5G and Cyber Security

How to make 5G networks more secure

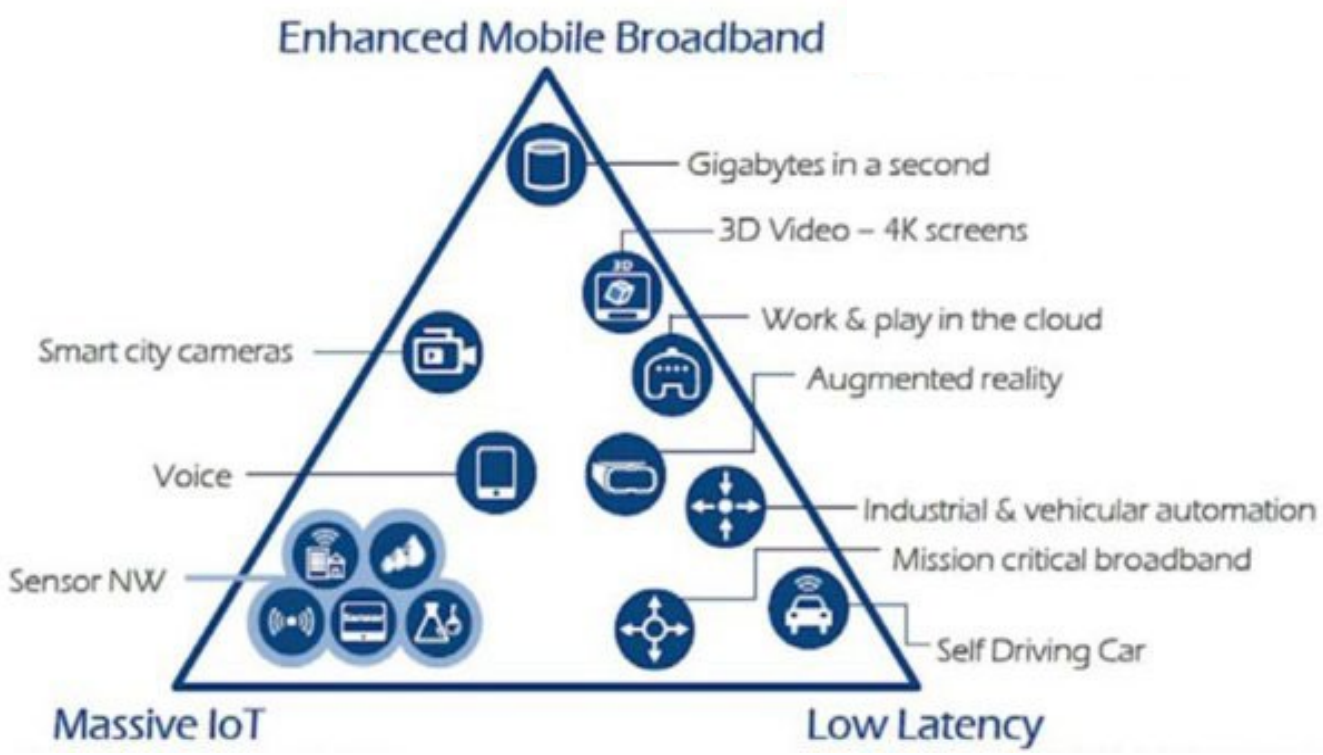
Kurt Reichinger
Austrian Regulatory Authority for Broadcasting and Telecommunications

CobCom 2020 | 07.07.2020

Agenda

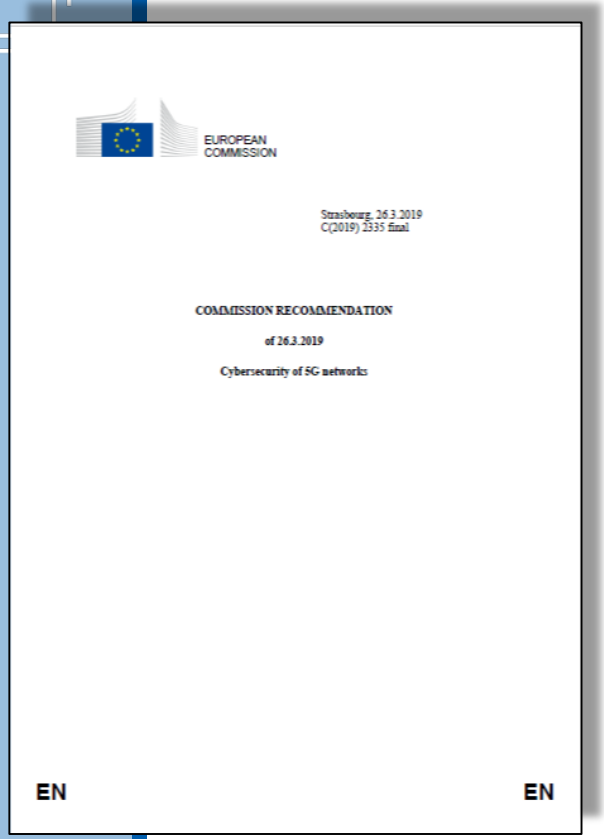
- 5G in a Nutshell
- 5G Security on European Level
- 5G Security on National Level
- Conclusions

