IT-security in light of the 4th industrial revolution

Attila Horváth PhD

Foundation for Information Society,
Principal researcher

OGIK 2016

NKFIH PD-109740

The Research project

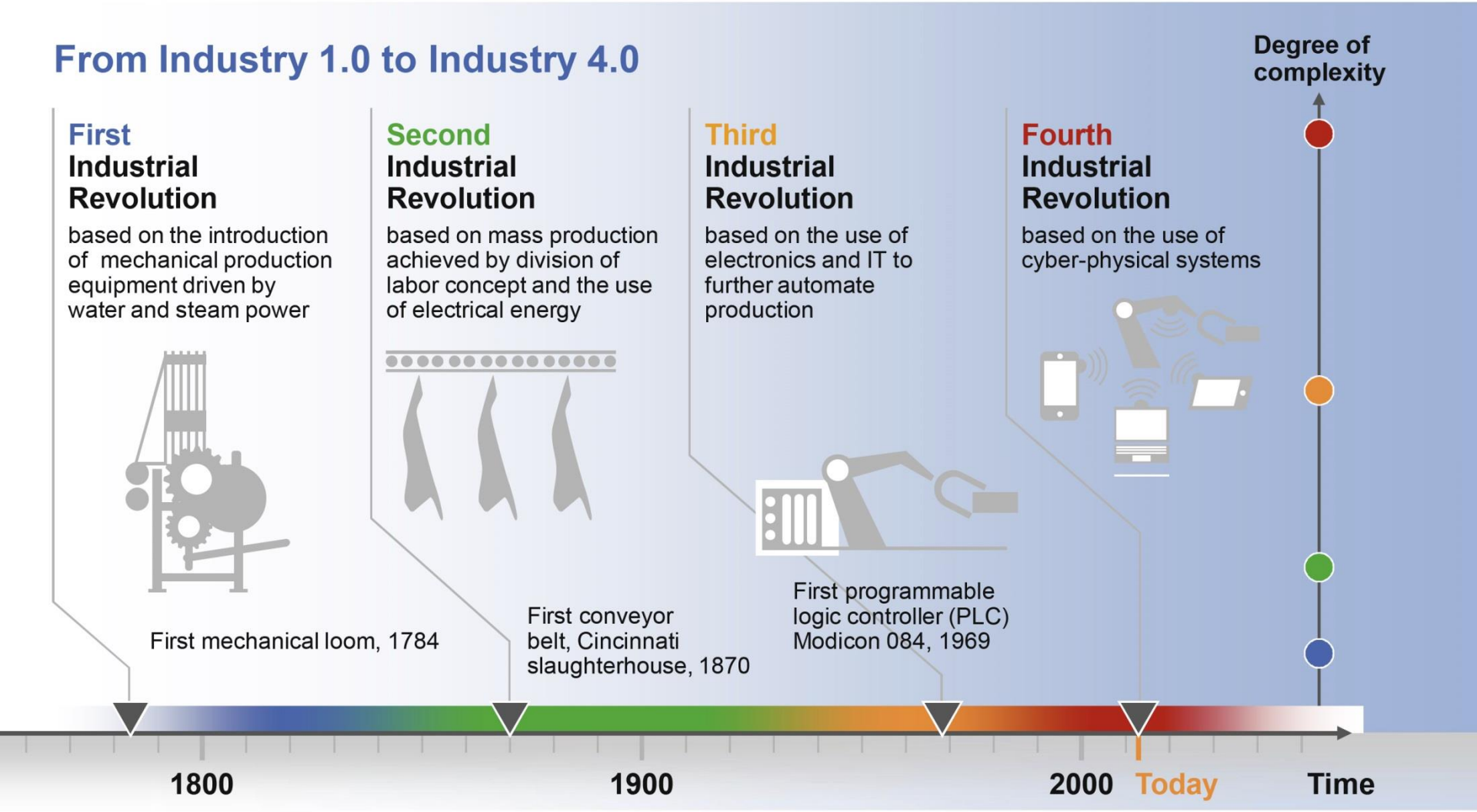
- 2013-2016.
- The effects of IT and network vulnerabilities on economy and society
- National Research, Development and Innovation Office – NKFIH PD-109740
- Foundation for Information Society – INFOTA Research Institute

