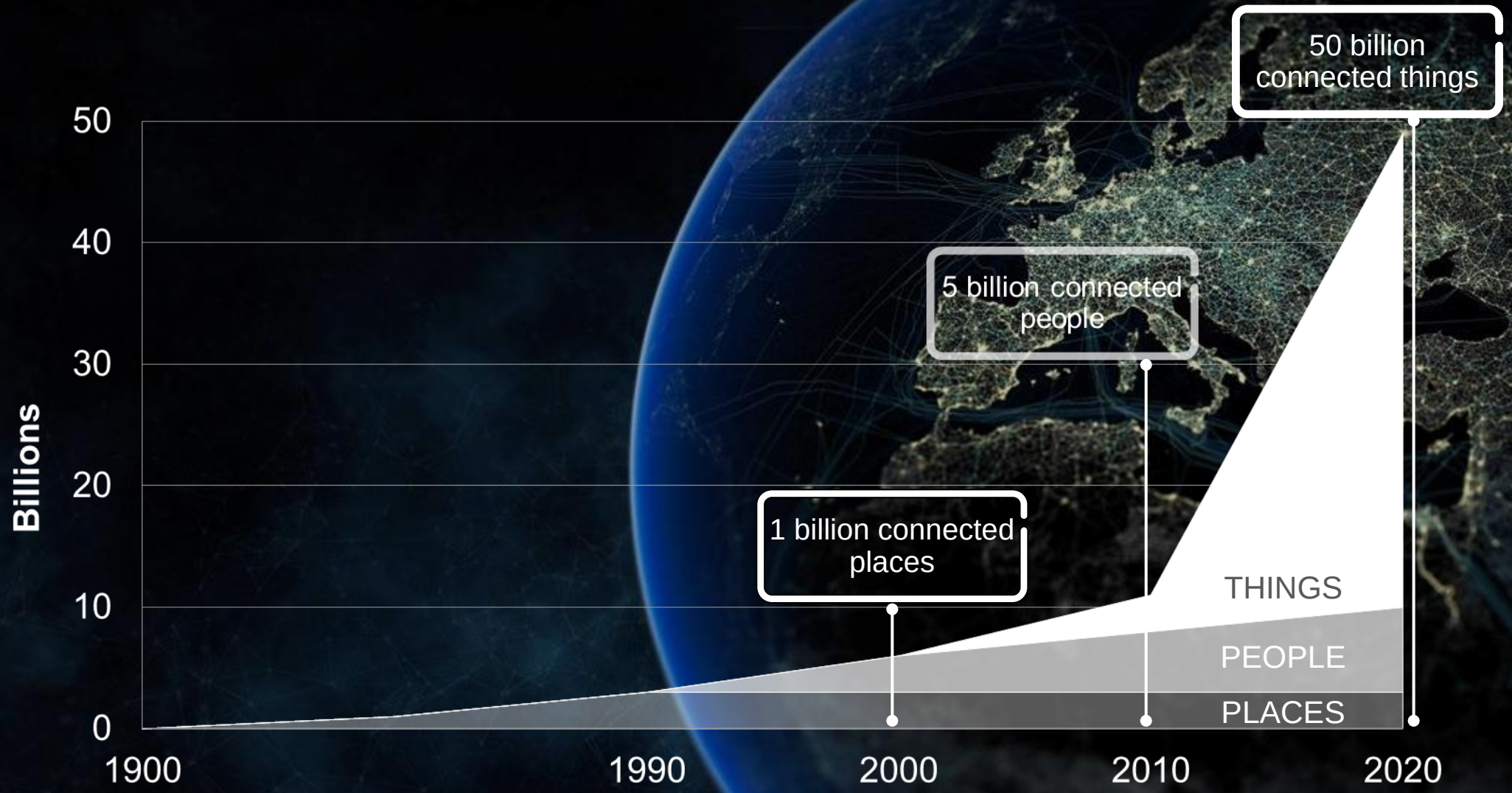
TV & MEDIA DELIVERY

35,000	Patents
25,000	R&D Employees
32B SEK	In R&D

1 BILLION	Subscribers managed by us
2.5 BILLION	Subscribers supported by us
64,000	Services professionals

227B SEK	Net Sales 2013
50%	LTE smartphone traffic handled by our networks
180	Countries with customers
114,000	Employees