5G in a Nutshell: Design Criteria



5G in a Nutshell: Technological Advances

- Advances in Radio Interface Technology – New Radio (NR)
  - Antennae Technologies – Massive MIMO und Beamforming
  - Using mm-Waves
- Advances in Core Network Technology
  - First „native cloud“ mobile technology
  - Software Defined Networks (SDN) and Network Function Virtualization (NFV)
  - Network as a Platform – Network Slicing


EUROPEAN COMMISSION

Strasbourg, 26.3.2019
C(2019) 2335 final

COMMISSION RECOMMENDATION

of 26.3.2019

Cybersecurity of 5G networks

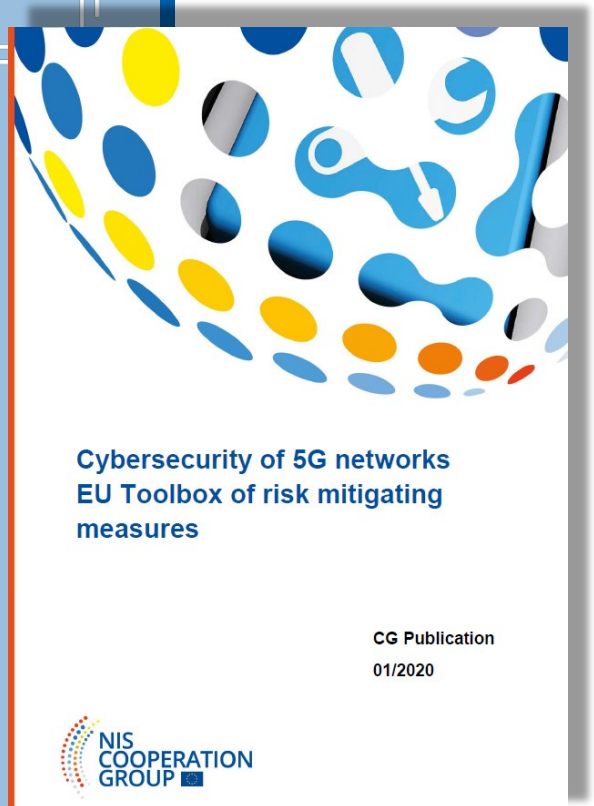
EN EN

Mar.2019: EC Recommendation on Cybersecurity of 5G-Networks

- National risk assessments by Member States focussing on security of 5G networks
- Assessment of mitigation measures already in place on national level
- Promotion of enhanced cooperation on EU level and preparation of an EU-wide coordinated risk assessment
- Development of a common toolbox for risk mitigation adressing the risks identified

Oct.2019: Report on EU Coordinated Risk Assessment

- Union-wide assessment of exposition to risks on basis of Member States‘ individual assessments
- Threat landscape by ENISA
- NIS-Cooperation Group
  - Austria: Federal Chancellery (=NIS Authority) + RTR
- Publication of Report in Oct.2020



Jan.2020: EU Toolbox

- Mitigation measures to adress the cybersecurity risks identified on national and EU level
- Preparation of Toolbox by NIS Cooperation Group
  - Austria: Federal Chancellery + RTR
- Publication: 29.01.2020

Toolbox: Strategic measures

- Strengthening the role of national authorities
- Performing audits on operators and requiring information
- Assessing the risk profile of suppliers and applying restrictions for suppliers considered to be high risk - including necessary exclusions to effectively mitigate risks for key assets
- Controlling the use of Managed Service Providers (MSPs) and equipment suppliers' third line support
- Ensuring the diversity of suppliers for individual MNOs through appropriate multi-vendor strategies
- Strengthening the resilience at national level
- Identifying key assets and fostering a diverse and sustainable 5G ecosystem in the EU
- Maintaining and building diversity and EU capacities in future network technologies

Toolbox: Technical measures

- Ensuring the application of baseline security requirements (secure network design and architecture)
- Ensuring and evaluating the implementation of security measures in existing 5G standards
- Ensuring strict access controls
- Increasing the security of virtualised network functions
- Ensuring secure 5G network management, operation and monitoring
- Reinforcing physical security
- Reinforcing software integrity, update and patch management
- Raising the security standards in suppliers' processes through robust procurement conditions
- Using EU certification for 5G network components, customer equipment and/or suppliers' processes
- Using EU certification for other non 5G-specific ICT products and services (connected devices, cloud services)
- Reinforcing resilience and continuity plans

