# 5G Security:

# Risks, Mitigation and Challenges

Gürkan Gür

Zurich University of Applied Sciences (ZHAW) InIT

**Innovationstreiber 5G: Technologie – Risiken – Anwendungsmöglichkeiten**
**09.11.2021 - Technopark Winterthur**

(*Joint work of INSPIRE-5Gplus team)

Zürcher Hochschule
für Angewandte Wissenschaften

zh
aw

INSPIRE-5Gplus

# INtelligent Security and PervasIve tRust for 5G and BEyond : INSPIRE-5Gplus

INSPIRE-5Gplus

- Make a revolutionary shift in the 5G (and Beyond) Security vision
  - ***Progress 5G Security*** and **devise a smart, trustworthy and liability-aware 5G security platform for future connected systems**, while contributing to its realization.
- Allow the advancement of security vision for 5G and Beyond through the adoption of
  - a set of emerging trends and technologies, such as **zero-touch management (ZSM), SD-SEC models, AI/ML techniques and Trusted Execution Environment (TEE)**
  - **new breed of SD-SEC assets and models** that will be developed to address some of the incumbent (e.g., adaptive slice security) or completely new (e.g., proactive security) challenges.

**Duration:** 3Y, start: 1 Nov 2019

**Programme:** H2020 RIA

**Project website:** http://inspire-5gplus.eu

# About Me (Highlights)

## Education

- **Bogazici University**, Istanbul, TURKEY.
  Ph.D. in Computer Eng., 2013.

- In addition to academia, more than 10 years of experience in technology companies (on-off mode)
-Involved in various ITEA, CELTIC, Innosuisse, and TÜBiTAK (TR) research projects as senior researcher, project coordinator and academic consultant
- Two patents (1 US, 1 TR)
- IEEE Senior member

**Current research interests:** Future Internet, information security, 5G/B5G networks and ICN

## Current position

- Senior Lecturer @ ZHAW in Switzerland

More information: www.zhaw.ch/en/about-us/person/gueu/

[Innovationstreiber 5G, 9 Nov. 2021]

# Outline

– **Key message**: 5G Networks: a Swiss Knife for connected services leading to **F**lexibility, **C**omplexity and **H**eterogenity conditions

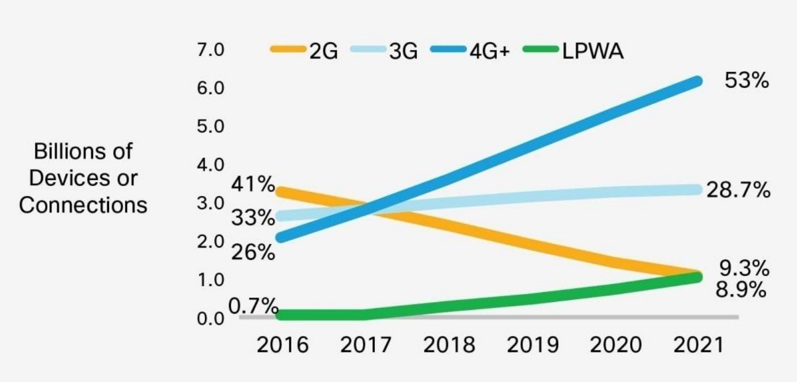
```
{Threats + Risks}× 5G Characteristics → Security Challenges
```

– Outline:

- 5G itself
- 5G characteristics and security
- Threats and solution arsenal
- Challenges and some ideas

# Networks are the lifeline of our civilization ...

- More and more reliance on networked infrastructure
  → Internet of Everything
- Mission critical services
- Massive and continuing traffic growth, esp. in mobile data traffic, high increase in wireless devices, networks, services and users



