Parlamentarier-Dinner Parldigi SATW

Cyber-Situation Schweiz

Prof. Andreas Wenger

Center for Security Studies (CSS)

9. März 2016

ETH zürich

CSS ETH Zurich

Cyber-Risiken sind multidimensional

Cyber-Phänomene

- Cyber-Krieg
- Cyber-Terror
- Cyber-Sabotage
- Cyber-Spionage
- Cyber-Kriminalität
- Hacktivismus

Attribution?

Schadenskategorien

Makro-Risiken — Kritische Infrastrukturen

Mikro-Risiken — Daten/Wissen

- politischer Schaden
- physischer Schaden
- Reputations-schaden
- ökonomischer Schaden

Gemeinsame Verantwortung; Sektorielle Konzepte; Dezentrale Umsetzung

Gegenmassnahmen

- **Technische**
  - Firewalls
  - Antivirensoftware
- **Organisatorische**
  - (funktionale) Entnetzung
- **Gesellschaftliche**
  - Sensibilisierung
  - Ausbildung
- **Politische**
  - Schutz kritischer Infrastrukturen
  - Public-Private Partnerships
- **Rechtliche**
  - Regulation

Verantwortliche Akteure

- **Staat**
  - Dezentrale Struktur
  - Bund
  - Kantone
- **Wirtschaft**
  - Grossfirmen
  - KMUs
  - Diverse Sektoren
- **Bürger**
  - Unterschiedliche Bedürfnisse
    - → Generationsabhängig

=> Ansatz: NCS 2012

Sozio-technischer Kontext: Cyber-Risiken nehmen zu

1. Zunehmende Vernetzung der Schweizer Bevölkerung, Internet of Everything

- Mobilere Vernetzung: Miniaturisierung, intelligente Kommunikation
- Automatisierung der industriellen Produktion; Industrie 4.0
- Netzbasierte Steuerung von Systemen und Geräten
- Exponentielles Datenwachstum: Big Data, Cloud Computing

2. Wachsende Bedeutung der Cyber-Sicherheit

- Verwundbarkeiten:
  - Ausfälle, Störungen, Manipulationen, gezielte Angriffe, etc.
- Kritische Sektoren:
  - Gesundheit, Energie, Finanzen, Transport, Verteidigung etc.

Politisierung und Militarisierung von Cyber-Konflikten

Hybrider Krieg

Ukraine 2014:
Cyber-Operationen
Desinformation
Propaganda

Terror

ISIS 2014:
Rekrutierung
Finanzierung

Makro-Risiken

Sabotage

Stuxnet 2010

Spionage

Snowden 2013

Mikro-Risiken

Hacktivismus

Vandalismus

Kriminalität

Renationalisierung Cyberraum – Cyber-Sicherheitspolitik

A. Cyber-Abschreckung + Verteidigung

- Offensive/defensive operationelle Fähigkeiten
- Neue Strukturen: Cyber-Kommandos
- Steigende Rüstungsausgaben

