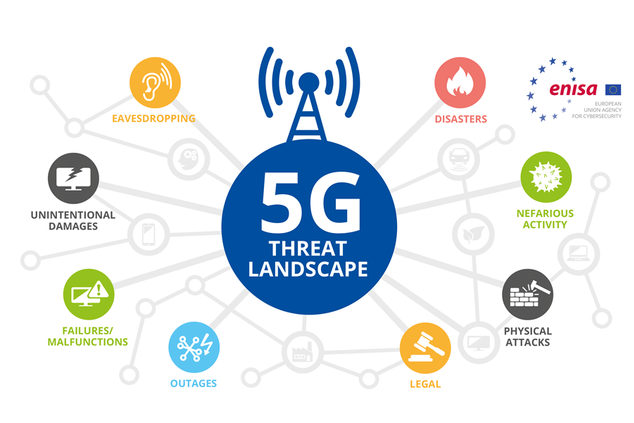
ENISA draws Threat Landscape of 5G Networks

ENISA, the European Union Agency for Cybersecurity publishes a Threat Landscape for 5G Networks, assessing the threats related to the fifth generation of mobile telecommunications networks (5G).

Published on November 21, 2019



Tagged with

* [Cybersecurity](https://www.enisa.europa.eu/search?Subject%3Alist=Cybersecurity)
* [5G Threats](https://www.enisa.europa.eu/search?Subject%3Alist=5G%20Threats)
* [5G](https://www.enisa.europa.eu/search?Subject%3Alist=5G)
* [ENISA](https://www.enisa.europa.eu/search?Subject%3Alist=ENISA)

ENISA with the support of the Member States, the European Commission and an Expert Group, published an extensive report on threats relating to 5G networks.

An EU-wide Coordinated Risk Assessment of 5G networks has been published on the 9th October 2019. It contained 10 high-level risk scenarios, based on the national risk assessments by EU Member States. Today’s  ENISA 5G Threat landscape complements the Coordinated Risk Assessment with a more technical and more detailed view on the 5G architecture, the assets and the cyber threats for those assets.

The ENISA 5G threat landscape contains:

* **A detailed architecture** outlining the most important 5G infrastructure components through 9 detailed zoom-ins of the 5G architectural elements mentioned in the coordinated risk assessment. These include the security architecture, slice architecture, edge computing architecture, software defined networks architecture, physical architecture, and others.
* **Detailed threat assessments** for the 5G infrastructure components. The assessed threats refine the threats reviewed in the coordinated risk assessment.

**Understanding threat exposure**

ENISA’s Executive Director, Juhan Lepassaar, made the following statement:

“*The arrival of 5G networks brings numerous security challenges just as the technology from 1G to 4G did previously. Today’s report will support stakeholders to carry out more detailed threat analyses and risk assessments focussed on particular elements of the 5G infrastructure to help understand* *their threat exposure*.*”*

**The on-going guide for gap analysis**

5G infrastructures possess a high degree of complexity due to the multiple features introduced by this technology. While 5G pilots are ongoing, standardisation work is also advancing as do vendor development activities towards migrations to 5G. In this still very dynamic environment, threat and risk assessments will need to be performed in an iterative manner to cover upcoming developments.

The developed 5G Risk Assessment and the 5G Threat Landscape are **initial steps** towards the longer maturity trajectory of 5G infrastructures, their deployment and adoption. They will need to be regularly updated in order to capture those changes appropriately. Certification of 5G components is perceived as a further trigger of threat and risk management activities.

**Next Steps**

The 5G toolbox, which are documents produced by the NIS Cooperation group and the Member States with the support of ENISA will be published towards the end of 2019. In this way, the toolbox will provide a number of different directions and options for the Member States to take.

Certification of 5G architecture components is a likely action depending on the exact designation of tools under the toolbox initiative carried out. The scope of 5G certification schemes needs to be determined by the European Commission with input from the Member States and duly communicated to ENISA.

ENISA will continue engaging on cybersecurity activities of 5G. Coordination with EU-wide activities will be key to the success of secure 5G practices.