

Council Conclusions on Significance and Security Risks of 5G Technology



eu crim

European Law Forum: Prevention • Investigation • Prosecution

Thomas Wahl

News

5G networks will become part of the crucial infrastructure for the operation and maintenance of vital societal and economic functions and a wide range of services essential for functioning of the internal market. The EU must maintain technological sovereignty, however, and promote its approach to cyber security in conjunction with future electronic communication networks. This is stressed in the [conclusions “The significance of 5G to the European Economy and the need to mitigate security risks linked to 5G,”](#) as adopted by the Transport, Telecommunications and Energy Council at its meeting on 3 December 2019. The conclusions set out political guidelines on how the EU should manage the future innovative 5G technology. The Council not only points out the assets of 5G (among others, the aim to make the EU the leading market for the deployment of 5G networks and the development of 5G-based solutions), but also outlines the challenges stemming from 5G technology. Hence, safeguarding the security and resilience of electronic communications networks and services (in particular as regards 5G), following a risk-based approach, is considered important. Against this background, the Council has established the following guidelines:

- Swift and secure roll-out of the 5G networks across the EU, which is key to enhancing the EU’s competitiveness;
- Building trust in 5G technologies is firmly grounded in the core values of the EU (e.g., human rights and fundamental freedoms, rule of law, protection of privacy, personal data and intellectual property); in the commitment to transparency, reliability, and inclusion of all stakeholders and citizens; and in enhanced international cooperation;
- A comprehensive approach and effective and proportionate security measures, with a focus on security and privacy by design as integral parts of 5G infrastructure and terminal equipment;
- Addressing and mitigating the challenges for law enforcement (e.g., lawful interceptions);
- Putting in place robust common security standards and measures that must be ensured by all businesses involved;
- Mitigating not only risks of 5G by means of standardization and certification, but also by means of additional measures;

Both the Member States and the Commission (with the support of ENISA) are encouraged to work together in order to ensure the security and integrity of 5G networks.

AUTHOR

Thomas Wahl

Senior Researcher
Max Planck Institute for the
Study of Crime, Security and
Law

ISSN: 1862-6947

<https://eu crim.eu>



About eucrim

eucrim is the leading journal which regularly informs about current developments in European criminal and “criministrative” law.

All news items are freely accessible at: <https://eucrim.eu/news/>

Stay informed by emailing to eucrim-subscribe@csl.mpg.de to receive alerts for new releases of issues.

The project is co-financed by the [Union Anti-Fraud Programme \(UAFP\)](#), managed by the [European Anti-Fraud Office \(OLAF\)](#).



**Co-funded by
the European Union**