5G implementation: Risks & mitigation strategies

Giuseppe Bianchi
Professor, Networking & Network Security, Univ. Roma «Tor Vergata»
Director, CNIT Network Assurance and Monitoring National LAB

Excellent 5G security design: enough?

Improved mgmt of Network Access Security (AMF vs SEAF)

Security & Access control for interconnection traffic

Auth home control; User Identity deconcealment

Careful credential mgmt

non3GPP access

N3IWF

L2 integrity

AMF

SEAF

S E

S E

AUSF

SIDF

ARPF

UDM

UDR

DU

CU

gNB

Serving network

Security Assurance for NFV

Home network

Improved key derivation → several different levels of trust (trust domains)

DU Distributed Unit
CU Central Unit

AMF Access Management Function
SEAF SEcurity Anchor Function

N3IWF Non 3GPP Inter Working 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

Yes, but….

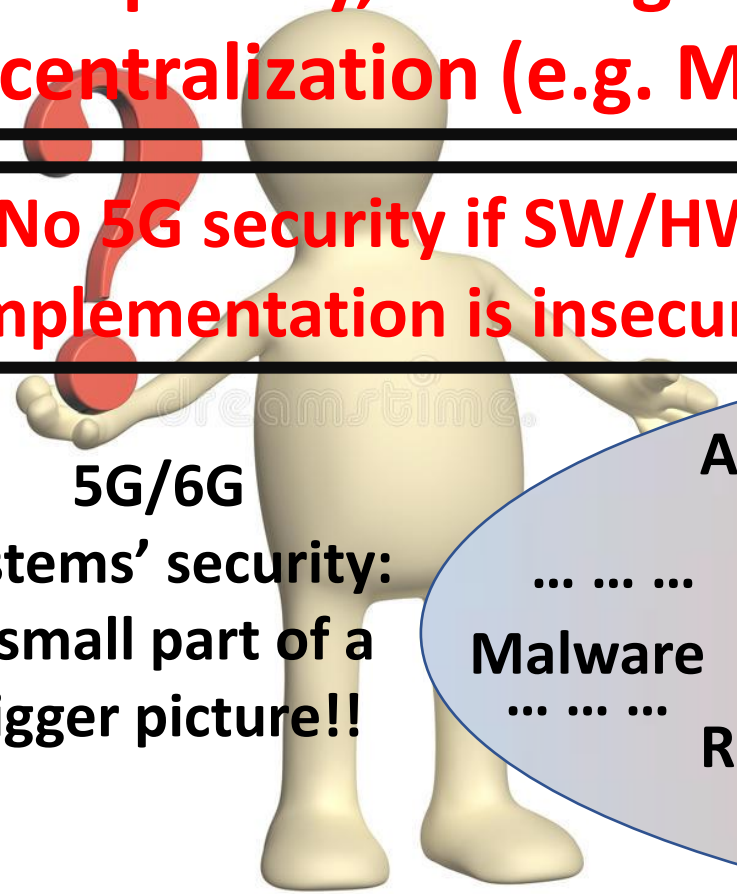
5G ITALY
The Global Meeting in Rome

SW networks, third party suppliers:
Complexity, heterogeneity, decentralization (e.g. MEC), …

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

… huge threat surface…

Lots of config & «optional/should» In the standard!

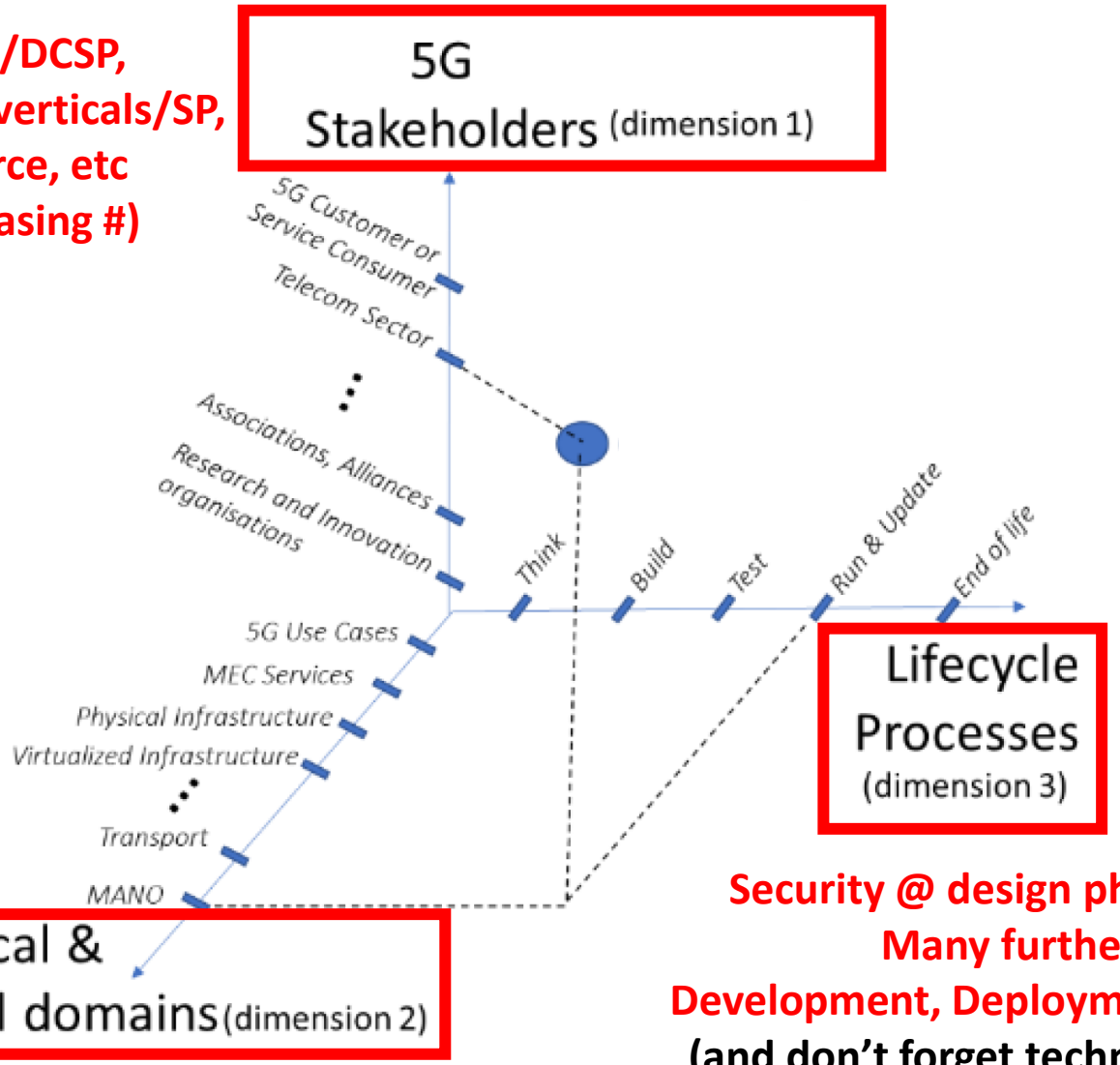


5G/6G systems' security: A small part of a bigger picture!!

Mobile/IoT security
Applications
… … …
Device manufacturing security
Interworking
Hardware
Firmware
Malware
… … …
Implementation
… … …
5G/6G security
Risk management
… … …
Side channels
… … …
Incremental deployment

Increased threat surface?

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



Heterogeneous technologies
Increased threat surface
Decentralization / edge computing

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

What about configuration «options»?

- **Is IMSI/SUPI protection ON?**
- **Is Integrity ON?**
  - **Just on control plane or also on data?**
- **Is certificate enrolment (TS 33.310) supported by gNB? Secure boot? …**
- *… very long list follows…*

To what extent? An example…

- **Requirement**: "The gNB **shall support confidentiality, integrity and replay protection** on the gNB DU-CU F1-U interface for user plane".
- Then **a NOTE** (!) says: "The above requirements allow to have F1-U **protected differently (including turning integrity and/or encryption off or on for F1-U)** from all other traffic on the CU-DU (e.g. the traffic over F1-C)".

So, options are the only problem?

NO!

- **Problems might remain even if security improvements were all mandatory!!**

- **Example: brand new 5G IMSI protection solution**

IMSI protection:what's this?

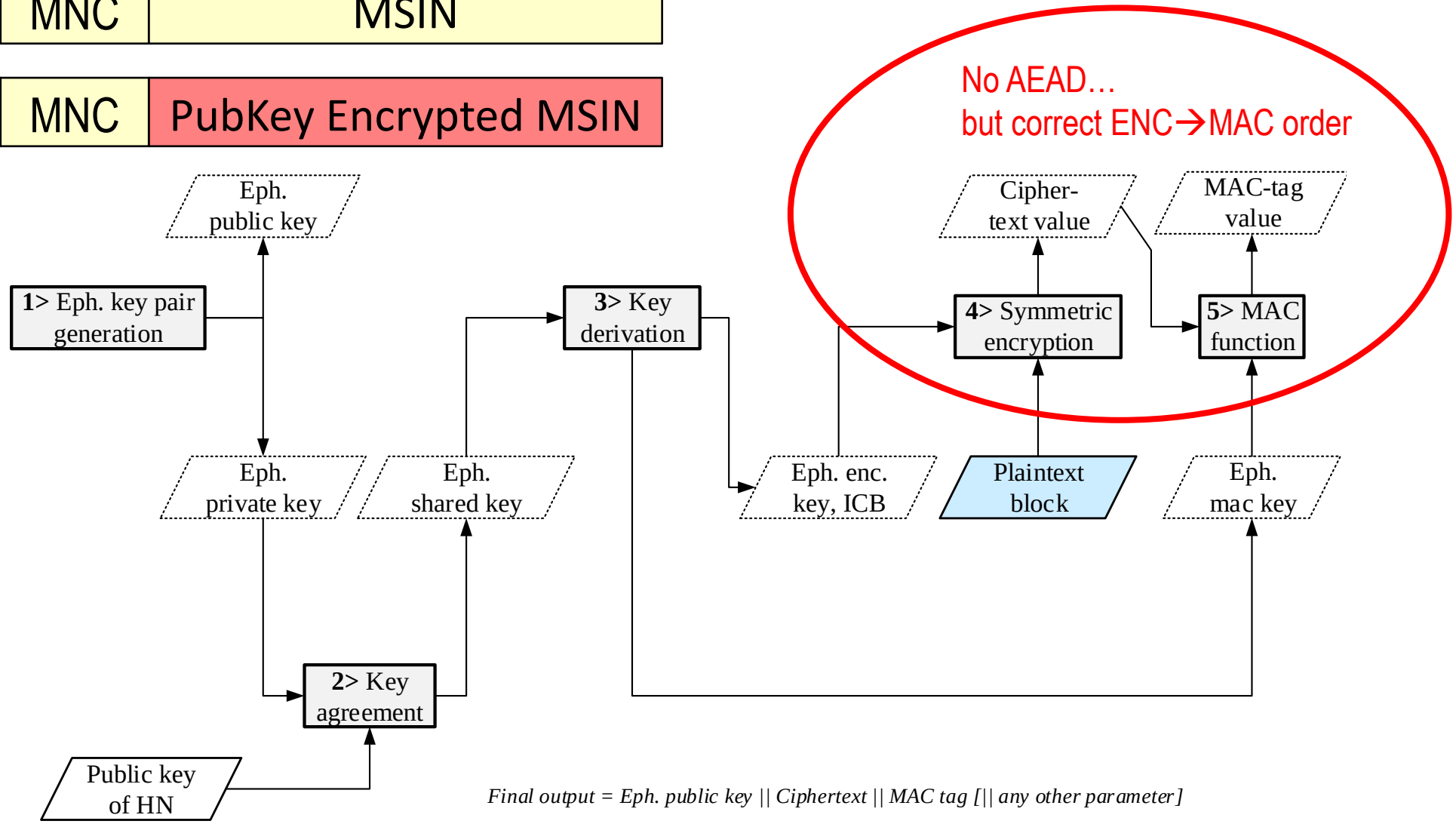
SUPI/IMSI:

MCC	MNC	MSIN

SUCI:

MCC	MNC	PubKey Encrypted MSIN

ECIES: Elliptic Curve Integrated Encryption Scheme



Final output = Eph. public key || Ciphertext || MAC tag [|| any other parameter]

Parenthesis: (EC) IES for the layman…

Ephemeral x → g^x

$(g^{HNkey})^x$

Hardness of DLOG

Derive ENC & AUTH keys
from DH-type exchange
(fresh at every new association)

Kc, Ka = HKDF($g^{(HNkey\ x)}$)

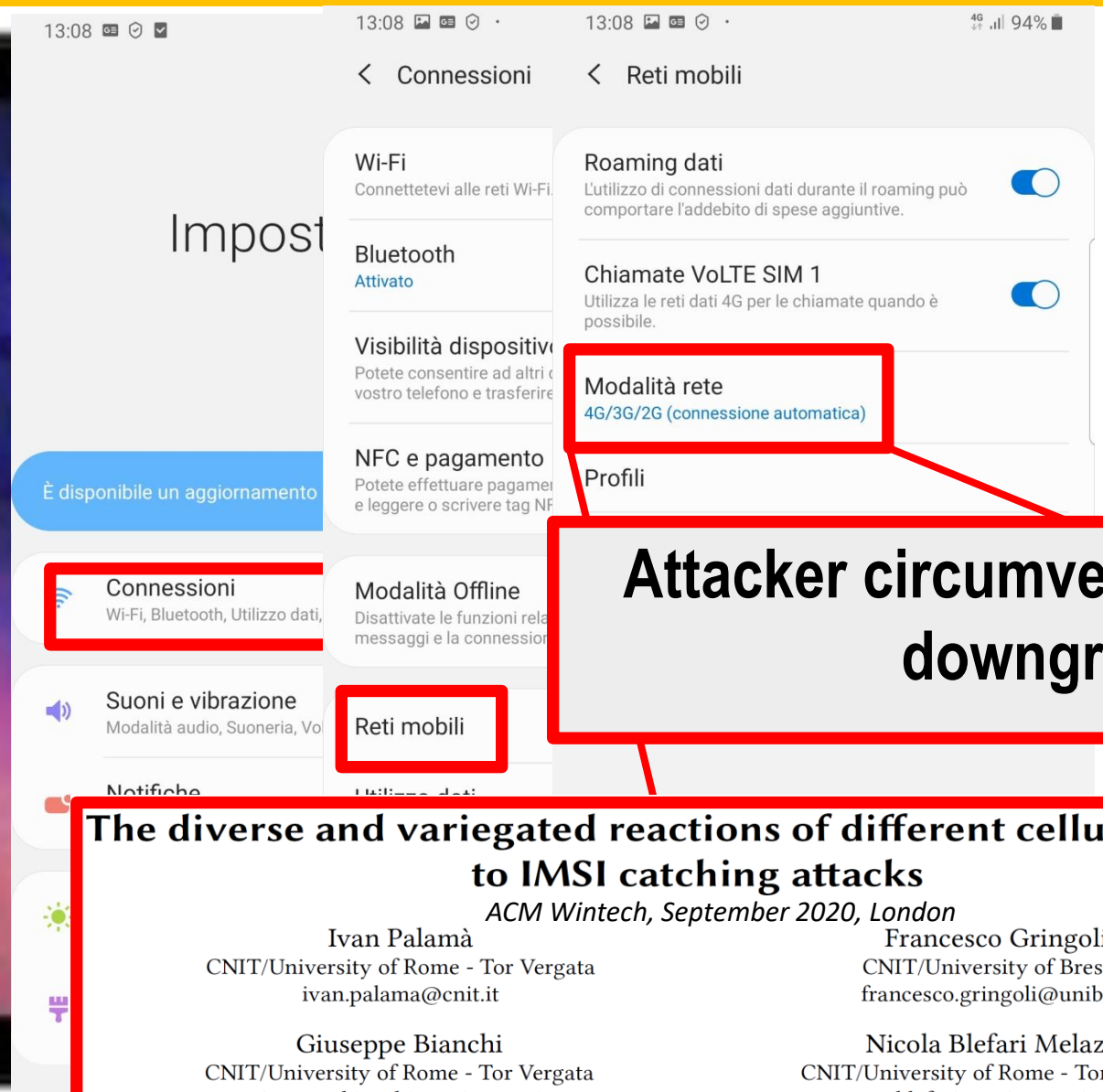
MCC	MNC	MSIN	$HMAC_{ka}$

$ENC = AES_{Kc}(SUPI)$ Auth=HMAC

- ephemeral g^x → No tracking possible
- Not even visiting domain «sees» IMSI(SUPI)

Send g^x along with above SUCI

But… no protection vs downgrade!



Attacker circumvents 5G protections by downgrading you!!

The diverse and variegated reactions of different cellular devices to IMSI catching attacks

ACM Wintech, September 2020, London

Ivan Palamà
CNIT/University of Rome - Tor Vergata
ivan.palama@cnit.it

Francesco Gringoli
CNIT/University of Brescia
francesco.gringoli@unibs.it

Giuseppe Bianchi
CNIT/University of Rome - Tor Vergata
giuseppe.bianchi@uniroma2.it

Nicola Blefari Melazzi
CNIT/University of Rome - Tor Vergata
blefari@uniroma2.it

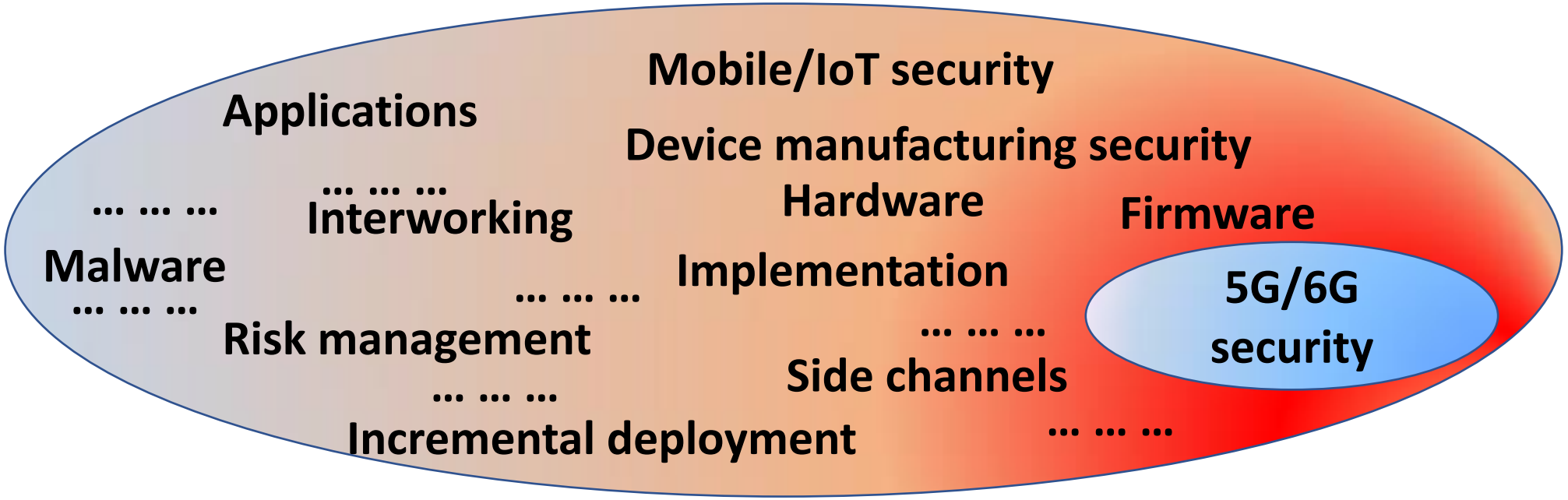
New Vulnerabilities in 5G Networks

Altaf Shaik
(Technische Universität Berlin, Germany)
Ravishankar Borgaonkar
(SINTEF Digital, Norway)

Blackhat 2019. USA

And implementation is always critical!

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



Just a (recent) example: NEF security

NEF: early implementations' security

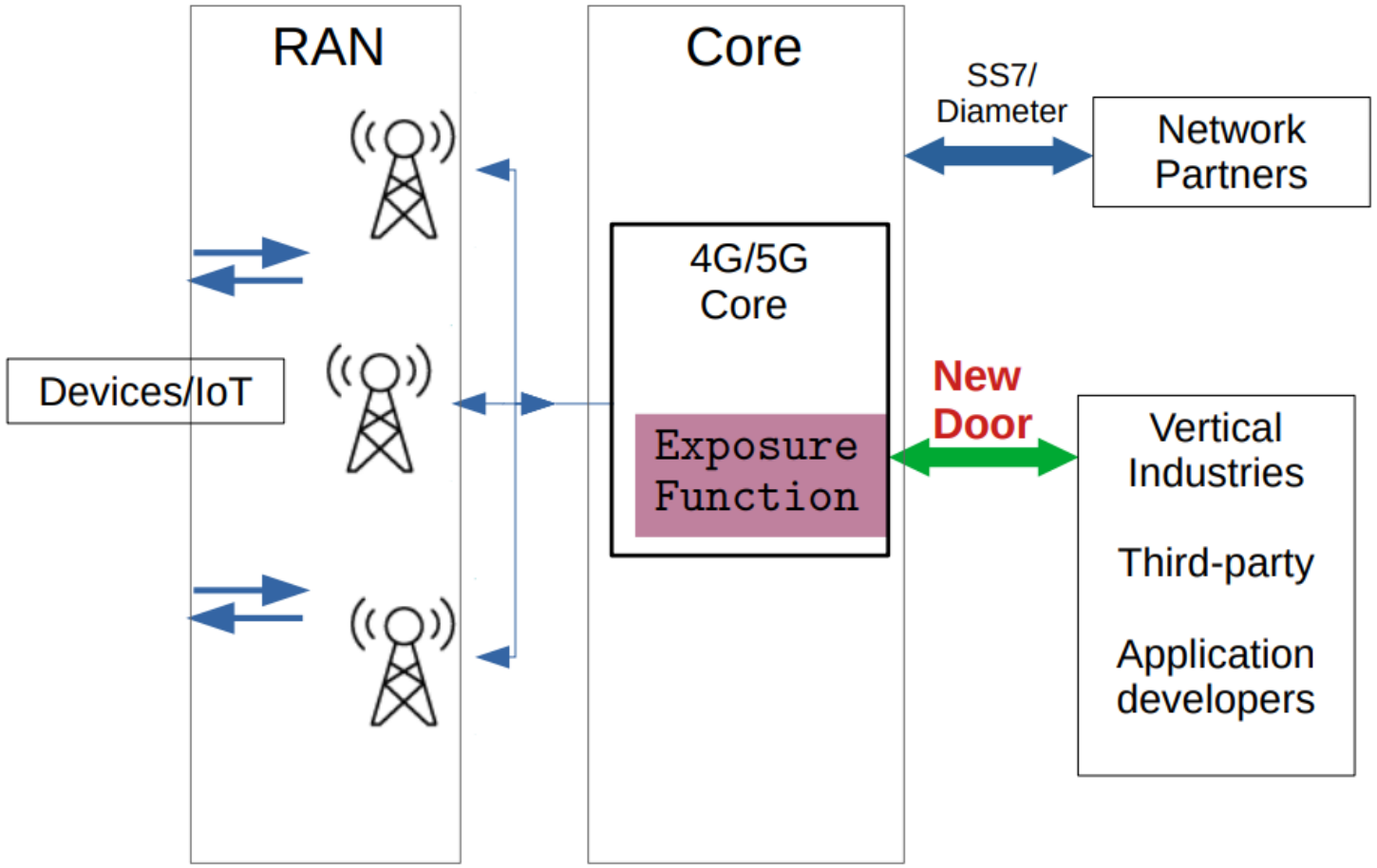
Attacks from a New Front Door
in 4G & 5G
mobile networks