REVOLUTIONS

Industrial revolution

- „Thorough change in the socitey, economy and technology”
- Prequisites (in all era):
  - Capital
  - R&D
  - Financing
  - Internetional commerce
  - Proper thinking and consiousness

Industrial (r)evolution



Key areas

- Industry 4.0
  - Virtual factories,
  - Automated processes,
  - Smart machines,
  - Cyber production system
  - Sustainability,
  - Networked systems
- The Internet of Things
  - Smart homes
  - Smart cities

Industry 4.0

Materials and Manufacturing Smart Technologies


Advanced materials


Additive manufacturing


Robotics


Distributed generation


Modular operations

Hálózatba kapcsolt szereplők


Advanced sensors


Remote-controlled operations


Facebook of assets


Smart machines

Informatika és Big Data


Advanced analytics & visualization


Advanced computing & Artificial intelligence


Virtual industrialization


Digital infrastructure

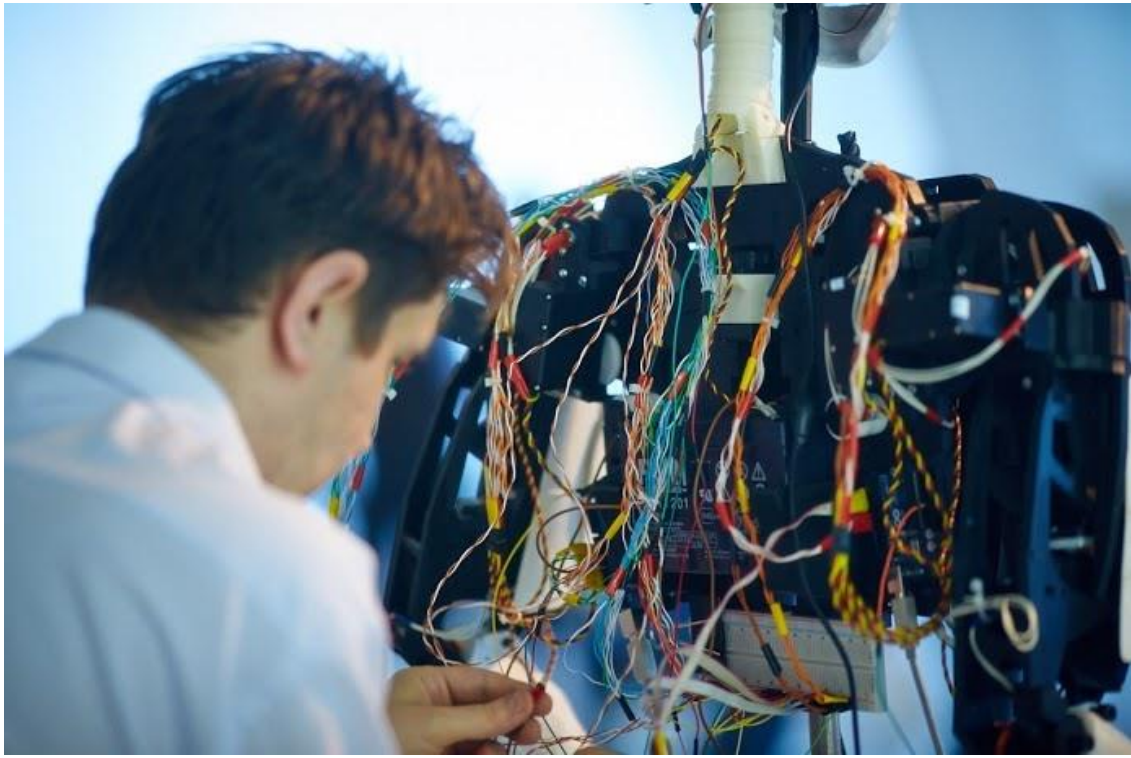

Cloud computing

Effects

- 25% growth in ROCE
- 7% growth in profits,
- 25% growth of effectiveness,
- Growth of return on assets,
- 30% less machinrey needed,
- 45% less workforce needed.

