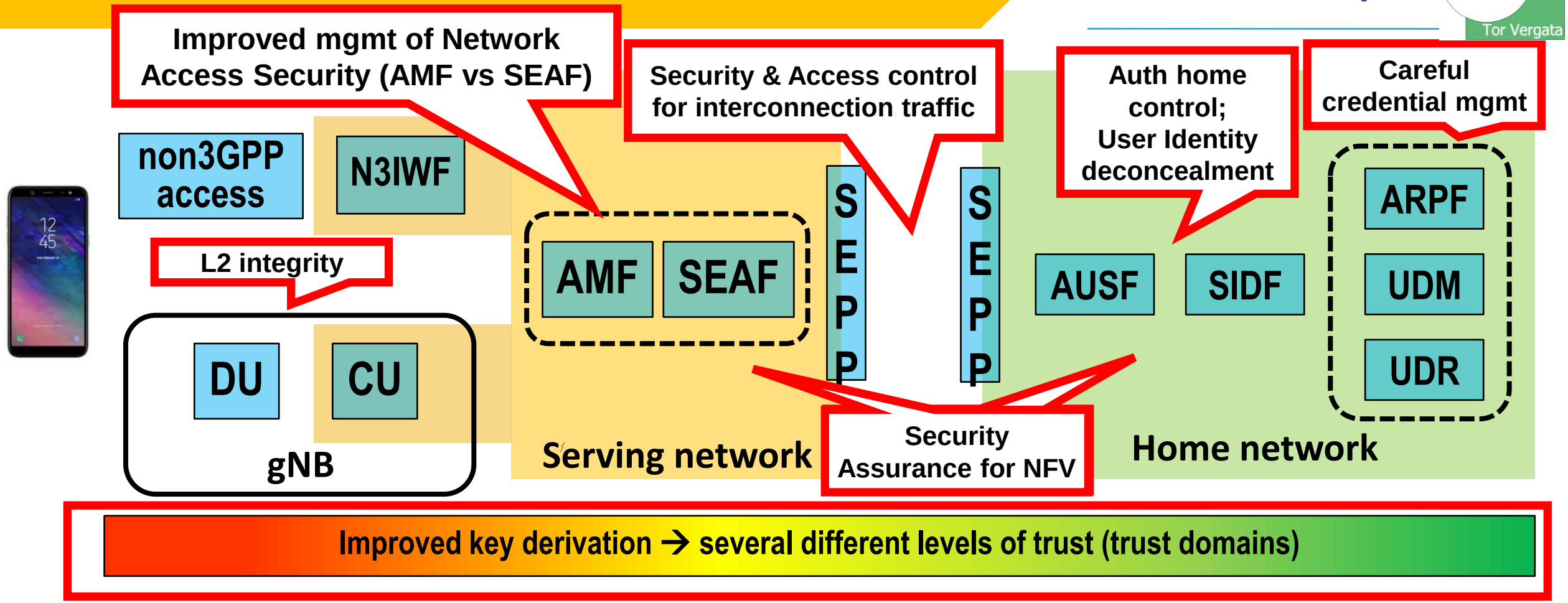
~~5G~~ *critical infrastructure Security*

Giuseppe Bianchi
Professor of Networking &
Network Security
University of Roma «Tor Vergata»

Excellent ~~5G~~ CI security design: is enough?