Dr. Altaf Shaik & Shinjo Park

TU Berlin
& FastIoT

Blackhat USA 2022

New front door: exposure function



NEF: early implementations' security

Summary of security analysis

- Oauth and TLS is used in majority of platform (5/9) but not all of them.
- Only 2 out of 9 IoT platforms are not affected with serious vulnerabilities and API risks
- IMSI is exposed outside of 3GPP network, same practice may apply for 5G IMSI (SUPI)
- Lack of rate-limits, strong password policies
- Internal software information and core network IP addresses are exposed
- Authorization vulnerability can destroy the IoT devices and the network
- Script/code injection vulnerability found in many platforms, and is missed when a internal pen-testing
- SMS and IP content inspection is not present in mobile and IoT networks
- Attacker can easily obtain access to IoT service platforms and service APIs with forged identity

We're talking about PRODUCTION platforms!

NEF: early implementations' security

Last Shaik' slide: Key takeaways

- Opening new door on mobile networks – strict identity and access control, zero-trust
- Standard Oauth and TLS mechanisms wont help achieve full security
- Insecure API Design/Configuration **=** risk for mobile core and IoT devices
- Telecom exposure API risks are new: application **logic flaws** – require rigorous application specific tests (not using general API security scanners)
- Firewalls won't always help – need security-by-design and testing into CI/CD pipelines
- APIs in Telecom is new **and require a Telecom API top 10** to help developers and operators understand the security risks

NEF: early implementations

API security = new concern for telcos!

Last Shaik' slide: Key ta

- Opening new door on mobile networks – str
- Standard Oauth and TLS mechanisms wont
- Insecure API Design/Configuration **=** risk for mobile core and IoT devices
- Telecom exposure API risks are new: application **logic flaws** – require rigorous application specific tests (not using general API security scanners)
- Firewalls won't always help – need security-by-design and testing into CI/CD pipelines
- APIs in Telecom is new **and require a Telecom API top 10** to help developers and operators understand the security risks

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

consorzio nazionale interuniversitario per le telecomunicazioni

Università di Roma Tor Vergata

best defense?

Prevention → controls!

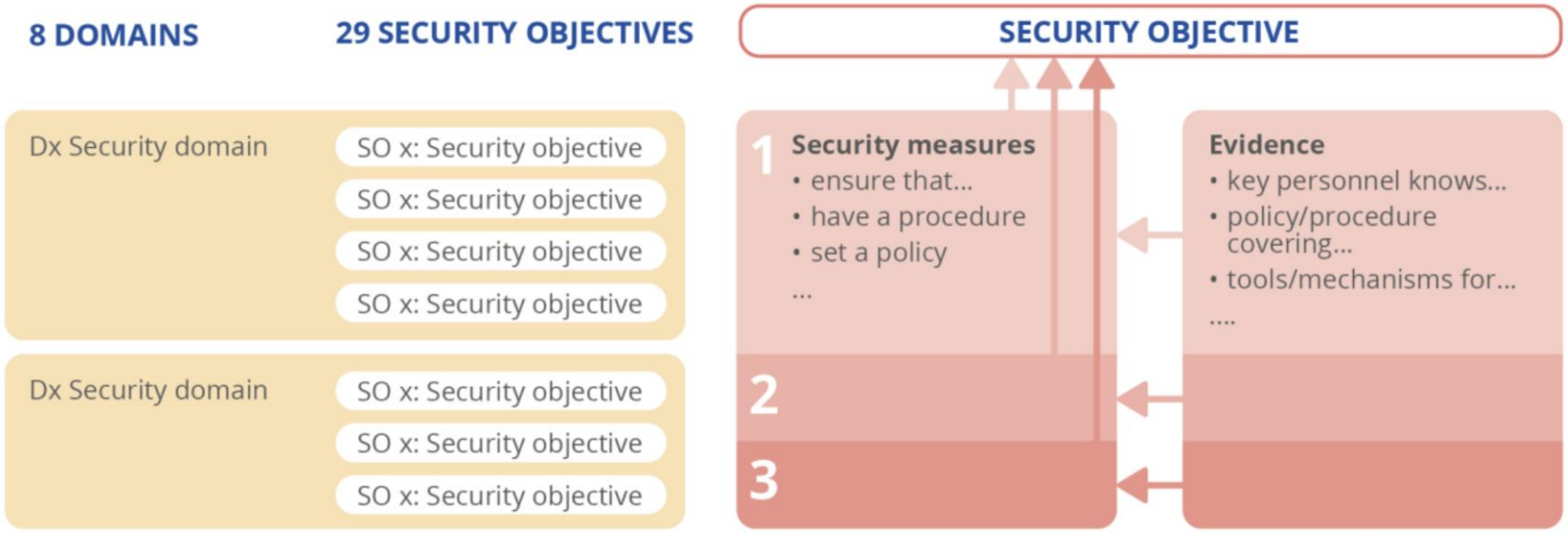
But of course, also related to prevention,
let's NOT forget secure design and threat intelligence
(not discussed today)

Which controls?

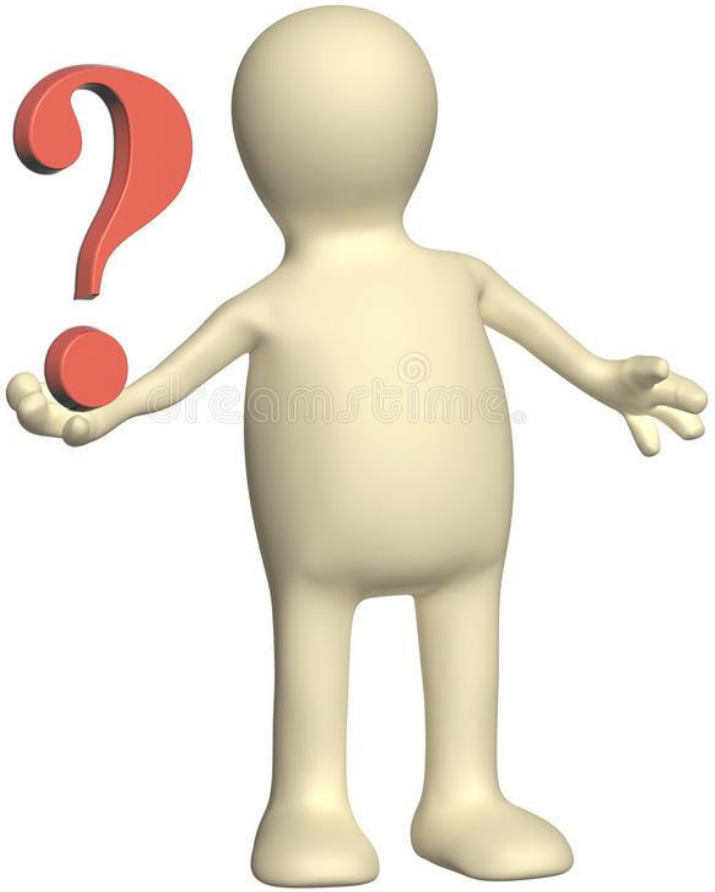
ENISA European Electronic Commun Code domains:

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?

Let's sample a few 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]
		Are there any controls in place to allow failsafe remote shutdown (or data clearing) for stolen	

#	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 controls in place, according to best practices, for the protection of any other cryptographic key material used to encrypt communication between network elements or between different networks[27]?	[a,b] [ii]
25	SO14	Are there appropriate controls in place for protection of VNF private keys to authenticate 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]

Let's sample a few 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]
		Are there any controls in place to allow failsafe remote shutdown (or data clearing) for stolen	

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 ection of any other cryptographic key ma ments or between different networks[27]?	[a,b] [ii]
25	SO14	Are there appropriate c enticate 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

Controls → more tech attention!

cnit consorzio nazionale interuniversitario per le telecomunicazioni

Università di Roma Tor Vergata

A real world story

Hello, what's your level of security?

No worries. military grade AES encryption

Are you kidding? When did this happen? WiFi WEP 1998? 2G 1999 disaster?

Ooops, but you «forgot» IV = 000000000

ZeroLogon attack, Couple of years ago, oct 2020!

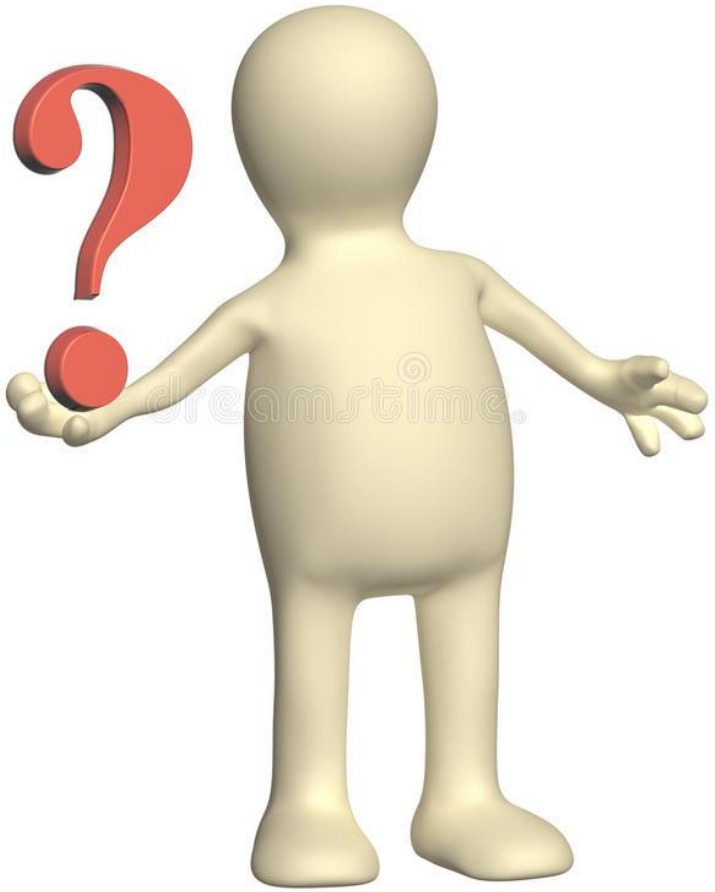
And tech mistakes might be way more subtle than a zero IV!