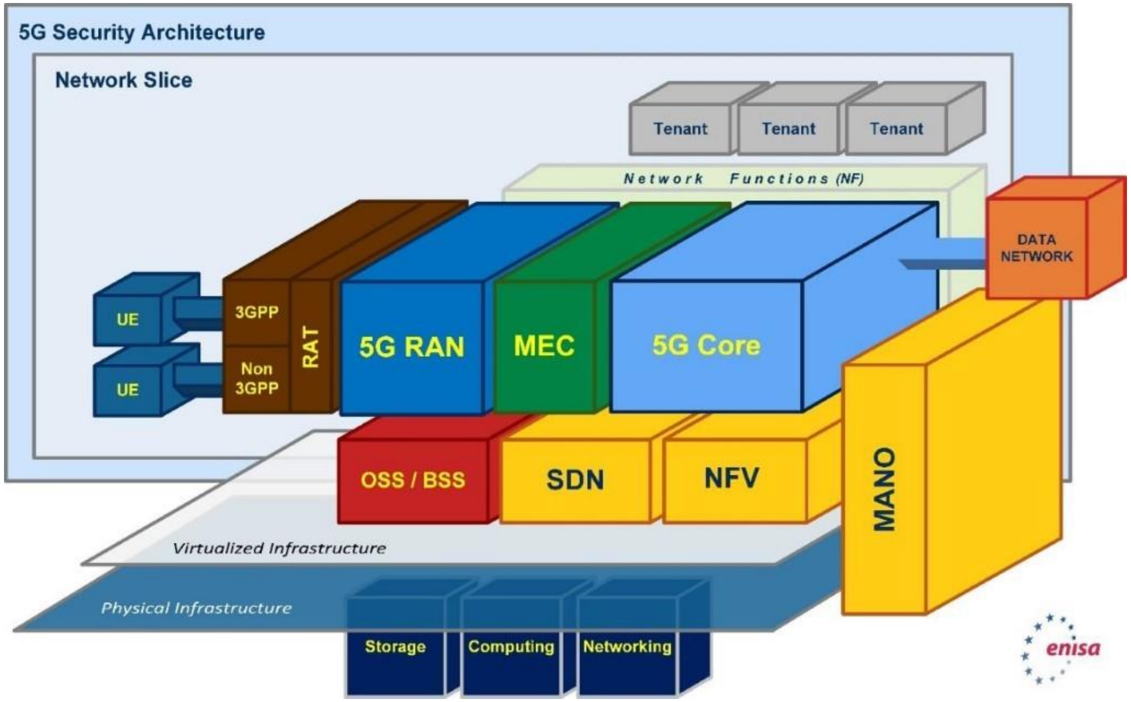
Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2016–2021, 2017. https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/mobile-white-paper-c11-520862.pdf

- More to come with IoT, MTC, 5G and Beyond
- Not solely networks anymore : Cloud resident and fog services, e.g. connected cars
- **COVID-19 pandemic!**

**Network is a critical infrastructure itself ...**

[Innovationstreiber 5G, 9 Nov. 2021]

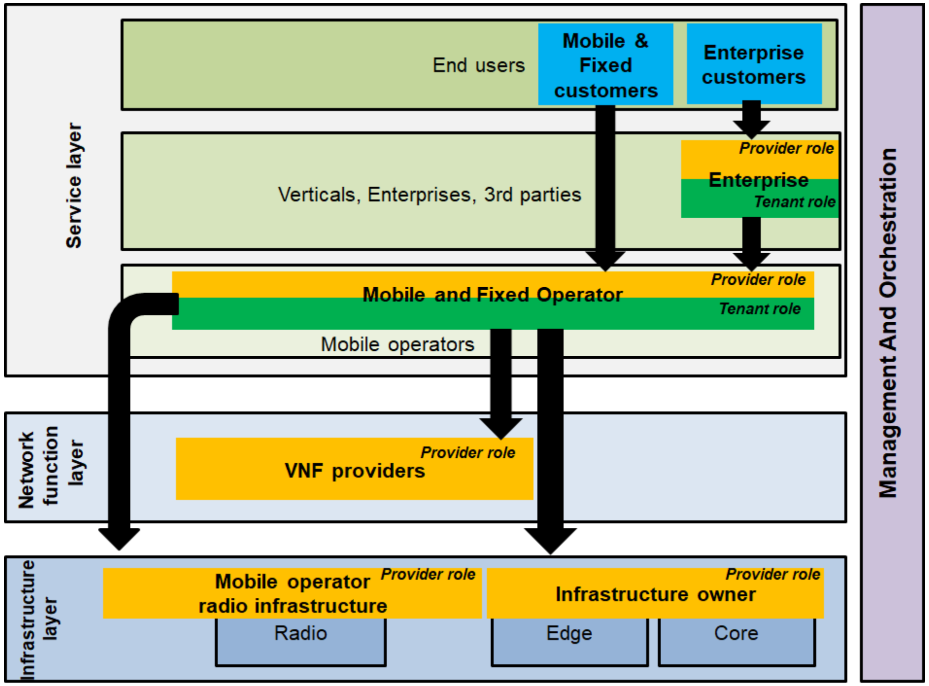
# 5G network architecture and security



**Source:** European Union Agency for Cybersecurity (ENISA)

# 5G network architecture (Another perspective)

- Example : operator offer enriched by partner[1]