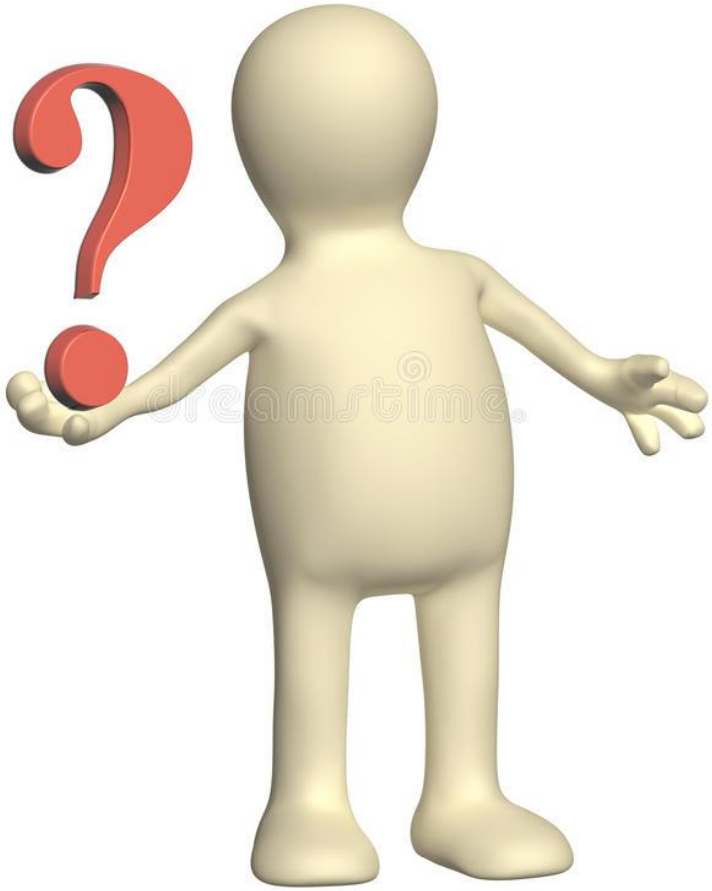
DU Distributed Unit
CU Central Unit

N3IWF Non 3GPP Inter Working Function

AMF Access Management Function
SEAF SEcurity Anchor Function

SEPP Security Edge Protection Proxy

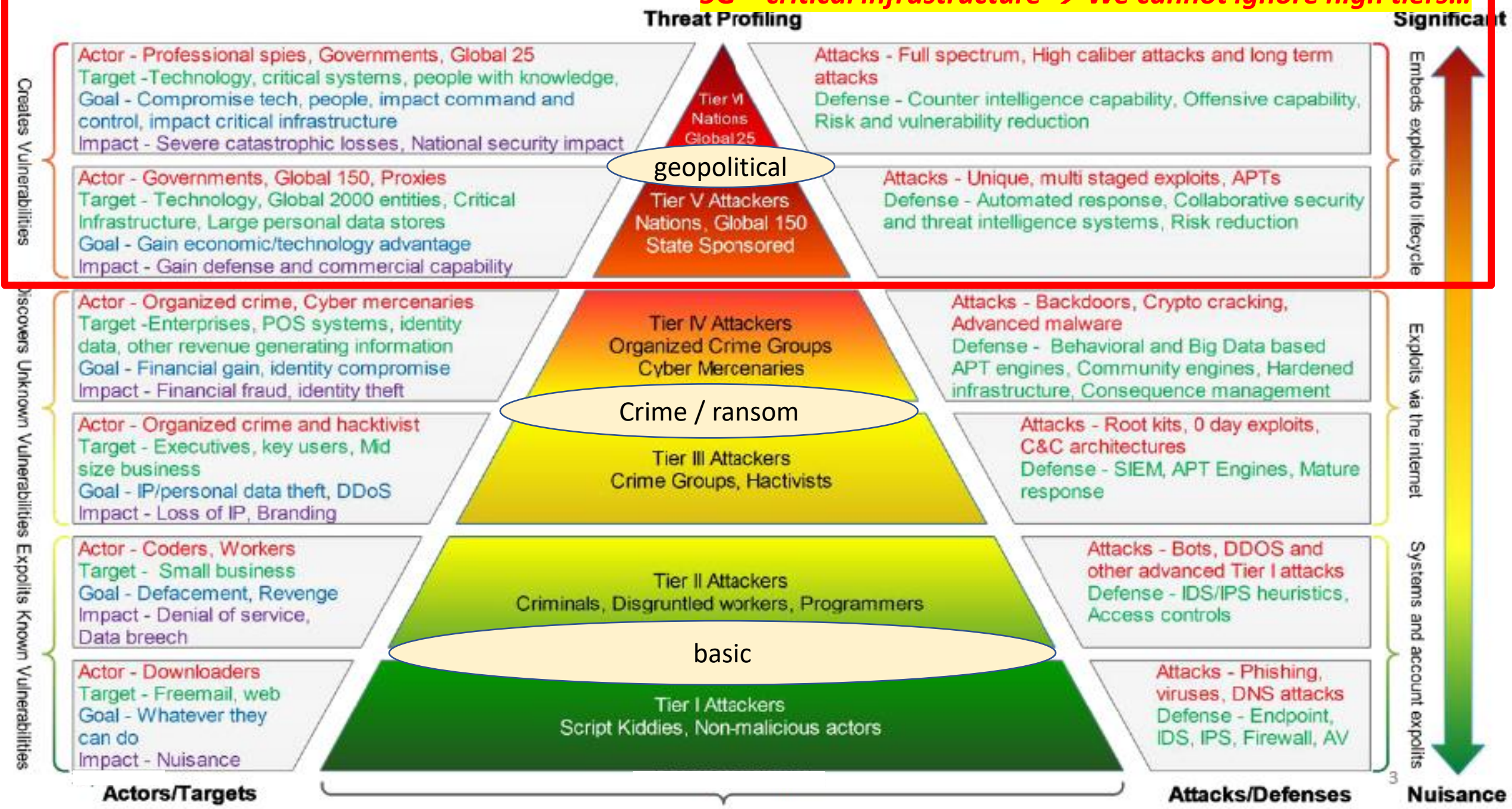
AUSF AUthentication Server Function
SIDF Subscription Identifier Deconcealment Fct
ARPF Auth credential Repository & Processing Fct
UDM Unified Data Management
UDR Unified Data Repository