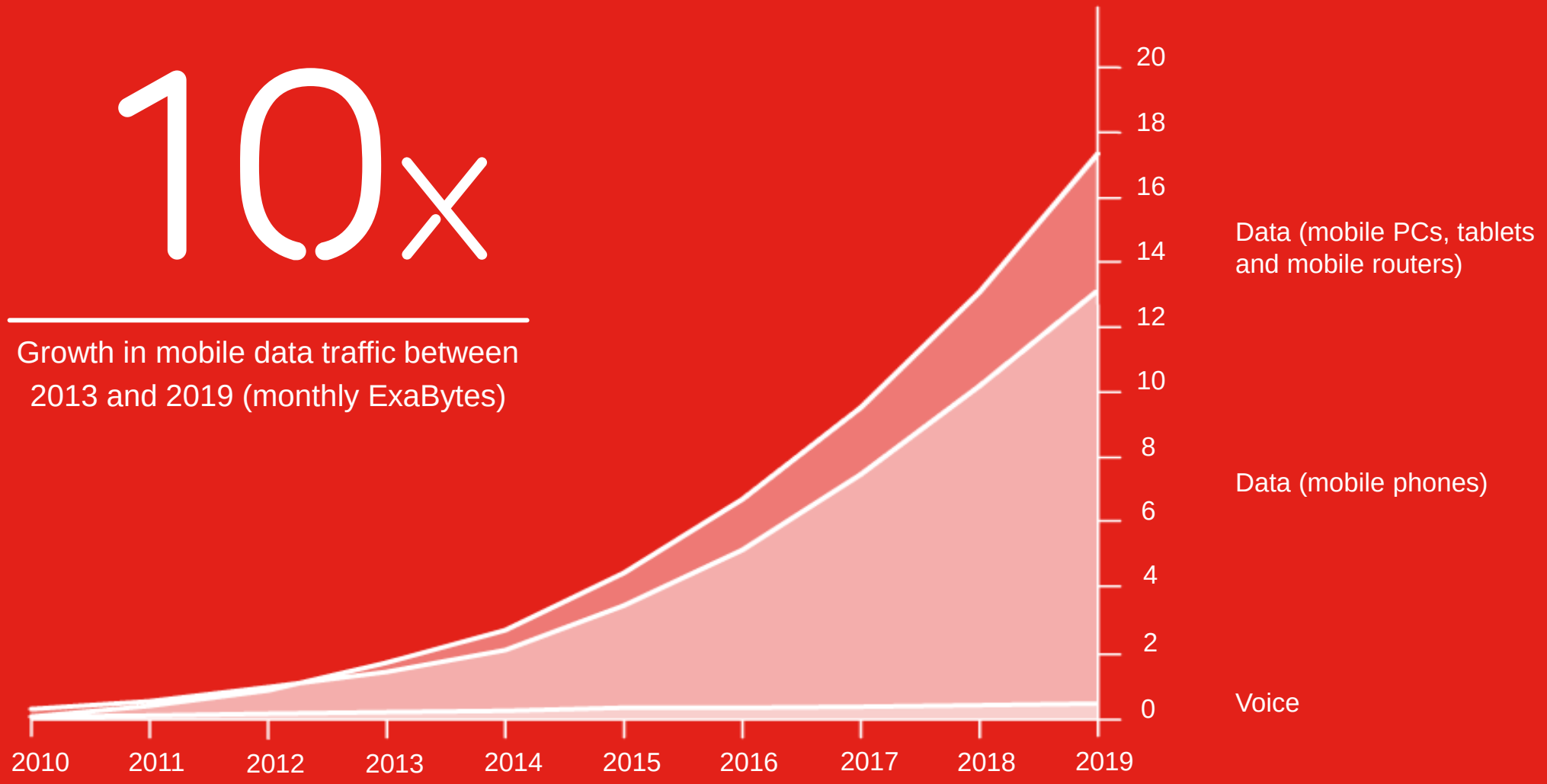
PACE OF CHANGE



MOBILE TRAFFIC GROWTH

10x

Growth in mobile data traffic between 2013 and 2019 (monthly ExaBytes)



