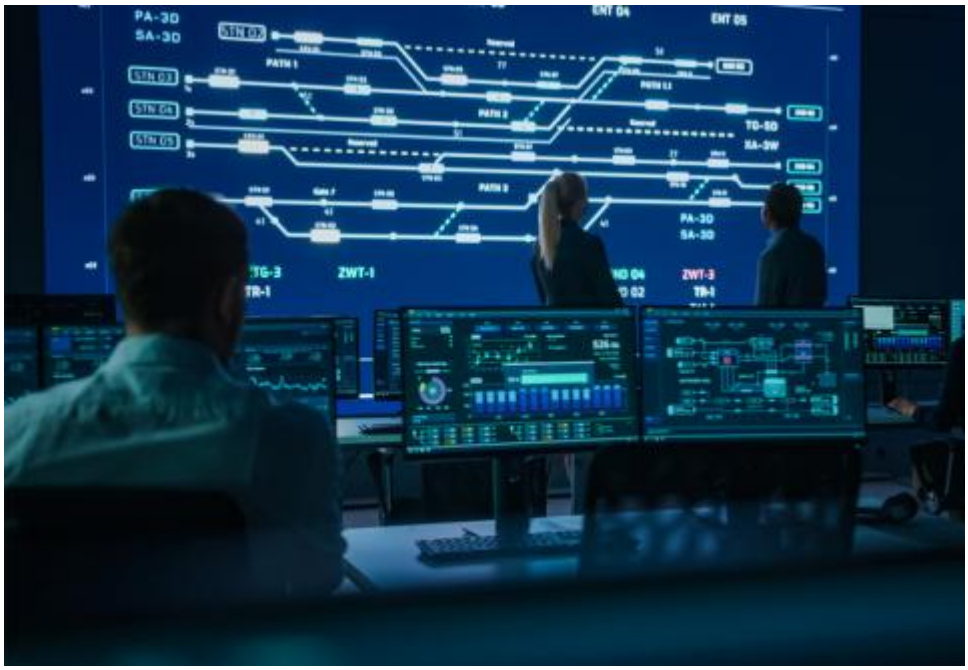
Cybersecurity of Open Radio Access Networks

This report, prepared by EU Member States with the support of the European Commission and ENISA, the EU Agency for Cybersecurity, analyses the cybersecurity implications of Open Radio Access Networks (RAN).



This new type of 5G network architecture will in the coming years provide an alternative way of deploying the radio access part of 5G networks based on open interfaces.

Background

The timely deployment of secure 5G networks is a high priority for the European Union. To contribute to this objective, EU Member States, with the support of the European Commission and ENISA, have developed a concerted approach to the cybersecurity of 5G networks. Through this concerted approach, EU Member States jointly assessed the main risks related to 5G networks ('EU Coordinated risk assessment') and defined a comprehensive and risk-based approach in the form of the EU 5G Toolbox adopted in January 2020.

As part of the next steps, the NIS Cooperation Group will continue to monitor and assess issues related to new trends and developments in the 5G supply chain. As Open RAN is a market trend in the evolution of 5G and 6G architectures, Member States have decided to conduct an in-depth analysis of the security implications of Open RAN to complement the coordinated risk analysis on 5G.

Downloads

Report on the cybersecurity of Open RAN (.pdf)
Download

Author

NIS Cooperation Group

Related topics

Cybersecurity

Related content

Cybersecurity of 5G networks: EU publishes report on the security of Open RAN

Press release | 11 May 2022

EU Member States, with the support of the European Commission and ENISA, the EU Agency for

Cybersecurity, published a report on the cybersecurity of Open Radio Access Networks (Open RAN).