Critical Infrastructures: Who's the (likely) attacker?

Defense must be tailored to the threat model

5G = critical infrastructure → We cannot ignore high tiers…



Point is: there's a security standard

consorzio nazionale interuniversitario per le telecomunicazioni

Università di Roma Tor Vergata

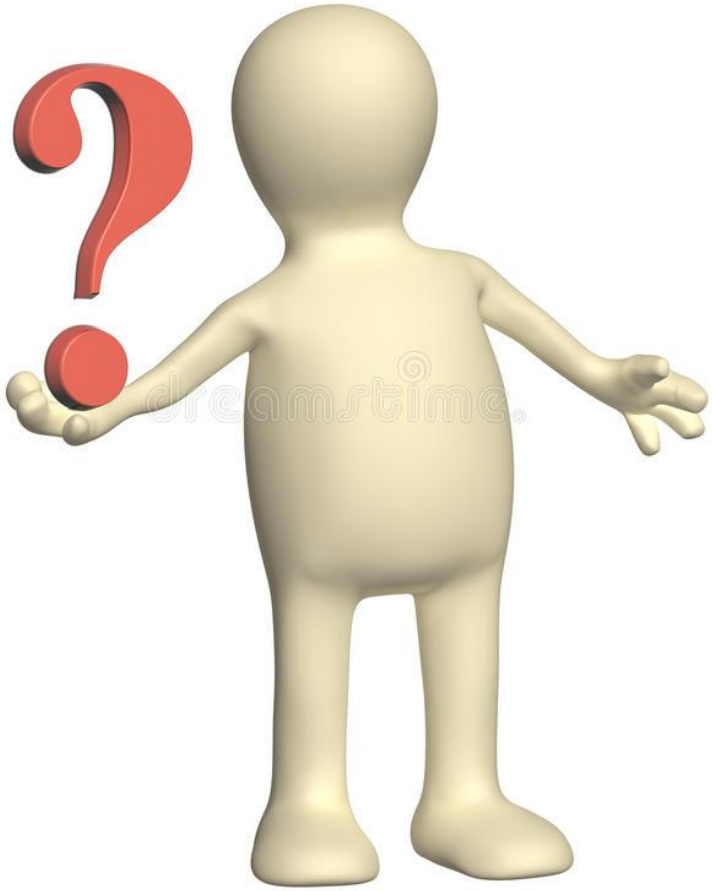
5G/6G systems' security: A small part of a bigger picture!!

No 5G security if SW/HW implementation is insecure!

Critical infrastructure = high tier threats
«They» might *design* vulnerabilities!

SW networks, third party suppliers:
Complexity, increased threat surface!

Too many «optional/should» In the standard!
Very risky! (you might believe you are secured, while…)



best defense?

