International Legal Regulation of Cybersecurity

U.S.-German Standards Panel 2018

Dr. Dennis-Kenji Kipker
University of Bremen
Washington DC, 10.04.2018

Gefördert vom
FKZ: 16KIS0213
bis 16KIS0216
Bundesministerium für Bildung und Forschung

der Bundeswehr Universität München
FRIEDRICH-ALEXANDER UNIVERSITÄT ERLANGEN-NÜRNBERG
DKE VDE DIN
Universität Bremen

Germany and European Union

German IT Security Act (2015)

EU Network and Information Security Directive (2016)

Outlook: EU Cybersecurity Act (2018)

- The German IT-Security Act (**IT-SiG**, 2015):
  - **Amending act** („Artikelgesetz“), no codification
  - Amended **various existing laws**, including:
    - Act on the Federal Office for Information Security (BSIG)
    - Atomic Energy Act (AtG)
    - Energy Industry Act (EnWG)
    - Telemedia Act (TMG)
    - Telecommunications Act (TKG)
    - Act on the Federal Criminal Police Office (BKAG)
  - IT-SiG entered into force on **25 July, 2015**
  - Mainly, but not exclusively referring to **Critical Infrastructures**
    - Energy, information technology, telecommunication, transport, traffic, health, water, food, finance and insurance **+** relevance of failure consequences
    - E.g. includes a general extension of power of the BSI according to Sec. 7 BSIG (warnings), Sec. 7a BSIG (examination of IT security)

EU Network and Information Security Directive (2016)

- IT-security regulation on the European level:
  - No codification: numerous **individual regulations**, **different legally binding nature**
  - Depending on the respective **business or infrastructure sector**
  - **Example:** Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (**eIDAS**)
- The European Network and Information Security Directive (**NIS Directive**, 2016):
  - NIS as key factor for a **functioning community and economy** of the EU
  - **Long term legislative procedure:** 2/2013 (first proposal by EC) – 8/2016 (entry into force)
  - Key element of the **EU Cybersecurity Strategy**
  - **Art. 288 TFEU:** Directive ≠ Regulation
  - National implementing act needed, Germany: **Slightly amended regulations of the IT-SiG**
  - Minimum harmonisation
  - **NIS Directive designed as „global approach** […] covering common minimum capacity building and planning requirements, exchange of information, cooperation and common security requirements for operators of essential services and digital service providers"

Dr. Dennis-Kenji Kipker
IGMR
University of Bremen

INFORMATION FLOWS AND PROTECTION PROCESSES IN THE IT SECURITY OF CRITICAL INFRASTRUCTURES AND DIGITAL SERVICE PROVIDERS

ITS KRITIS
GEFÖRDERT VOM Bundesministerium für Bildung und Forschung

Threats to availability, integrity, authenticity and confidentiality of IT systems

Countermeasures

OPERATORS
Applicability according to Sec. 2 para. 10, 11, Sec. 10 para. 1 BSIG

Sec. 8a, 8c BSIG – Technical and organisational measures (TOM) for IT security of KRITIS and digital service providers

- ▶ Technical protection of the IT systems that are essential for the functioning of KRITIS and digital service providers
- ▶ Measures correspond to „state of the art“
  - ISMS (ISO 27001; BSI IT baseline protection)
  - B3S (UP KRITIS)
- ▶ Cost-benefit calculation as an adequacy assessment
- ▶ Providing evidence of TOM by means of audits, controls, certifications

Evaluation

PDCA
plan – do – check - act

BCM

Contact point BSI

COOPERATION

Contact point Operators

BSI

ENISA
Cooperation/ European information exchange according to EU NIS Directive

Sec. 8b, 8c BSIG – Notification requirements and central reporting point for IT security

Operators and providers issue urgent reports to the BSI:

- ▶ Significant disruptions of the IT that led OR might lead to failure/ disruption of the functioning of KRITIS and digital service providers
- ▶ Information about the disruption, technical conditions, the assumed/actual cause, the type of the institution/ installation concerned and about the operator's sector
- ▶ KRITIS: Pseudonymised notification principally sufficient, identification of the operator necessary only in exceptional cases

BSI as central reporting point for IT security:

- ▶ Collecting and evaluating information from the operators and digital service providers (partly in collaboration with the BBK)
- ▶ Warning and alarm messages
- ▶ Updating situation report about information security
- ▶ Information for operators, providers and supervisory authorities
- ▶ Long-term annual reports for the public

CYBERSECURITY STRATEGY OF THE GERMAN FEDERAL GOVERNMENT (2011 + 2016)

(BSIG amended with specific regulations such as Sec. 109 TKG, Sec. 11 EnWG, Sec. 44b AtG; Opening clause in Sec. 8d para. 2 no. 5, para. 3 no. 5 BSIG, e. g. for health telematics)

- Outlook: New EU Cybersecurity Act (announced for 2018):
  - Part of the newly announced **EU Cybersecurity Strategy**, September 2017
  - Protecting not only Critical Infrastructues + Digital Service Providers, but also the **digital interior market** in general
  - Comprehensive reorganisation of **ENISA**
  - Stronger exchange of information among IT-security authorities of the member states
  - **New European IT-security certification**: Making certification easier, cheaper, and transnational due to EU wide recognition of Member State certification
  - **Legislative procedure**: LIBE (European Parliament Committee on Civil Liberties, Justice and Home Affairs) and IMCO (Committee on the Internal Market and Consumer Protection) (draft) reports issued, picking up on the **CEN-CENELEC** position paper and the role of standards in the future cybersecurity certification framework, referencing to international and EU standards
  - **September 2018**: EP plenary voting