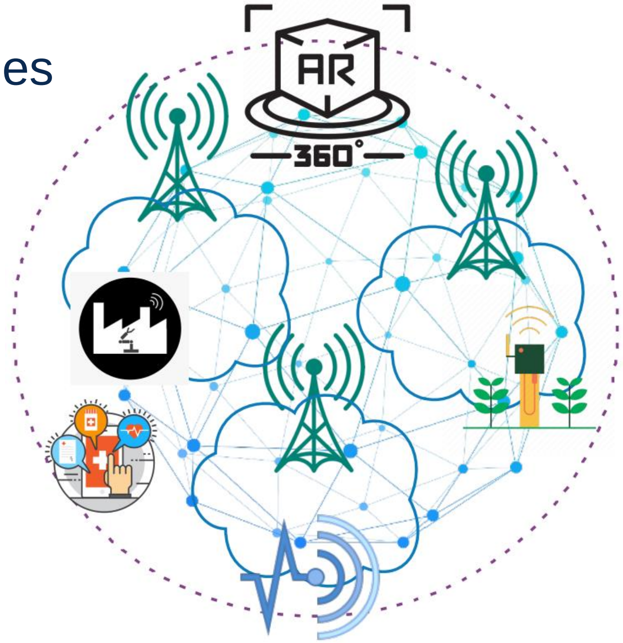
**Multi-party & multi-layer 5G infrastructure for service delivery**

[1] NGMN Alliance, "5G White Paper," Next generation mobile networks, white paper, vol. 1, 2015.

[2] C. Gaber *et al.*, "Liability-Aware Security Management for 5G," *2020 IEEE 3rd 5G World Forum (5GWF)*, 2020, pp. 133-138, doi: 10.1109/5GWF49715.2020.9221407.

# 5G characteristics - I

- Scale
  - Billions of devices (IoT)
  - Very high bitrates, ultra-low latency, QoS guarantees
  - Different modes of connectivity
  - Visibility and governance
  - Omnipresence
    - Novel services
    - Physical presence



- Softwarization
  - Software-defined networking
  - Virtualization
  - Cloudification
  - Network slicing
  - Software-oriented operation

