CERTAVO

# Welcome!

**Dr. Dennis-Kenji Kipker**

Executive Director

Certavo GmbH – international compliance management

dennis.kipker@certavo.de

+49 421 218 66049

# International Regulation of Cybersecurity: New Paths and New Problems

I. Technical and political background of Cybersecurity Regulation

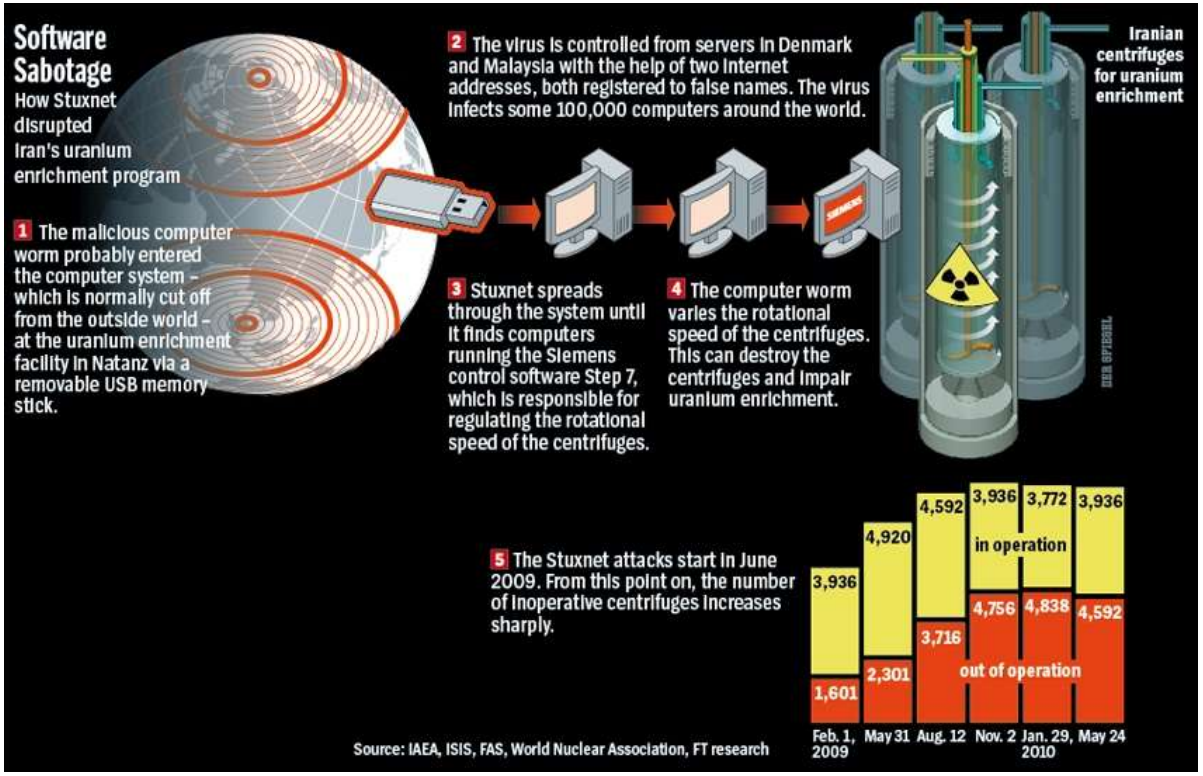
II. Cybersecurity as an interdisciplinary challenge

