Bundesministerium
des Innern

Critical Information Infrastructure Protection

Implementing a Cybersecurity Strategy in CIIP

Swiss Cyber Storm 4 – International IT-Security Conference

13 June 2013, Lucerne

Dr. Michael Pilgermann

Section IT3 – IT-Security

Office of the Chief Information Officer at the Federal Ministry of the Interior

Agenda

- Critical Infrastructure Protection in Germany
- Cybersecurity and Critical Infrastructure Protection
- National CIIP Implementation Plan (UP KRITIS)
- Regulatory framework

Critical Infrastructures
Definition

Organisations and facilities

- that are of **major importance** for the community and
- whose **failure or impairment** would cause
  - a sustained shortage of supplies,
  - a significant disruption of public order,
  - or other dramatic consequences.

Critical Infrastructures
Sectors

Energy	Electricity, Gas, Oil
ICT	Telecommunication, Information Technology
Transportation & Traffic	Air Traffic, See ~, Railway ~, Road ~, Logistics
Health	Medical supply, Medicines, Laboritories
Water	Supply, Disposal
Feeding	Food-Industry, ~ Trade
Finance & Insurance	Banking, Stock Market, Insurance, Financial Services
State & administration	Government & Administration, Parliament, Justice, Emergency Services, Civil Protection
Media & Culture	TV & Radio, Press, Culture, symbolic buildings

National CIP Strategy

- Joint work of all Federal Ministries,
  - guided by the Ministry of the Interior (BMI)
  - and the Federal Office for Civil Protection and Disaster Assistance (BBK)
- Adopted by the Cabinet of Ministers on June 17, 2009.
- Summarizes the federal administration‘s aims and objectives and political-strategic approach already applied in practice
- Starting point for consolidation and new developments

Shared responsibility

Information security is a **shared** responsibility of

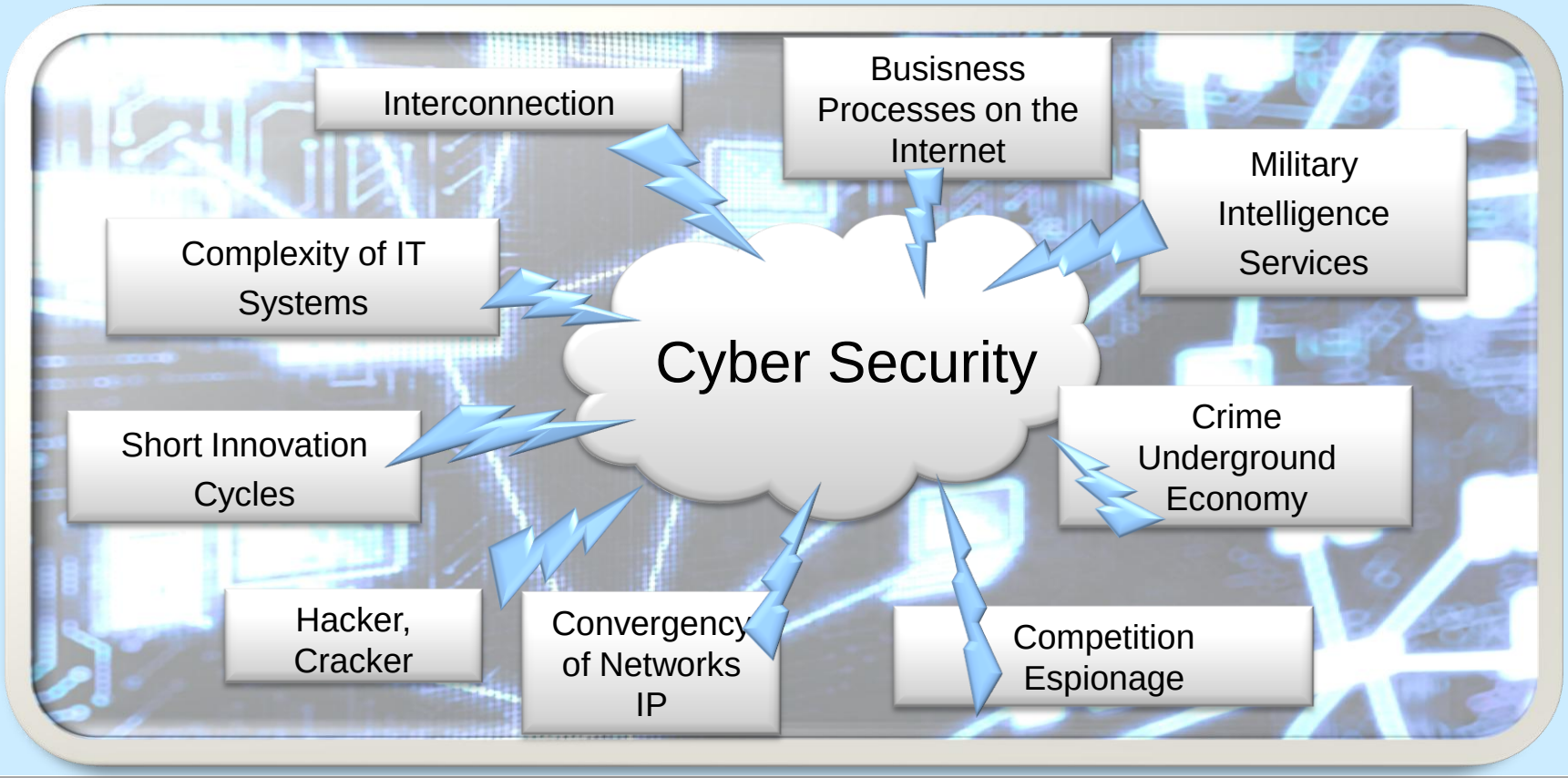
- the **state** (safeguarding internal security)
- **critical infrastructure operators** (companies and organisations – dependable delivery of services that are vital for state and society)
- **citizens** (secure own IT, show awareness to IT-related threats such as, e.g., phishing or botnetting)