More later ☺

What is the potential impact of CVE-2020-1472?

The successful exploitation of CVE-2020-1472 allows an attacker to impersonate any computer on the network, disable security features that protect the Netlogon process, and change a computer's password associated with its Active Directory account.

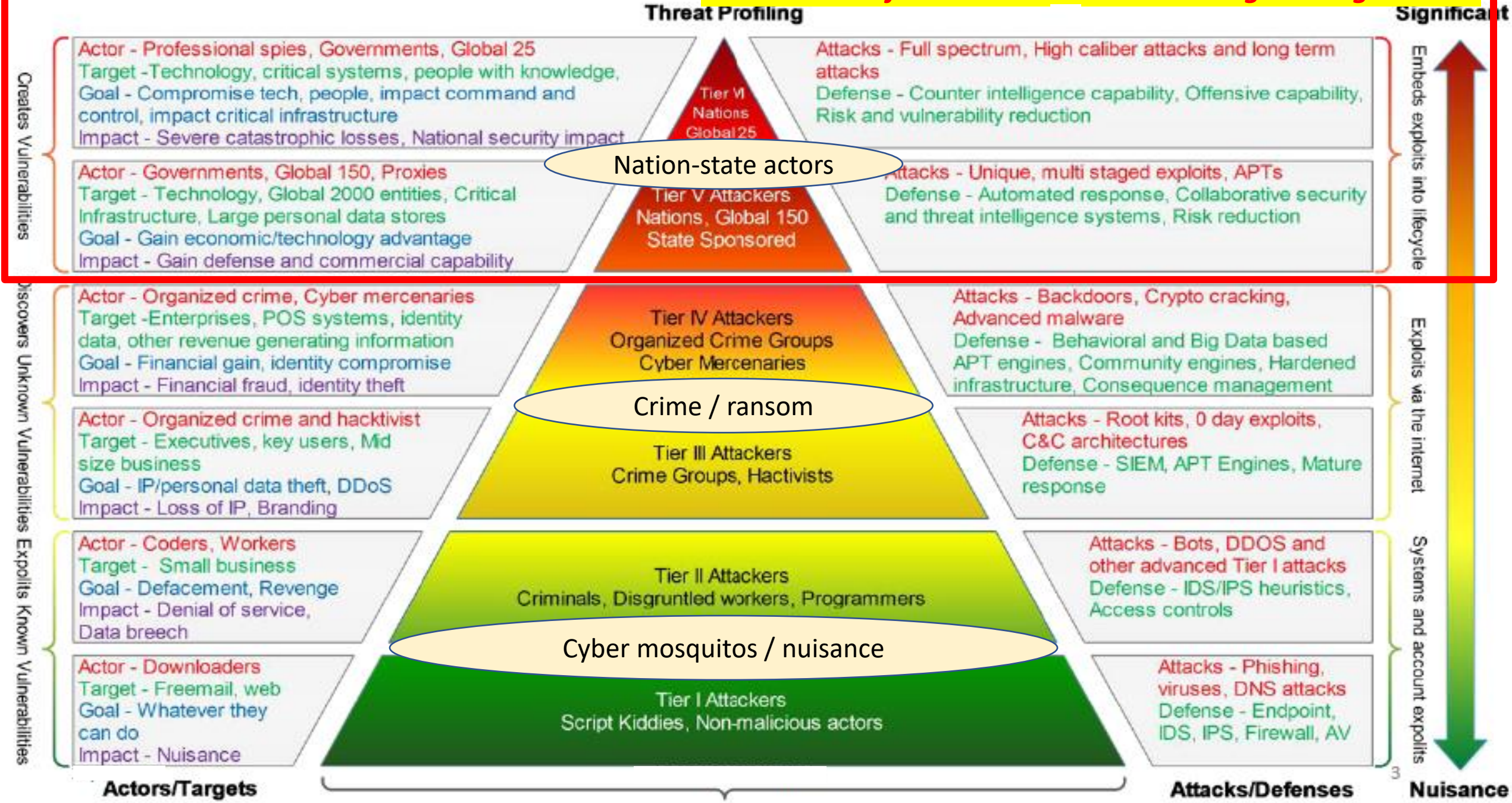
But the really crucial issue is…



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

Defense must be tailored to the threat model

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



5G = critical infrastructure → We cannot ignore high tiers

Threat Profilin

Creates Vulnerabilities

Actor - Professional spies, Governments, Global 25
Target -Technology, critical systems, people with knowledge,
Goal - Compromise tech, people, impact command and control, impact critical infrastructure
Impact - Severe catastrophic losses, National security impact

Actor - Governments, Global 150, Proxies
Target - Technology, Global 2000 entities, Critical Infrastructure, Large personal data stores
Goal - Gain economic/technology advantage
Impact - Gain defense and commercial capability

Tier VI Nations Global25

Nation-state act

Tier V Attackers Nations, Global 15 State Sponsored

Discovers Unknown Vulnerabilities Exploits Known Vulnerabilities

Actor - Organized crime, Cyber mercenaries
Target -Enterprises, POS systems, identity data, other revenue generating information
Goal - Financial gain, identity compromise
Impact - Financial fraud, identity theft

Actor - Organized crime and hacktivist
Target - Executives, key users, Mid size business
Goal - IP/personal data theft, DDoS
Impact - Loss of IP, Branding

Tier IV Attackers Organized Crime Gr Cyber Mercenarie

Crime / ranso

Tier III Attackers Crime Groups, Hacti

Actor - Coders, Workers
Target - Small business
Goal - Defacement, Revenge
Impact - Denial of service, Data breech

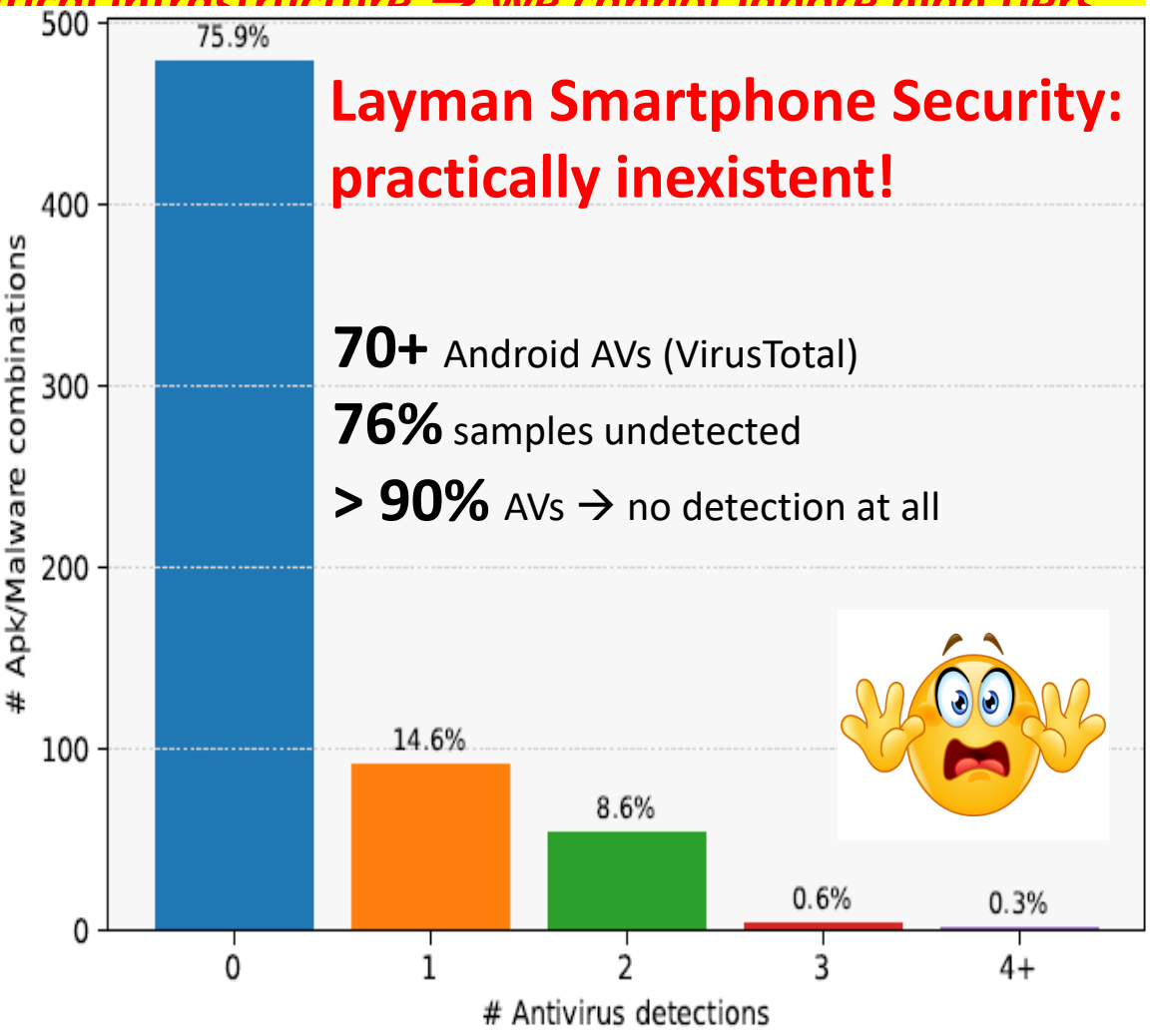
Actor - Downloaders
Target - Freemail, web
Goal - Whatever they can do
Impact - Nuisance

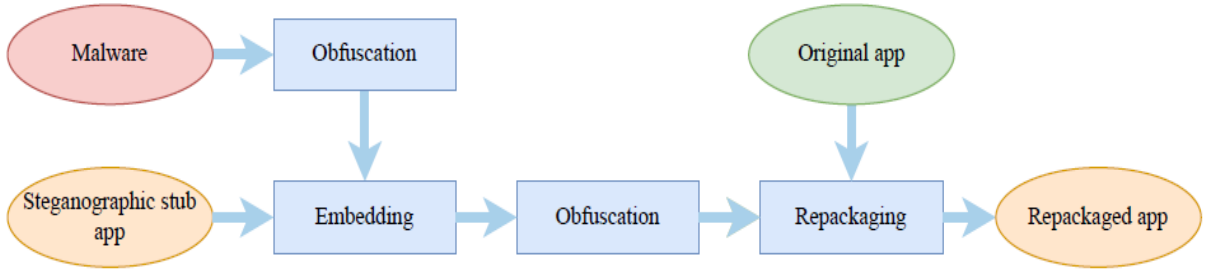
Tier II Attackers Criminals, Disgruntled workers