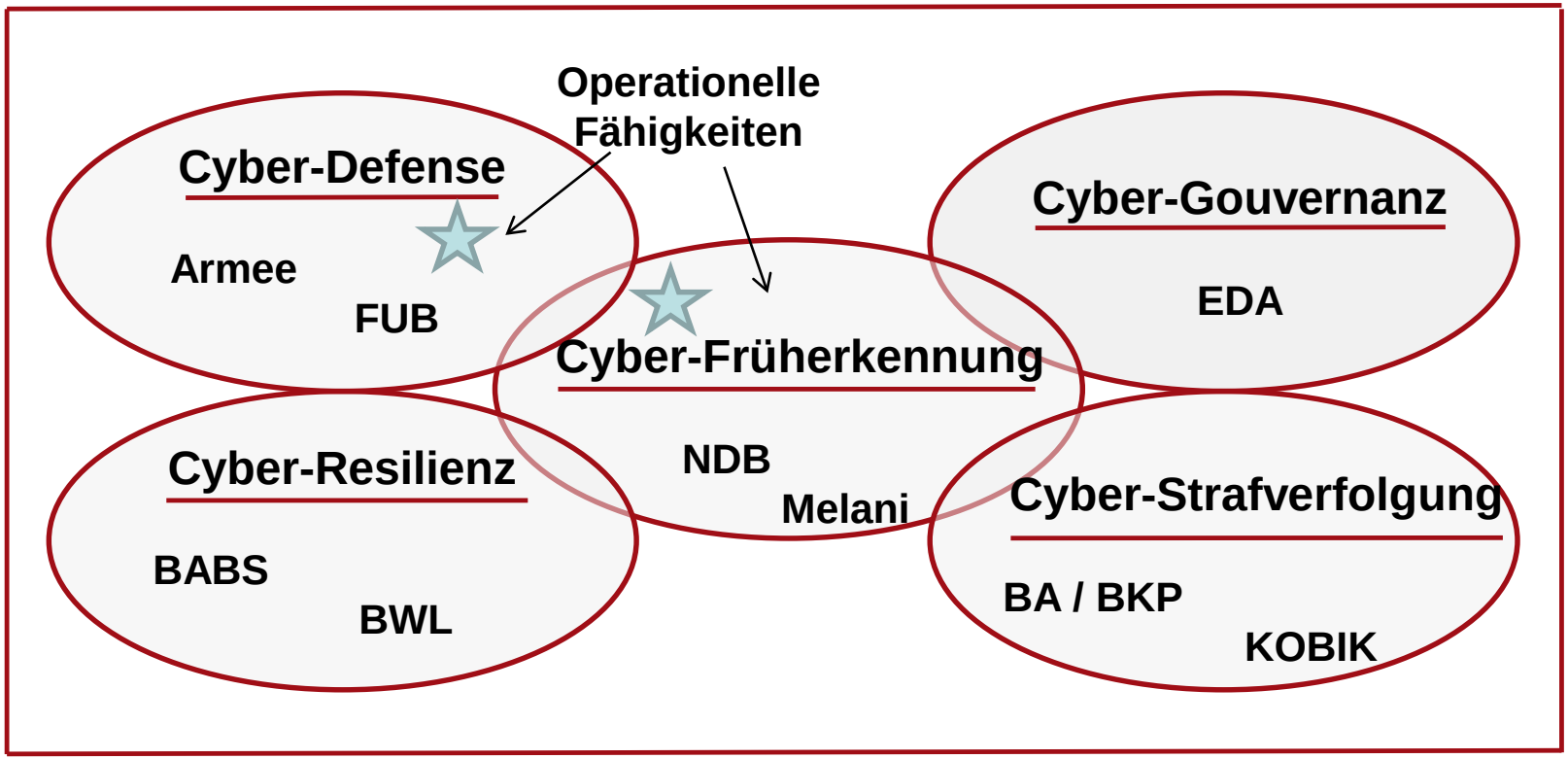
Eskalations-gefahr

Stabilisierung

B. Entwicklung von Cyber-Normen

- Internet Gouvernanz
- Völkerrecht: Cyber-Waffe?
- Vertrauensbildende Massnahmen: z.B. OSZE
- Rüstungskontrolle: z.B. Zero-Day Exploit