III. Chinese Cybersecurity Law: Comparative Approaches

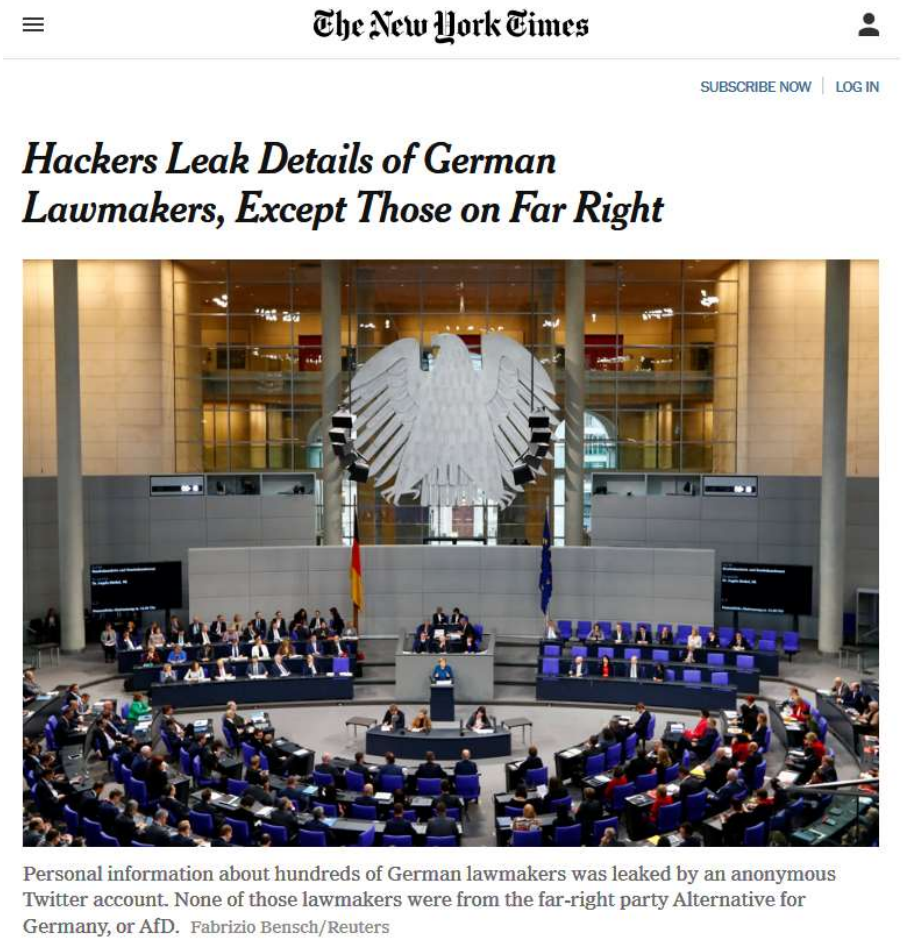
IV. Conclusion and Outlook

# Technical and political background of Cybersecurity Regulation

# Stuxnet (2010)



# January 2019: Cyberattack on Members of the German Parliament

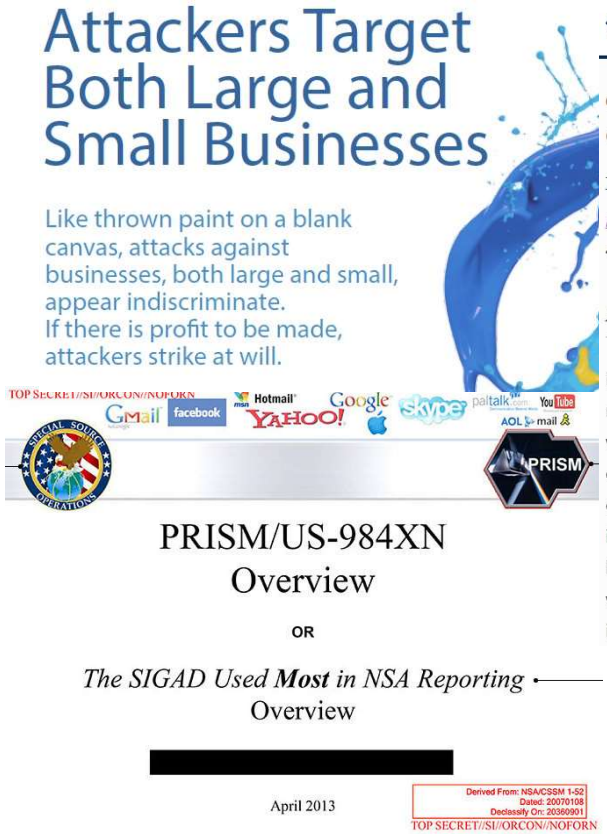
# September 2020: Cyberattack on hospitals in Germany

The New York Times

## *Cyber Attack Suspected in German Woman's Death*

Prosecutors believe the woman died from delayed treatment after hackers attacked a hospital's computers. It could be the first fatality from a ransomware attack.

# Multilateral threat situation






Source: Symantec Internet Security Threat Report 2016/2017

# Risk analysis as a basic requirement of adequate IT Security Compliance


- The regular and systematic carrying out of risk analysis measures is an essential precondition to realize an adequate and effective IT Security Compliance:
  - **Business Continuity Management (BCM)**
  - **Information Security Management System (ISMS)**
  - **Plan-Do-Check-Act Circle (PDCA)**
- Necessity to identify protection goals (assets)

Do we need a reactive or a preventive legal regulation of IT security?

What could be the primary legal source for IT security regulation? Civil, punitive or public law?

# “Germany's Merkel warns against cyber attacks on infrastructure”

BERLIN (Reuters) - German Chancellor Angela Merkel said on Tuesday protecting infrastructure from potential cyber attacks was a top priority and the federal government had to work together with localities on that.