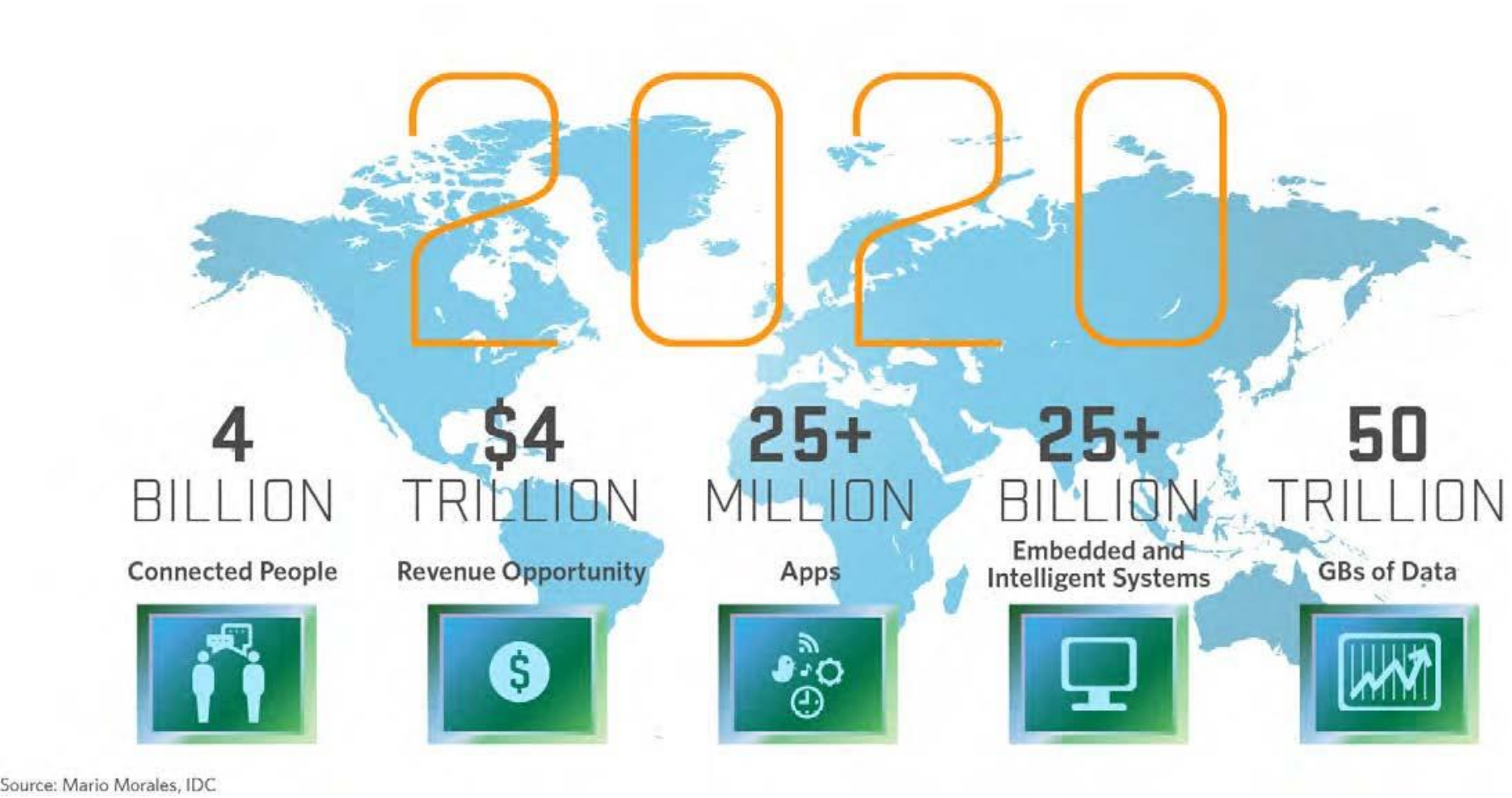
Quantified effects - EU

- 420 billion EUR added value
- 7-10 million new workplaces
  - IT sector
  - Services
  - Eduction
  - Healthcare
  - Mobility