Prevention → controls!

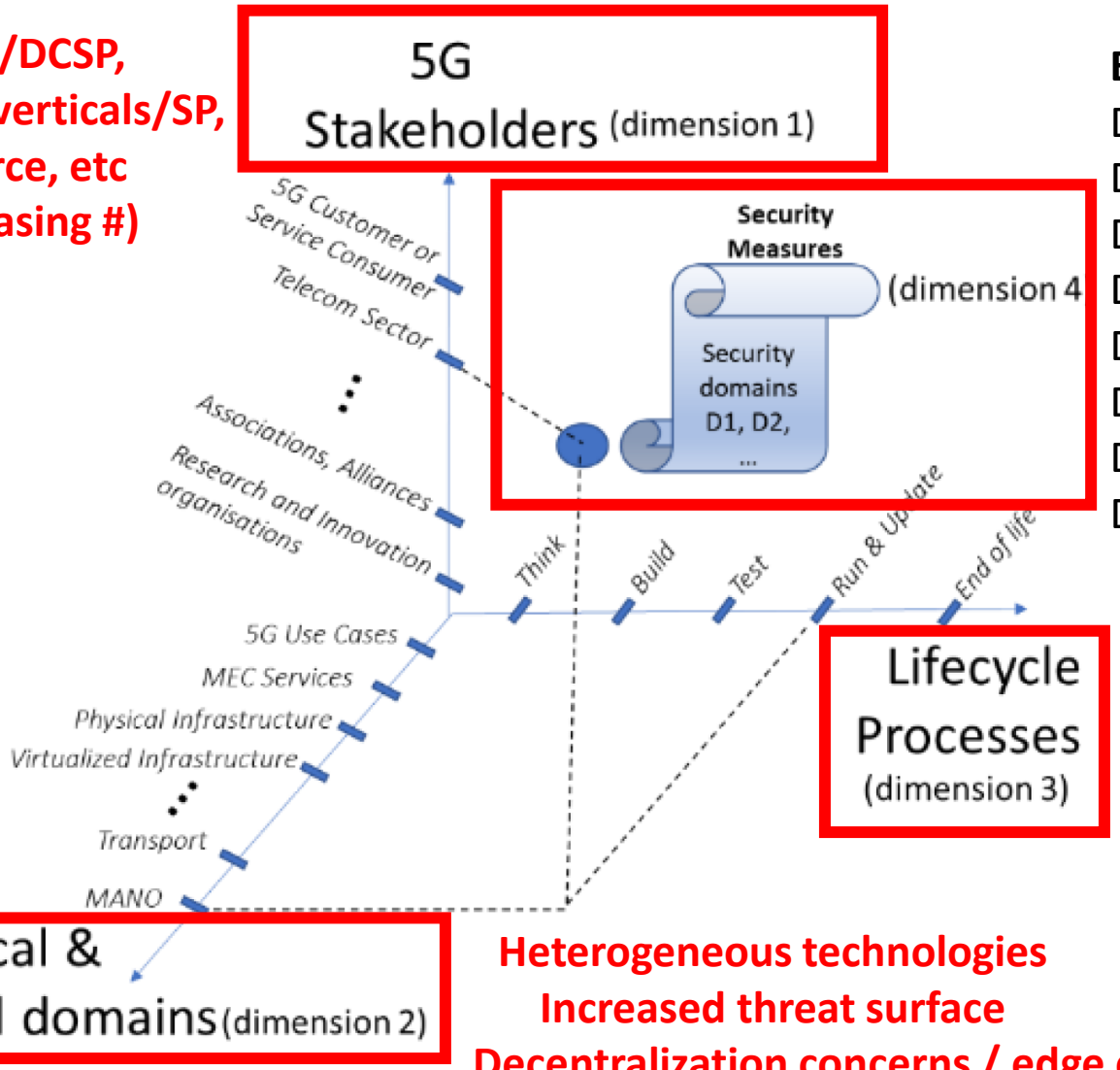
But of course, also related to prevention,
let's NOT forget design and threat intelligence
(not discussed today)

Security measures/controls. OK. But… Multiple complex dimensions into play!