“Today we have a huge amount of possibilities to paralyze infrastructure from cyber attacks and it is...very very difficult.”

“The German government has **updated its cyber security strategy** and we are very happy to work with localities on this,” she said in a speech to the association for local infrastructure companies.

Source: Reuters, 14 March 2017, https://www.reuters.com/article/us-germany-merkel/germanys-merkel-warns-against-cyber-attacks-on-infrastructure-idUSKBN16L19H

# German Cybersecurity Strategy (2016)

- **Protection of critical information infrastructures:** Defined as the main priority of cyber security because of their increasing importance  for all economic areas, focused onto public private partnerships.
- **Secure IT systems in Germany:** Focus on overall security especially for citizens and small and medium-sized businesses. Users need appropriate and consistent information on risks related to the use of IT-systems and on security measures they can take to use cyberspace in a secure manner.
- **Strengthening IT security in the public administration:** State authorities have to serve as role model for data security. Creation of a common, uniform and secure network infrastructure in the federal administration.
- **National Cyber Response Centre:** To optimize operational cooperation between all state authorities and improve co-ordination of protection and response measures for IT incidents, a National Cyber Response Centre will be set up.

# German Cybersecurity Strategy (2016)

- **Effective crime control in cyberspace:** Strengthening the capabilities of law enforcement agencies, the Federal Office for Information Security in combating cyber crime, also with regard to protection against espionage and sabotage.
- **Effective co-ordinated action to ensure cyber security in Europe and worldwide:** Support of the EU action plan for the protection of critical information infrastructures, and the extension of the ENISA. Cooperation with UN, OSCE, Council of Europe, OECD, NATO.
- **Use of reliable and trustworthy information technology:** Intensifying the research on IT security and critical infrastructure protection.
- **Tools to respond to cyber attacks:** If the state wants to be fully prepared for cyber attacks, a co-ordinated and comprehensive set of tools to respond to cyber attacks must be created in cooperation with the competent state authorities.

# The European Cybersecurity Strategy

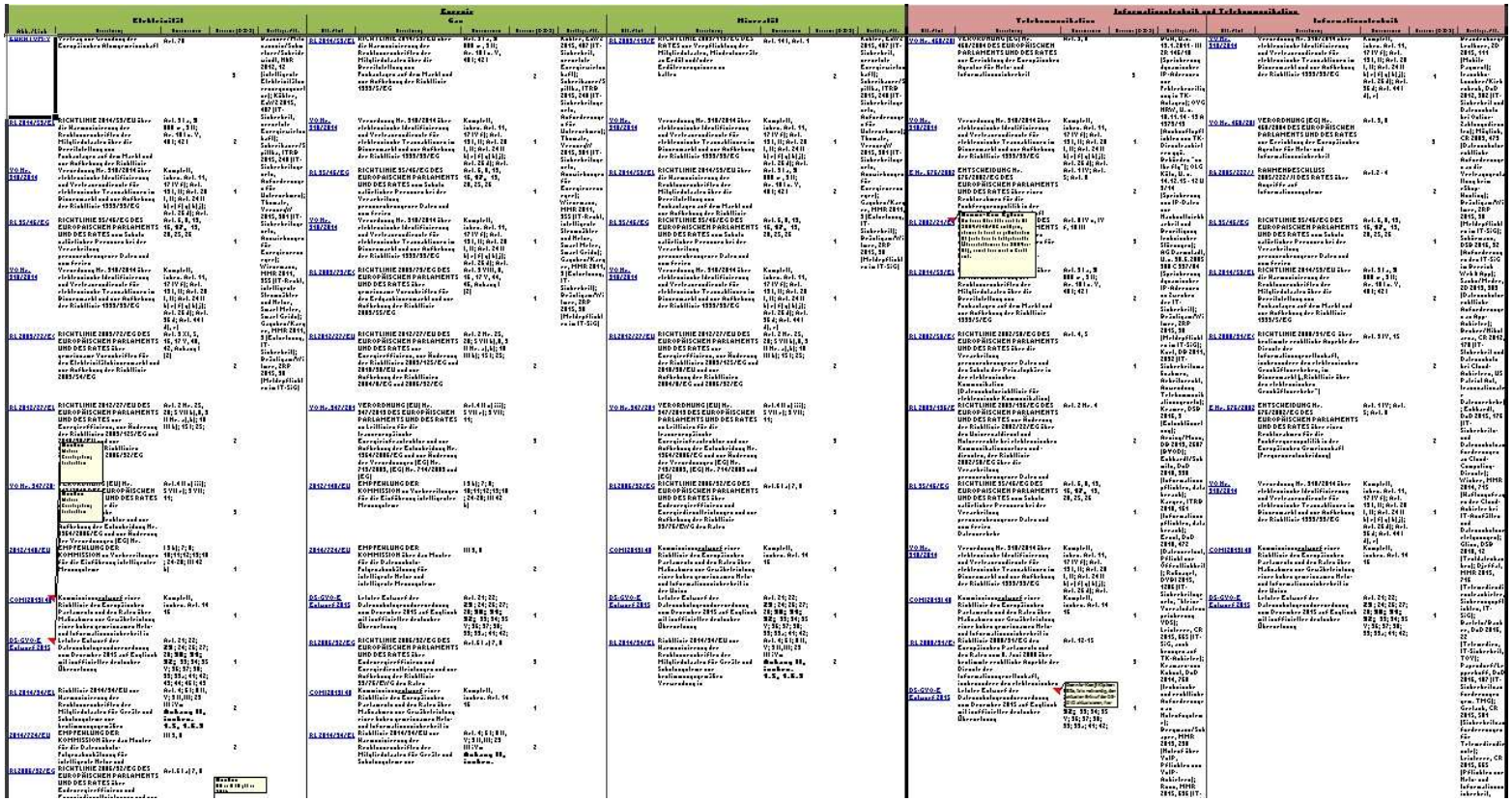
**13. September 2017, State of the Union Address, former President Jean-Claude Juncker:**

