



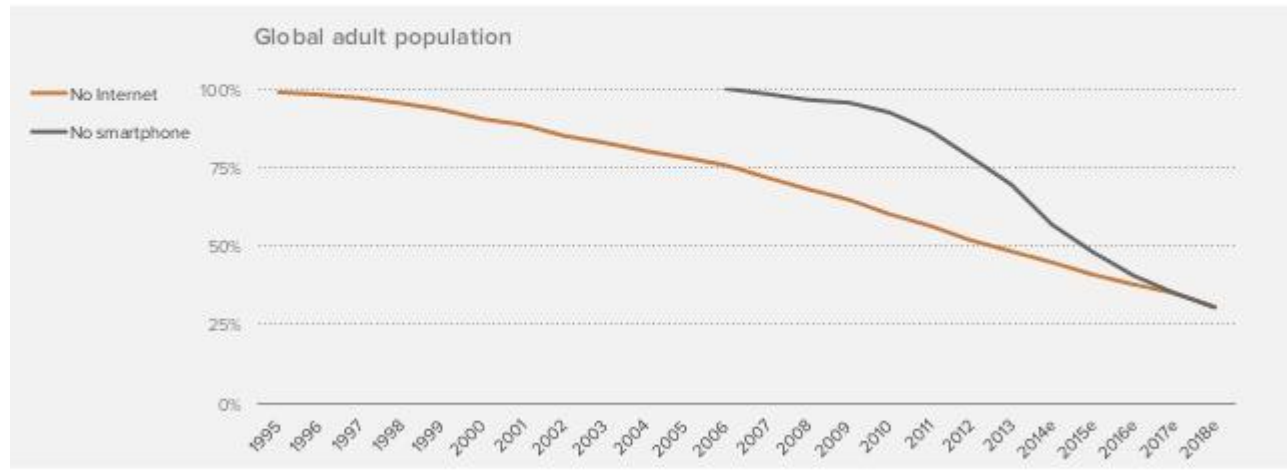
Quantum Safe Communication – Preparing for the Next Era

Dong-Hi SIM (a.k.a Donghee Shim)
Head of Global Standards, SK Telecom
ITU Workshop on Quantum Information Technology
June 5 -7, 2019

What does Mobile Deployment mean?

The end of the unconnected

Smartphones drive much greater internet penetration



ANDREESSEN HOROWITZ

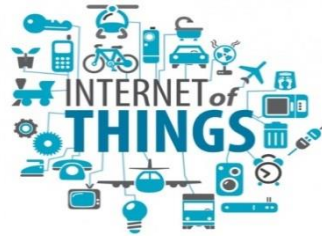
Source: a16z, World Bank, Apple, Google, Nokia

Now things are getting connected and even more intelligent to provide service at offline

Internet of Information

Internet of Things

Internet of Actions



So What?

**Cybersecurity is expanded to Physical Space
as Internet is becoming Internet of Actions**

Life or Death Situation can happen in Internet of Actions



POS hacking via HVAC

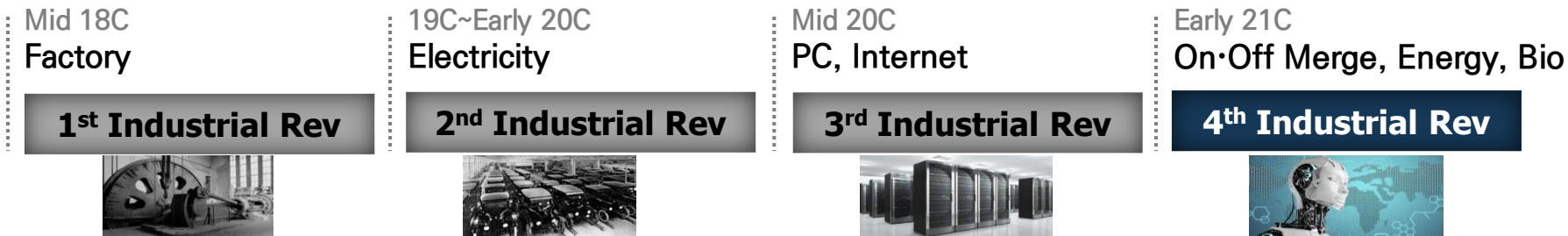
- Massive customer data breach('14.01)
- 40M debit and credit card info
- Hackers gained access to Target POS system using login credentials belonging to an HVAC company

