Ancona, 5/2/2020

5G e Sicurezza Nazionale

Nicola Blefari Melazzi

Professor, University of Rome
Tor Vergata
http://blefari.ee.uniroma2.it/

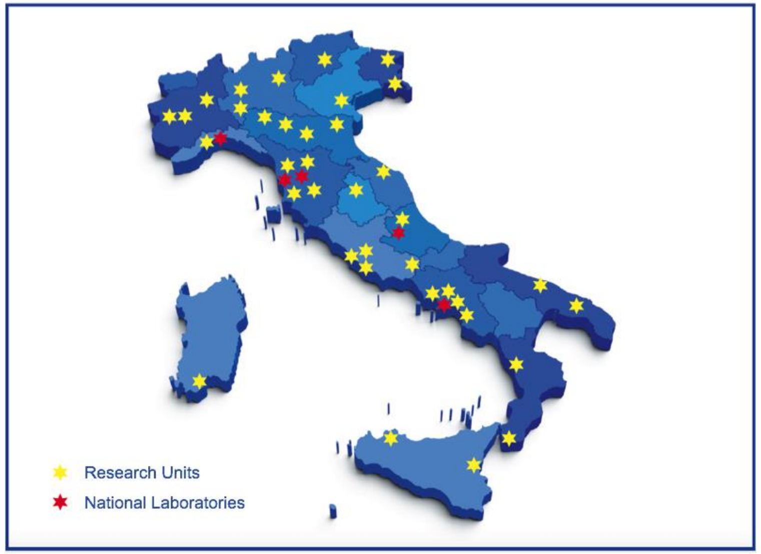
Università di Roma
Tor Vergata

Director of CNIT
www.cnit.it

cnit
consorzio nazionale
interuniversitario
per le telecomunicazioni

What is CNIT? (www.cnit.it)

- National Inter-University Consortium for Telecommunications (**37 Italian Universities+8 CNR research units**)
- Mission: basic and applied research and advanced education in ICT
- 1300+ researchers; **100+ own employees**
- Funding from private companies and competitive programs only:
  - H2020: 48 projects, **11 of them coordinated by CNIT**
  - 2018: 124 projects (39 EU+37 Ntl+48 Industry), 19M€; Recent results: **5 EU projects on applications of ICT**; **3 EU projects on 5G ranked #1 in their calls**; 1 on cybersecurity (EU competence network); 1 on autonomous vehicles; Flagship Graphene, Flagship Quantum Information
  - Organizer of ECOC 2018 and 5G Italy 2018 and 2019 (https://www.5gitaly.eu/)



- No “structural” funding, a problem for overhead and labs equipment
  - e.g., Germany 30%, Spain 50%, Switzerland 50% of total budget

5G: Evolution

Better performance (speed, density, …)

Currently being deployed

Interest for private and temporary 5G networks (e.g. port, factory, campus, concert)

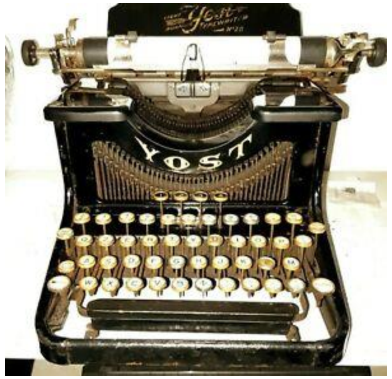
5G: Revolution

Diversified vertical services

Main novelties

- New usage scenarios and new (non-human users)
  - larger ecosystem, with more stakeholders, more heterogeneity
- End-to-End, including the whole network, not only the cellular section
  - Independence between RAN and CN
  - Control and user plane separation
- The software network
  - From a typewriter (HW) to a personal computer (SW)
    - Huge security implications!
  - Virtualization and Orchestration
  - Cloud (and edge cloud), SDN, NFV
  - Service-based Architecture in the CN

