



Regulierung kommt immer zu spät. Was braucht es zur Stärkung der Cybersicherheit?

Judith Bellaiche, Nationalrätin und CEO Swico



Cybersicherheit im Parlament



2008 - 2010

2023



Forderungen – Form und Schärfe

**Bewusstsein
Orientierung**



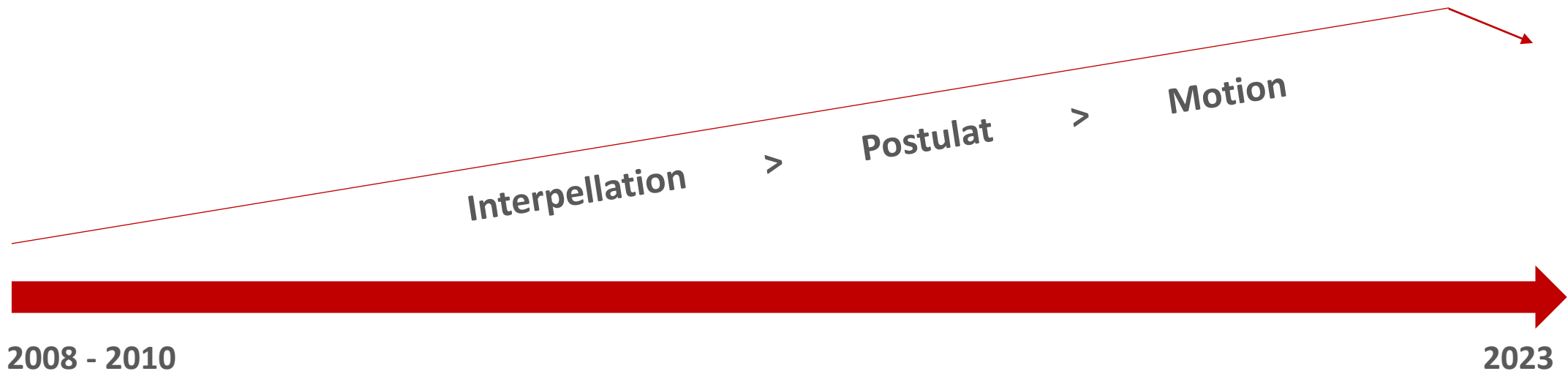
**Berichte
Rechenschaft**



**Konkrete
Massnahmen**

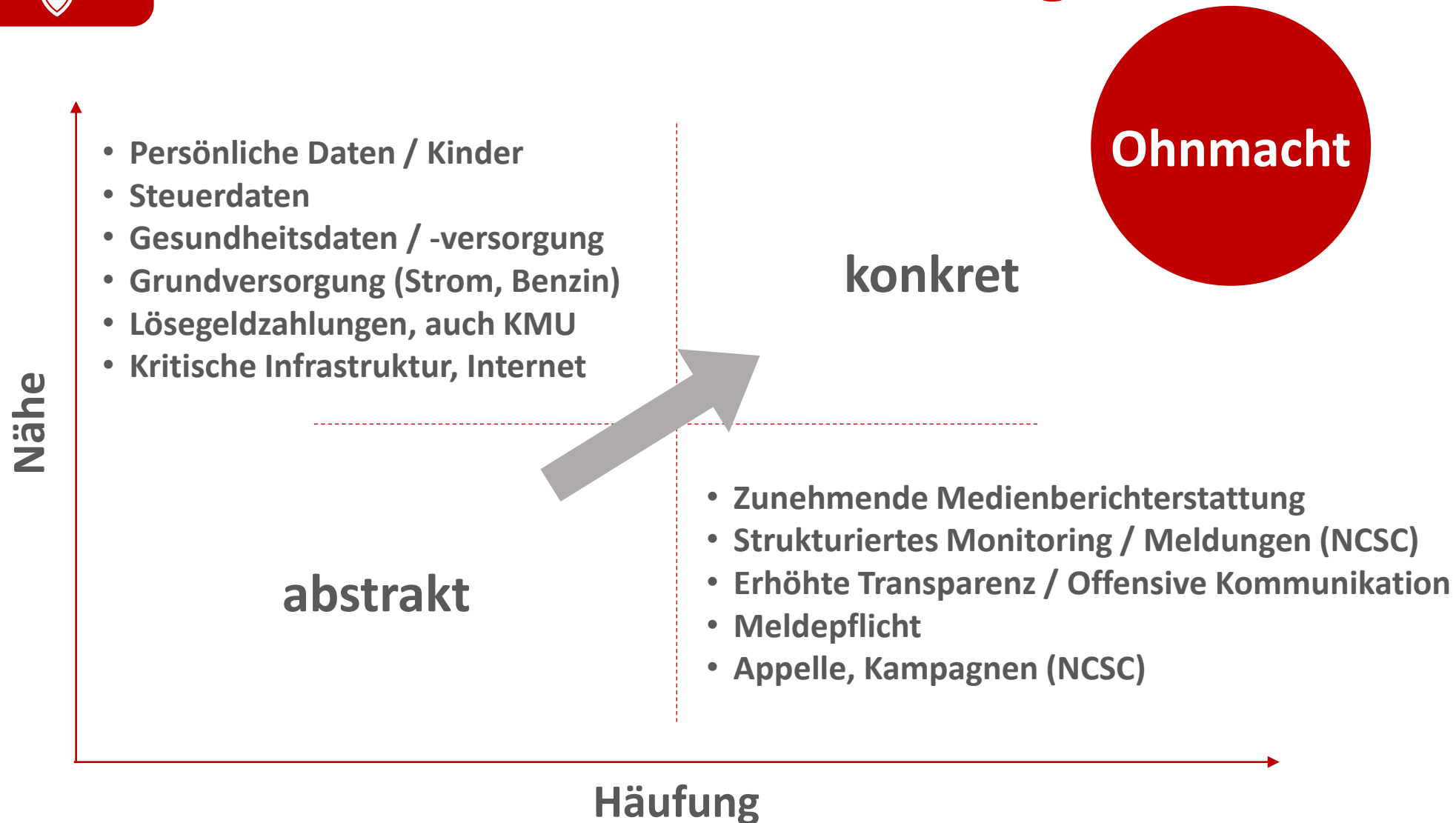