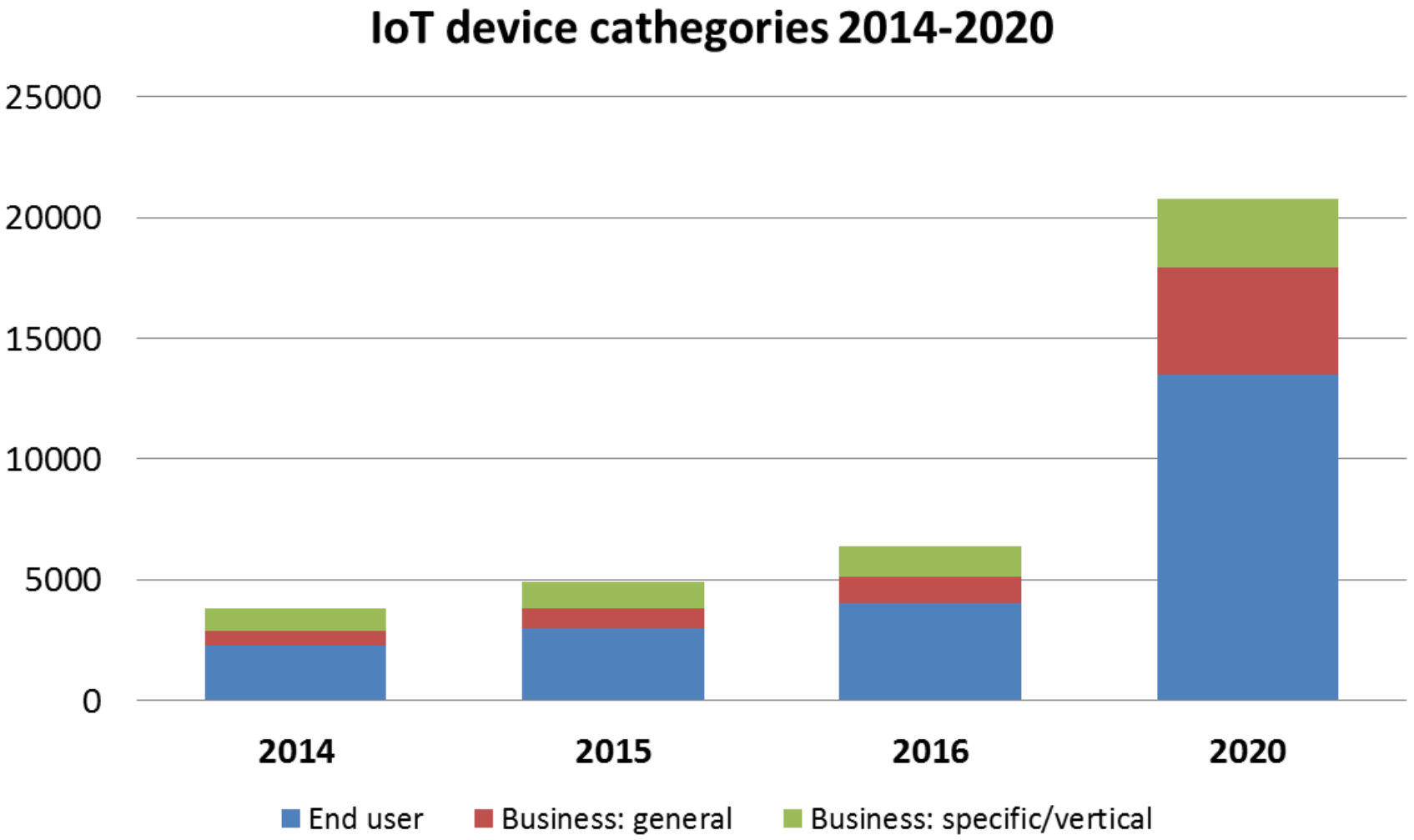
THE INTERNET OF THINGS

What to expect?



Source: Mario Morales, IDC

Personal & Professional



Smart homes


05.06.40
PERSONAL NUTRITION
SUGGESTED MEA
ANALYSIS
FOOD LOG
3:33 PM
24°

Smart cities

Virtual reality

SECURITY IN A CONNECTED WORLD

New attack types

- Multi-exploit: intelligent testing of potential vulnerablities
- Multi-effect: Data leaks, ransomware, botnet
- It is not about Windows any more:
  - Routers, TVs, industrial controllers, flight systems, critical infrastructure, mobile devices
- Eg. the Shellshock case
  - Level 10 NVD
  - 22.487 attacking IP addresses

New targets

- Wearable devices
- Smart homes
- Smart infrastructure
- Medical devices
- Self driving cars

Personal smart, wearable devices, Smarthome Components

- Simplicity is the key
  - Out of the box operation
- Out of the box security?
  - Default configuration
  - No power user/advanced setup
  - Unsuitable for professional environment
- BYOD