"*In the past three years, we have made progress in keeping Europeans safe online. But Europe is still not well equipped when it comes to cyber-attacks. This is why, today, the Commission is proposing new tools, including a European Cybersecurity Agency, to help defend us against such attacks.“*

Europeans place great trust in digital technologies. They open up new opportunities for citizens to connect, facilitate the dissemination of information and form the backbone of Europe's economy. However, they have also brought about new risks as non-state and state actors increasingly try to steal data, commit fraud or even destabilise governments. Last year, there were more than 4,000 ransomware attacks per day and 80% of European companies experienced at least one cybersecurity incident. The economic impact of cyber-crime has risen five-fold over the past four years alone.

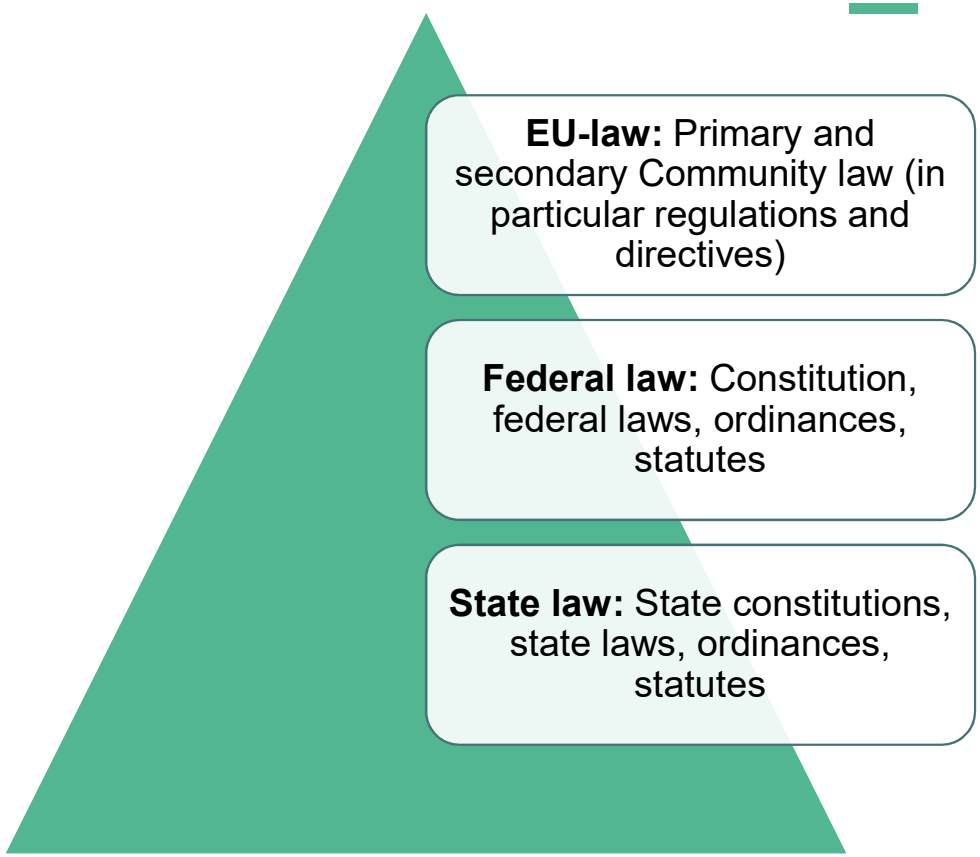
To equip Europe with the right tools to deal with cyber-attacks, the European Commission and the High Representative are proposing a wide-ranging set of measures to build strong cybersecurity in the EU. This includes a proposal for an **EU Cybersecurity Agency** to assist Member States in dealing with cyber-attacks, as well as a new **European certification scheme** that will ensure that products and services in the digital world are safe to use.