Russia

Russian Cybersecurity Doctrine (2000, 2016)

New Russian Cybersecurity Law (2018)

- Russian Cybersecurity Doctrine (2000, 2016):
  - **1st Cybersecurity Doctrine in 2000**: Did not even mention the Internet
  - **2nd Cybersecurity Doctrine in 2016**:
    - **Goal**: Protection of the national interests of the Russian Federation in cyberspace
    - Generally not focused on economic, but mostly on **political and military interests**
    - Closely linked to the **National Security Strategy** of the Russian Federation
    - Effective cybersecurity also includes: Strengthening of the **military**, safeguarding digital **weapon systems**, protection of the national interests of Russian **allies**

New Russian Cybersecurity Law (2018):

- Federal Law on Security of Critical Russian Information Infrastructure (entry into force: **01/01/2018**)
- Foundation of a **nationwide IT-security system** with the aims of detection, prevention and elimination of cybersecurity risks
- Duties **comparable to German IT-SiG** and to **EU NIS Directive**
  - Technical and organisational measures
  - Duties to report to competent Russian authorities
  - Register of important IT-infrastructure objects
- Definition of **Critical Information Infrastructure**: Public institutions, legal entities, and companies in different sectors: health, science, transport, communication, energy, finance, defense, mining, chemical industry → **broader than IT-SiG**

China

Cybersecurity Law (2016)

Measures on Security Review of Network Products and Services (2017)

- Chinese Cybersecurity Law (2016):
  - **Double focus**: Network security and data protection
    - Difference to German and EU law: IT-security and data protection are separated (e.g. EU NIS Directive/EU GDPR), China: **holistic approach** to IT-regulation
  - **Network security**: Chinese networks should be in a stable and reliable state of work, measures should be taken against intrusions, destruction or the unlawful use of network resources
    - TOM, risk assessment, real name registration, information exchange, certification, education, best practices, IT-security representatives, emergency response plans, severe penalties
  - **Data protection**: Protection of personal information, which allows identification of individuals
    - Confidentiality, earmarking principle, informed consent for data use, regulation of privacy breaches, rights of persons concerned → **Chinese data protection level below GDPR** → BCR possibly apply

Measures on Security Review of Network Products (2017)

- Measures on Security Review of Network Products + Services (2017):
  - **Basis:** Artt. 24, 25 of the Chinese National Security Law; Artt. 23, 35 of the Chinese Cybersecurity Law
  - **Goal:** Improvement of security and controllability of IT-network products and services
  - **Measure:** "Cybersecurity Review" for key products, which affect national security and public interest
  - **Responsibility**: Cyberspace Administration of China (CAC), Cybersecurity Review Committee, Cybersecurity Review Expert Committee, third parties/companies
  - **Process**: Intense collaboration between companies and authorities, laboratory tests, site inspections, online-surveillance, background supervision
  - **Importance**: Certified products will be given priority in Chinese market; products which failed will not be used in China

United States

Cybersecurity National Security Action Plan (2016)

Cybersecurity Information Sharing Act (2015)

…

- IT-security regulation in the U.S.:
  - **Cybersecurity National Security Action Plan** (CNAP, 2016): Measure and strategies for protection against cyberattacks
  - Variety of sector specific regulations concerning IT-security on **national level** as well as in the **federal states**
  - **Self regulation** of the private sector is also promoted by the authorities
  - Examples of sector specific laws on national level:
    - **Health Insurance Portability and Accountability Act** (HIPAA, 1996): Data security of electronically stored medical data
    - **Financial Services Modernization Act** (Gramm-Leach-Bliley Act, 1999): Data security of financial institutions
    - **Federal Information Security Management Act** (FISMA, 2002): Secure data processing of Federal Authorities
    - **Cybersecurity Information Sharing Act** (CISA, 2015): Information exchange about data security between government and companies
  - Insufficient IT-security measures of companies may by sanctioned by the **Federal Trade Commission** (FTC)

International Legal Regulation of Cybersecurity

Conclusion + Outlook

Conclusion + Outlook:

- Many different approaches for cybersecurity on international level during the recent years: “**hot topic**”
- **Germany and Europe**: Addressing cybersecurity issues as **uniform approach** on “from the scratch”
- Current technical challenges force national states to promote cybersecurity regulation, e.g. **Japan** with a new legislative approach especially for **IoT-devices**
- Cybersecurity not only as legal, but also as a **task for international standardization**:
  - Technical concretization of legal cybersecurity requirements
  - Support to a consistent interpretation of (newly announced) legal provisions
  - Means to conduct a transnational cybersecurity certification

Dr. Dennis-Kenji Kipker
Scientific Managing Director
University of Bremen
Universitätsallee GW1
28359 Bremen
Tel.: +49 421 218 66049
Mail: kipker@uni-bremen.de

Visit our website: www.itskritis.de
Follow us on Twitter: @itskritis

der Bundeswehr Universität München
FAU FRIEDRICH-ALEXANDER UNIVERSITÄT ERLANGEN-NÜRNBERG
DKE VDE DIN
Universität Bremen