Information security can only be achieved if all groups accept their responsibility

Agenda

- Critical Infrastructure Protection in Germany
- **Cybersecurity and Critical Infrastructure Protection**
- National CIIP Implementation Plan (UP KRITIS)
- Regulatory framework

Cybersecurity Strategy
Motivation



Cyber Threat

Untargeted attacks

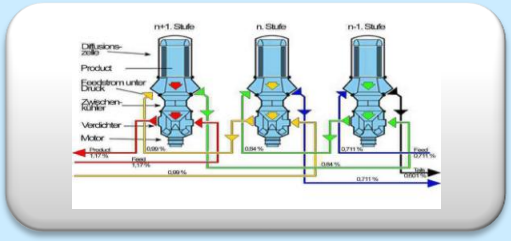
- Sabotage, fraud, etc.
- **SPAM, virus, worms, trojans, Drive-by-Downloads**

Targeted attacks

- espionage & sabotage
- **social-engineering + trojans**

Individual attacks (scalpel)

- sabotage of specific IT systems (and infrastructures) with high harm potential
- complex, long-lasting preparation
- **zero-day-exploits**
- **Faked certificates**

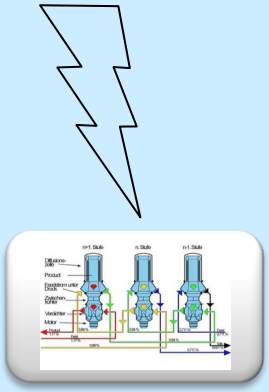


Cyber and IT security
as priority of national government since 2009

Nov. 2009 — ***Fall 2010*** — ***Feb. 2011***

IT-Security in coalition agreement

- Strengthen IT security in public and non-public area; esp. CIIP
- Concentrate competences at Federal CIO
- Further develop BSI as national Cybersecurity agency
- Prevent unfair passing-on of IT-risks to end-user