Cyber mosquitos /

Tier I Attackers Script Kiddies, Non-malic

Actors/Targets





5G risk assessment
by NIS cooperation group, 2019

	Risk categories
Risk scenarios related to insufficient security measures	*R1: Misconfiguration of networks*
	R2: Lack of access controls
Risk scenarios related to 5G supply chain	*R3: Low product quality*
	R4: Dependency on any single supplier within individual networks or lack of diversity on nation-wide basis
Risk scenarios related to modus operandi of main threat actors	*R5: State interference through 5G supply chain*
	R6: Exploitation of 5G networks by organised crime or Organised crime group targeting end-users
Risk scenarios related to interdependencies between 5G networks and other critical systems	*R7: Significant disruption of critical infrastructures or services*
	R8: Massive failure of networks due to interruption of electricity supply or other support systems
Risk scenarios related to end user devices	*R9: IoT (Internet of Things) exploitation*

5G risk assessment
by NIS cooperation group, 2019

Technical

Geo-political

societal

Cascade effects

	Risk categories
Risk scenarios related to insufficient security measures	*R1: Misconfiguration of networks* *R2: Lack of access controls*
Risk scenarios related to 5G supply chain	*R3: Low product quality* *R4: Dependency on any single supplier within individual networks or lack of diversity on nation-wide basis* *R5: State interference through 5G supply chain*
Risk scenarios related to modus operandi of main threat actors	*R6: Exploitation of 5G networks by organised crime or Organised crime group targeting end-users*
Risk scenarios related to interdependencies between 5G networks and other critical systems	*R7: Significant disruption of critical infrastructures or services* *R8: Massive failure of networks due to interruption of electricity supply or other support systems*
Risk scenarios related to end user devices	*R9: IoT (Internet of Things) exploitation*

The EU position

The dependence of many critical services on 5G networks would make the consequences of systemic and widespread disruption particularly serious. As a result, ensuring the cybersecurity of 5G networks is an issue of strategic importance for the Union, at a time when cyber-attacks are on the rise and more sophisticated than ever.

Ensuring European sovereignty should be a major objective, in full respect of Europe's values of openness and tolerance.[3] Foreign investment in strategic sectors, acquisition of critical assets, technologies and infrastructure in the Union and supply of critical equipment may also pose risks to the Union's security.

COMMISSION RECOMMENDATION

of 26.3.2019

Cybersecurity of 5G networks

R5. State interference through 5G supply chain?
No evidence but.. yes, «they» might DESIGN vulnerabilities

A very, very subtle error (?), real world story from another domain

Hello, «more secure» messaging application!
What do you offer me now in 2013?

Let me recap DH details..

Indeed, we offer a secure chat:
end-to-end Diffie-Hellman,
with final anti-MITM «auth code»!
Not even our servers can intercept you

Alice

Compute
$K = (g^{yx}) \bmod p$

choose random
$x \in \{0,1\}^s$

$g^x \bmod p$

$g^y \bmod p$

Bob

choose random
$y \in \{0,1\}^s$

Compute
$K = (g^{xy}) \bmod p$

SAME CODE? GOOD! Nobody can intercept us!

R5. State interference through 5G supply chain?
No evidence but.. yes, «they» might DESIGN vulnerabilities

A very, very subtl… …from another domain

Hello, «more secure» me…
What do you offer me no…

Let me recap DH details.

…we offer a secure chat:
…end Diffie-Hellman,
…al anti-MITM «auth code»!
…n our servers can intercept you

Alice

Compute
$K = (g^{yx}) \bmod p$

XOR with this truly random NONCE

choose random
$x \in \{0,1\}^s$

$g^x \bmod p$

$g^y \bmod p$

Bob

choose random
$y \in \{0,1\}^s$

Compute
$K = (g^{xy}) \bmod p$

XOR with this truly random NONCE

SAME CODE? GOOD! Nobody can intercept us!

Implementation bug? or (deniable!) bugdoor?

Università di Roma

cnit consorzio nazionale interuniversitario per le telecomunicazioni

A very, very subtle error (?), real world story from another dom

BUT, why the heck did you add this:
Key = g^{ab} XOR server-nonce ??
As a further protection?? AARGHH!!

Malicious server may now match any arbitrary endpoit fingerprint and create a MITM!
design error? Bugdoor? You decide! Real world story
https://habr.com/en/post/206900/
(in russian, otherwise not much known)

Alice

Compute
$K_x = (g^{zx}) \bmod p$

And now: $K = K_x$ N_x

choose random
$x \in \{0,1\}^s$

$g^x \bmod p$

$g^z \bmod p$

Bob

Compute
$K_y = (g^{zy}) \bmod p$

And now: $K = K_y$ N_y

choose random
$y \in \{0,1\}^s$

$g^y \bmod p$

$g^z \bmod p$

SAME CODE, but central (foreign country) server IS INTERCEPTING US!!

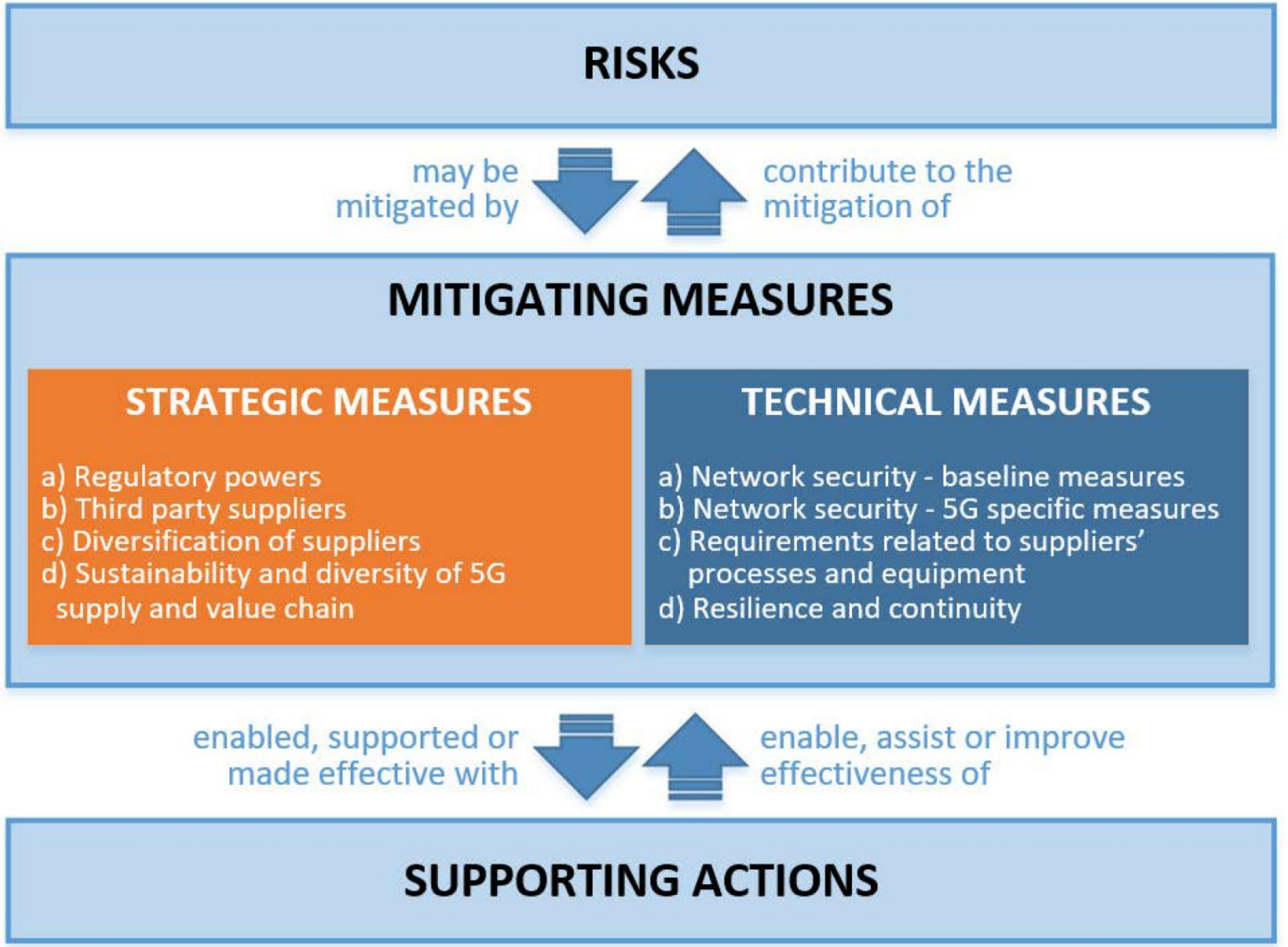
The EU position

The dependence of many critical services on 5G networks would make the consequences of systemic and widespread disruption particularly serious. As a result, ensuring the cybersecurity of 5G networks is an issue of strategic importance for the Union, at a time when cyber-attacks are on the rise and more sophisticated than ever.

Ensuring European sovereignty should be a major objective, in full respect of Europe's values of openness and tolerance.[3] Foreign investment in strategic sectors, acquisition of critical assets, technologies and infrastructure in the Union and supply of critical equipment may also pose risks to the Union's security.

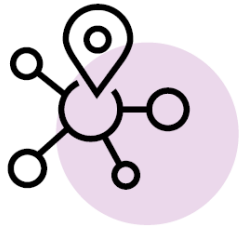
This Recommendation addresses cybersecurity risks in 5G networks by setting out guidance on appropriate risk analysis and management measures at national level, on developing a coordinated European risk assessment and on establishing a process to develop a common toolbox of best risk management measures.