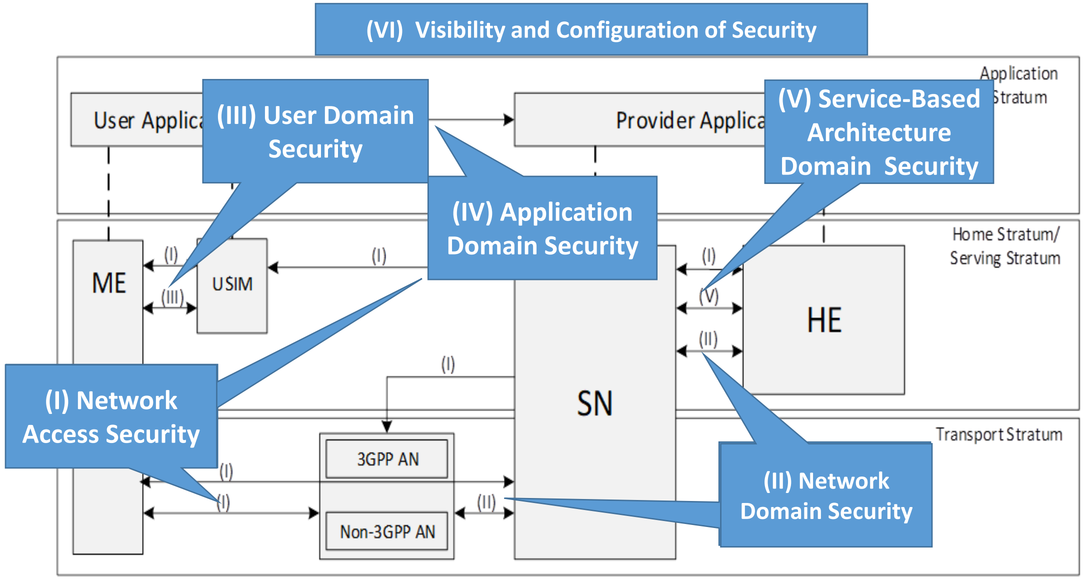
  - New Radio, new spectrum, massive MIMO, …



cnit

Generations and security

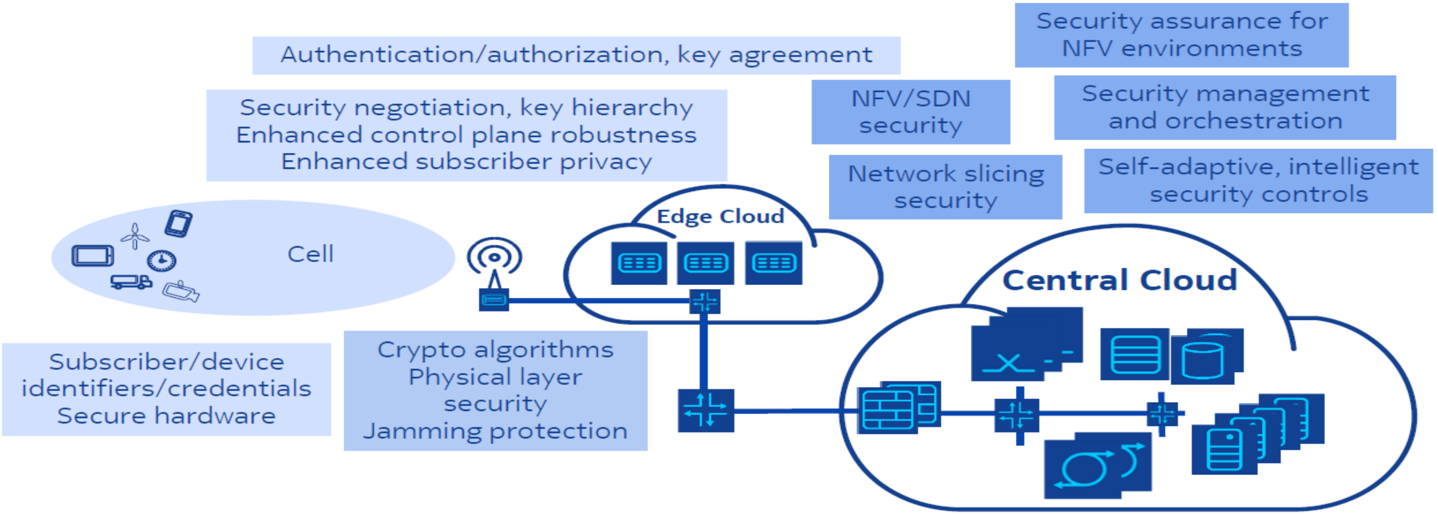
- 1G, 1980s, up to 2.4Kbps: portability
  - [virtually no security]
- 2G, 1990s, up to 64Kbps : from analog to digital, SMS, WAP
  - client authentication, encryption [Security by obscurity, no BS authentication, no core network security]
- 3G, 2000s, up to 10Mbps: data services
  - Encryption and (in part) Integrity, mutual authentication, core network security
- 4G, 2010s up to 300Mbps : Internet-integrated, video
  - Systematic approach, security architecture