**Neue Aufgaben
Verbote**





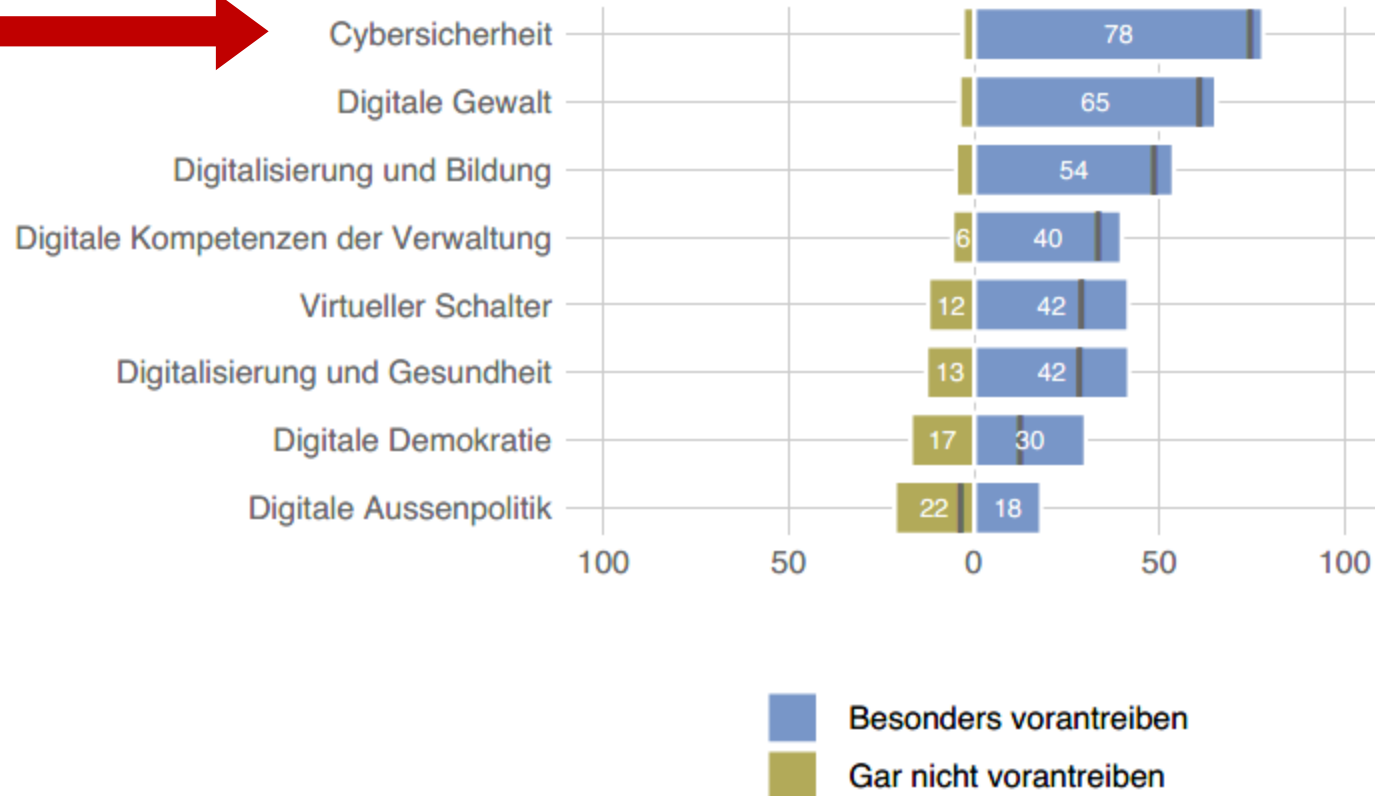
Bewusstseinsveränderung





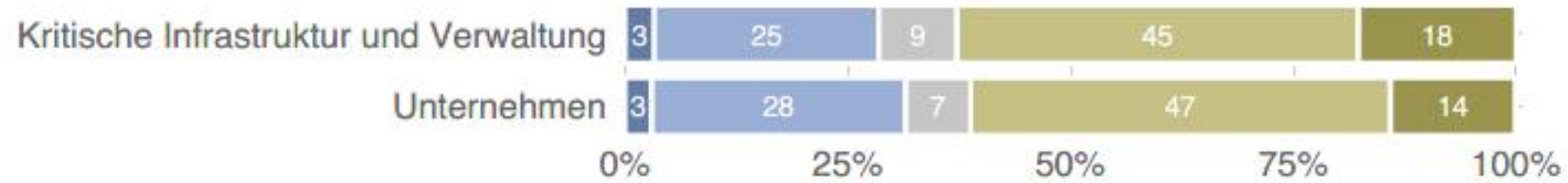
Auswirkungen auf die Bevölkerung?