Implementation of 5G Toolbox in Austria

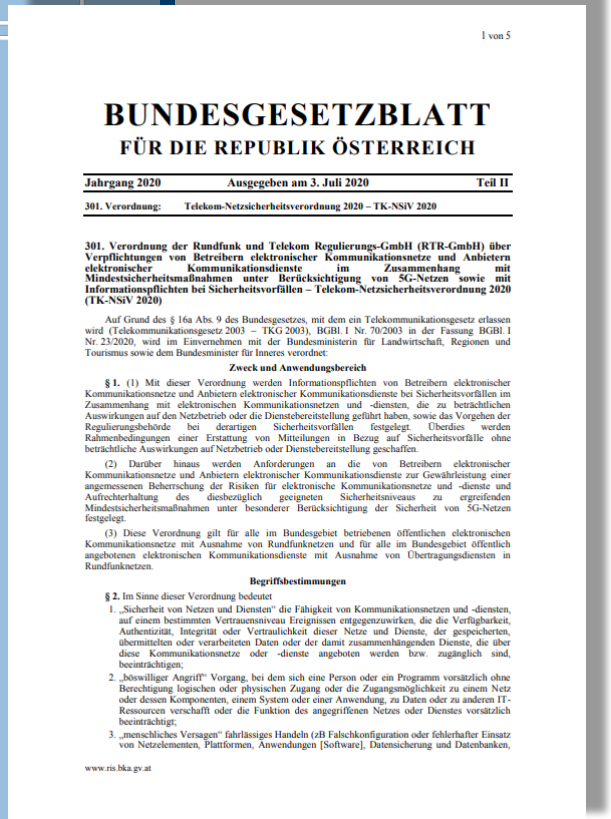
- Ordinance acc. to Art 16a (9) TKG 2003
  - With the consent of the Federal Minister of Transport, Innovation and Technology and of the Federal Minister of the Interior, and with due attention to the relevant international regulations, to the type of network or service, to the technical possibilities, to the protection of personal data and to other user interests worth protecting, the regulatory authority may issue an ordinance implementing Articles 16 and 16a and stipulate provisions on (1.) the security of network operation; (2.) the maintenance of network integrity; (3.) the interoperability of services; (4.) preventive security measures; (5.) the specification of security policies, especially identity and access administration; and (6.) procedures for operators of public communications networks or services in the case of security breaches.
- Other legal provisions necessary

Broad stakeholder involvement

- Jan. 2020 Publication of toolbox
  Preparation of ordinance proposal by RTR
- Feb. 2020 First discussion of ordinance proposal with Federal Ministries
  Discussions with operators and federations
- Mar. 2020 Discussion of ordinance proposal with operators and Federal Ministries as part of the current telecoms‘ sector risk assessment by RTR („CoT“)
- Apr. 2020 Finalising of ordinance proposal in coordination with BMLRT, BMI and BKA
  Start of public consultation
  Workshop with 5G equipment vendors

Jun. 2020 End of public consultation
Evaluation of inputs from the public consultation
Finalising of ordinance in coordination with BMLRT, BMI and BKA

Jul. 2020 Publication of ordinance



1 von 5

BUNDESGESETZBLATT

FÜR DIE REPUBLIK ÖSTERREICH

Jahrgang 2020 **Ausgegeben am 3. Juli 2020** **Teil II**

301. Verordnung: **Telekom-Netzsicherheitsverordnung 2020 – TK-NSiV 2020**

301. Verordnung der Rundfunk und Telekom Regulierungs-GmbH (RTR-GmbH) über Verpflichtungen von Betreibern elektronischer Kommunikationsnetze und Anbietern elektronischer Kommunikationsdienste im Zusammenhang mit Mindestsicherheitsmaßnahmen unter Berücksichtigung von 5G-Netzen sowie mit Informationspflichten bei Sicherheitsvorfällen – Telekom-Netzsicherheitsverordnung 2020 (TK-NSiV 2020)

Auf Grund des § 16a Abs. 9 des Bundesgesetzes, mit dem ein Telekommunikationsgesetz erlassen wird (Telekommunikationsgesetz 2003 – TKG 2003), BGBl. I Nr. 70/2003 in der Fassung BGBl. I Nr. 23/2020, wird im Einvernehmen mit der Bundesministerin für Landwirtschaft, Regionen und Tourismus sowie dem Bundesminister für Inneres verordnet:

Zweck und Anwendungsbereich

§ 1. (1) Mit dieser Verordnung werden Informationspflichten von Betreibern elektronischer Kommunikationsnetze und Anbietern elektronischer Kommunikationsdienste bei Sicherheitsvorfällen im Zusammenhang mit elektronischen Kommunikationsnetzen und -diensten, die zu beträchtlichen Auswirkungen auf den Netzbetrieb oder die Dienstebereitstellung geführt haben, sowie das Vorgehen der Regulierungsbehörde bei derartigen Sicherheitsvorfällen festgelegt. Überdies werden Rahmenbedingungen einer Erstattung von Mitteilungen in Bezug auf Sicherheitsvorfälle ohne beträchtliche Auswirkungen auf Netzbetrieb oder Dienstebereitstellung geschaffen.