Autopilot Hacking

- Tencent Keen Security Lab('19.03)
- Remotely gain root privilege of Autopilot SW & Control the steering system
- Can disturb the autowipes functions
- Can mislead the Tesla car into the reverse lane with minor changes on the road



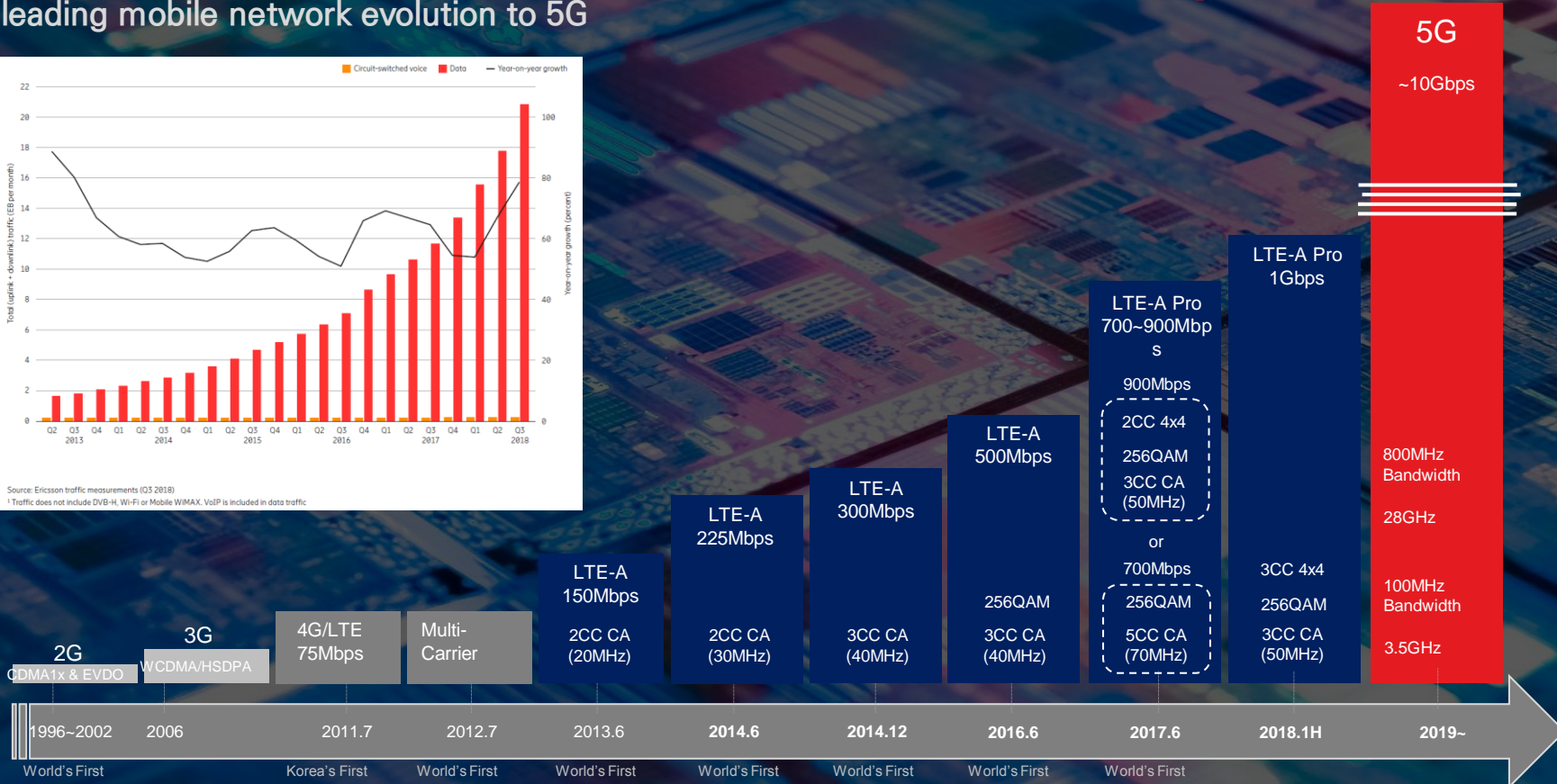
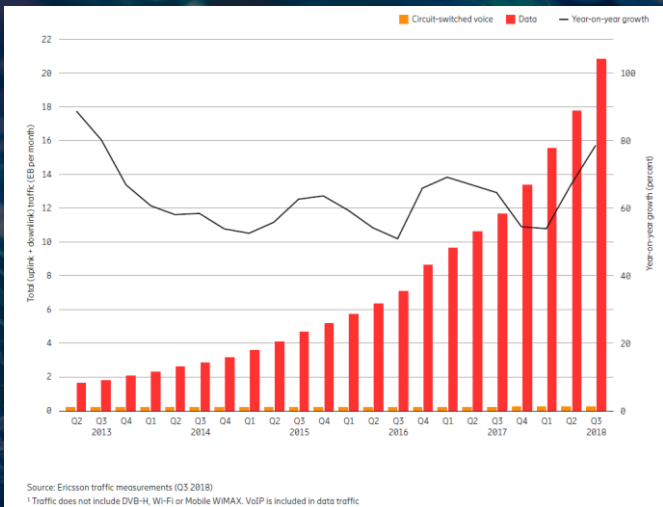
Now is the early stage of 4th Industrial Revolution, to create 'Unprecedented Value' in the offline with online tech