#1





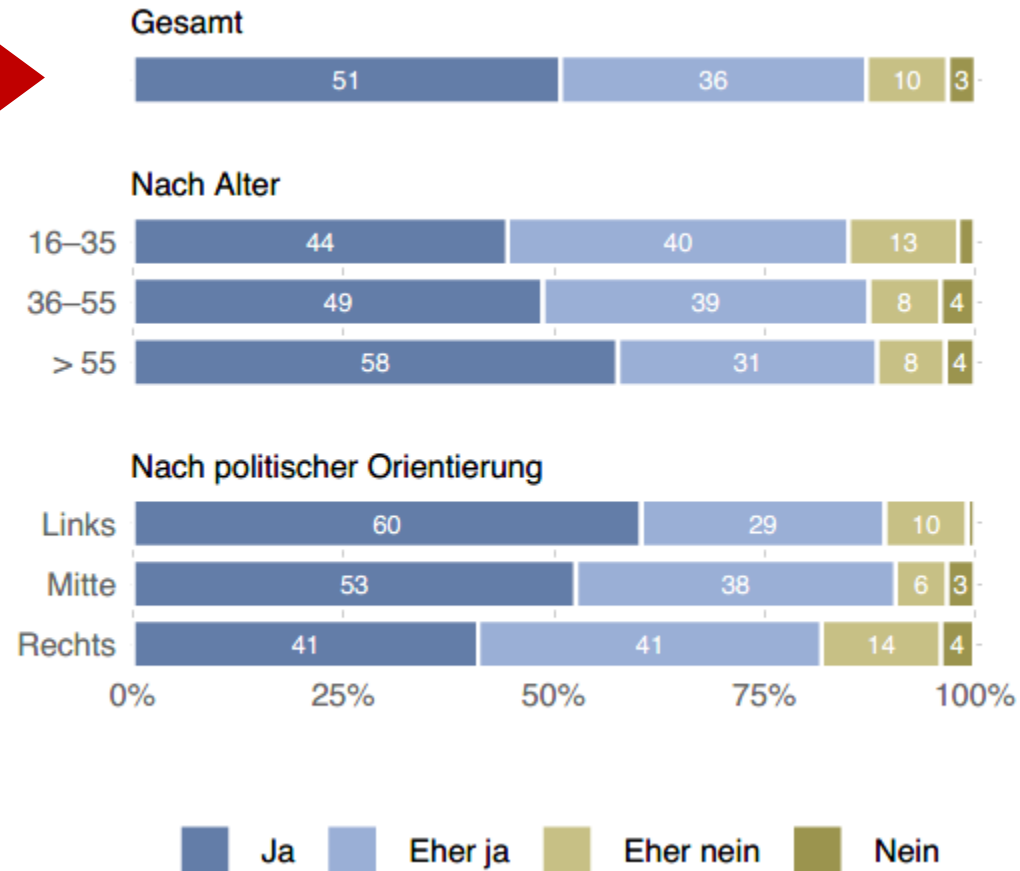
Beurteilung der Cybersicherheit





Schutz der Unternehmen als staatliche Aufgabe

87%





Cybersicherheit als politische Aufgabe?

Schutz von kritischer Infrastruktur i.S. Grundversorgung

- Meldepflicht bei Angriffen (resp. Schwachstellen?)
- Ex post

Prävention

- Innerhalb Bevölkerung/Wirtschaft

Staat hat Vorbildfunktion

- In Bezug auf technische Sicherheit
- In Bezug auf Lieferketten
- In Bezug auf Umgang mit Daten



Staat als Akteur

1. Technische Sicherheit

- Beschaffung an Sicherheit orientieren
- Anforderungen formalisieren (Standards)
- Nachweise einfordern
- Kein Vertrauensprinzip

2. Umgang mit Daten

- Stringente Prozesse
- Einhaltung der Prozesse
- Datensparsamkeit
- Kein Vertrauensprinzip

**Nicht
delegierbar**



(Nicht) Vertrauen regulieren ex ante

Technische Standards vorgeben

- Datenspeicherung
- Datenverarbeitung
- Softwareentwicklung?

Nachweise einfordern

- Compliance Reporting

Rechtsdurchsetzung

- Datenschutzgesetz (Strafen)
- Haftpflichten



(Nicht-)Vertrauen regulieren

Kein Vertrauensprinzip

= Kulturfrage

= Führungsfrage

***“Cyber-attacks, rather than natural catastrophes,
will become uninsurable.”***

Mario Greco, ZURICH



Fazit

Staatliche Regulierung orientiert sich am schützenswerten Rechtsgut

- Welches Rechtsgut ist betroffen
- In welchem Ausmass ist es betroffen
- Wer trägt den Schaden (Ursache vs. Wirkung)