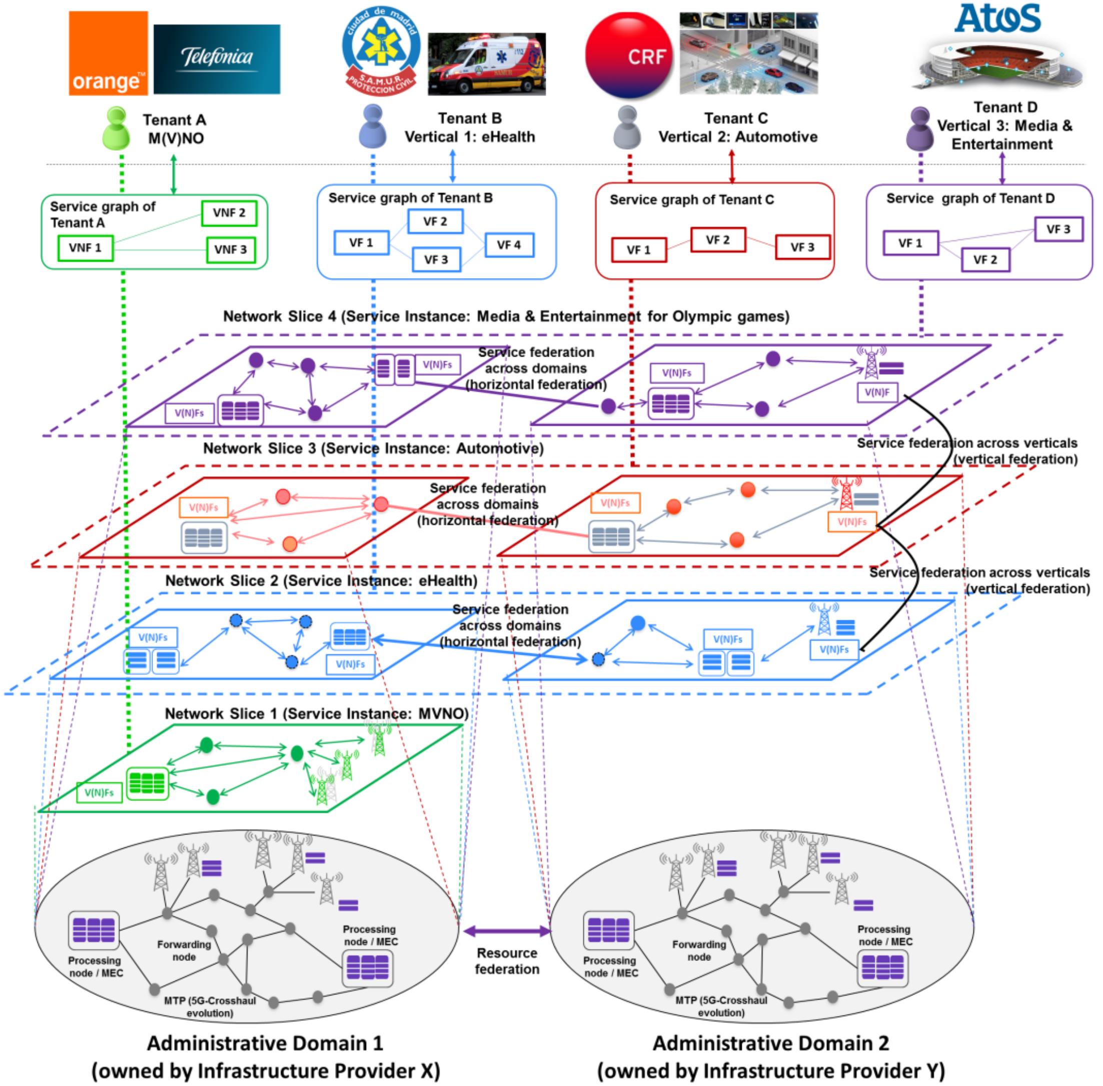
[Innovationstreiber 5G, 9 Nov. 2021]

# 5G characteristics - II

- Complexity
  - Open systems (no vendor lock-in)
  - Different actors: service providers, OTT..
    - Fragmentation
  - Verticals (slicing)
    - Critical services relying on the infrastructure (service-based paradigm
  - Management for SLAs
  - Convergence
  - Mobile applications and devices
- Flexibility
  - APIs
  - Fast service deployment
  - Automation and closed-loop control (not a silver bullet!)
  - AI/ML driven optimizations and automation
  - Integration of «3rd-party» technologies

[Innovationstreiber 5G, 9 Nov. 2021]

# An example 5G network instantiation with verticals ...


orange
Telefónica
Tenant A
M(V)NO
S.A.M.U.R. PROTECCION CIVIL
Tenant B
Vertical 1: eHealth
CRF
Tenant C
Vertical 2: Automotive
Atos
Tenant D
Vertical 3: Media & Entertainment
Service graph of Tenant A
VNF 1
VNF 2
VNF 3
Service graph of Tenant B
VF 1
VF 2
VF 3
VF 4
Service graph of Tenant C
VF 1
VF 2
VF 3
Service graph of Tenant D
VF 1
VF 2
VF 3
Network Slice 4 (Service Instance: Media & Entertainment for Olympic games)
V(N)Fs
V(N)F
Service federation across domains (horizontal federation)
Network Slice 3 (Service Instance: Automotive)
Service federation across verticals (vertical federation)
Service federation across domains (horizontal federation)
Network Slice 2 (Service Instance: eHealth)
Service federation across verticals (vertical federation)
Service federation across domains (horizontal federation)
Network Slice 1 (Service Instance: MVNO)
Processing node / MEC
Forwarding node
MTP (5G-Crosshaul evolution)
Resource federation
Administrative Domain 1
(owned by Infrastructure Provider X)
Administrative Domain 2
(owned by Infrastructure Provider Y)

**5G-Transformer users**
Mobile (Virtual) Network Operators
Vertical Industries

**Vertical Slicer (VS)**

Logical entry point for verticals to support the creation and management of their transport slices in a short time-scale