„Stuxnet“

„Duqu“

Cybersecurity Strategy

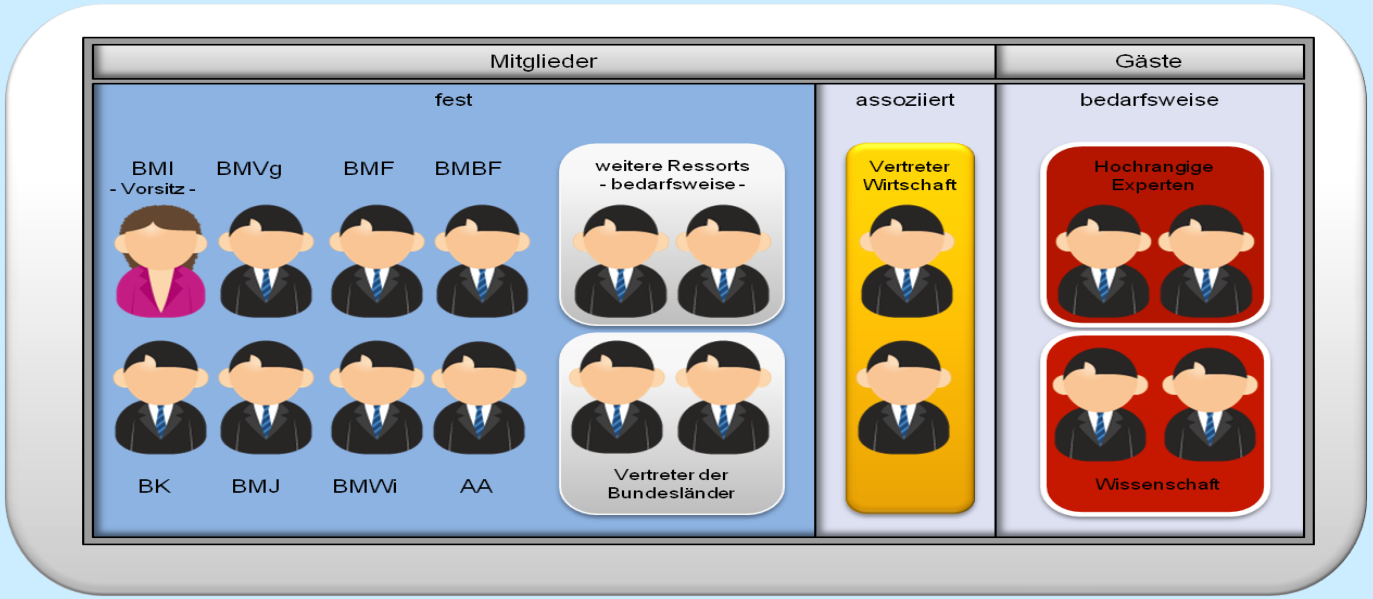
Bundesministerium des Innern

Cybersecurity Strategy

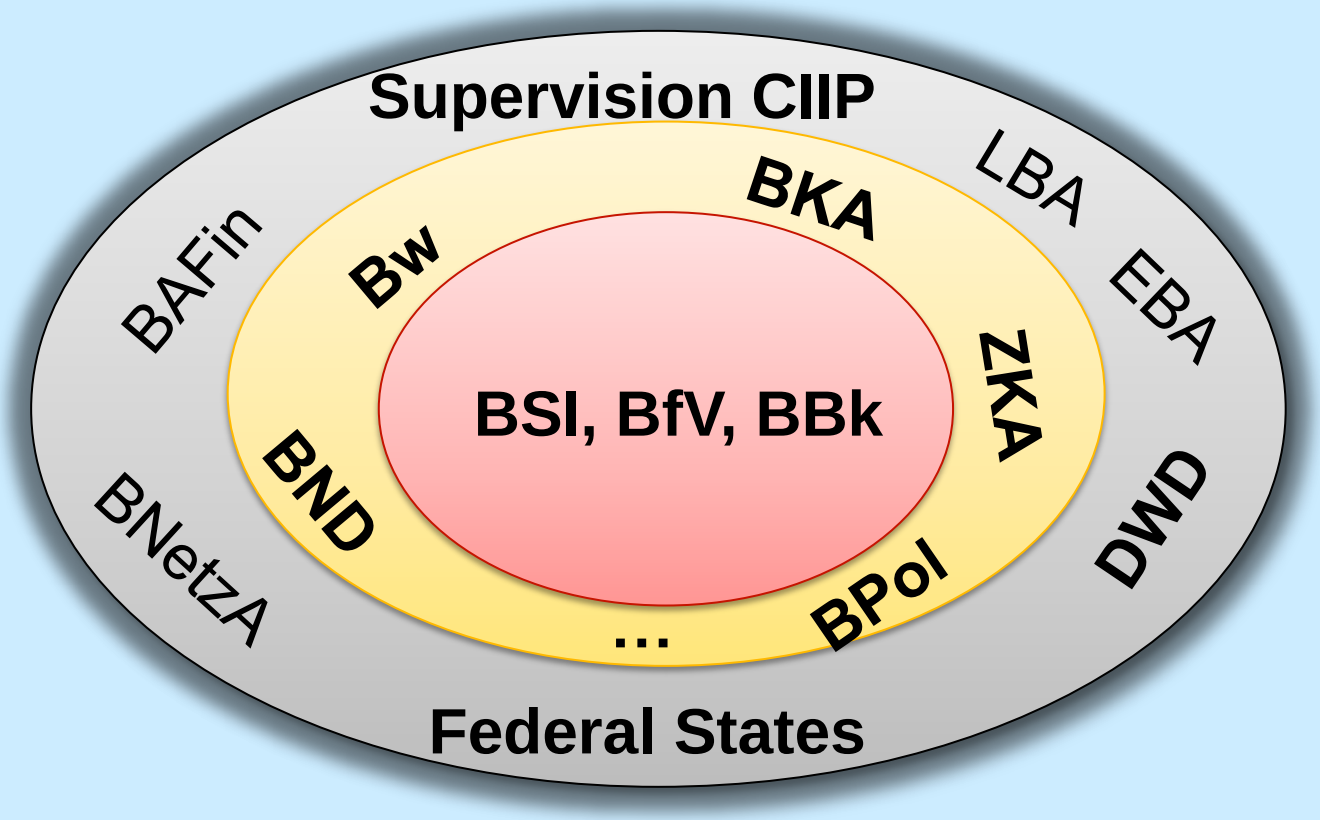
- National Cyber Security Council
- National Cyber Response Center
- Critical IT Infrastructure
- IT of Citizens
- IT in the Public Administration
- Use of Reliable and Trustworthy Information Technology
- International Cooperation (EU, worldwide)
- Response to Cyber- Attcks
- Effective Crime Control
- Personnel development Fed. Gov.