# An overwhelming variety of data security laws



Source: D. Kipker IGMR/IT Security Standards Collection (2020)

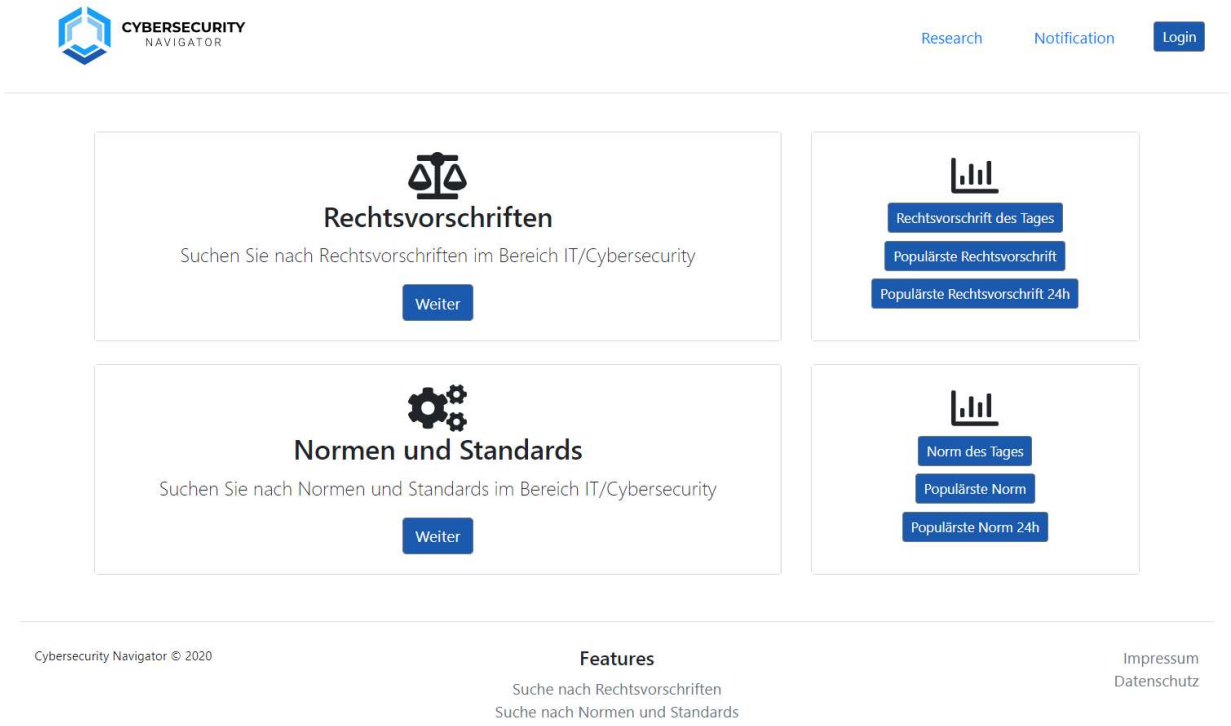
# Current EU and German legal framework on cybersecurity: Overall view




- **EU Network and Information Security Directive** (NIS, 2016)
- **EU General Data Protection Regulation** (GDPR, 2016, 2018, also requirements for data security inter alia according to Art. 32, as far as personal data is concerned)
- **EU Cybersecurity Regulation** (Cybersecurity Act, CSA, 2019)
- **EU Regulation for a Centre of Excellence on Cybersecurity** (2018, draft)

- **IT-Security Law** (IT-SiG, 2015)
  - BSI-Kritisverordnung (BSI-KritisV, 2016, 2017)
- **IT-Security Law 2.0** (IT-SiG 2.0, 11/2020, draft)
- **2. Data Protection Adaptation and Implementation Act EU** (2. DSAnpUG-EU, 2019, Adaptation of the sector-specific German data protection law also with regard to IT security)

# The Cybersecurity Navigator




CYBERSECURITY
NAVIGATOR

# Cybersecurity as an interdisciplinary challenge

## Security requirements

# “Security is a process, not a product”


Bruce Schneier
(US American IT-Security Expert)