**Service Orchestrator (SO)**

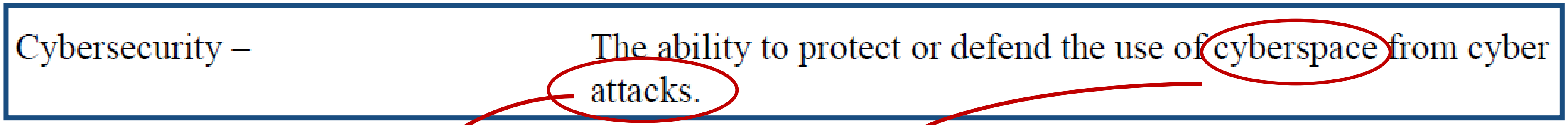
Federation of transport networking and computing resources from multiple domains and allocation to slices

**Mobile Transport and Computing Platform for Verticals (MTP)**

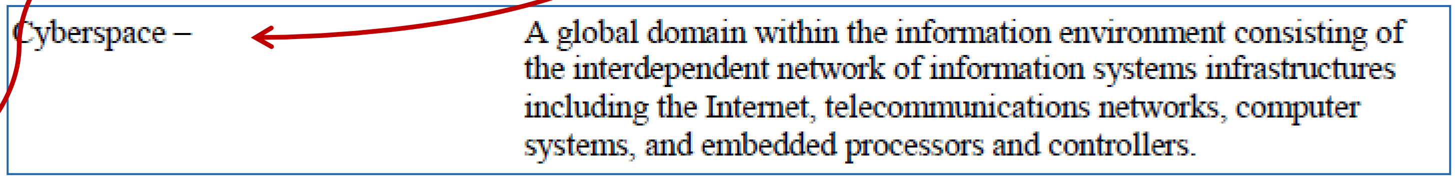
Underlying unified transport stratum for integrated fronthaul and backhaul networks

**Source:** 5G-Transformer: 5G Mobile Transport Platform for Verticals Project

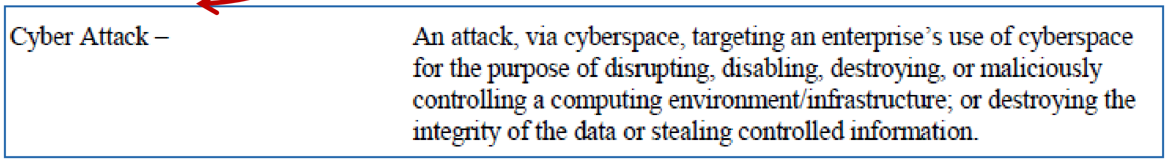
# What is «cyber»security? A quick reminder ...



Cybersecurity – The ability to protect or defend the use of cyberspace from cyber attacks.

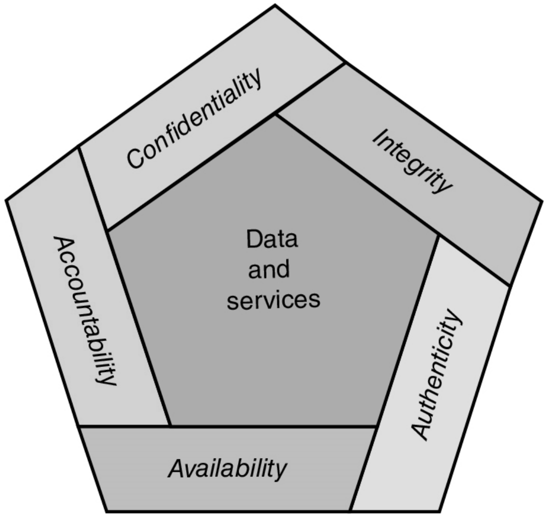


Cyberspace – A global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.



Cyber Attack – An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information.