Influence of ICT Technology extended to Offline

SK Telecom Mobile Network History

leading mobile network evolution to 5G



5G Opens up New Possibility

With the vision of “Transforming Offline Things into Online/Mobile”, SK Telecom is trying to differentiate 5G in terms of Speed, Latency, Stability and Security

SKT's perspective

By transforming offline objects into mobile ones

5G realizes
Cyber Physical System
in 4th industrial revolution era

Value Proposition

SKT 5GX

EXCEED
EXPAND
EXCELLENT
EXCITING
EXPLORE
EXTRAORDINARY

Brand new 5G Experience

① Speed

② Latency

③ Stability

④ Security

Personal Experiences stored & replayed



- What do you like
- are Enthusiastic about



- Who are you talking to
- What kind of talk



- Bedtime habit
- What kind of dream

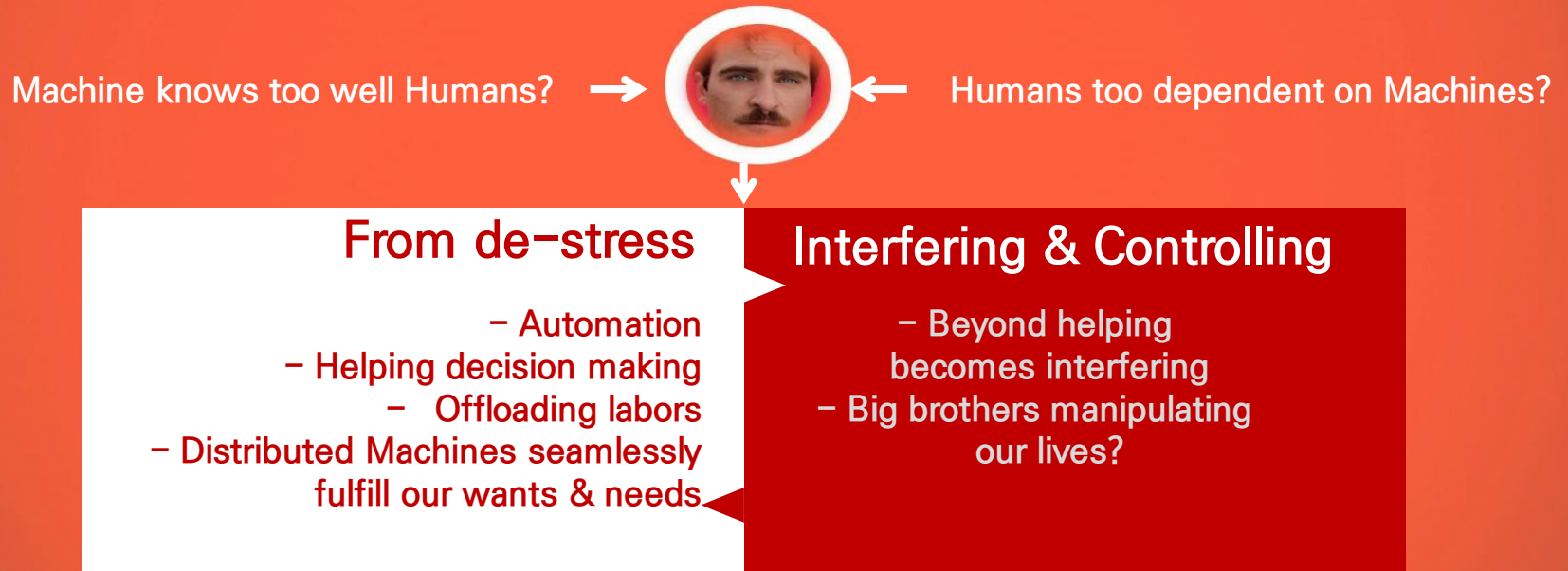


Private life

Sensors & Wearables
will store
vivid experiences
even can be replayed

Should be Concerned

Human–Machine Partnership



Security Everywhere

End to End Security of Everything

Megatrends - Security Threats

- **Computing Power Increases**
 - Making public key cryptography ever more vulnerable
- **Hacking is on the rise**
 - in a society increasingly relying on ICT
- It is now common knowledge that governments are also engaged in **massive eavesdropping projects**