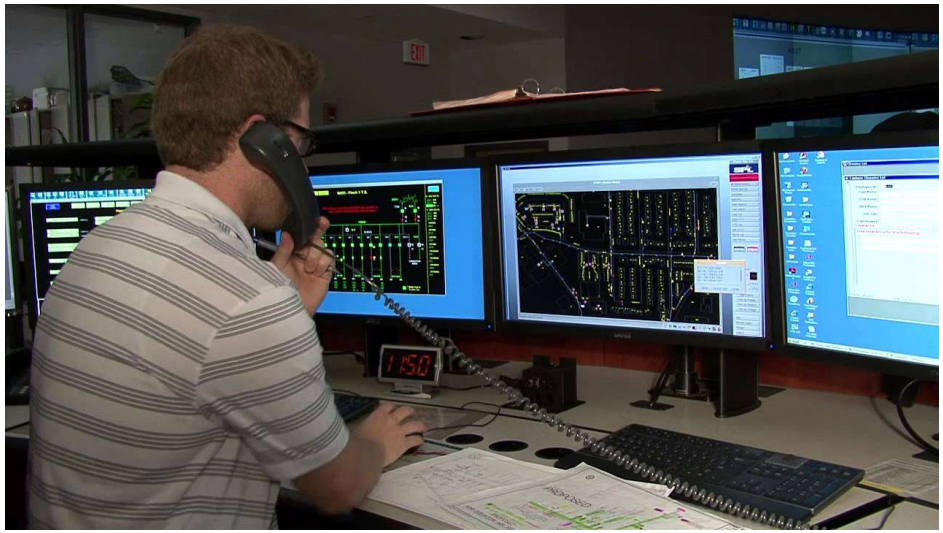
# How to realize an effective level of Cybersecurity practically?

*Article 14*

**Security requirements and incident notification**

1. Member States shall ensure that operators of essential services take **appropriate and proportionate technical and organisational measures** to manage the risks posed to the **security** of network and information systems which they use in their operations. Having regard to the **state of the art**, those measures shall ensure **a level of security of network and information systems appropriate to the risk posed**.

2. Member States shall ensure that operators of essential services take **appropriate measures** to prevent and minimise the impact of incidents affecting the **security** of the network and information systems used for the provision of such essential services, with a view to ensuring the continuity of those services.



# How to realize an effective level of Cybersecurity practically?

*Article 14*

**Security requirements and incident notification**

- What are “appropriate and proportionate technical and organisational measures”?
- How can the “state of the art” be legally defined?
- What is “a level of security of network and information systems appropriate to the risk posed”?
- What are “appropriate measures” that should be taken by the operators of essential services?
- What does “security” mean?

# Indefinite legal terms in Cybersecurity Law

**EU NIS Directive, recital 1:** Member States shall ensure that operators of essential services take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in their operations. Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk posed.

