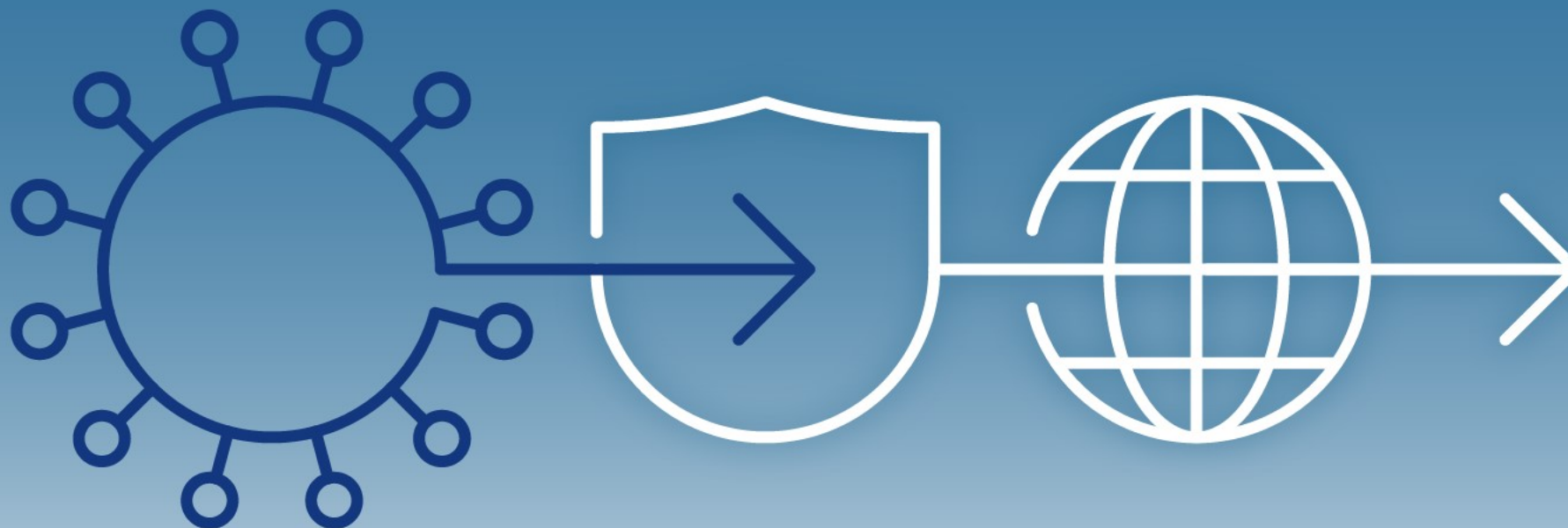


Konferencja Naukowa Bezpieczeństwo w Internecie – Cyberpandemia

22-23 października 2020 r.



 Sektorowa Rada
ds. Kompetencji
Telekomunikacja
i Cyberbezpieczeństwo


UNIwersYTET KARDYNAŁA
STEFANA WYSZYŃSKIEGO
W WARSZAWIE


POLSKIE TOWARZYSTWO INFORMATYCZNE


Naukowe Centrum
Prawno-informatyczne

Overcoming cyber-threats in Germany

Cyber Security Strategy for Germany

Mateusz Badowski

European Legal Studies Institute
Faculty of Law
University of Osnabrück

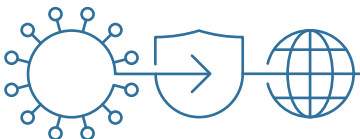
Department of Informatics Law
Faculty of Law and Administration
Cardinal Stefan Wyszyński University





Agenda

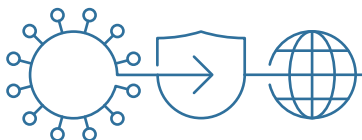
- Introduction
- The Cyber Security Council
- Cyber Security Strategy for Germany
 - Framework conditions
 - Basic principles of the Cyber Security Strategy
 - Strategic objectives and measures
- The IT Security Act and implementation of the NIS-Directive
- Amendment of the Cyber Security Strategy for Germany





Cyberspace

Cyberspace is the virtual space of all IT systems linked at data level on a global scale. The basis for cyberspace is the Internet as a universal and publicly accessible connection and transport network which can be complemented and further expanded by any number of additional data networks. IT systems in an isolated virtual space are not part of cyberspace.