Source: November 2013 Ericson Mobility Report

SECURITY DRIVERS FOR 2G, 3G, 4G

One basic service to protect

- Connectivity, in particular voice

Security needed for trust and business

- User privacy: user data encryption, basic identity protection
- Reliable charging: strong authentication

Slight changes in threats over time

- Led to “incremental” improvements in new generations

Has worked very well

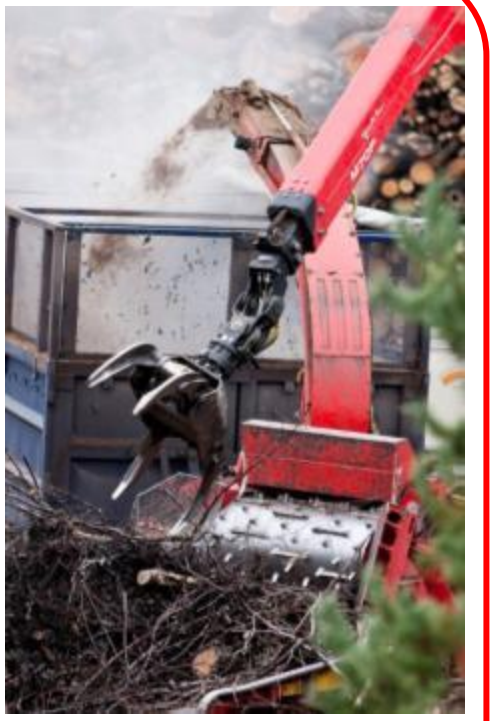
- Some “legacy” crypto problems in 2G, but largely a success

5G USE CASE EXAMPLES

Broadband experience everywhere anytime

Massive Machine Type Communication

Entertainment, Education



Critical Machine Type Communication

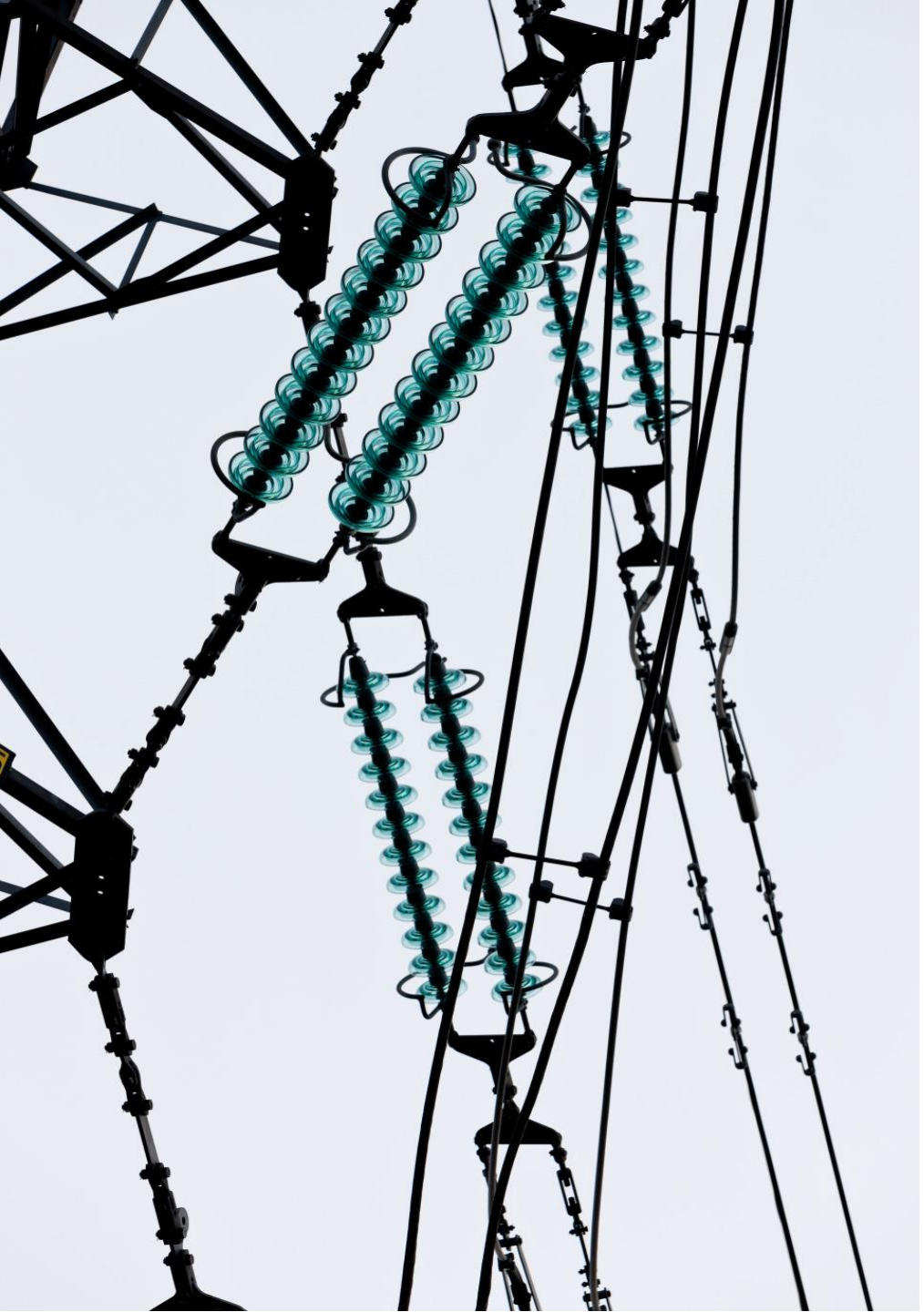
WHAT DEFINES 5G SECURITY?