Umfassende Cyber-Schutzstrategie – Schwerpunktbildung



Regulation

Partnerschaften

Gesetze

Kantone

F & E

Internationale Partner

Gesellschaft

Wirtschaft

Cyber-Risiken: Grundlegende Herausforderungen

1. Der Cyber-Raum ist grundsätzlich unsicher

2. Der Markt produziert nicht genügend Sicherheit

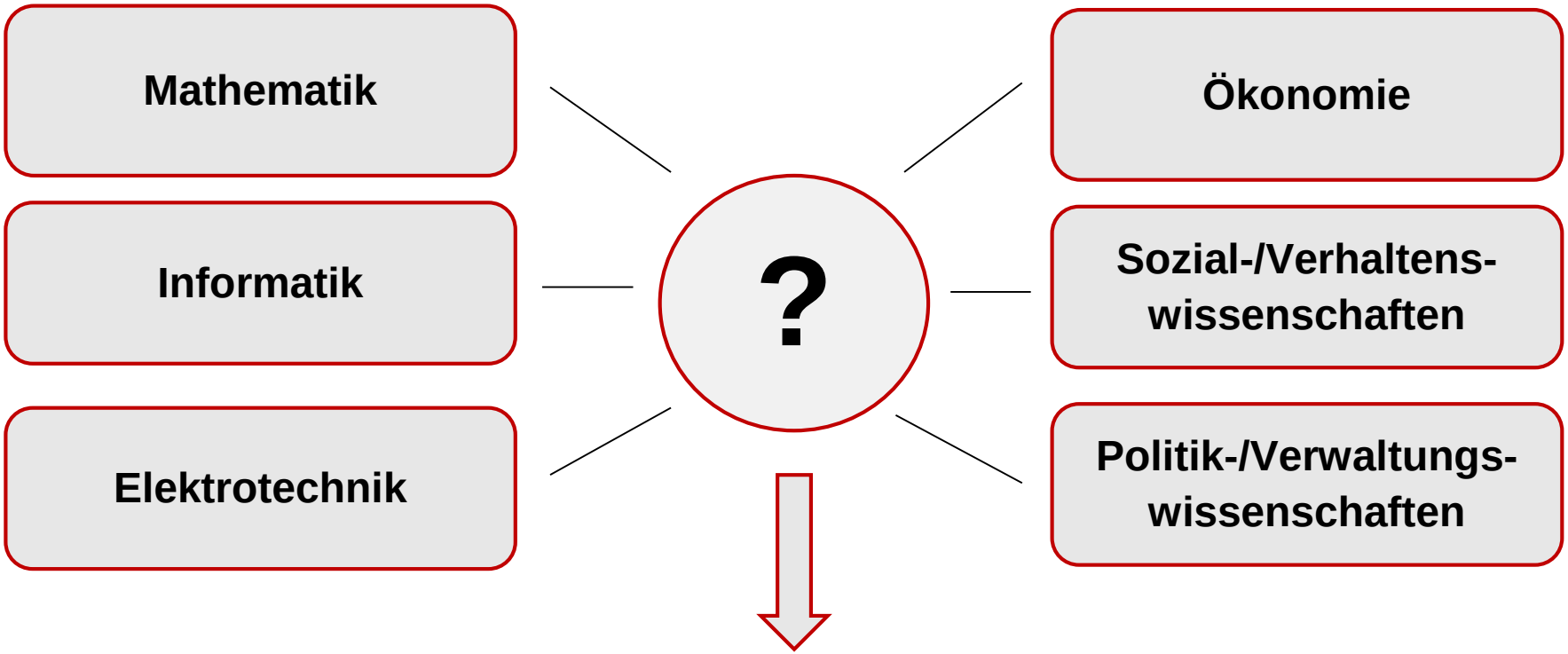
3. Der Cyber-Hype ist ökonomisch und politisch profitabel

4. Das Wissen über Cyber-Risiken ist limitiert

5. Die Cyber-Sicherheit hat auch eine nationale Dimension

6. Der Staat allein kann den Cyber-Raum nicht schützen

Interdisziplinäre Forschung & Ausbildung



Herausforderungen

- Anreizsysteme
- Peer Review / Publikationsorgane
- Career Tracks
- Forschungsplattformen