(VI) Visibility and Configuration of Security
Application Stratum
User Applic
(III) User Domain Security
Provider Applica
(V) Service-Based Architecture Domain Security
(IV) Application Domain Security
Home Stratum/ Serving Stratum
ME
USIM
(I)
(III)
(I)
(I)
(V)
(II)
HE
SN
(I)
(I) Network Access Security
Transport Stratum
3GPP AN
Non-3GPP AN
(I)
(I)
(II)
(II) Network Domain Security

Generations and security

- 5G, 2020: new services, whole network, softwarization, cloud
  - Many (small and not-so small) tailored/chirurgic improvements
    - Proof of Presence
    - Unified Flexible Authentication / Support for multiple protocols (also non 3GPP)
    - No more transmission of IMSI (SUPI) in clear; SUCI = Public key (ECIES) encryption of SUPI
    - L2 message integrity
    - Security Edge Protection Proxy
    - Rogue base stations
      - downgrading

Elements of a 5G Security Architecture


Security assurance for NFV environments
Authentication/authorization, key agreement
Security negotiation, key hierarchy
Enhanced control plane robustness
Enhanced subscriber privacy
NFV/SDN security
Security management and orchestration
Network slicing security
Self-adaptive, intelligent security controls
Edge Cloud
Cell
Central Cloud
Subscriber/device identifiers/credentials
Secure hardware
Crypto algorithms
Physical layer security
Jamming protection

Source: Nokia Bell labs, P. Schneider, 2018

Security: high-level challenges

- More realms of applications: increase in attack surface
  - Ultra Reliable and Low Latency scenarios -> more critical situations
  - IoT scenarios -> more and widespread applications, heterogeneous terminals
  - Multiplication of both types of stakeholders and numbers of tenants and third-party suppliers
  - Distribution of responsibilities also more complex
- Softwarization and slicing
  - Inherently more risky
- Signalling traffic
  - Increasing share of total; need of specific protection

- Flexible security, tailored to specific scenarios
  - Security-as-a-Service: more complex but also more powerful and effective

Credits to Giuseppe Bianchi

Security: specific issues

- Softwarization and slicing
  - Slice isolation
  - Programmability platform (e.g. P4) security
  - Network management and orchestration security-aware
  - Software modules implementing security services (e.g. monitoring)
- IoT
  - Massive coordinated IoT attacks
  - Lightweight cryptographic solutions, integrated within communication protocols
  - Multi-tenant, heterogeneous, flexible, large scale access-control
  - Scalable monitoring techniques
- New communication technologies
  - Specific security solutions for dense networks, MIMO networks
  - New (e.g. quantum) physical layer cryptographic techniques
  - Radio waves designed for security purposes

cnit

Security: new requirements

- Beyond confidentiality, integrity and availability, need to address:
  - location security (www.locus-project.eu) and privacy
  - trustworthiness of information/integrity of remote platforms
  - contextual correctness
  - proof of possession
  - support for highly limited devices such as sensors
  - tailored security at the service and device level: differentiated security services on request
  - dynamic composition of services -> modular security guarantees within the system
- Not only systems' security but also implementation security
  - Not nearly a new 5G concern → remember Greek Wiretapping case, 2004/05
  - Which approach for vulnerability assessment process?