The 5G EU Toolbox



EU 5G toolbox: strategic measures

- SM01 Strengthen role of national authorities;
- SM02 Perform audits on operators
- SM03 Assess risk profile of suppliers (and restrict/exclude if necessary)
- SM04 Control use of Managed Service Providers
- SM05 Ensure diversity of suppliers (multi-vendor)
- SM06 Strengthen resilience at national level;
- SM07 Identify key assets
- SM08 Maintain and build EU technology



STRATEGIC MEASURES

- Regulatory powers
- Third party suppliers
- Diversification of suppliers
- Sustainability and diversity of 5G supply and value chain

EU 5G toolbox: technical measures

- **TM01 Baseline secure network design and architecture**
- **TM02 Implement/adopt 5G security standards;**
- **TM03 Strict access controls;**
- **TM04 VNF security;**
- **TM05 Network mgmt, operation, monitoring;**
- **TM06 Physical security;**
- **TM07 SW integrity, update, patch mgmt;**
- **TM08 Robust procurement conditions for suppliers;**
- **TM09 EU 5G certification (tbd as of today)**
- **TM10 EU certification for non 5G-specific ICT;**
- **TM11 Resilience and Continuity Plans**

TECHNICAL MEASURES

- Network security – baseline measures
- Network security – 5G specific measures
- Requirements related to suppliers' processes and equipment
- Resilience and continuity

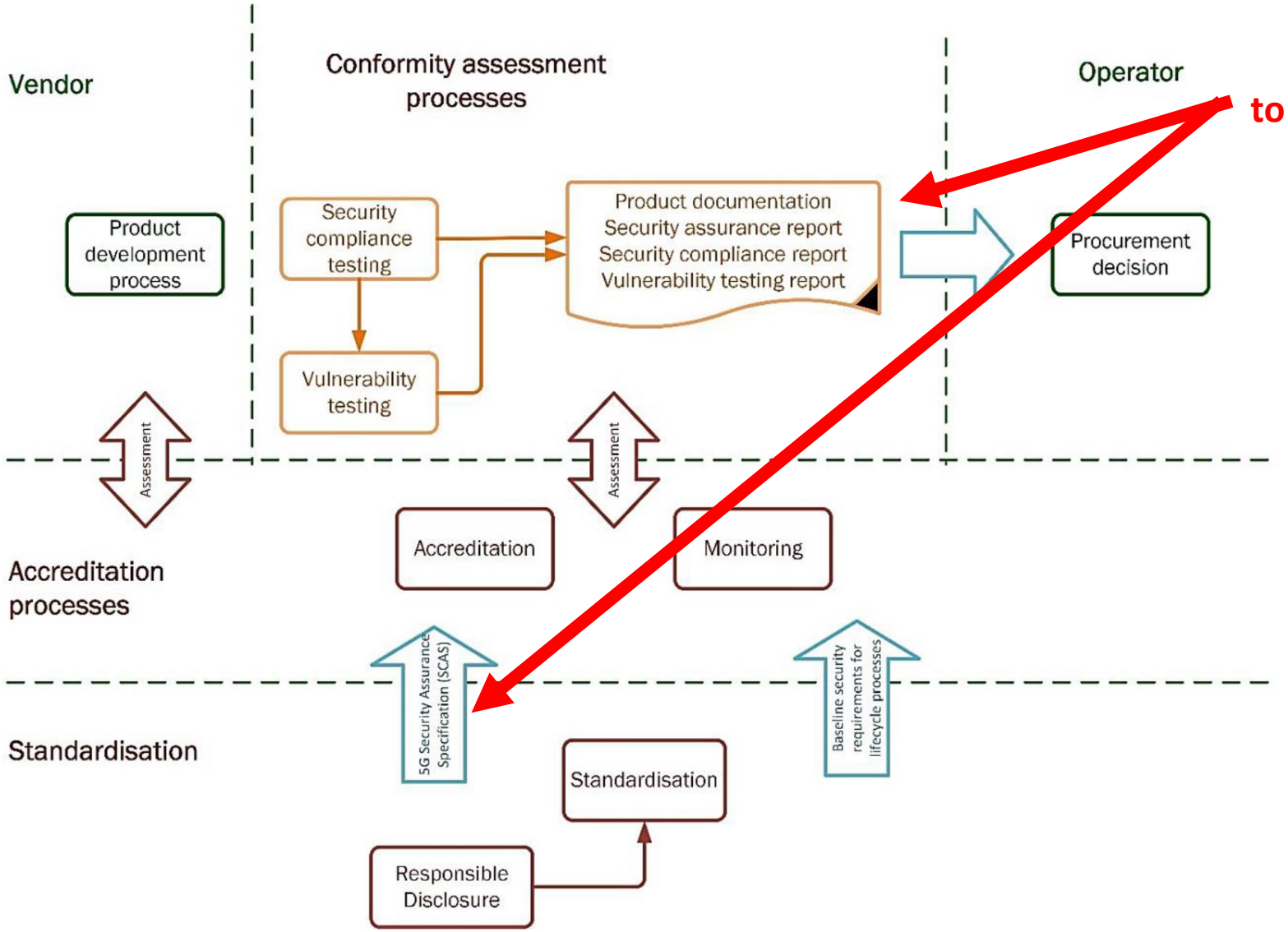
EU 5G toolbox: targeted support actions

- SA01 Develop guidelines and best practices on network security;
- SA02 Reinforce testing and auditing capabilities at national and EU level;
- SA03 Support and shape 5G standardisation;
- SA04 Guidance on implementation of security measures in 5G standards;
- SA05 Technical and organisational security through EU-wide certification;
- SA06 best practices on assessing risk profile of suppliers;
- SA07 Improve incident response and crisis management;
- SA08 Assess interdependency between 5G and other critical services;
- SA09 Enhance cooperation, coordination and info sharing mechanisms;
- SA10 Ensure publicly funded 5G projects do include cybersec risks

A pragmatic 3GPP step: SCAS tests!

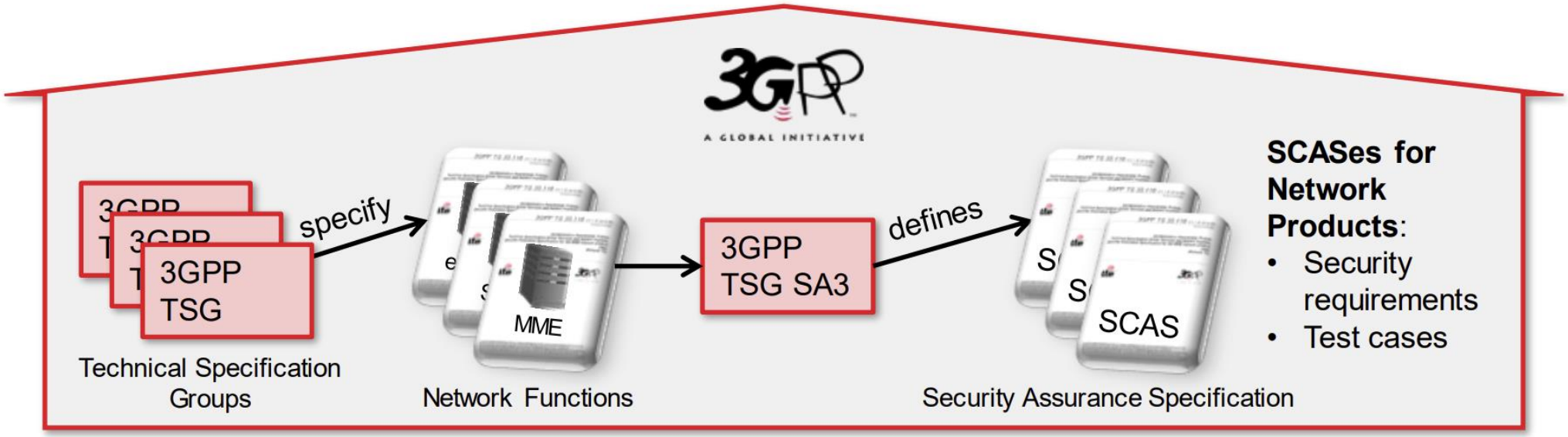
TS 33.116	Security Assurance Specification (SCAS) for the MME network product class
TS 33.216	Security Assurance Specification (SCAS) for the evolved Node B (eNB) network product class
TS 33.326	Security Assurance Specification (SCAS) for the Network Slice-Specific Authentication and Authorization Function (NSSAAF) network product class
TS 33.511	Security Assurance Specification (SCAS) for the next generation Node B (gNodeB) network product class
TS 33.512	5G Security Assurance Specification (SCAS); Access and Mobility management Function (AMF)
TS 33.513	5G Security Assurance Specification (SCAS); User Plane Function (UPF)
TS 33.514	5G Security Assurance Specification (SCAS) for the Unified Data Management (UDM) network product class
TS 33.515	5G Security Assurance Specification (SCAS) for the Session Management Function (SMF) network product class
TS 33.516	5G Security Assurance Specification (SCAS) for the Authentication Server Function (AUSF) network product class
TS 33.517	5G Security Assurance Specification (SCAS) for the Security Edge Protection Proxy (SEPP) network product class
TS 33.518	5G Security Assurance Specification (SCAS) for the Network Repository Function (NRF) network product class
TS 33.519	5G Security Assurance Specification (SCAS) for the Network Exposure Function (NEF) network product class
TS 33.520	5G Security Assurance Specification (SCAS); Non-3GPP InterWorking Function (N3IWF)
TS 33.521	5G Security Assurance Specification (SCAS);Network Data Analytics Function (NWDAF)
TS 33.522	5G Security Assurance Specification (SCAS); Service Communication Proxy (SCP)
TS 33.523	5G Security Assurance Specification (SCAS); Split gNB product classes
TS 33.527	Security Assurance Specification (SCAS) for 3GPP virtualized network products
TS 33.528	Security Assurance Specification (SCAS) for Policy Control Function (PCF)
TS 33.537	Security Assurance Specification (SCAS) for the Authentication and Key Management for Applications (AKMA) Anchor Function Function (AAnF)
TR 33.818	Security Assurance Methodology (SECAM) and Security Assurance Specification (SCAS) for 3GPP virtualized network products
TR 33.926	Security Assurance Specification (SCAS) threats and critical assets in 3GPP network product classes
TR 33.927	Security Assurance Specification (SCAS) threats and critical assets in 3GPP virtualized network product classes

(note: a further set of tests in a bigger picture)

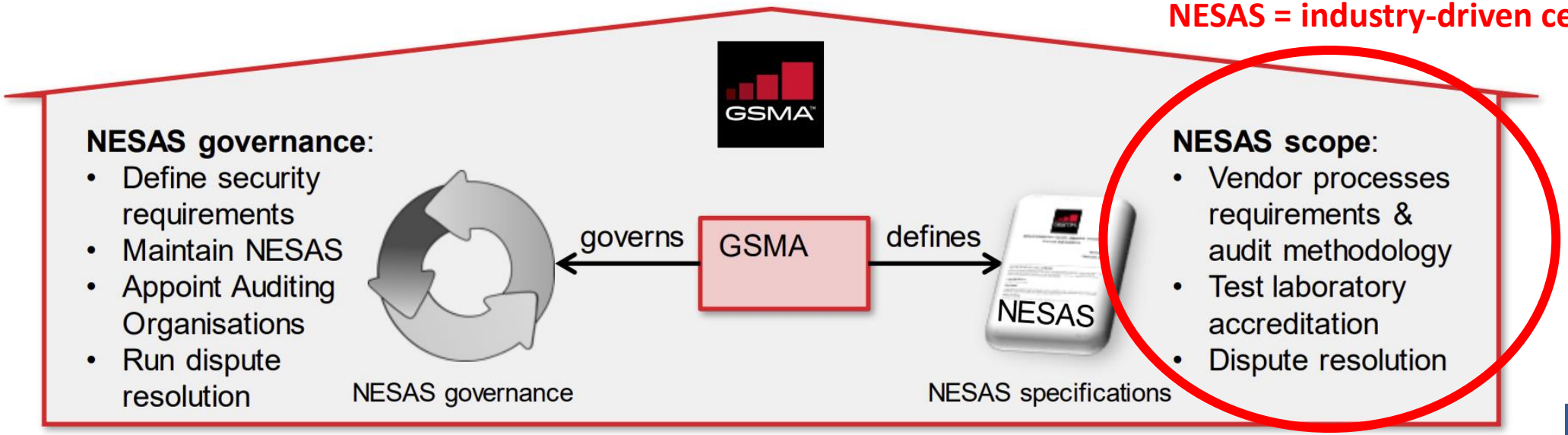


SCAS = specific tech addition (!) to remaining classical security testing, processes and governance!