Personal smart, wearable devices, Smarthome Components - examples

- Apple Watch
  - Bluetooth protocol vulnerability
  - Reconnect watch without PIN to any host
- Smart termostats, baby monitors, Smart TVs, IP cameras are potential gateways

Smart critical infrastructure

- Specialized industrial attackers: Stuxnet, Flame, Duqu, etc.
- manufacturers do not allow changes or updates to the hardware-controlling systems
- operating systems that are obsolete, vulnerable and yet connected to the Internet
- public-facing connection to the Internet in order to carry out maintenance and management tasks
- 'if something works, don't touch it,'

Smart critical infrastructure

- management policies
- secure connections
- Firewalls
- Unique connection settings and specific protocols
- Integrated management and security
- „It's a good thing to fix the roof before it starts to rain.”

Medical devices are seriously ill

Anything with an IP (>1000/hospital)

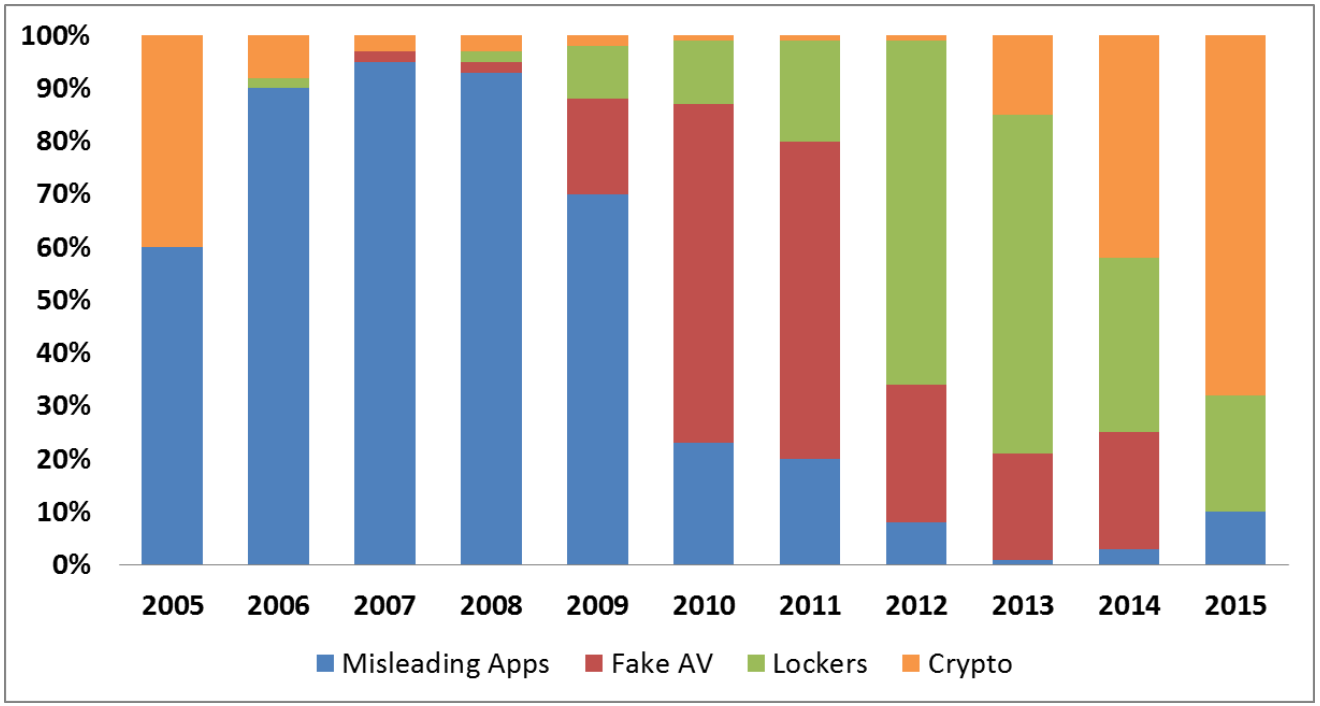
- MRIs
- X-rays
- Infusion pumps
- Medical ventillators
- CTs
- Anaesthetic machines
- Defibrillators
- Etc.