Optical Fiber Hacking

- A simple equipment can penetrate into optical fiber network to intercept and de-information



- Kingfisher International(Australia) optical cable tapping equipment delivered to SKT Quantum Lab
- **Anyone can order without restrictions. Only \$500!**

Problems of the security of currently used Public Key Cryptography

- **Human Ingenuity**
 - Public key cryptography is based on mathematical problems which could be BROKEN by future technology
- **Moore's Law**
 - The increase in computing power makes it increasingly easier to break public key cryptography
- **Quantum Physics**
 - Public key cryptography is vulnerable to quantum computing which can solve certain mathematical problems exponentially faster than classical computers

Vulnerable to Quantum attack

- **Any Cryptosystem based on mathematical complexities**
 - Integer Factoring & Discrete Logarithms(RSA, DSA, DH etc)
 - Almost all public key cryptography use these types of ciphers
- **Any Security Protocol from the above public key ciphers**
- **Any products or security systems from these protocols**
 - **Some symmetric key ciphers like AES are believed to be Quantum-safe, whereas many public key ciphers are known not to be**

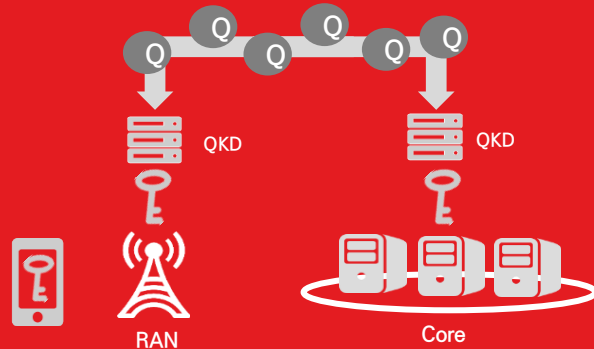
Quantum Key Distribution(QKD)