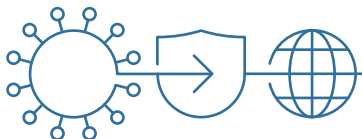


Critical infrastructures

Critical infrastructures are organizations or institutions with major importance for the public good, whose failure or damage would lead to sustainable supply bottlenecks, considerable disturbance of public security or other dramatic consequences.

At federal level, the following areas have been identified:

- Energy
- Information technology and telecommunication
- Transport
- Health
- Water
- Food
- Finance and insurance sector
- State and administration
- Media and culture

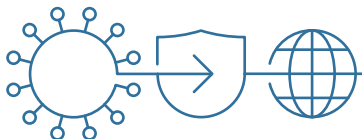




National Cyber Security Council

The members of the National Cyber Security Council are representatives of:

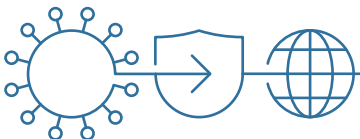
- Federal Chancellery
- Ministry of Foreign Affairs
- Federal Ministry of the Interior
- Federal Ministry of Defense
- Federal Ministry for Economics and Technology
- Federal Ministry of Justice and Consumer Protection
- Federal Ministry of Finance
- Federal Ministry of Education and Research
- Representatives of the federal states





Cyber Security Strategy for Germany

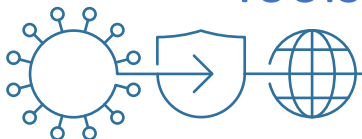
- Framework conditions
- Basic principles of the Cyber Security Strategy
- Strategic objectives and measures





Strategic objectives and measures

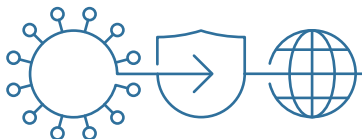
- Protection of critical information infrastructures
- Secure IT systems in Germany
- Strengthening IT security in the public administration
- National Cyber Response Centre
- National Cyber Security Council
- Effective crime control also in cyberspace
- Effective coordinated action to ensure cyber security in Europe and worldwide
- Use of reliable and trustworthy information technology
- Personnel development in federal authorities
- Tools to respond to cyber attacks





Legal Acts

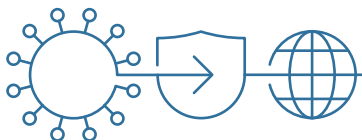
- Law to Increase the Security of Information Technology Systems (IT Security Law) of July 17, 2015
- Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union





Amendment of the Cyber Security Strategy for Germany

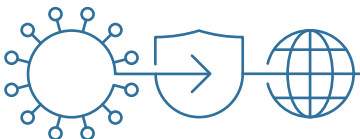
- Which main topics and goals of the current strategy have proven themselves?
- Which appointments, structures and measures have a positive effect on the achievement of goals?
- Which key issues and goals of the strategy from 2016 are seen as achieved or outdated and therefore require less attention in the future?
- Which focus topics and goals have been added since the update of the cybersecurity strategy from 2016 and therefore need to be mentioned?
- Which agreements, structures and measures can the state, society and business establish and agree on in order to achieve the necessary goals?





Proposals for amendment of Cyber Security Strategy for Germany

- More usability of IT security solutions- inclusion of „Security by Design”
- Improvement of company protection through faster communication and optimized crisis management
- Greater involvement of companies and institutions that are not critical infrastructures



Overcoming a cyber-threats in Germany

Cyber Security Strategy for Germany

Mateusz Badowski

mateusz.badowski@uni-osnabrueck.de



Sektorowa Rada
ds. Kompetencji
Telekomunikacja
i Cyberbezpieczeństwo



UNIwersytet Kardynała
STEFANA WYSZYŃSKIEGO
W WARSZAWIE



POLSKIE TOWARZYSTWO INFORMATYCZNE



Naukowe Centrum
Prawno-informatyczne