(2) Darüber hinaus werden Anforderungen an die von Betreibern elektronischer Kommunikationsnetze und Anbietern elektronischer Kommunikationsdienste zur Gewährleistung einer angemessenen Beherrschung der Risiken für elektronische Kommunikationsnetze und -dienste und Aufrechterhaltung des diesbezüglich geeigneten Sicherheitsniveaus zu ergreifenden Mindestsicherheitsmaßnahmen unter besonderer Berücksichtigung der Sicherheit von 5G-Netzen festgelegt.

(3) Diese Verordnung gilt für alle im Bundesgebiet betriebenen öffentlichen elektronischen Kommunikationsnetze mit Ausnahme von Rundfunknetzen und für alle im Bundesgebiet öffentlich angebotenen elektronischen Kommunikationsdienste mit Ausnahme von Übertragungsdiensten in Rundfunknetzen.

Begriffsbestimmungen

§ 2. Im Sinne dieser Verordnung bedeutet

1. „Sicherheit von Netzen und Diensten" die Fähigkeit von Kommunikationsnetzen und -diensten, auf einem bestimmten Vertrauensniveau Ereignissen entgegenzuwirken, die die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit dieser Netze und Dienste, der gespeicherten, übermittelten oder verarbeiteten Daten oder der damit zusammenhängenden Dienste, die über diese Kommunikationsnetze oder -dienste angeboten werden bzw. zugänglich sind, beeinträchtigen;
2. „böswilliger Angriff" Vorgang, bei dem sich eine Person oder ein Programm vorsätzlich ohne Berechtigung logischen oder physischen Zugang oder die Zugangsmöglichkeit zu einem Netz oder dessen Komponenten, einem System oder einer Anwendung, zu Daten oder zu anderen IT-Ressourcen verschafft oder die Funktion des angegriffenen Netzes oder Dienstes vorsätzlich beeinträchtigt;
3. „menschliches Versagen" fahrlässiges Handeln (zB Falschkonfiguration oder fehlerhafter Einsatz von Netzelementen, Plattformen, Anwendungen [Software], Datensicherung und Datenbanken,

www.ris.bka.gv.at

Network Security Ordinance 2020

- Telekom-Netzsicherheitsverordnung 2020

- Currently, available in German only
- https://www.rtr.at/en/tk/TK_NSiV_2020

Security measures for 5G network operators

- Specific requirements for 5G operators with more than 100.000 customers
- Proof of fulfillment of information security management system according to recognized standards by means of an audit report until 31.12.2021, and regularly thereafter;
- Proof of fulfillment of 5G specific security standards (3GPP, ENISA) by means of a declaration of conformity until 30.06.2021, and regularly thereafter;
- Proof of fulfillment of additional requirements (on request by RTR)
  - NOC/SOC on premises within the EU
  - Monitoring and physical protection of critical components
  - Protection of manangement traffic
  - Access for qualified personnel only
  - Secure processes for software updates and patch manangement
  - Multi-vendor strategy
- Information on vendors of 5G components and functions with relevance for security used in the network

Toolbox Measures not addressed in Ordinance

- High Risk Supplier List
  - Currently no legal basis in Austrian Telecommunications Act
- EU-wide certification of 5G equipment
  - To be expected in 2-3 years time
  - Currently adressed with declaration of conformity
- Multi-vendor approach on national level
  - Not included due to excessive intervention intensity
- Monitoring of Foreign Direct Investment (FDI)
  - No legal basis in Austrian Telecommunications Act

Conclusions

- 5G is a major driver for further digitalisation in the EU
- Security and trust are key for the success of 5G
- Risk assessments have been performed across the EU
- Risk mitigation measures have been identified and published in toolbox
- Measures now to be implemented by EU Member States
- In Austria:
  - Successful cooperation with Federal Ministries responsible for security
  - Established PPP process involving authorities, operators, vendors, federations and the Internet community
  - Network Security Ordinance published on 03.07.2020

5G and Cyber Security

How to make 5G networks more secure

Kurt Reichinger
Austrian Regulatory Authority for Broadcasting and Telecommunications

CobCom 2020 | 07.07.2020