Università di Roma Tor Vergata

cnit consorzio nazionale interuniversitario per le telecomunicazioni

TLC, cloud/DCSP, policy makers, verticals/SP, open source, etc (Ever increasing #)



ENISA European Electronic Commun Code domains:

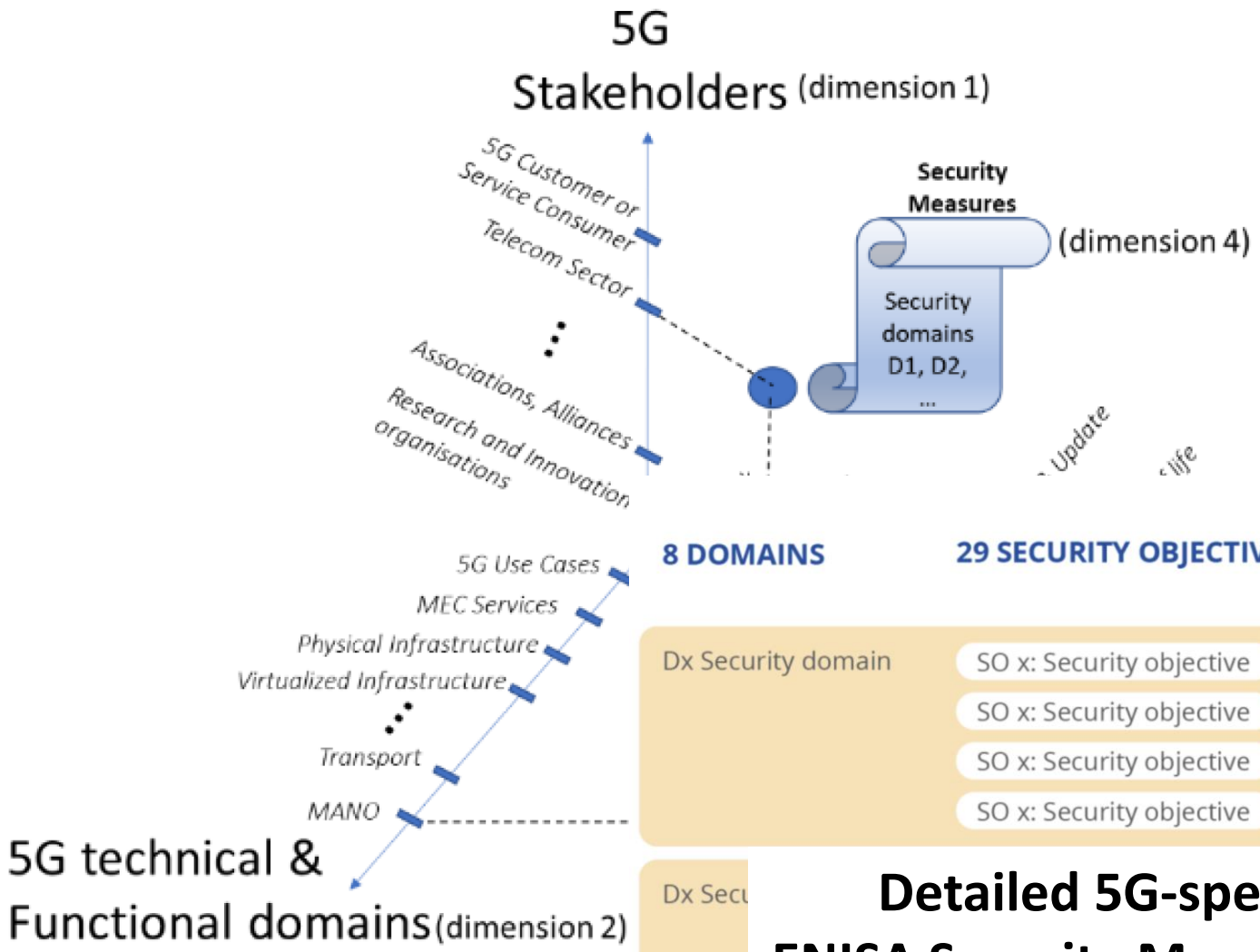
DOMAIN D1: GOVERNANCE AND RISK MANAGEMENT
DOMAIN D2: HUMAN RESOURCES SECURITY
DOMAIN D3: SECURITY OF SYSTEMS AND FACILITIES
DOMAIN D4: OPERATIONS MANAGEMENT
DOMAIN D5: INCIDENT MANAGEMENT
DOMAIN D6: BUSINESS CONTINUITY MANAGEMENT
DOMAIN D7: MONITORING, AUDITING AND TESTING
DOMAIN D8: THREAT AWARENESS