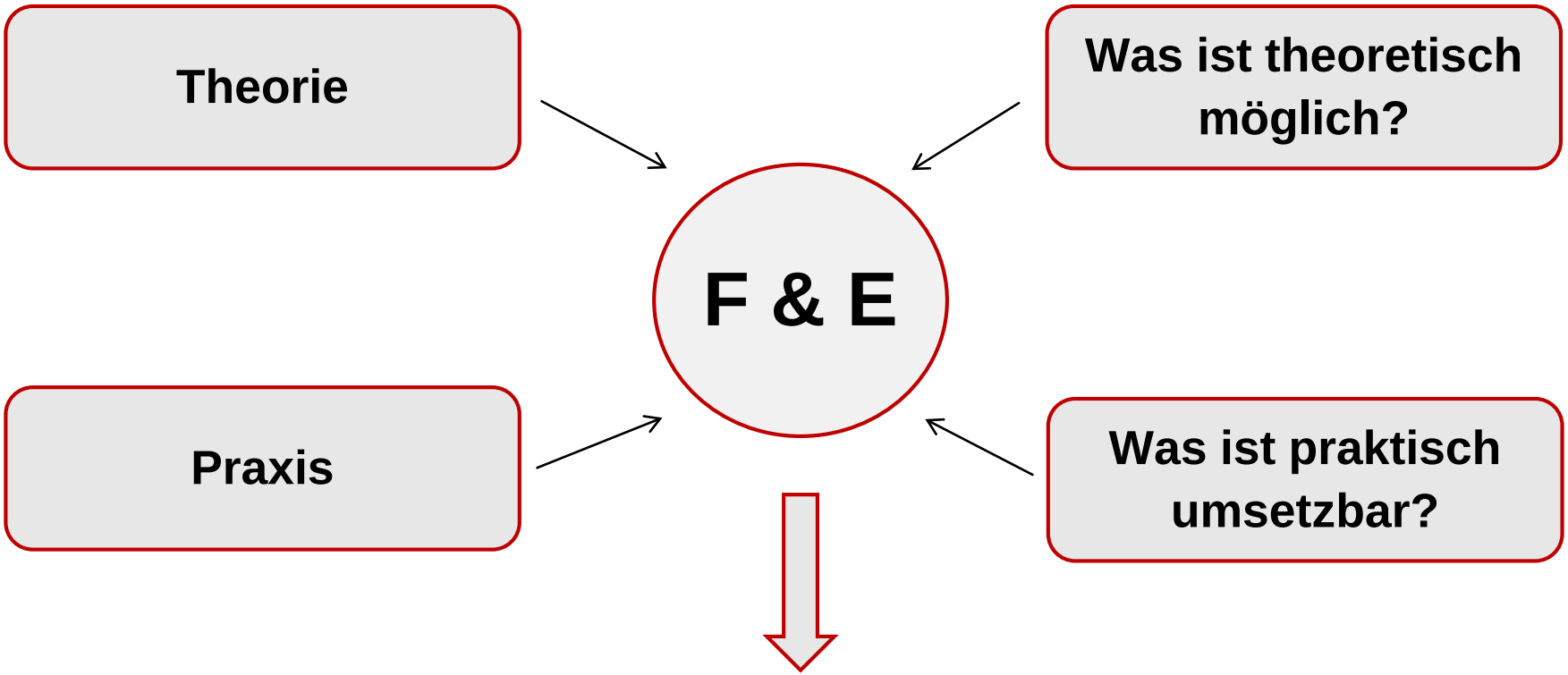
ETH Zürich: Forschung

- Institute of Science, Technology & Policy (ISTP)

ETH Zürich: Ausbildung

- Master in Information Security
- Master in Science, Technology and Policy

Duale Forschung & Ausbildung



Herausforderungen

- Rückkopplung Theorie und Praxis
- Engineering, Experimentieren, Wartung etc.
- Zusammenarbeit Industrie und Wirtschaft
- Shared Lab Spaces

ETH Zürich

- Zurich Information Security Center (ZISC)
  - Gemeinsame Definition von Projekten
  - Gemischte Teams