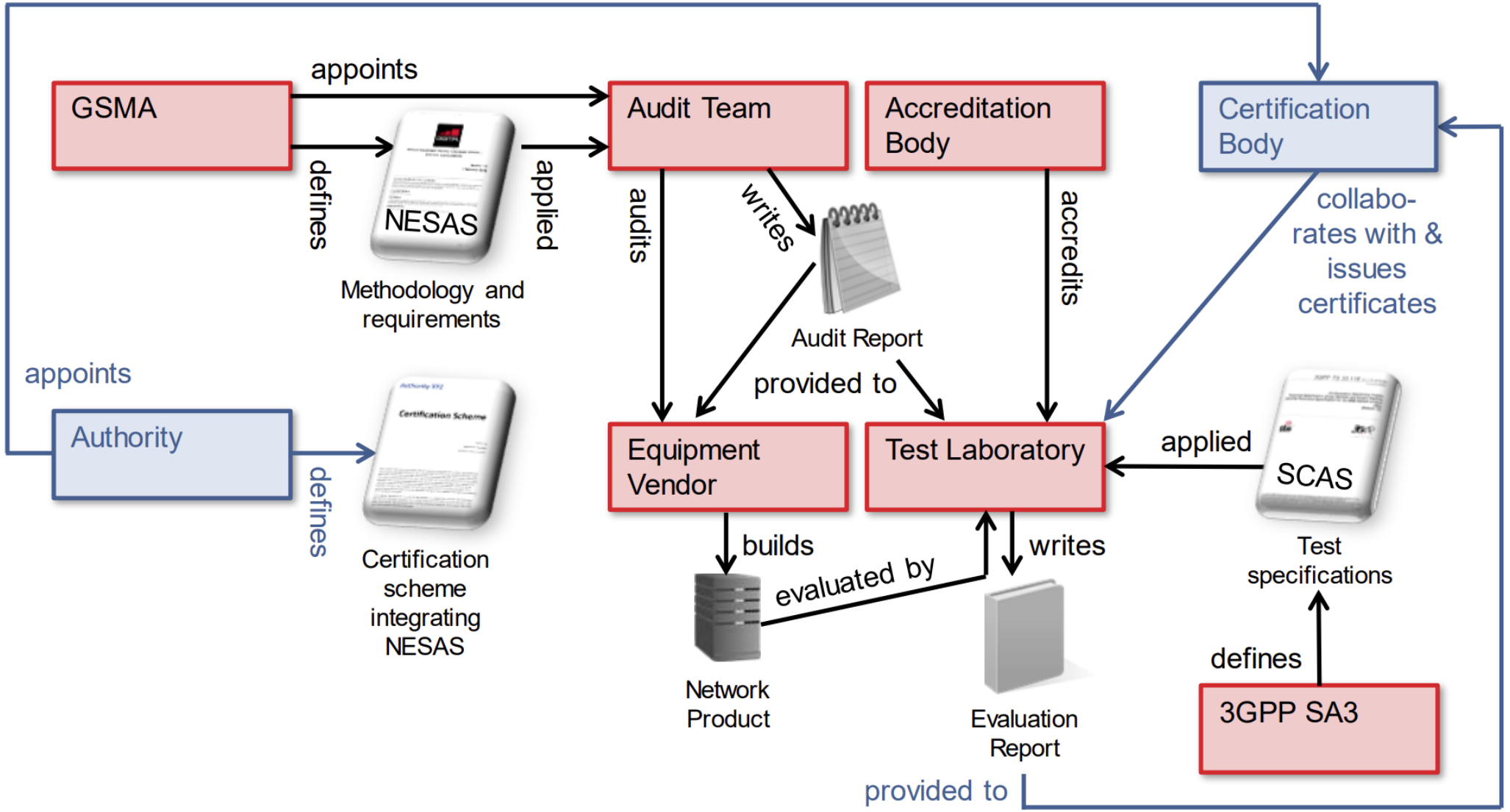
Promoted by GSMA NESAS



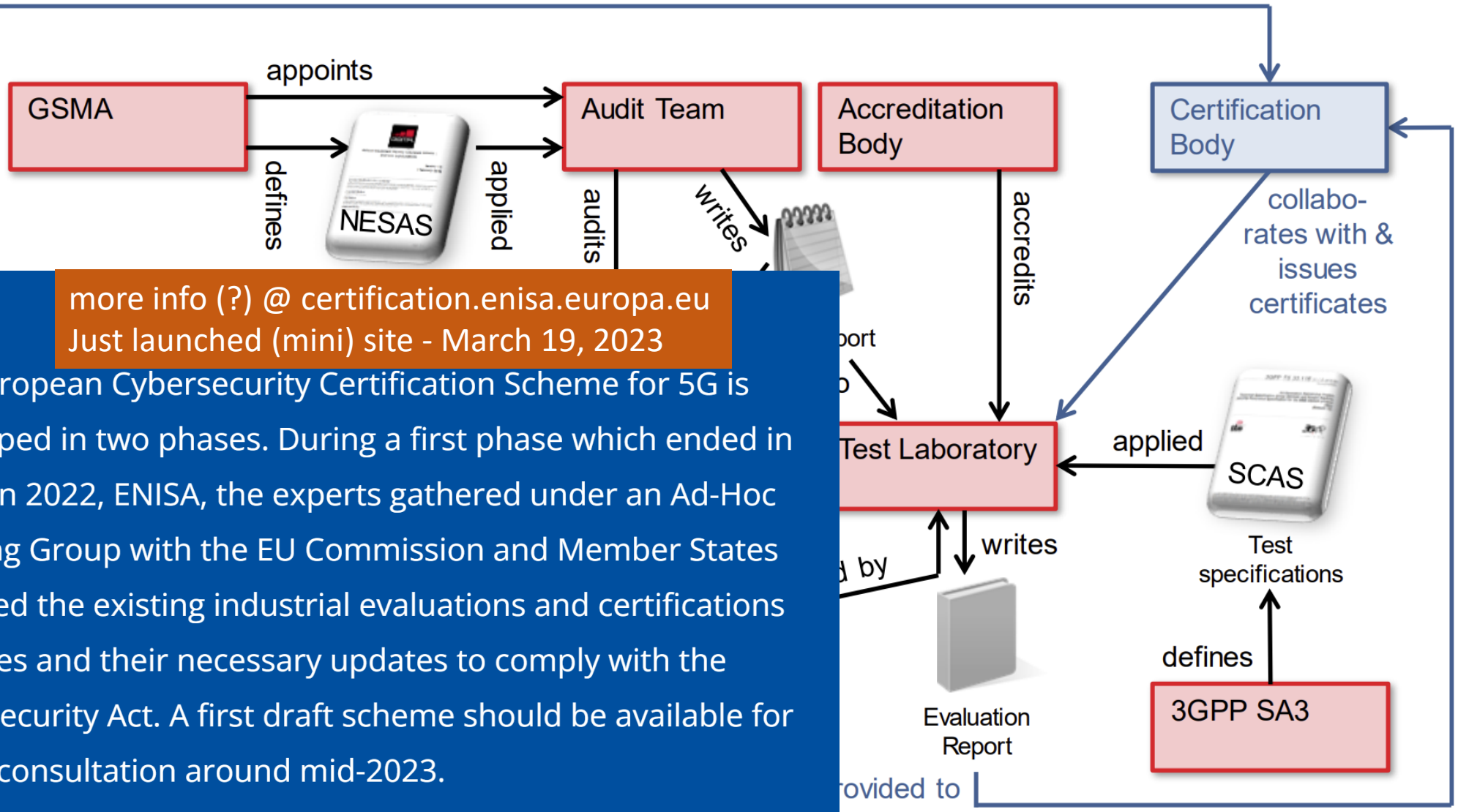
NESAS = industry-driven certification



NESAS «within» 5G certification? (ongoing)



NESAS «within» 5G certification? (ongoing)



EU5G

more info (?) @ certification.enisa.europa.eu
Just launched (mini) site - March 19, 2023

The European Cybersecurity Certification Scheme for 5G is developed in two phases. During a first phase which ended in Autumn 2022, ENISA, the experts gathered under an Ad-Hoc Working Group with the EU Commission and Member States analysed the existing industrial evaluations and certifications schemes and their necessary updates to comply with the Cybersecurity Act. A first draft scheme should be available for public consultation around mid-2023.

But… a couple of challenges

1. **From "compliance checklists"** *(is measure applied?)* **to "assurance tests"** *(concretely verify its application via formal test/procedure)*
   - **5G SCAS → valuable and promising approach,**
     but just a FIRST (good) STEP!
   - Must be complemented with deeper tech tests
     - *Remember this previous slide: encryption is not an ON/OFF check!!*

SO13	Is encryption applied for protection of confidentiality of user and signalling data between user equipment and base stations?

   - *and it is just an example of many other "Devils hiding in deep-tech details"*

But… a couple of challenges

1. **From "compliance checklists"** *(is measu*
   tests" *(concretely verify its application v*
   - **5G SCAS → valuable and promising ap**
     but just a FIRST (good) STEP!
   - Must be complemented with deeper te
     - *Remember this previous slide: encrypti*

SO13	Is encryption applied for protection of confide equipment and base stations?

   - *and it is just an example of many other*
     "Devils hiding in deep-tech details"

