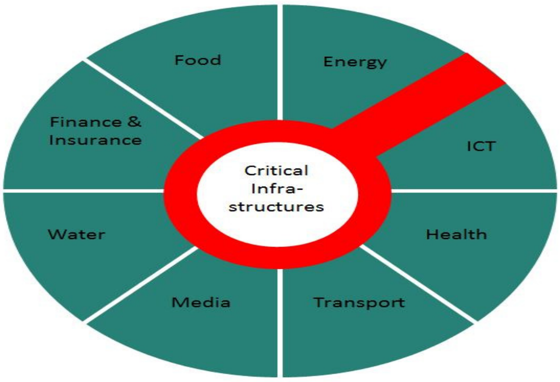
How vulnerable are critical infrastructures?

In brief

- Today, social and economic processes are highly dependent on different technologies and their interaction.
- Critical infrastructures are therefore the "main artery" of the digitally networked society and their functionality is essential for the provision of services of general interest.
- System failures due to external risk factors, errors inherent to the system or unknown weak points can seriously impair the stability of societal processes.
- The creation of effective security measures requires above all a greater awareness of the previously underestimated problem of system dependencies.

What is it about?

Critical infrastructures (CI) are a complex, wide-ranging field. The term covers all infrastructures (systems, facilities, processes or networks etc.) that are essential to the functioning of societal processes. CI can be divided into sectors ranging from food and energy, transport, telecommunications, media, finance and insurance to social and health care. Accordingly, negative impact on or a breakdown of one or more infrastructure components in these essential areas can cause serious harm to the agency and effectiveness of the economy, the government, and social welfare. CI systems enable various functions and services which in turn influence the extent of vulnerability. Austria is therefore deliberately opting for a function-oriented approach instead of a sectoral separation of CI areas (as, e.g., in Germany). In addition to areas of public services of general interest, strategically important companies and institutions are therefore also considered relevant functionaries. From a systemic perspective, two central (interrelated) cross-sectional technologies can be identified, on which practically all other CI areas depend: energy supply (in particular the electricity grid) and IT systems. Energy and information are all-encompassing, centralised commodities; for the state, public health care institutions, industry and companies as well as for private households.



Sectors of critical infrastructures

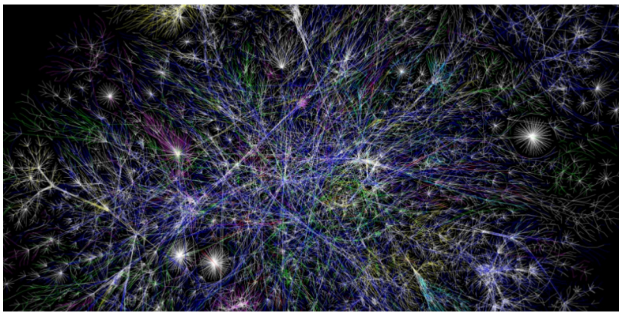
Ultimately, the increasing dependence on critical infrastructures has a negative effect on the capacity to self-organisation of all social actors (state and private institutions, companies and civil society). However, this capacity is essential for crisis management. Consequently, reducing such dependency goes hand in hand with increasing awareness of the problem to strengthen society's resilience. The diversity of potential risks can make the protection of critical infrastructures very difficult. The spectrum generally ranges from natural disasters, technical accidents, human error to crime and terrorism as well as dangers in cyberspace (cyberattacks). Special risks are so-called electromagnetic impulses (EMPs) which can significantly disrupt or even destroy technical systems. EMPs are relatively complex to generate, which is usually the prerogative of military actors who have access to special weapon systems. However, EMPs can also be found in nature: in the form of rather harmless lightning strikes, but they can also be observed in space weather phenomena in the form of solar and magnetic storms. Although these EMPs have a rather low probability of occurrence, they are relatively unpredictable and therefore not to be underestimated. EMPs can cause severe chain reactions (cascade effects) and thus serious damage.

Basic data

Project title:	Digital breakdown
Project team:	Strauß, S., Krieger-Lamina, J., Walter, P.
Duration:	01/2015 – 04/2017
Funded by:	Austrian Academy of Sciences

Hyperconnectivity and increase in system dependencies

Irrespective of the various risks, the core problem is society's increasing dependence on technical systems – especially on energy and information systems – and this tendency is on the rise (mainly because of extensive digitisation). Because of their high degree of complexity and networking, IT systems are an Achilles' heel of critical infrastructures. With more networking and dependencies, risks of cascading effects also increases: if a critical component fails, major system failures in other CI areas are likely to follow.



Complexity and system dependencies increase with networking

Despite numerous "cyber risks" (e. g. cyberattacks such as "WannaCry", botnets such as "Mirai" from everyday devices, or serious security breaches such as "Spectre" etc.), one aspect should not be overlooked: these risks are a symptom of increased vulnerability – as a serious side-effect of increasing networking and technical dependencies. However, malfunctions can still be of analogue as well as of digital nature. Increasing complexity and a lack of knowledge on the interplay of system components are enormous risk factors. Thus the most common cause for failures of any type is increasing interdependency paired with inadequate security concepts. Drastic examples are power plants and even nuclear power stations being accessible directly via the Internet. But also seemingly harmless components carry risks as demonstrated by, e. g., the hack of a digital car radio: lack of safety concepts allowed taking over control of the vehicle. Vulnerabilities in system design are therefore a key security risk. Underestimated dependencies can be particularly problematic: high complexity can lead to unintentional neglect of critical system components. An example is the often implicit dependence of IT systems on satellite systems. They are not only used for navigation, but (amongst other things) also for clock/time synchronisation in IT systems (e. g. in the power grid or in financial accounting). Failures of such components can endanger the stability of a system as a whole. Essentially, the security of critical infrastructures depends on system interfaces which therefore require special protection.

What to do?

Up until now, the problem of system dependencies has been underestimated. Greater awareness is required to increase the effectiveness of security measures and thus the overall level of protection. Key issues are:

- Interfaces connect various system elements (e. g. control components with Internet or mobile phone connection). They should therefore be understood as crucial points and protected accordingly. Unsafe, impaired or faulty interfaces can destabilise critical infrastructures.
- Critical infrastructures should be systematically analysed for weaknesses in order to identify and secure central system dependencies (including hidden ones).
- The redundancy and substitutability of central components and functions of critical infrastructures should be increased in order to reduce the risk of cascade effects.
- Emergency care and stable communication systems resistant to crisis should be provided to maintain the capacity to communicate and act in the event of a disaster; the role of computer emergency response teams (CERTs) as a focal point for crisis management should be strengthened.
- Standards and guidelines for crisis and disaster management as well as electromagnetic compatibility should be evaluated and adapted where necessary.
- More research is needed on the impact of networking and system dependencies as well as on security-by-design to effectively protect critical infrastructures.

Further reading

Strauß, S., Krieger-Lamina, J. (2017): Digitaler Stillstand: Die Verletzlichkeit der digital vernetzten Gesellschaft – Kritische Infrastrukturen und Systemperspektiven. Bericht Nr. ITA 2017-01, Wien: ITA
epub.oeaw.ac.at/ita/ita-projektberichte/2017-01.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); Strohgasse 45/5, A-1030 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 published in print in small numbers only and are 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. 33en, March 2018 | epub.oeaw.ac.at/ita/ita-dossiers/ita-dossier033en.pdf |
Co-authors: Krieger-Lamina, Jaro; Peissl, Walter