telemach

European Commission

Contact point Directive (EU) 2015/1535

Sent by email to: grow-dir2015-1535-central@ec.europa.eu

Notification number: 2023/0634/SI

Ljubljana, January 3, 2024

Subject: **Comments and proposals from Telemach Slovenija in relation to the draft of new "*General Act on Additional Security Requirements and Restrictions*"**

Pursuant to the Notification Message from European Commission no. 2023/0634/SI from 9 November 2023 regarding the new proposal by the Agency for Communication Networks and Services of the Republic of Slovenia ("**AKOS**") of the new legislation being prepared in Slovenia, the General Act on Additional Security Requirements and Restrictions ("**General Act**"), [stakeholder] is submitting its position and opinions on the new proposal of the General Act within the deadline as determined on European Commission's website.[1]

SUMMARY

1. All of the domestic and foreign expert sources, cited by AKOS in relation to the inclusion of RAN among the *critical elements* support, in fact, **the opposite conclusion**, i.e. that RAN does not belong among the critical elements;
2. There was no proper **risk assessment** that would need to be implemented before reaching any conclusions as to which elements can be identified as critical;
3. The proposed solution deviates from **reasonable approaches, taken in other jurisdictions** on this exact subject matter, such as in Austria, Germany, Finland, and Hungary;
4. AKOS went beyond the mandate given by ZEKom-2;

[1] https://technical-regulation-information-system.ec.europa.eu/en/notification/25093, accessed on 18. 12. 2023.

5. ***Chilling effect:*** widespread and serious economic consequences that the General Act, if adopted in its current form, would have for the national economy and society.
6. The General Act in fact represents technical barriers to trade and is also contrary to EU law.

1. Known Facts and Technical (expert) Basis

The key change that AKOS introduces in the new proposal, is that Radio Area Network ("**RAN**") is now categorized as a critical element and may be subject to the decision of the Government of the Republic of Slovenia that prohibits its use. However, it must be highlighted that AKOS did not provide any reasons for reaching such a decision. Moreover, publicly available sources and the state of the art suggest that contrary to the position of AKOS, such a definition of RAN as a critical element has no expert or technical basis.

In line with the National 5G Cybersecurity Risk Assessment in the Republic of Slovenia,[2] the EU Coordinated Risk Assessment of the Cybersecurity of 5G Networks[3] and the Cybersecurity of 5G networks - EU Toolbox of risk mitigating measures ("**EU 5G Toolbox**"),[4] prepared by the NIS Cooperation Group and the ENISA Guidelines,[5] there seems to be an unanimous consensus that **RAN (and management systems and supporting services) should be considered merely as having "HIGH" or "MODERATE"** risk profile as opposed to CORE and NFV, which are considered as "CRITICAL".

[2] The National 5G Cybersecurity Risk Assessment of the Republic of Slovenia was prepared on the basis of contributions from four telecommunications operators (Telekom Slovenije, T-2, Telemach, A1) and national authorities responsible for national security (Ministry of the Interior, Police, Ministry of Defence, Slovene Intelligence and Security Agency, Government Office of the Republic of Slovenia for the Protection of Classified Information), jointly coordinated by the Agency for Communication Networks and Services of the Republic of Slovenia.and the Ministry of Public Administration.

[3] EU Coordinated Cybersecurity Risk Assessment for 5G Networks: https://ec.europa.eu/commission/presscorner/detail/en/IP_19_6049.

[4] Toolbox: EU-200129-Cybersecurity-of-5G-networks-EU-Toolbox-of-risk-mitigating-measures P39-P40, available at: https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures.

[5] Guidelines available at: https://www.enisa.europa.eu/publications/5g-supplement-security-measures-under-eecc.

CATEGORIES OF ELEMENTS AND FUNCTIONS		EXAMPLES OF KEY ELEMENTS
Core network functions	**CRITICAL**	User Equipment Authentication, roaming and Session Management Functions
		User Equipment data transport functions
		Access policy management
		Registration and authorization of network services
		Storage of end-user and network data
		Link with third-party mobile networks
		Exposure of core network functions to external applications
		Attribution of end-user devices to network slices
NFV management and network orchestration (MANO)	**CRITICAL**	
Management systems and supporting services (other than MANO)	**MODERATE/HIGH**	Security management systems
		Billing and other support systems such as network performance
Radio Access network	**HIGH**	Base stations

Picture 1 - Source: Cybersecurity of 5G networks EU Toolbox of risk mitigating measures, page 39.

Therefore, we must reiterate that the security requirements, contained in the List of critical network elements and associated information systems, included in the General Act, are completely contradicting with the sources cited in that Act. In light of these circumstances, we also point out that the Second Progress Report on the Implementation of the EU Toolbox on 5G Cybersecurity by the European Commission,[6] which AKOS also cited as a source for its decision to define RAN as a *critical element*, does **not** refer to the RAN as a critical element, notwithstanding the comments or press statements for Commissioner Breton's which accompanied the report.