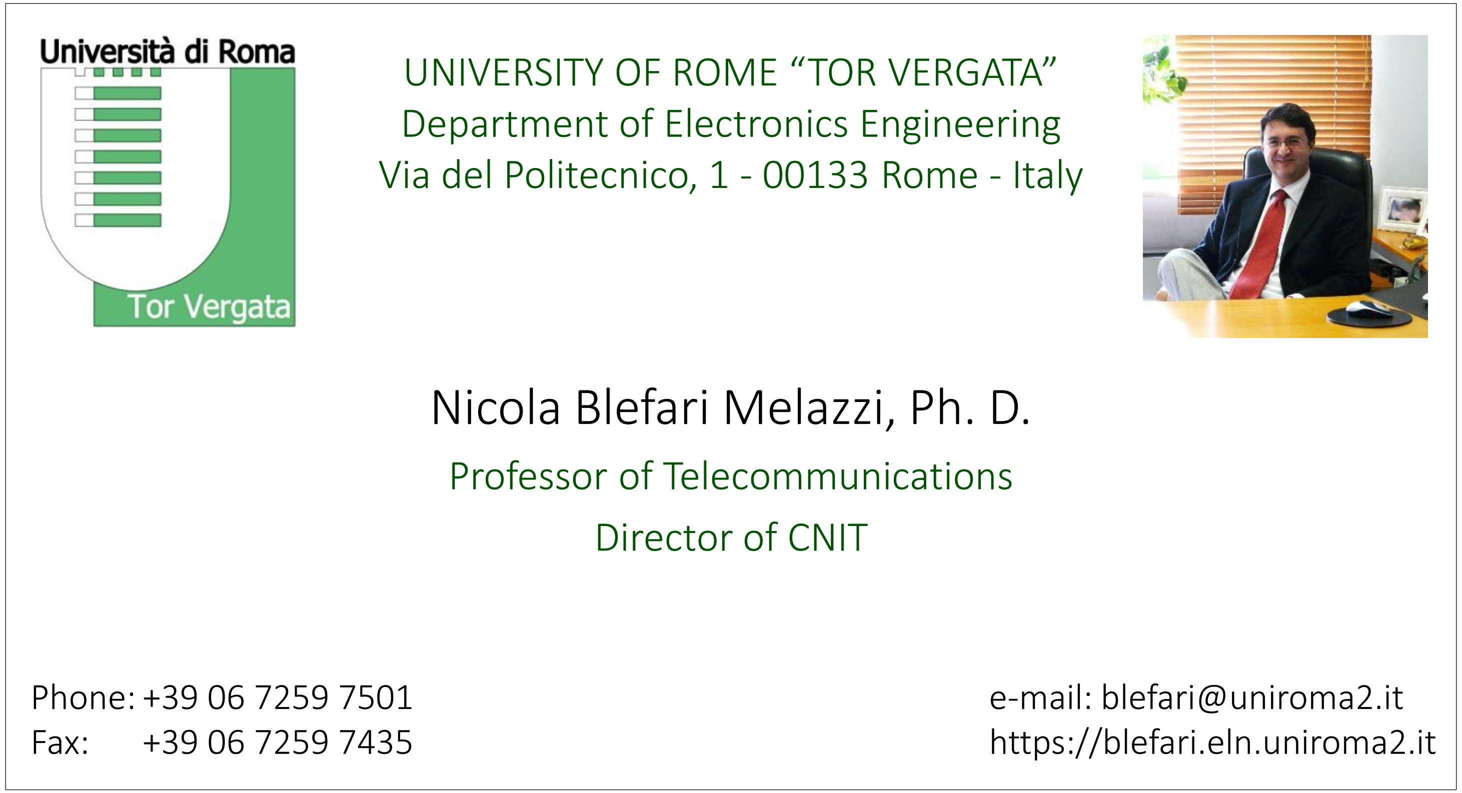
Antennas and Engineers

- Network deployment
  - Investments
  - Thresholds, regulations, rules, bureaucracy and red tape (“antennas”)

- People (“engineers”)
  - 208k people aged 20-34 left Italy in the last ten years
  - Italy has the lowest percentage of people with a university degree in Europe
  - Italy has the third lowest percentage of STEM degrees in Europe

cnit

Thank you



Università di Roma

Tor Vergata

UNIVERSITY OF ROME “TOR VERGATA”
Department of Electronics Engineering
Via del Politecnico, 1 - 00133 Rome - Italy

Nicola Blefari Melazzi, Ph. D.