NIST Interagency Report (IR) 7298 Revision 2 **"Glossary of Key Information Security Terms",** 2013
http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf



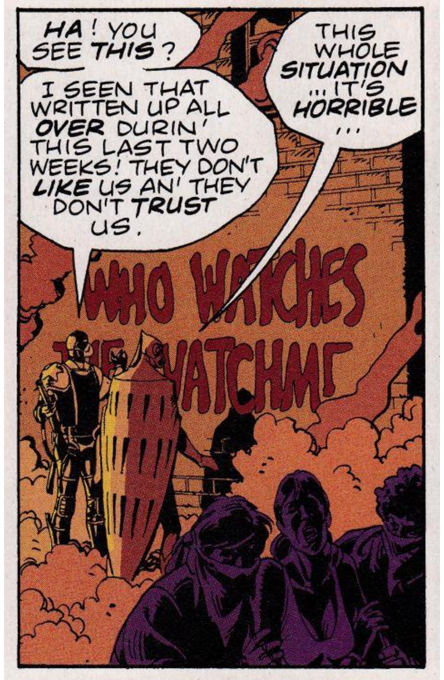
# Current 5G security solutions

| Segment | Rationale | Specific SotA elements |
|---|---|---|
| **Infrastructure/Platform Level** | Focus on core 5G technologies for 5G networks (e.g., SDN or NFV security) | RAN, network softwarisation, MEC domain, Trusted Execution Environment (TEE) as an enabler in the infrastructure |
| **Management/Automation Level** | Soft techniques and enablers, more generally applicable impacting general ICT security (e.g., AI/ML security) | Zero touch Service Management (ZSM), DLT, trust and liability, cyber threat intelligence, security via AI/ML and security for AI/ML |
| **Service/Vertical Level** | Service and end user perspectives, verticals, use-case driven security solutions | Verticals, services, IoT as a key service domain |

**Source:** INSPIRE-5Gplus project, Deliverable D2.1 5G Security: Current Status and Future Trends
https://zenodo.org/record/4569519

# But who watches the watchmen?

- **Securing AI/ML : An emerging topic for 5G and Beyond 5G[3] systems security ...**
    - **Adversarial Machine Learning:** Bad guys distorting your learning
    - **Adversarial** environment, **mimicry** attacks
    - E.g., some adversaries may be capable to design training data that will mislead the learning algorithm.


HA! YOU SEE THIS?
I SEEN THAT WRITTEN UP ALL OVER DURIN' THIS LAST TWO WEEKS! THEY DON'T LIKE US AN' THEY DON'T TRUST US.
THIS WHOLE SITUATION ... IT'S HORRIBLE ...
WHO WATCHES
THE WATCHME

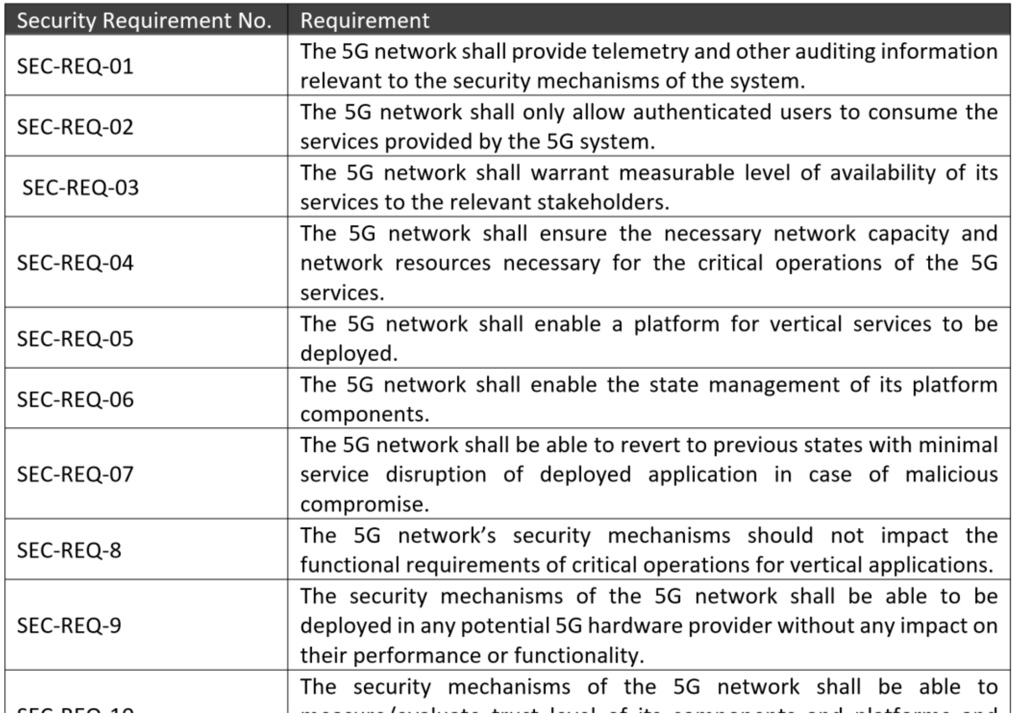
Copyright: DC Comics
Alan Moore, Dave Gibbons

[3] P. Porambage, G. Gür, D. P. M. Osorio, M. Liyanage, A. Gurtov and M. Ylianttila, "The Roadmap to 6G Security and Privacy," in *IEEE Open Journal of the Communications Society*, vol. 2, pp. 1094-1122, 2021, doi: 10.1109/OJCOMS.2021.3078081.