It must be pointed out that the statements, aimed at journalists, must be disregarded, since they are in **direct contradiction with the EU's own core document "EU 5G Toolbox",** whereas the Second Implementation Report confirms that RAN is, once again, highly sensitive, and not critical.

[6] Available at: https://digital-strategy.ec.europa.eu/en/library/second-report-member-states-progress-implementing-eu-toolbox-5g-cybersecurity.

Moreover, following ETSI/3GPP standards, i.e. TR 121 915 - V.15.0.0,[7] which classifies network assets with different levels of risk, only the Core Network Functions and the Management and Orchestration of the NFV Network are identified as critical. **Radio Access Network (RAN) is clearly defined as merely having "HIGH" risk profile, and not having "CRITICAL" risk profile.**

Thus, there is neither a legal nor a technical basis[8] for including the RAN among the so-called "*Critical Network Elements*". On the contrary, the entire corpus of sources shows explicitly against such inclusion.

2. Objective Methodology for Defining Criticality

Globally accepted and widely used information security standards suggest ways to implement risk assessments, define the criticality of a particular element or system, and, based on both, suggest measures and controls to manage risks. For example, the NIST Cybersecurity Framework SP 800-53 sets out the basic steps for conducting a risk assessment and the actions that follow from the risk assessment itself:

1) Risk Assessment;
2) The Risk Assessment carried out determines the criticality of each element that may be affected by vulnerability, and identifies potential vulnerabilities;
3) Putting in place measures and controls to manage the risks identified.

As mentioned above under point 2, the ETSI/3GPP standard, i.e. TR 121 915 - V.15.0.0 introduces the classification of network elements based on risk assessment. **It is therefore not possible to ascertain on what basis the proposed General Act amends this classification without carrying out a risk assessment and identifying any deviation from established methods, or from the referenced 3GPP standard.**

Prejudging criticality without having done a Risk Assessment represents an incomprehensible departure from good EU practice and ENISA and EU Commission guidelines.

With regard to an actual, objectively perceptible practice, we note that there are no reports on any RAN intrusions or vulnerabilities of which we are aware. Moreover, in the world's largest report on cyber intrusion for the years 2022 and 2023, *DBIR Verizon 2023 Data Breach*

[7] Available at: https://www.etsi.org/deliver/etsi_tr/121900_121999/121915/15.00.00_60/tr_121915v150000p.pdf.
[8] And if there would be, AKOS should disclosed it immediately.

Investigations Report | Verizon,[9] there is not even a single case of a breach of a RAN subsystem from anywhere in the world.

Therefore, the proposed characterization of RAN as critical in conjunction with the possibility of governmental ban of RAN equipment as envisioned in articles 115-117 of ZEKom-2 is disproportionate.

3. Practice in Other EU Countries

Defining RAN as critical is not common practice in the EU. For example, Austria does not introduce a definition in relation to Critical Network Components.[10] The German competent authority, including the regulatory authority for the Cyber Security Regulatory Authority (Das Bundesamt für Sicherheit in der Informationstechnik, "**BSI**") and the telecommunications regulatory authority BNetzA (Bundesnetzagentur, "**BNetzA**"), do not define critical components at their own discretion. Operators must, based on a list provided by BSI and BNetzA, determine which component is considered a *'critical component'*. The Finnish telecoms authority Traficom defines the EU 5G Toolbox as "*key network functions and measures used to control and manage network access and network traffic in a meaningful way*" (emphasis added), with a specific list that does **not** does include 5G radio access network (RAN) and network elements for interconnection of 5G networks equipment, and for secret surveillance of electronic communications network.[11] Hungary does not introduce a definition of critical network elements.

4. The Problem of Determining the Content of the Legal Transactions That Operators Will Enter Into With Suppliers

Article 3(1)(8) of the proposed General Act sets out the guidelines to be followed by the operator when concluding supply contracts, while Article 6(5) of the proposed General Act requires the operator to avoid long-term contracts with suppliers. Both provisions go beyond the statutory mandate under paragraph 6 of Article 116 of ZEKom-2, as they clearly exceed the power to lay down "*other, in particular technical, guidelines*", as the statutory mandate reads, since this is a prohibition that cannot be imposed by AKOS regulation and is thus contrary to the provisions of Article 87 of the Constitution of the Republic of Slovenia.

---

[9] Available at: https://www.verizon.com/business/resources/reports/dbir/.

[10] Relevant Austrian legislation available at: https://www.ris.bka.gv.at/Dokumente/Erv/ERV_2021_1_190/ERV_2021_1_190.pdf.