Bundesministerium des Innern

National Cyber Security Council



National Cyber Response Center



Agenda

- Critical Infrastructure Protection in Germany
- Cybersecurity and Critical Infrastructure Protection
- **National CIIP Implementation Plan (UP KRITIS)**
- Regulatory framework

CIIP Implementation
Objectives

- Improve transparency (regarding vital processes)
- Robust foundations through standardized and auditable security level
- Autonomy of vital (IT) processes
- Ensure product and service security
- Prevent threats through continous IT situation analysis and mutual early warning
- Prepare for serious situations by running exercises
- Improve national know-how and strength through cooperation

CIIP Implementation Plan
History

CIP Implementation Plan
(UP KRITIS)

- Foundations
  - Joint responsibility for IT security in CI
  - Expansion of cross-sector and public-private cooperation
- Guiding Principle and Objectives
  - Achieve a uniformly high status of basic IT security in critical infrastructures
  - Establish a framework for trustful cooperation
  - Coordinated action in the event of a national IT crisis
- Published 5 September 2007
- Currently under revision (Dec. 2013 final)
  - Adjust objectives / install sector exchanges

Re-Enforcement of CIIP

- Re-enforcement of CIIP with National Cybersecurity-Strategy in February 2011
  - Evaluation/advancement of CIIP Implementation Plan
  - **Evaluation of existing policy framework**
- Top-level discussions with the relevant sectors
  - Summer 2011: 7 Minister meetings with all CI sectors

Bundesministerium des Innern

Top-level discussions May – September 2012
Main Outcomes

- Very high inter-dependencies (special role of energy and ICT)
- Present situation is heterogeneous
  - e.g. some sectors have elaborated minimum standards, risk management and security concepts, reporting infrastructure
- Number of sectors lacking standards – no transparency
- Potential for mutual information exchange on IT situation and threats

Agenda

- Critical Infrastructure Protection in Germany
- Cybersecurity and Critical Infrastructure Protection
- National CIIP Implementation Plan (UP KRITIS)
- **Regulatory framework**

Proposal for GER NIS Law
Key Provisions

- Key Operators of CI
  - Minimum requirements for IT security (self-regulation / recognised standards)
  - Reporting serious IT security incidents
- Electronic communication providers
  - State-of-the-art protection of infrastructures from illegal intervention
  - Malicious software: Reporting serious IT security incidents; information and assistance of users
- Information society service providers
  - Implement protection measures to a reasonable extent
- Federal Office for Information Security
  - Annual reports to raise public awareness

Proposal for NIS Law
State of Play

- MoI-Proposal (publicly available) in inter-service consultation
- In parallel (deadline passed):
  - Feedback from around 40 business and expert associations
  - Feedback from Länder (federal states)
- As a result, currently preparation of revised proposal

Deadline: elections of Federal Parliament in Sep. 2013

- Last ordinary plenary session: 24.06. - 28.06.2013
- Generally, broad political support

Bundesministerium des Innern

Proposal for National NIS Law
Draft NIS-Directive (EU)

	GER NIS LAW	NIS-DIRECTIVE (EU)
addressee	•CI operators •Telecommunication and electronic service providers	•CI operators with exceptions (e.g. water) •Some electronic service providers •Public administration
Requirements for CI operators (also telec. and electr. services)	•Minimum IT security requirements, state of the art •Reporting of IT incidents, which (may) have impacts on the maintenance of operation of their CI.	•Minimum IT security requirements, state of the art •Reporting of IT incidents, which have impact on security of core services

Bundesministerium des Innern

Proposal for national NIS law – NIS-directive

	GER NIS LAW	NIS-DIRECTIVE (EU)
Requirements ICT sector	Reporting of disturbances of telec. networks/services	non
Use of reported incident information	Sharing with CI operators	Public sharing
Enforcement	Audits	Authority for -further checks, -request for information, -instructions

Bundesministerium
des Innern

Many thanks for your attention!

Dr. Michael Pilgermann

Section IT3 – IT-Security

Office of the Chief Information Officer at the Federal Ministry of the Interior

michael.pilgermann@bmi.bund.de