# Expectations of the industry ...

- More secure
- Cheaper
- Better
- Easier to manage

...



| Security Requirement No. | Requirement |
|---|---|
| SEC-REQ-01 | The 5G network shall provide telemetry and other auditing information relevant to the security mechanisms of the system. |
| SEC-REQ-02 | The 5G network shall only allow authenticated users to consume the services provided by the 5G system. |
| SEC-REQ-03 | The 5G network shall warrant measurable level of availability of its services to the relevant stakeholders. |
| SEC-REQ-04 | The 5G network shall ensure the necessary network capacity and network resources necessary for the critical operations of the 5G services. |
| SEC-REQ-05 | The 5G network shall enable a platform for vertical services to be deployed. |
| SEC-REQ-06 | The 5G network shall enable the state management of its platform components. |
| SEC-REQ-07 | The 5G network shall be able to revert to previous states with minimal service disruption of deployed application in case of malicious compromise. |
| SEC-REQ-8 | The 5G network's security mechanisms should not impact the functional requirements of critical operations for vertical applications. |
| SEC-REQ-9 | The security mechanisms of the 5G network shall be able to be deployed in any potential 5G hardware provider without any impact on their performance or functionality. |
| SEC-REQ-10 | The security mechanisms of the 5G network shall be able to measure/evaluate trust level of its components and platforms and |

**Source:** INSPIRE-5Gplus project, Deliverable D2.1 5G Security: Current Status and Future Trends
https://zenodo.org/record/4569519

# Open issues (Product ideas?) - I

## Tools for ...

- Device management (identity management, authenticaiton, authorization)
- SLA management and monitoring
  - E.g., slice isolation
  - Automated incentives and penalties
  - Difficulties to manage vertical SLA and regulation compliance
- HW based security (TEE (Trusted Execution Environment), Trusted Computing (TC) concepts)
- Remote attestation (of VMs and containers)

[Innovationstreiber 5G, 9 Nov. 2021]

# Open issues (Product ideas?) - II

## Tools for ...

- Liability contractualization and monitoring
  - Interdisciplinary nature (e.g., business and legal aspects)
  - Accountability → Root Cause Analysis (RCA)
- Certification tools and compliance verifiers
  - Regulations (dynamic and painful for service providers and operators)
- Active security and threat analysis of complex systems (inc. MEC and IoT)
- Physical protection of infrastructure
- Lightweight network and service monitoring
  - Scalability challenges
  - EU Green Deal

[Innovationstreiber 5G, 9 Nov. 2021]

# Open issues (Product ideas?) - III

## Tools for ...

- AI weaponization for good
  - ETSI ZSM paradigm for security management
  - AI based software testing
- SW security tools (e.g., against implementation issues)
  - E.g., automated and active testing/scanning of the infrastructure
- Better mathematical tools for analysis and verification
  - Publicly-verifiable proofs of compliance
- AI «securers»
  - Adversarial AI
  - Explainability

Thank you for your attention!

Da hol ich mir Inspiration!

INNOVATION KICK

Dienstag, 9. November 2021, 17.15 Uhr

INNOVATIONS-TREIBER 5G:

Technologie – Risiken – Anwendungsmöglichkeiten

TECHNOPARK®
WINTERTHUR

www.tpw.ch TECHNOPARK® Winterthur
Technoparkstrasse 2, 8406 Winterthur

***Email: gurkan.gur@zhaw.ch***

***Project: www.inspire-5gplus.eu***

***Twitter: @inspire_5gplus***

**Acknowledgment**:
The research conducted by INSPIRE-5Gplus receives funding from the European Commission H2020 programme under Grant Agreement Nº 871808. The European Commission has no responsibility for the content of this presentation.