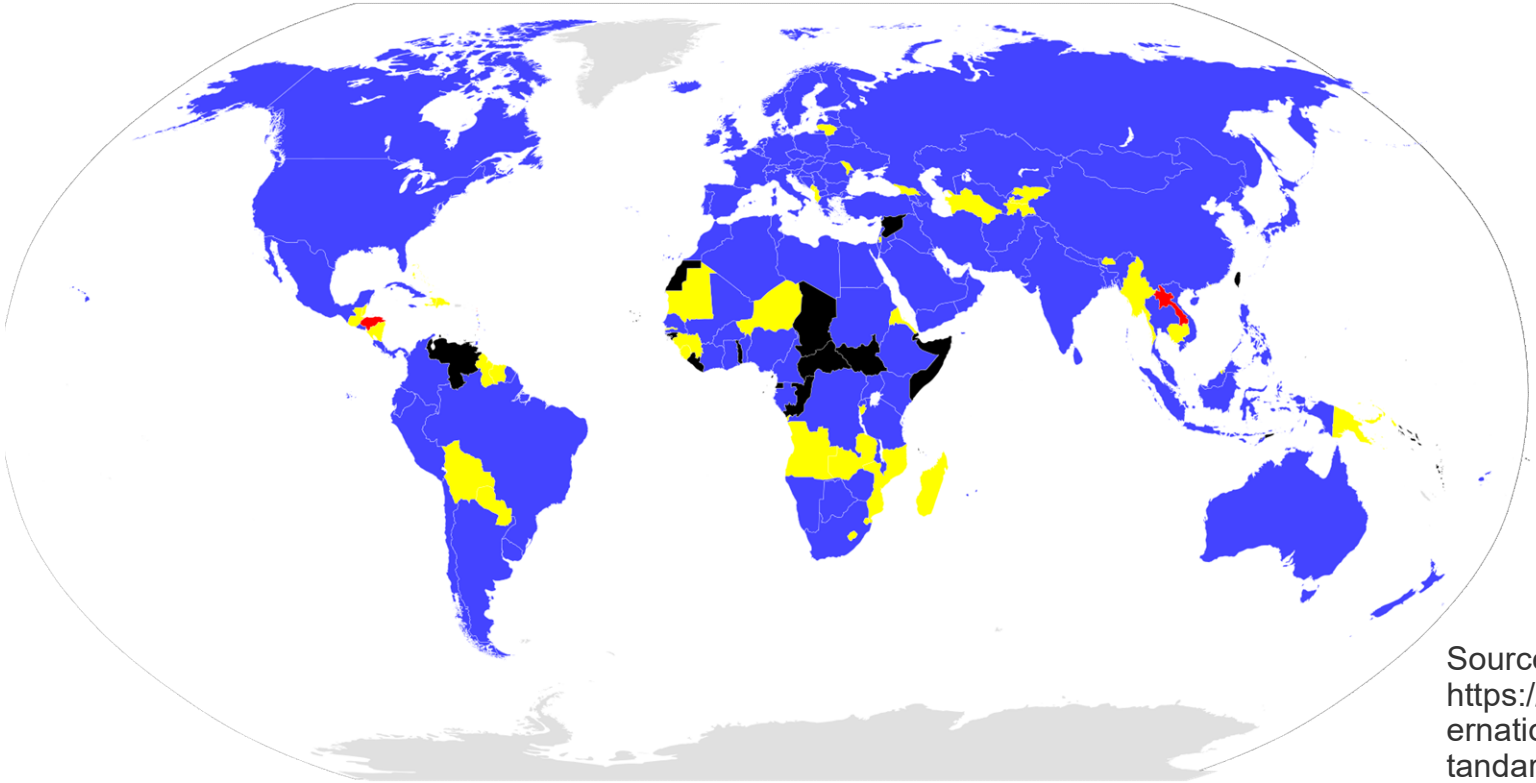
**EU NIS Directive, recital 53:** To avoid imposing a disproportionate financial and administrative burden on operators of essential services and digital service providers, the requirements should be proportionate to the risk presented by the network and information system concerned, taking into account the state of the art of such measures. In the case of digital service providers, those requirements should not apply to micro- and small enterprises.

# IT-Security as an interdisciplinary challenge

- So called “indefinite legal terms” as a connecting factor for the technical implementation of legal specifications
- **Indefinite legal terms:** Openly formulated legal terms, which are normally not concreticized by the law itself, but on the basis of further definitions, which may also be a part of an extralegal framework.
- Several sources of indefinite legal terms do exist as a part of the international IT-Security and Data Protection Law:
  - Art. 14 EU NIS Directive: Security requirements
  - Art. 32 EU GDPR: “Taking into account the **state of the art**, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk […].”
  - Art. 4 E-Privacy Directive: “The provider of a publicly available electronic communications service must take appropriate technical and organisational measures to safeguard security of its services, if necessary in conjunction with the provider of the public communications network with respect to network security. Having regard to the **state of the art** and the cost of their implementation, these measures shall ensure a level of security appropriate to the risk presented.”