[11] https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/Regulation_on_critical_parts_of_a_communications_ network.pdf.

Additionally, EU Toolbox allows risks to be mitigated by **less invasive measures**, which means that such provisions are not necessary to achieve the legal objectives and are thus disproportionate.

5. Chilling Effect

Restrictions of competition by acts and practices of government are prohibited under Chapter 7 of Prevention of Restriction of Competition Act ("**ZPOmK-2**"). The same applies under the EU law.

It is in line with the dynamics of the market situation, that in the event of the most serious restrictions on free economic initiative, i.e. the prohibition of doing business with a particular undertaking, the mere possibility of such prohibition already creates actual economic consequences and market effects. That is because **rational economic actors in the market always try to assess and limit the risk and, on the basis of the perceived risks, to take appropriate business decisions**. In the face of uncertainty, the rational decision is therefore the one that reduces uncertainty, i.e. reduces it to a predictable.

The regulator's decision on critical elements should be predictable and based on expert criteria known in advance. Considering that AKOS has proposed to include RAN among the critical elements for the second time, while all available relevant sources show that it should have done the opposite, **it points to an unpredictable or even arbitrary decision-making process, which is thus essentially outside of the legal and professional reasoning.** This sends a signal to the market that measures need to be taken to limit the risk, even though, for example, no formal act has yet been adopted for the risk to directly translate into actuality.

We are concerned that the mere inclusion of the RAN among critical infrastructure would constitute a market distortion that could not be remedied, and the resulting damage will be catastrophic for Slovenian 5G market (and beyond) with a creation of inevitable duopoly. Due to its small size size, none of the Slovenian telecommunications operators can utilise a countervailing buying power to be able to depress the prices paid to sellers or easily switch between alternative suppliers. The remaining suppliers thus have neither the capacity nor the incentives to adequately replace the existing competitive ecosystem simultaneously in all EU countries. Slovenia can therefore expect a slow-down in the deployment of 5G networks, leading to a slow-down in the development of the ICT sector and a lag in the digitization of the society. The goals of the Second digital agenda for Europe, including gigabit connectivity, 5G and 6G, European data spaces and infrastructure are dependent on heavy investment and fast rollout of the newest technologies. For the reasons described above, the option to arbitrarily ban the supplier of the most expensive part of the network at some future unspecified date will make it impossible to achieve these goals.

telemach

6. Conclusion

From the above, we conclude that the inclusion of RAN together with the monitoring of the operation and management of the network (RAN/O-RAN) in the List of critical network elements and associated information systems, included in the General Act, is contrary to the relevant expert and technical sources and, at the same time, cannot be implemented in practice at all except with the full (extremely financial and financially and organisationally demanding) network replacement in the case of the identification of certain RAN equipment and third level support services as prohibited. Such a definition would the operator would firstly suffer direct harm, but at the same time indirect market harm that would be difficult to repair, which would be difficult to compensate not only for the operator but also for end-users, with fast and obvious reduction in consumer welfare.

To avoid this, we urge the AKOS to adjust the List of critical network elements and associated information systems by deleting the following from the table the categories:

- Radio Access Network; and

- Monitoring the operation and management of the mobile communication network, including the access part (RAN/O-RAN) in the category Management Systems and Other Supporting Systems

as shown in Annex 1.

Sincerely,

telemach
Telemach Slovenija d.o.o. 1

Tomislav Čizmić

President of the Management Board
Telemach Slovenija d.o.o.

telemach

Annex 1 - Proposed deletion of categories and functionality

Critical network elements	Functionalities of the network and information systems
Subscriber management and encryption mechanisms	- Session management (voice and data), - authentication of users and equipment with the network, - management and storage of keys for authorization of subscribers and network components (UICC/eUICC, digital certificates/HSM), - functions for secure authentication, protection of communication integrity (encryption) and storage of user keys, network and management components, - management of access rights.
Interconnection	- Hosting features and interfaces to other networks and services.
Managed network services	- Registration and authorisation of network services, - storage and processing of communication, location and traffic data, - exposure of network and network functions to external applications and services.
Management and orchestration of virtualised network functions (NFV) and network orchestration (MANO), including virtualisation infrastructure	- Management functions of orchestration and configuration of NFV regardless of the type of implementation (VM, container, micro-services), - virtualisation functions for the implementation and use of NFV, - Network Slice Selection Function (NSSF).
~~Radio access network~~	~~- Base stations that support 5G technology or higher.~~
Management systems and other support systems	~~- Monitoring the operation and management of the mobile communication network, including the access part (RAN/O-RAN).~~

	- systems for detecting security events, anomalies, threats and their management (security functions including SIEM/SOAR)
Legal interception	- Functions of access to the communication content and data on user traffic by the competent authority