- **How to securely distribute symmetric keys between distant parties without relying on insecure legacy public key algorithms?**
 - A security solution is as secure as its weakest link and in network encryption, the current weakest link is the key distribution based on public key cryptography
- **QKD answers this question**
 - QKD is a technology uses Quantum Physics to secure the distribution of symmetric encryption keys
 - i.e. Quantum cryptography solves the problem of key distribution by allowing the exchange of a cryptographic key between two remote parties with **ABSOLUTE security**, guaranteed by the fundamental **LAWS of PHYSICS**
 - This key can then be used securely with conventional cryptographic algorithms

Security based on Physics

SK Telecom has been developing quantum cryptography and invested in Swiss quantum company, IDQ

Quantum Key Distribution (QKD)



- 2011~ Launched R&D program on Quantum Crypto
- 2016.6.21 Applied World's first Quantum Crypto to LTE backhaul network between Sejong and Daejeon Cities
- 2018.2.25 Invest in IDQ(ID Quantique (World leading company in Quantum-safe crypto solutions)
- 2018.12.1 Applied World's First Quantum Crypto to 5G Network(B2B Site)



- When a third party tries to intercept information in the middle, the sender and receiver will know it
→ **hacking is fundamentally impossible**

Quantum Random Number Generation



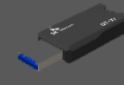
Support any type of 5G device



Chip Type



PCIe Type



USB Type

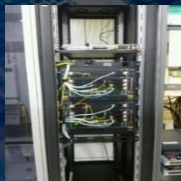
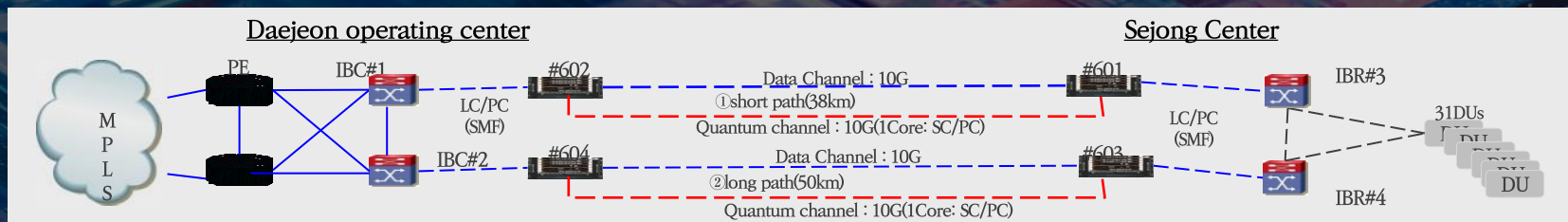


Server Type

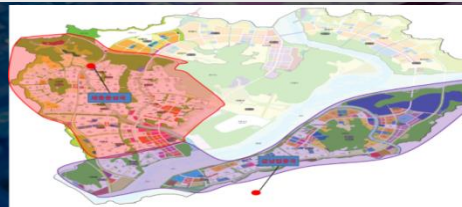
- **Quantum random number generation chip is smaller than a nail** and can be mounted on various IoT devices as well as autonomous vehicles, smartphones and drones

QKD Deployment in LTE

SKT deployed its Quantum Key Distribution system for LTE network with 350,000+ subscribers in Sejong City in South Korea



QKD system in Daejeon



Sejong coverage



QKD system in Sejong

**Security emerges
the most important issue in 5G era**

**SK Telecom is determined to provide
the most secure 5G network & focus on
expanding the ecosystem of
quantum cryptography technologies**