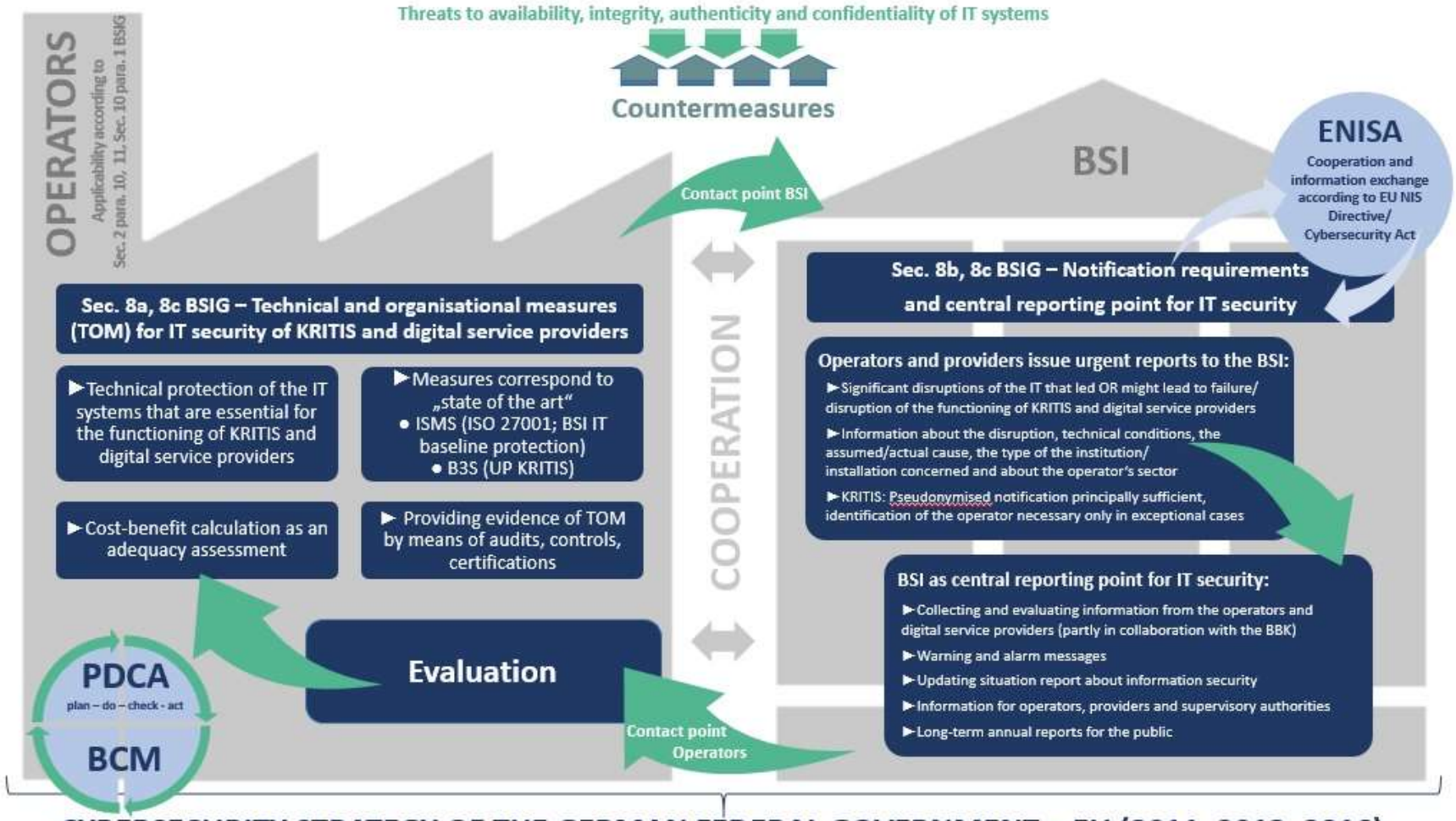
# IT-Security as an interdisciplinary challenge: Use of indefinite legal terms

# European or internationally accepted standards



Source:
https://en.wikipedia.org/wiki/International_Organization_for_Standardization

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



# Chinese Cybersecurity Law: Comparative Approaches

# China
# Cybersecurity Law (CSL: 2016, 2017)


- **Double focus:** Network security and data protection
  - Significant difference to EU law: Cybersecurity 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

# Chinese Cybersecurity Regulation: Specific (international) problems

- **"Disconnection" of VPN**
  - Transmission of sensitive company data: Relevant for transnationally operating (German) companies
  - Unclear legal basis: Articles 5, 58 CSL?
  - Various announcements and "deadlines"
  - So far, however, no significant results/consequences
  - Problematic in the future: Use of only state-licensed VPNs
- **Product certification**
  - Strict requirements for IT imports to China regarding "specific cyber security products" and "critical network equipment”
  - Specification by various Chinese authorities: CAC, MIIT, MPS, CNCA
  - Product catalog: Routers, switches, servers, firewalls with defined performance limits
  - Development of corresponding Chinese national test standards
- **Data localization**
  - Data, which are generated during the operation of Critical Infrastructures, are to be stored in China
  - Duty to be extended to all networked applications (?)

# Conclusion and Outlook

# Conclusion and 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”
- **Similar organizational concepts** throughout the world, but different political goals and approaches
- Current technical challenges force national states to promote cybersecurity regulation, e.g. **Japan** with a new approach especially for **IoT-devices**
- Cybersecurity not only as legal, but also as a **task for international standardization** (e.g. CSL):
  - Technical concretization of legal cybersecurity requirements
  - Support to a consistent interpretation of (newly announced) legal provisions
  - Means to conduct a transnational cybersecurity certification

# Thank you for your attention!

**Dr. Dennis-Kenji Kipker**

Executive Director

Certavo GmbH – international compliance management

dennis.kipker@certavo.de

+49 421 218 66049