- ***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!)***

But… a couple of challenges

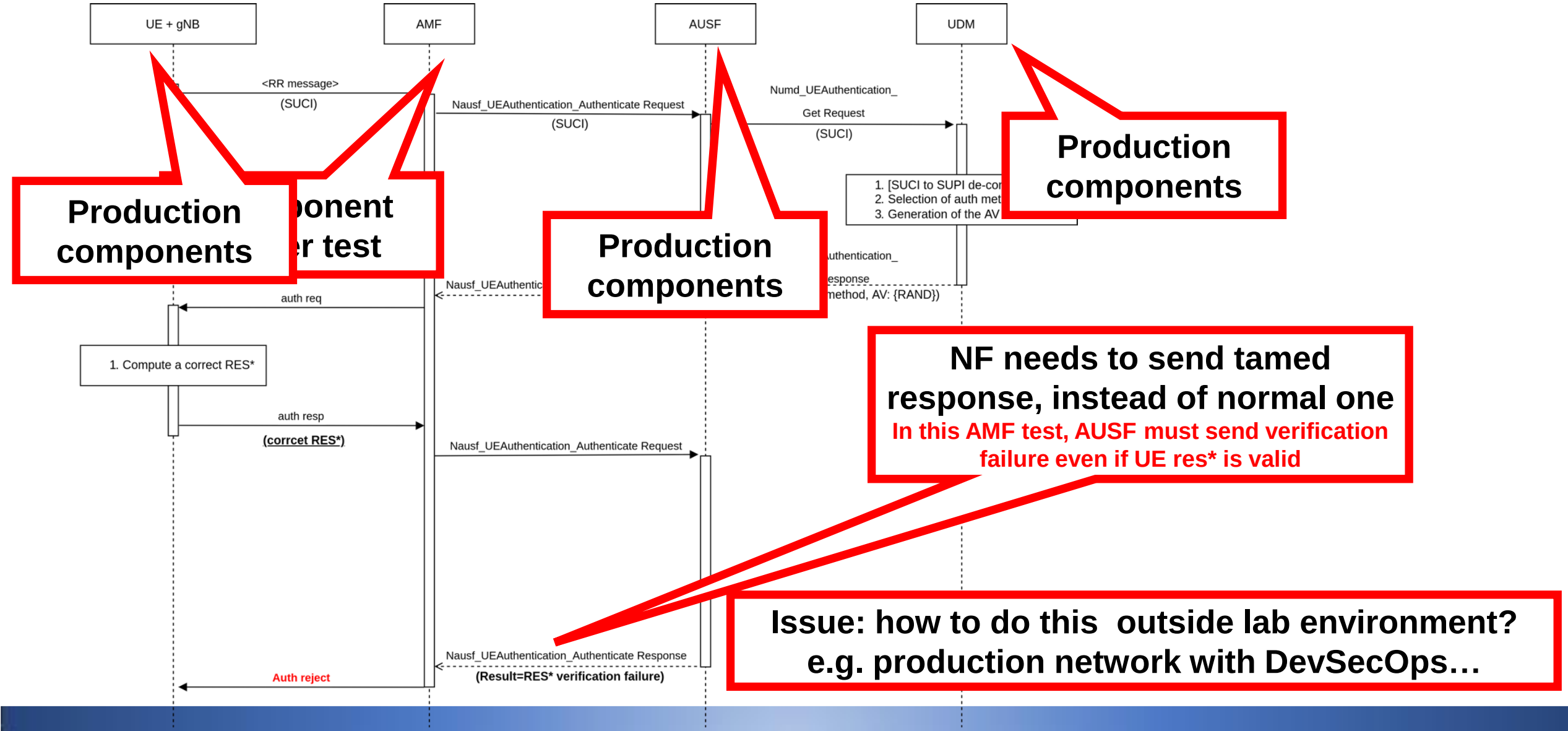
1. **From "compliance checklists"** *(is measure applied?)* **to "assurance tests"** *(concretely verify its application via formal test/procedure)*
   - **5G SCAS → valuable and promising approach,**
     but just a FIRST (good) STEP!
   - Must be complemented with deeper tech tests
     - *Remember this previous slide: encryption is not an ON/OFF check!!*

SO13	Is encryption applied for protection of confidentiality of user and signalling data between user equipment and base stations?

   - *and it is just an example of many other "Devils hiding in deep-tech details"*

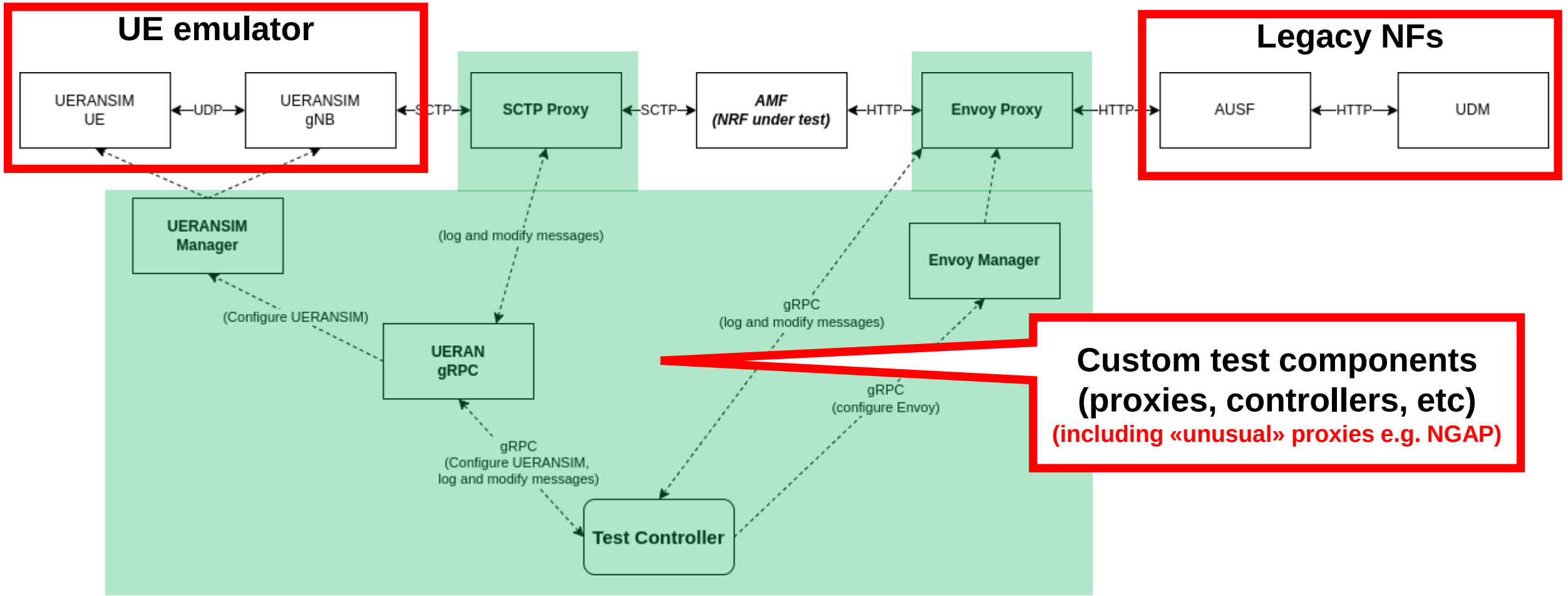
2. **From one-time certification to continuous verification / DevSecOps**
   - **5G virtualized Service Oriented Architecture → perfect use case**
   - **But CI/CD in an operational network is easy to say, but MUCH harder to do…**

Issue: Tests involving multiple NFs
(example for concreteness: AMF)



Issue: Tests involving multiple NFs
(example for concreteness: AMF)

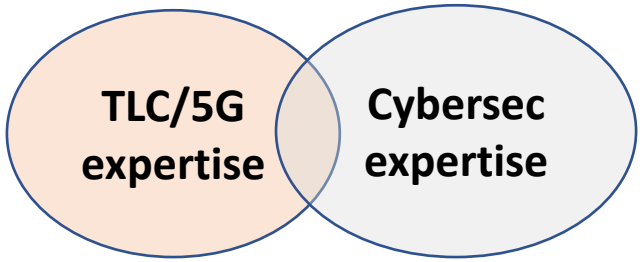
(our) Test architecture: non trivial!



The final challenge: people!!

how to raise, train, and retain in Italy (!) a new generation of qualified people - Four problems:

- *Cybersecurity: union of 20+ (!) knowledge areas! (source: cybok 2021)*
- *Huge skill gap (80% struggle to find candidates- source De Zan)*
- *5G security experts must FIRST be 5G experts!*
- *High tier threats → very deep expertise/skills*



Hard to find people with thorough training in *BOTH* fields

Thank you!
Giuseppe.Bianchi@uniroma2.it

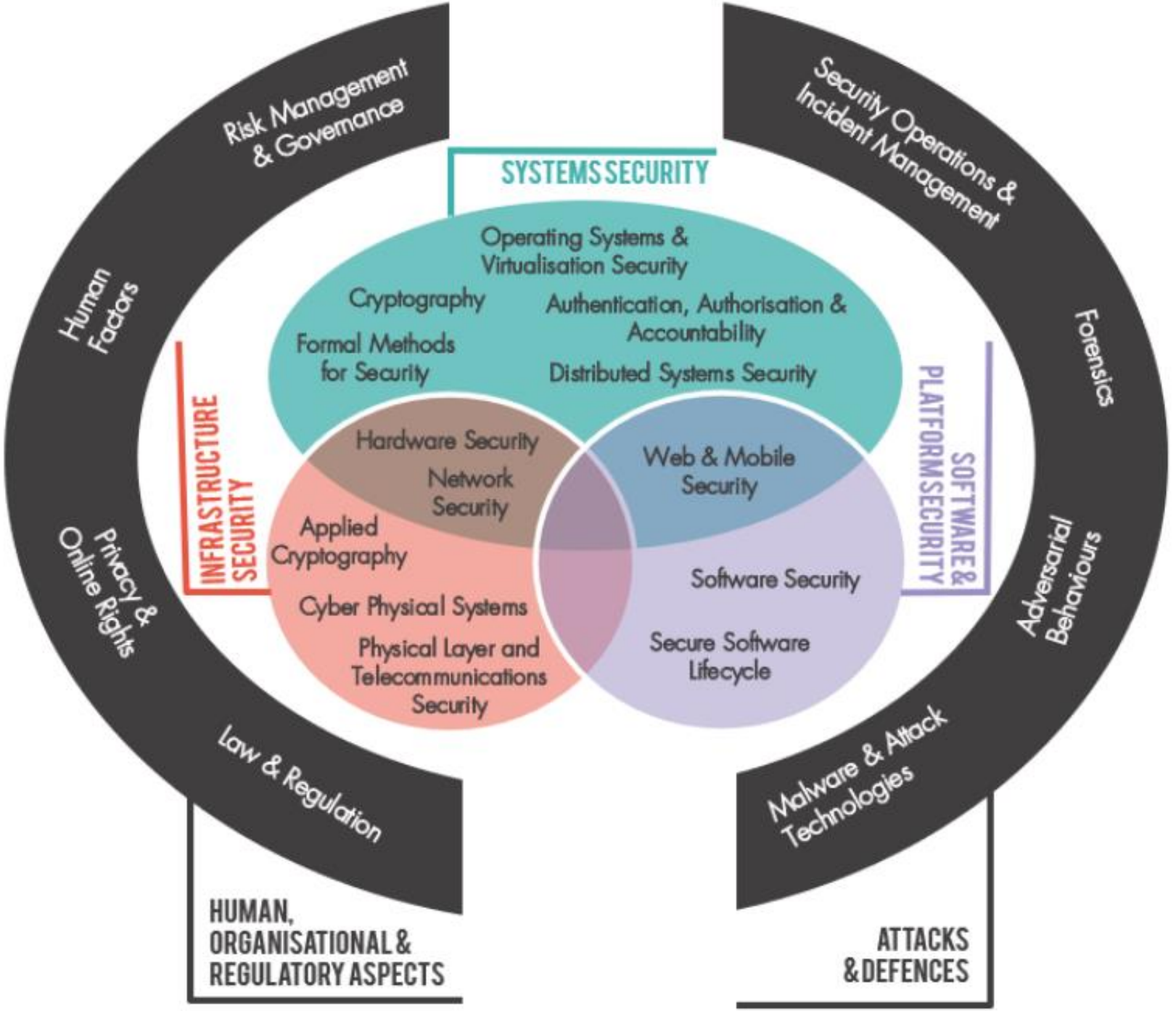
The final challenge

how to raise, tr
generation of q

- ***Cybersecurity: union***
- ***Huge skill gap*** *(80% strug*
- ***5G security experts n***
- ***High tier threats → v***

Tha

Giuseppe.Bian



Last but not least: AI will introduce further security issues!
(a real world story, April 23, 2013, 1:07 PM)

Last but not least: AI will introduce further security issues!
(a real world story, April 23, 2013, 1:07 PM)

They made millions with almost no effort!

(attacking AP twitter accout easier than attacking banks)