# HOW VULNERABLE ARE DIGITALISED INFRASTRUCTURES?

## IN BRIEF

- Digital connectivity has a considerable impact on entire infrastructure domains.
- Differences in the logic of data usage between services of general interest and digital added value create tensions.
- Data-driven business models enable new optimisation approaches but also lead to new challenges.
- Key problem areas are: insufficient security, growing economic and technological dependencies, and the negative effects on fundamental rights.

## WHAT IS IT ABOUT?

Vulnerability is a central issue in digitalisation.
The digital transformation does not inherently make social infrastructures more vulnerable, but increases the complexity of underlying systems and processes. Moreover, the impact of digital technologies in society is growing, increasingly affecting services of general interest, i.e. almost all public services.
Without governance and effective control measures to manage complexity, the risk of system errors and failures increases. The so-called recent CrowdStrike incident in July 2024, where numerous IT systems crashed worldwide, is a showcase for global impact due to critical system errors. The spectrum of critical incidents ranges from (cyber)attacks and software errors to serious security flaws and the abuse of technological and economic power. This exacerbates a fundamental problem of digitalisation: information and power asymmetries. Whilst unequal power relations are nothing new, they significantly increase in digitalised infrastructures. Growing dependence on globally networked technologies and the disproportionately high commercialisation of data driven by platform economy aggravate the problem. Various sectors are under intense pressure to adapt to digitalisation. This pressure, predominantly exerted by technology and platform providers, affects infrastructure services in many respects. Their extensive ability to predetermine system designs and shape digital services leads to a gradual shift in power in many areas of infrastructure, e.g. cloud software, energy networks, the end-consumer market, and the mobility sector.

Credits: iStock

Increasing the level of digital connectivity is changing infrastructures, making them more vulnerable.

This enormous market power of a few players further complicates responsible digitalisation of infrastructures. Furthermore, infrastructures originally organized as decentralised networks are gradually becoming more centralised over additional digital network layers. The strong pressure to adapt is affecting the institutional level (infrastructure and service operators) and is also being transferred to the individual level, i.e. people and households, via digitalised applications. In addition to security of supply issues, this also has significant consequences for security and privacy. Growing volumes of data, use of biometrics, and the integration of "classic" infrastructure services with data-based business models pose new threats. Despite many advantages, the digitalisation of social infrastructures raises fundamental questions that need to be renegotiated in society: How critical are economic and technological dependencies in infrastructures and public services? What are the different roles between state and private actors in the provision of services of general interest? How can resilience be strengthened, and by what means, whilst ensuring a stable security of supply?

## BASIC DATA

| | |
|---|---|
| **Project title:** | DiVuGi - Digitalization, vulnerability and (critical) societal infrastructures |
| **Project team:** | Stefan Strauß, Steffen Bettin |
| **Duration:** | 05/2022 - 11/2022 |
| **Funded by:** | Rat für digitale Ökologie (GER) |

# KEY RESULTS

Digitalised infrastructures are more intrusive than "traditional" ones, extending further into the private sphere. As a result, institutional problems, such as growing economic and technological dependencies, increasingly impact at the individual level. In addition to security risks, the integration of infrastructure services with data-driven business models also poses new challenges for the protection of fundamental rights, autonomy, and self-determination.

Bild: Bing/DallE

Digitalised infrastructures are more intrusive than "traditional" ones and have a greater impact on privacy.

The drive for more efficient health/social/care services can involve new surveillance technologies, such as remote biometric recognition, behavioral pattern analysis, and more. Whilst this has mainly been seen in authoritarian states with high levels of social surveillance, the dangers are also increasingly affecting democratic systems. Using labels such as "smart city", for example, urban infrastructures are being extensively digitalised, often alongside forms of state and private surveillance.

*Inadequate minimum security standards* are a major problem: The security of infrastructures depends heavily on the system architecture. The prevailing paradigm of networking "by default" harbours growing security risks: Insufficient or inadequate decoupling of (sub)systems increases the likelihood of errors, vulnerabilities, and attacks. The integration of digitally networked components into technical infrastructure systems changes their nature and is system-critical. Failure of such system components can jeopardise the functionality of the entire system. Without protection, the risk of failure increases and reliability decreases.

Technical capabilities for remote access or system shutdown pose new threats. The potential for abuse is enormous and could escalate into a global problem of social destabilisation. Examples are the growing dependence on satellite systems as a critical subsystem, or remote access to digitized self-driving vehicles.

# WHAT TO DO?

**The increasing complexity and security issues of digital networks have been greatly underestimated. Effective governance and control measures are required. This involves:**

- Raising more awareness on vulnerability of digitalised infrastructures, their degree of connectivity, and the specifics of their system architectures.
- Understanding the security relevance of external system components, operational interfaces, embedded technologies, and integrated third-party software is essential. This helps preventing vulnerabilities and unnecessary risks.
- Implementing higher minimum standards for data protection, privacy, and security: Technical and organisational weaknesses are major causes of disruptions and outages.
- Reducing economic and technological dependence on digital platforms and business models: Security of supply should not depend on external technologies.
- Clear rules, regulations, and boundaries for remote access to reduce the risk of essential basic functions being restricted or deactivated via remote control.
- Greater expertise and systemic knowledge of the social impacts of digitalised infrastructures and interdependencies.
- More research and interdisciplinary and transdisciplinary exchange of knowledge and experience between different infrastructure sectors.

## FURTHER READING

Strauß, S., & Bettin, S. (2023). Digitalisierung, Vulnerabilität und (kritische) gesellschaftliche Infrastrukturen. Entwicklungsstand, Trends und zentrale Herausforderungen (Endbericht) (p. 130). Wien. [in GERMAN]
*epub.oeaw.ac.at/ita/ita-projektberichte/ITA-pb-2023-01.pdf*

## CONTACT

**Stefan Strauß**
**Email:** *tamail@oeaw.ac.at*
**Phone:** +43 1 51581-6582

IMPRINT: Owner: Austrian Academy of Sciences; Legal person under public law (BGBl. 569/1921 i.d.F. BGBl. I 130/2003); Dr. Ignaz Seipel-Platz 2, A-1010 Vienna; Editor: Institute of Technology Assessment (ITA); Bäckerstraße 13, A-1010 Vienna; *www.oeaw.ac.at/ita/en*. | Frequency: The ITA Dossiers are published irregularly and publish the research results of the ITA. The ITA Dossiers are exclusively made available open access to the public via the Internet portal "epub.oeaw": *epub.oeaw.ac.at/ita/ita-dossiers* | ISSN: 2306-1960 | This work is licensed under a Creative Commons Attribution 4.0 International License: *creativecommons.org/licenses/by/4.0/* | ITA Dossier no. 78en January 2025 | *epub.oeaw.ac.at/ita/ita-dossiers/ita-dossier078en.pdf*