Medical devices are seriously ill

- Can be discovered in search engines (eg. Shodan)
- Experiment: in 6 months – 55k login attempt, 55 succesful logins, 24 explits, 299 malwares
- Hospital WIFI
- Phisically set passwords, ports, or no protection at all
- 85% of healthcare devices can be accesd by just trying common GE settings
- Data breach, botnet, targeted attack, patients!!!! (pain inhibitor)
- Windows XP – no AV

Ransomeware

- Locker (device)
- Crypto (data)



Ransomeware

New targets

- NAS devices
- TVs, set-top-boxes
- Routers
- Fridges, household
- Mobile, wearable
- Smart homes
- Cars!!!

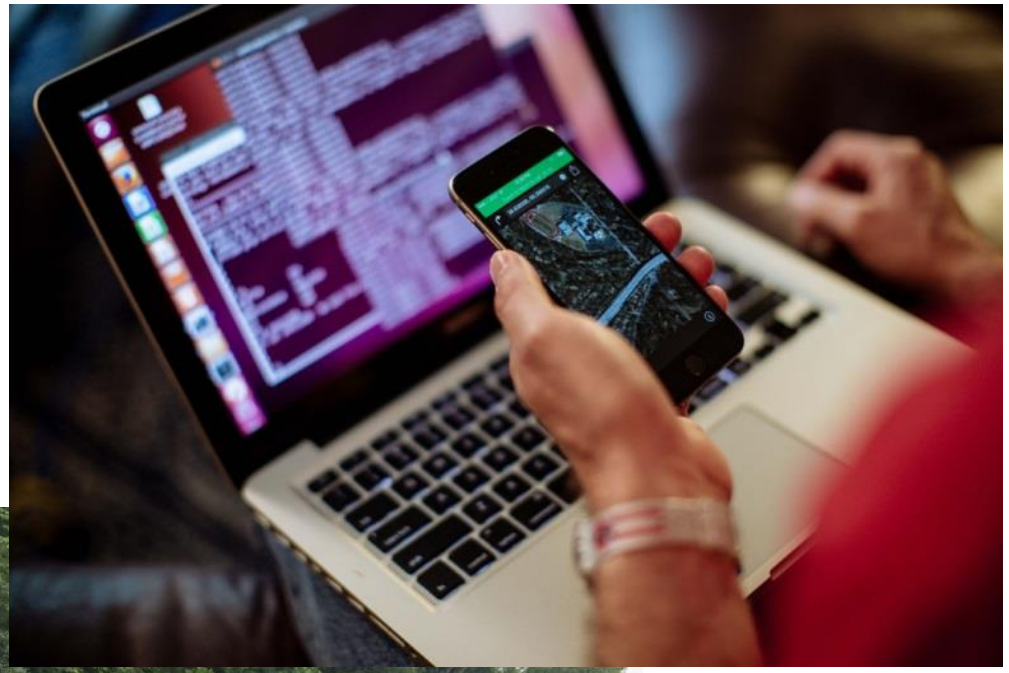
New methods

- Cyber currency (BitCoin)
- Mobile
  - Encrypt SD card
  - Set new PIN
  - Internal storage locker
  - Infect smartwatch like devices
- Dynamic pricing (20-700 USD)