NEW BUSINESS & TRUST MODELS

NEW SERVICE DELIVERY MODELS

INCREASED PRIVACY CONCERNS

EVOLVED THREAT LANDSCAPE



BUSINESS AND TRUST MODELS

Re-use of 5G outside telco, new actors in value chain

New types of roaming agreements, e.g. between traditional operator and industry vertical

Third party VNFs running inside 5G network

The concept of “device” will change in nature, e.g. capillary networks, sensors ranging from low cost “motes” to absolutely mission critical ones

5G SERVICE DELIVERY

More agile and cost-effective deployment of new services on all layers

Network components
Mobility policy data plane

VNF VNF VNF

vEPC

Distribute

Network components

Mobility Policy Data plane

VNF VNF VNF VNF

HSS-S vEPC CSCF MSC-S

Virtualization

SDN-enabled network

Toolbox to build dedicated service

PRIVACY

Amount of end-to-end encrypted traffic has already grown dramatically after mass surveillance allegations

Big data generated in 5G systems open enormous opportunities but also potential for unprecedented privacy breaches

EVOLVED THREAT LANDSCAPE

Society has become more dependent on communication systems

Trend increases with mission-critical use of 5G, IoT, and the Networked Society

Increased threat level to our systems and software

- increased attack surface
- increased value for attackers of telecom systems
- increased damage when attacks happens