Weiterbildung

- MAS, DAS, CAS, etc.
- Technology & Policy

1. Nationale F & E Pläne: USA, Deutschland, Israel, etc.

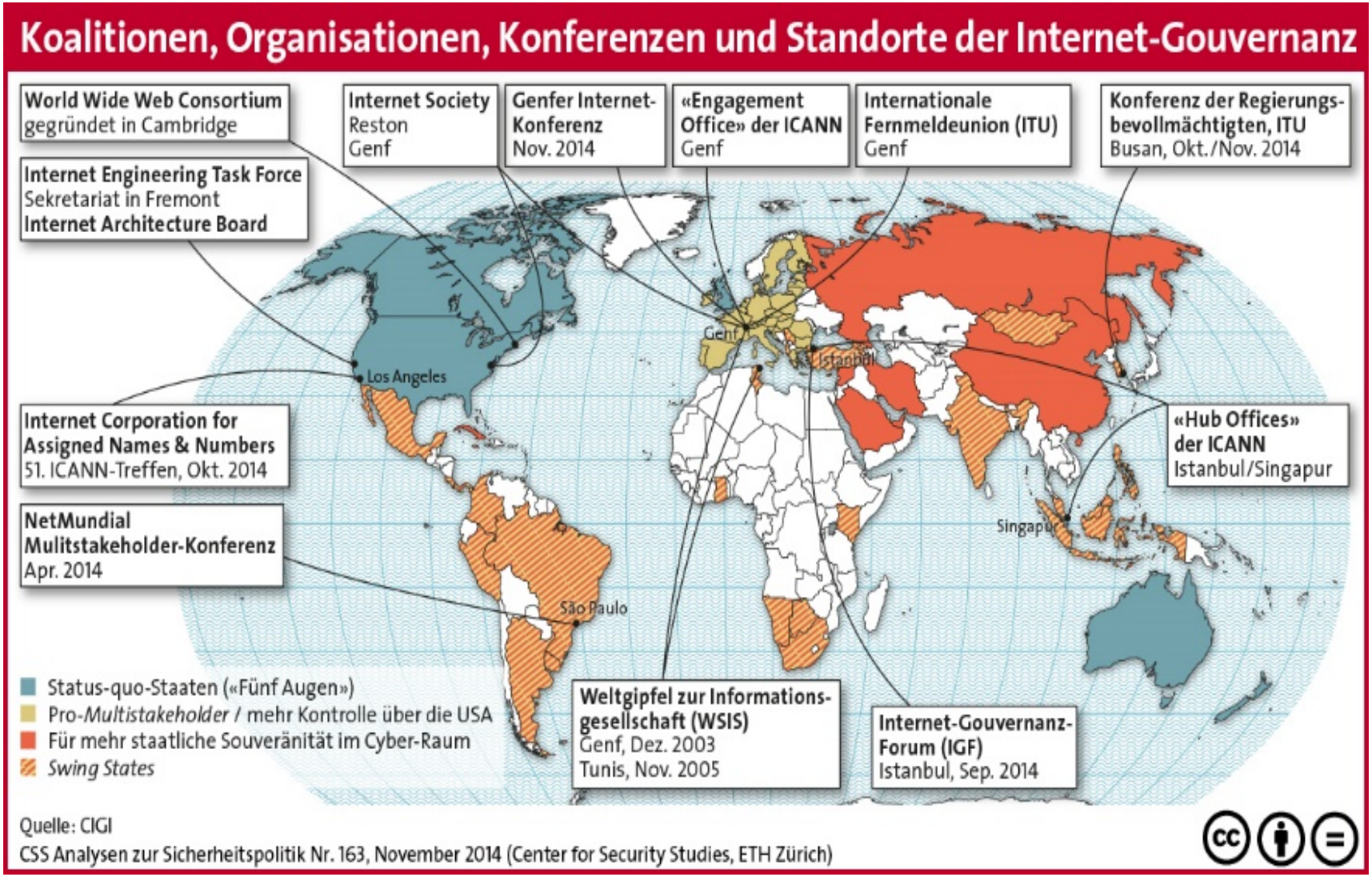
- NCS M1: Koordination der staatlichen Bedürfnisse / Themen.
- Identifikation relevanter Cyberforschungsthemen
- NCS M 7/8: Etablierung neuer Angebote in der Kompetenzbildung

2. Themenfeld: technische Grundlagen

3. Themenfeld: industrielle Sektoren / Systeme

4. Themenfeld: politisch-gesellschaftliche Steuerung

Koalitionen, Organisationen, Konferenzen und Standorte der Internet-Gouvernanz



Quelle: CIGI

CSS Analysen zur Sicherheitspolitik Nr. 163, November 2014 (Center for Security Studies, ETH Zürich)