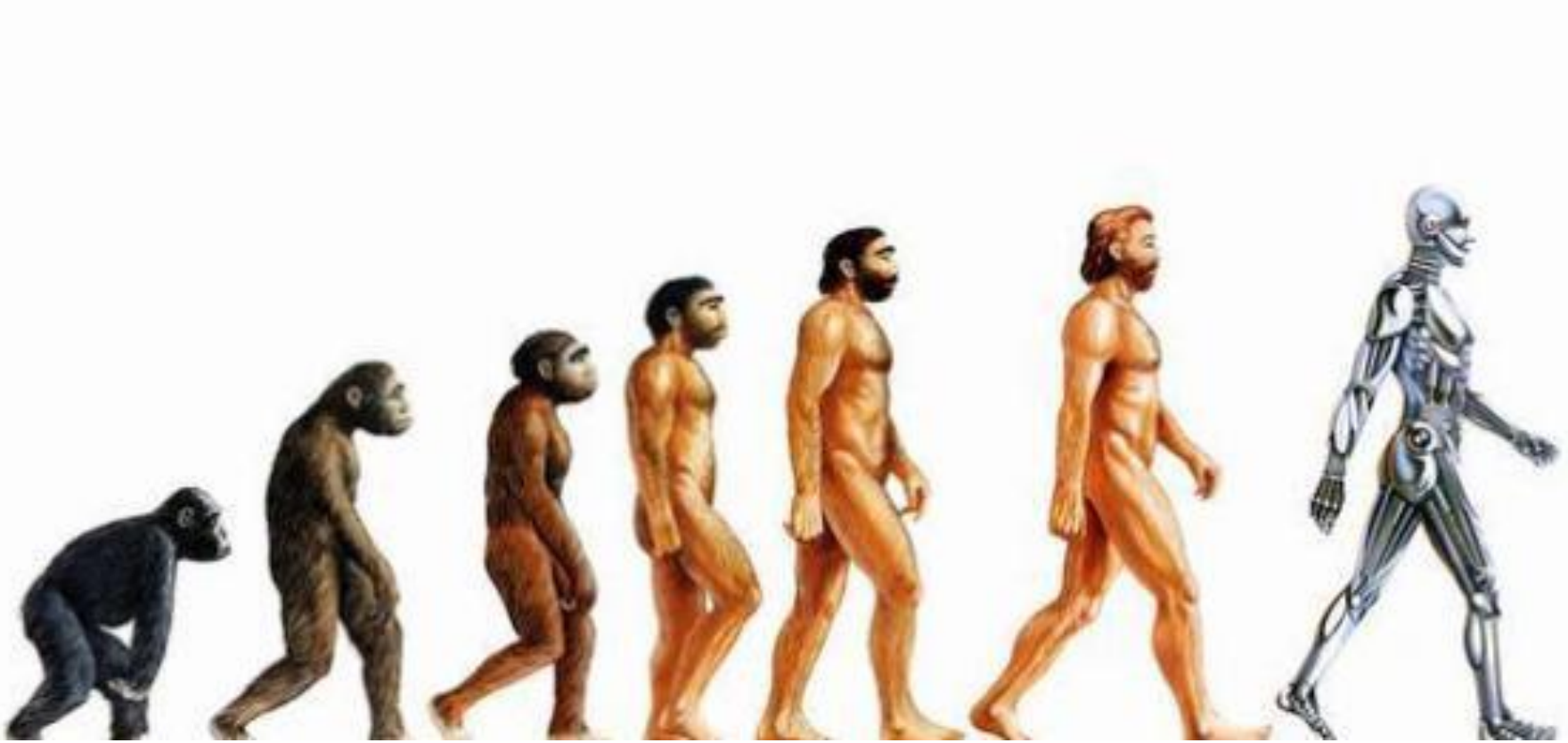
Smart and self-driving cars example: Jeep Cherokee

Remotely controlled

- lights
- air circulation
- wipers
- entertainment system
- steering
- transmission
- brakes

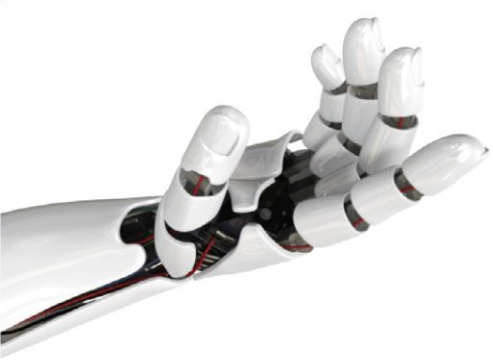


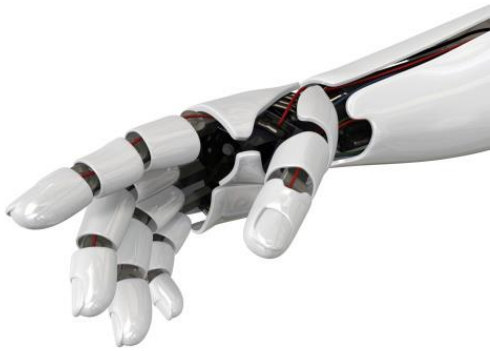
A brave new world?



Thank you for your attention!

www.infota.org





Dr. Horváth Attila

+36 70 504 6654

horvath.attila@infota.org

https://hu.linkedin.com/in/**drattilahorvath**