KEY SECURITY AREAS FOR 5G

Cyber-attack resistance

Trust and assurance

Privacy

Virtualization and SW security

- Coop with KTH already established

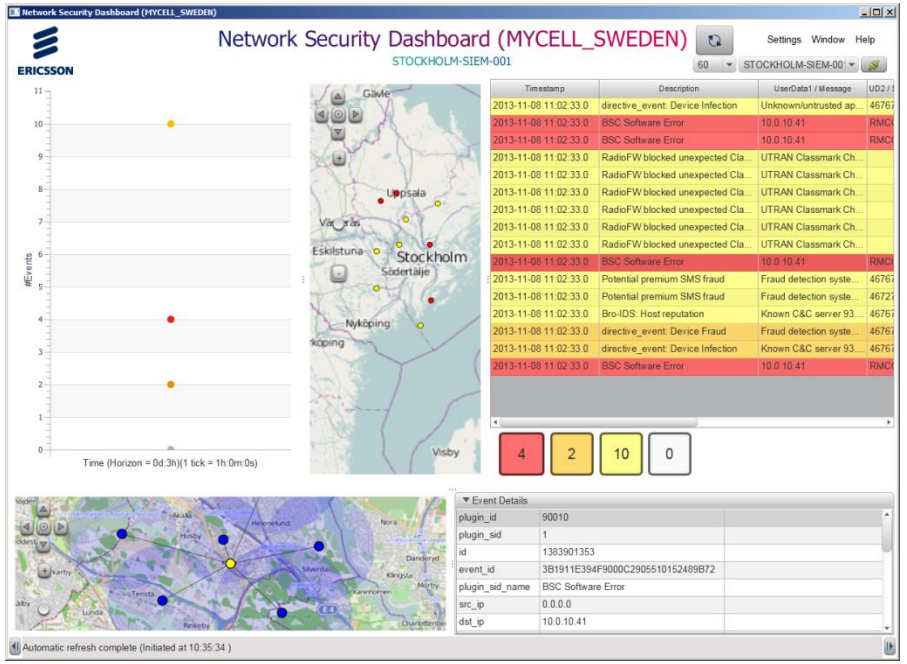
CYBER-ATTACK RESISTANCE

We have so far assumed “friendly” devices, following standard radio protocols

- But new tools for attackers…

Software Defined Radio

Should consider protection against malfunctioning or malicious M2M devices at all layers down to PHY layer



PoC demo at MWC 2014

TRUST, ASSURANCE, COMPLEXITY

- 5G systems will mix equipment from
  - Telecom providers (e.g. Ericsson)
  - IT providers (e.g. Cisco, IBM)
  - Industry/automation (e.g. ABB)
  - Plethora of “devices” (meters, cars,….)
- 5G role as critical infrastructure may require special compliance and “security certifications”
  - General IT Assurance (ISO 15408, “Common Criteria”)
  - Road safety (ISO 26262)
  - Health (ISO 27799)
  - Smart grid (IEC)
  - National regulations
- How can we manage these complex systems?
  - Can we avoid network-wide multi-certification?
  - Can we use common “trust anchors” for all use-cases?

PRIVACY (VERY CONCRETE EXAMPLE)

- So called “IMSI catchers” are making headline news
- “Wearable” devices will increase threats
- We should improve security against “tracking” in 5G

Secret surveillance of Norway's leaders detected

Members of parliament and the prime minister of Norway are being monitored by means of secret espionage equipment.

Andreas Bakke Foss , Per Anders Johansen , Fredrik Hager-Thoresen

Oppdatert: 16.des. 2014 14:53

Del Tweet E-post Lagre artikkelen i leselisten

Norway's major secrets are being administered here, right in the centre of Oslo. A number of the most important state institutions are situated within a radius of one kilometer: The Prime minister's office, the Ministry of defence, Stortinget (parliament) and the central bank, Norges Bank. Ministers, state secretaries, members of parliament, state officials, business executives and other essential staff engaged in protecting the nation's security, our military and our oil wealth – totalling more than 6000 billion kroner (NOK) - are working within this area.

The norwegian parliament - Stortinget - is situated in the centre of Oslo.
FOTO: Monica Strømdahl

But passers-by are hardly aware of the following fact: In several locations someone has installed secret transmitters which most probably behave like fake mobile base stations. These so called IMSI-catchers can monitor all mobile activity in the vicinity.

The people who run this surveillance equipment may in principle monitor every person moving in and out of the parliament building, the goverment offices or other institutions in the area. They can also select

SISTE NYTT

WASHINGTON D.C. IS LITTERED WITH PHONY CELL TOWERS

THE RUSSIAN EMBASSY, WHITE HOUSE, SUPREME COURT, AND OTHER LANDMARKS HAVE SOME NOSY NEIGHBORS, CLAIMS THE MAKER OF AN ULTRASECURE MOBILE PHONE.

By Andrew Rosenblum Posted September 18, 2014

80 Shares

SUMMARY

- We believe 5G Security to consist of four main “new” topics
  - New trust models
  - New ways to deliver services
  - Increased concerns for privacy
  - Evolved threat landscape

ERICSSON