Security @ design phase not nearly enough;
Many further crucial phases:
Development, Deployment, Integration & testing…
(and don't forget technology decommissioning!)

Heterogeneous technologies
Increased threat surface
Decentralization concerns / edge computing (MEC)

Source: ENISA 5G cybersecurity

Complex 5G Landscape

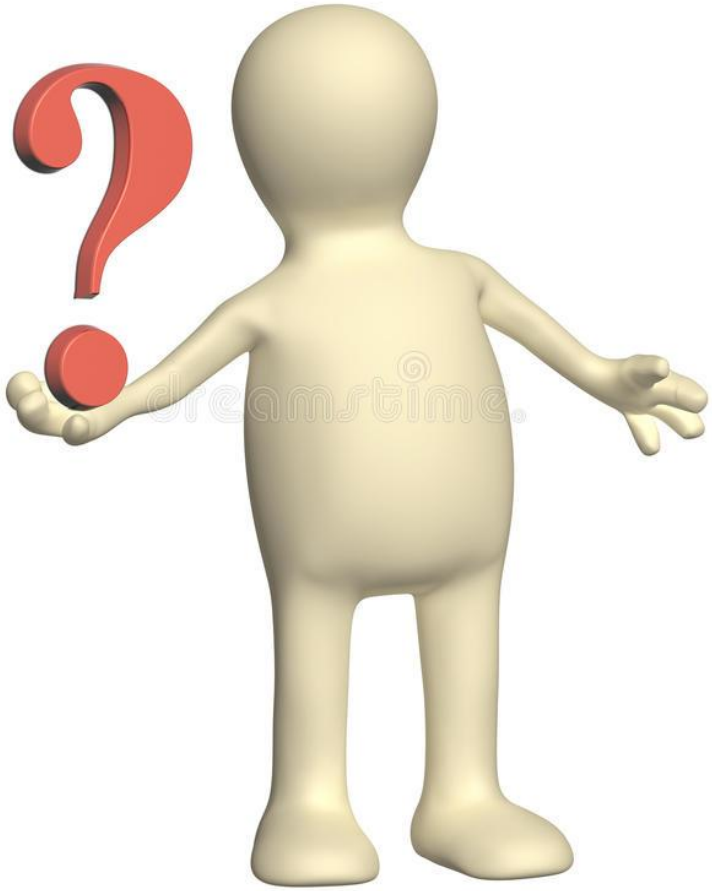


ENISA European Electronic Commun Code domains:

DOMAIN D1: GOVERNANCE AND RISK MANAGEMENT
DOMAIN D2: HUMAN RESOURCES SECURITY
DOMAIN D3: SECURITY OF SYSTEMS AND FACILITIES
DOMAIN D4: OPERATIONS MANAGEMENT
DOMAIN D5: INCIDENT MANAGEMENT
DOMAIN D6: BUSINESS CONTINUITY MANAGEMENT
DOMAIN D7: MONITORING, AUDITING AND TESTING
DOMAIN D8: THREAT AWARENESS

Detailed 5G-specific analysis carried out in:
ENISA Security Measures, 5G supplement, July 2021

Source: ENISA 5G cybersecurity



But are
(these so far pretty high level)
checks sufficient?