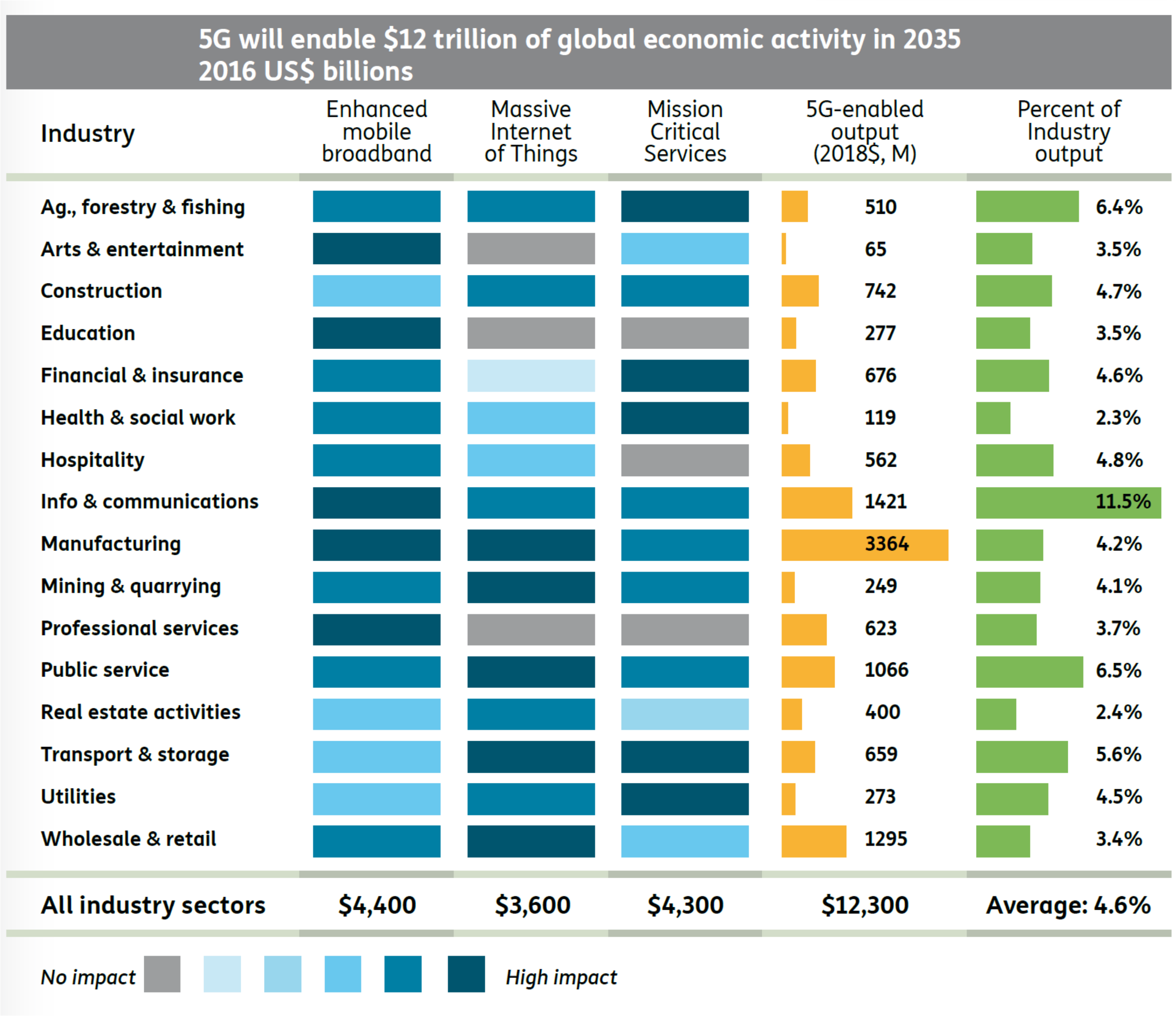
Professor of Telecommunications

Director of CNIT

Phone: +39 06 7259 7501
Fax: +39 06 7259 7435

e-mail: blefari@uniroma2.it
https://blefari.eln.uniroma2.it

Economical Impact



5G will enable $12 trillion of global economic activity in 2035
2016 US$ billions

Industry	Enhanced mobile broadband	Massive Internet of Things	Mission Critical Services	5G-enabled output (2018$, M)	Percent of Industry output
Ag., forestry & fishing	◉	◉	●	510	6.4%
Arts & entertainment	●	○	◕	65	3.5%
Construction	◕	◉	◉	742	4.7%
Education	●	○	○	277	3.5%
Financial & insurance	◉	◔	●	676	4.6%
Health & social work	◉	◕	●	119	2.3%
Hospitality	◉	◕	○	562	4.8%
Info & communications	●	◉	◉	1421	11.5%
Manufacturing	●	●	◉	3364	4.2%
Mining & quarrying	◉	●	◉	249	4.1%
Professional services	●	○	○	623	3.7%
Public service	◉	●	◉	1066	6.5%
Real estate activities	◕	◉	◑	400	2.4%
Transport & storage	◕	●	●	659	5.6%
Utilities	◕	◉	●	273	4.5%
Wholesale & retail	◉	●	◕	1295	3.4%
All industry sectors	**$4,400**	**$3,600**	**$4,300**	**$12,300**	**Average: 4.6%**

No impact ○ ◔ ◑ ◕ ◉ ● *High impact*