Exmple from D1 (Gov & risk Mgmt):

Università di Roma Tor Vergata

cnit consorzio nazionale interuniversitario per le telecomunicazioni

#	SO	Checks to consider	Ref.[15]
1	SO2	Is the list of identified risks aligned with the main risks for 5G networks identified in the Coordinated risk assessment?	[a,e] [i,vi]
		Are threats related to the exposure to potentially high risk suppliers or managed service providers, [illegible] deration?	[a,e] [i,vi]
3	SO2	Has a potential dependency on a single supplier of 5G equipment been considered when assessing the main risks for security of networks and services?	[a,e] [i,vi]
4	SO4	Does MNO have security requirements placed on third parties as part of contractual arrangements & is there a mechanism to monitor that suppliers are meeting said contractual arrangements?	[e] [vi]
5	SO4	Does MNO require suppliers to comply with relevant EU certification schemes for 5G network components, customer equipment and/or suppliers' processes or for other non 5G-specific ICT products and services, such as end-user devices and/or cloud services[16]?	[e] [vi]
6	SO4	Does MNO require suppliers to demonstrate quality level of internal information security processes, including having security by design, built in the product development process?	[e] [vi]
7	SO4	Does MNO require suppliers to adhere to best practices and industry standards throughout the lifetime of the product?	[e] [vi]

… certification(s), quality, processes, etc

Exmple from D3 (Technical):

#	SO	Checks to consider	Ref.
1	SO9	Are there documented, additional, risk-based controls for physical security for MEC and base stations included in the policy for physical security measures?	[d] [ii,iv]
2	SO9	Are there documented additional, adequate physical infrastructure controls (for example perimeter security for infrastructure and administrative premises, alarms and CCTV for detecting and recording incidents), especially for equipment locations which are unmanned, in place?	[d] [ii,iv]
[illegible]	[illegible]	Are there any controls in place to allow failsafe r[illegible] shutdown ([illegible] e-authentication or configuration after [illegible]	[illegible]

Need for physical security means

Harden & control encryption

#	SO	Checks to consider	Ref.
21	SO13	Is encryption applied for protection of confidentiality of user and signalling data between user equipment and base stations?	[a] [i,ii]
22	SO14	Are there appropriate controls in place, according to best practices, for the protection of cryptographic key material in UICC (or eUICC)[26]?	[a,b] [ii]
23	SO14	Are appropriate controls in place, according to best practices, for the protection of cryptographic key material for encryption of subscriber permanent identifiers (SUPI)?	[a,b] [ii]
24	SO14	Are there appropriate c[illegible] ection of any other cryptographic key ma[illegible] ments or between different networks[27]?	[a,b] [ii]
25	SO14	Are there appropriate c[illegible] nenticate NF exchanges in the 5G core network?	[a] [ii]
26	SO14	Where cryptographic key material is stored on third party key servers, are there appropriate contractual arrangements in place with the server provider to ensure security of this key material?	[a,b] [i]

Easy to say, isn't it?

... well, see next slide

More and more technical attention!

Università di Roma

cnit consorzio nazionale interuniversitario per le telecomunicazioni

A real w

Hello, what's your level of security?

Ooops, but you «forgot» IV = 000000000

And tech mistakes might be way more subtle than a zero IV!

- ***25 years of Bleichenbacher oracles***
  - ***DROWN 2016, ROBOT 2018 @ Facebook & Cisco, etc***
- ***Side channel threats/leaks***
  - ***EM leaks, time channels, CPU over-optimization (e.g. spectre, meltdown), frequency leaks (e.g. hertzbleed 2022), etc***
- ***Side/limit cases: checks forgotten → disaster***
  - ***ECDSA Nonce reuse (Sony playstation 2010, Ethereum bots, etc), Java Psychic signature (april 2022), Certificate reuse across sites, etc***
- ***Just the top of a tech iceberg (remember, we have to protect against high tier threats, not against script kiddies!)***

Checks: need change of pace!

From: is (measure) in place / applied?

To: HOW, <u>technically</u>, (measure) has been applied
AND HOW security can be controlled / assured

5G infrastructures: promising initial security assurance work (SCAS)
but can (should!) be improved and "DevSecOps-ed"
→ automated & continuous 5G security testing

BUT we have a problem: we need MORE PEOPLE capable to understand all this…
…in addition of mastering 5G subtleties!!

The real challenge: how to raise, train, and retain in Italy (!) a new generation of qualified people.

Thank you!
Giuseppe.Bianchi@uniroma2.it

Giuseppe Bianchi
Professor of Networking &
Network Security
University of Roma «Tor Vergata»