Die Nationale Strategie Cyber Defense: Status und Rolle der ICT-Experten

COMPASS Bier-Talk
3. November 2011, Jona

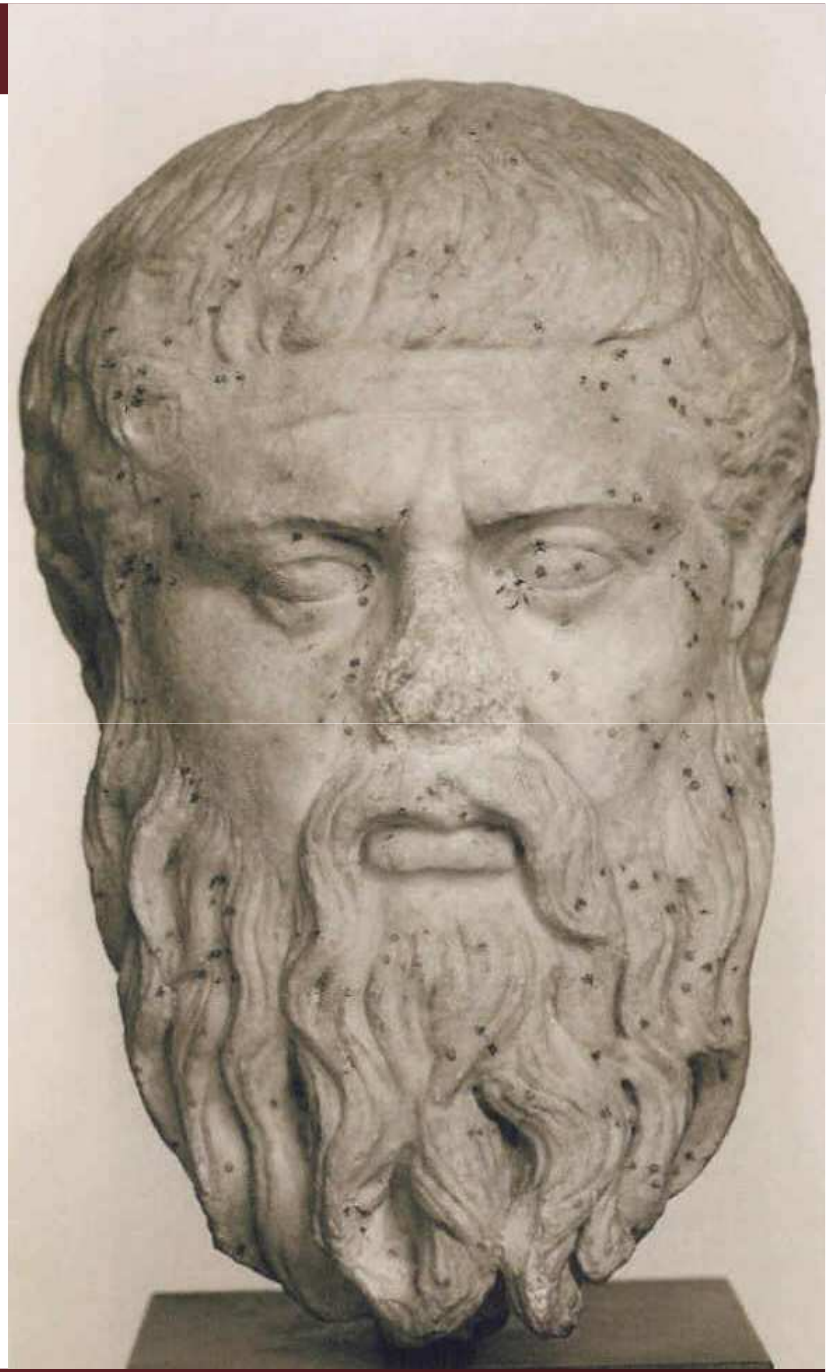
Mark A. Saxer
Vorstand ISSS, Leiter SIG-CYD, GF Swiss Police ICT

Gérald Vernez
VBS, Stv Projektleiter NSCYD

Ausgangslage

1. Öffentliche und staatliche Sicherheit sind **Staatsaufgaben**.
2. Der Staat ist u.a. durch ein **Staatsterritorium** definiert.
3. Der Cyberspace ist aber grenzenlos.

- Wenn Staatsaufgaben **territorial** verfasst sind – gibt es folglich keinen öffentliche Sicherheit im grenzenlosen Raum? Ist staatliche Sicherheit herstellbar?
- Oder geht die **Funktion** der Staatsaufgabe vor, wonach der Einzelne zu schützen ist?



Nationale Strategie Cyber Defense (NSCYD)

- 10. Dezember 2010: Bekanntgabe des Projektes und der Ernennung Div Nydegger
- 31. März 2011: Erste öffentliche Präsentation
- Anschliessend: Vier grosse Workshops (Hauptworkshops) und verschiedene Sektorentreffen
- Z.B. am 1. Juli Sektortreffen Polizei (Forensik)
- 20. Oktober 2011: Ausweitung Zeitrahmen

Der Auftrag

Originalfolie Stand 31. März 2011

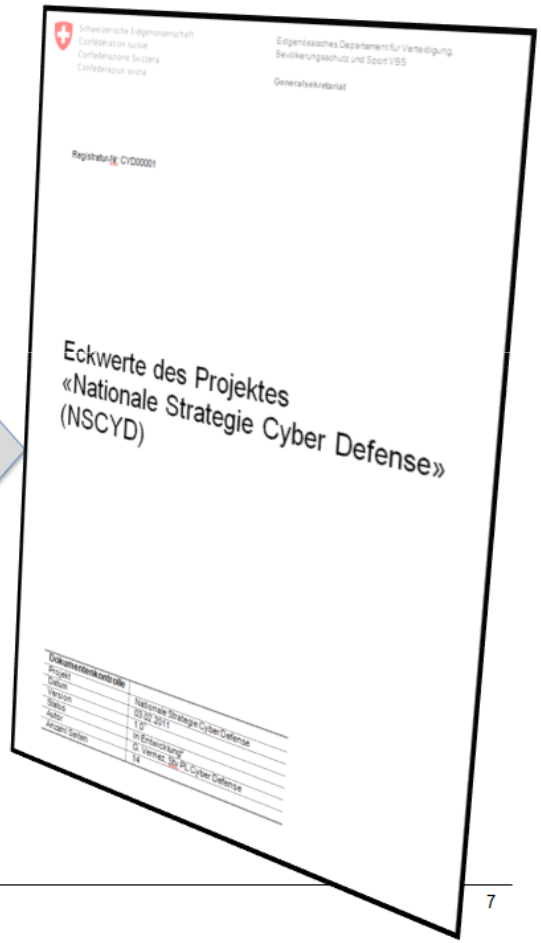
INTERN

Projekt Cyber Defense

Auftrag

„… Das VBS wird beauftragt, unter Einbezug aller betroffenen Akteure aus den anderen Departementen, Schlüsselbereichen und Aufsichtsbehörden eine Arbeitsgruppe einzusetzen. …, **bis Ende 2011** in enger Zusammenarbeit mit der Entwicklung der Strategie des Bundesrates für den Schutz kritischer Infrastrukturen umfassende und vertiefte Abklärungen zum Thema vorzunehmen und darauf basierend eine gesamtheitliche Strategie des Bundes gegen Cyber-Bedrohungen zu erarbeiten.

… **Bis Ende März 2011** wird der Delegierte dem Chef VBS ein erstes Konzept vorlegen, das allfällige Sofortmassnahmen, die weitere Stossrichtung des Projekts und die dafür nötigen Massnahmen aufzeigt.“

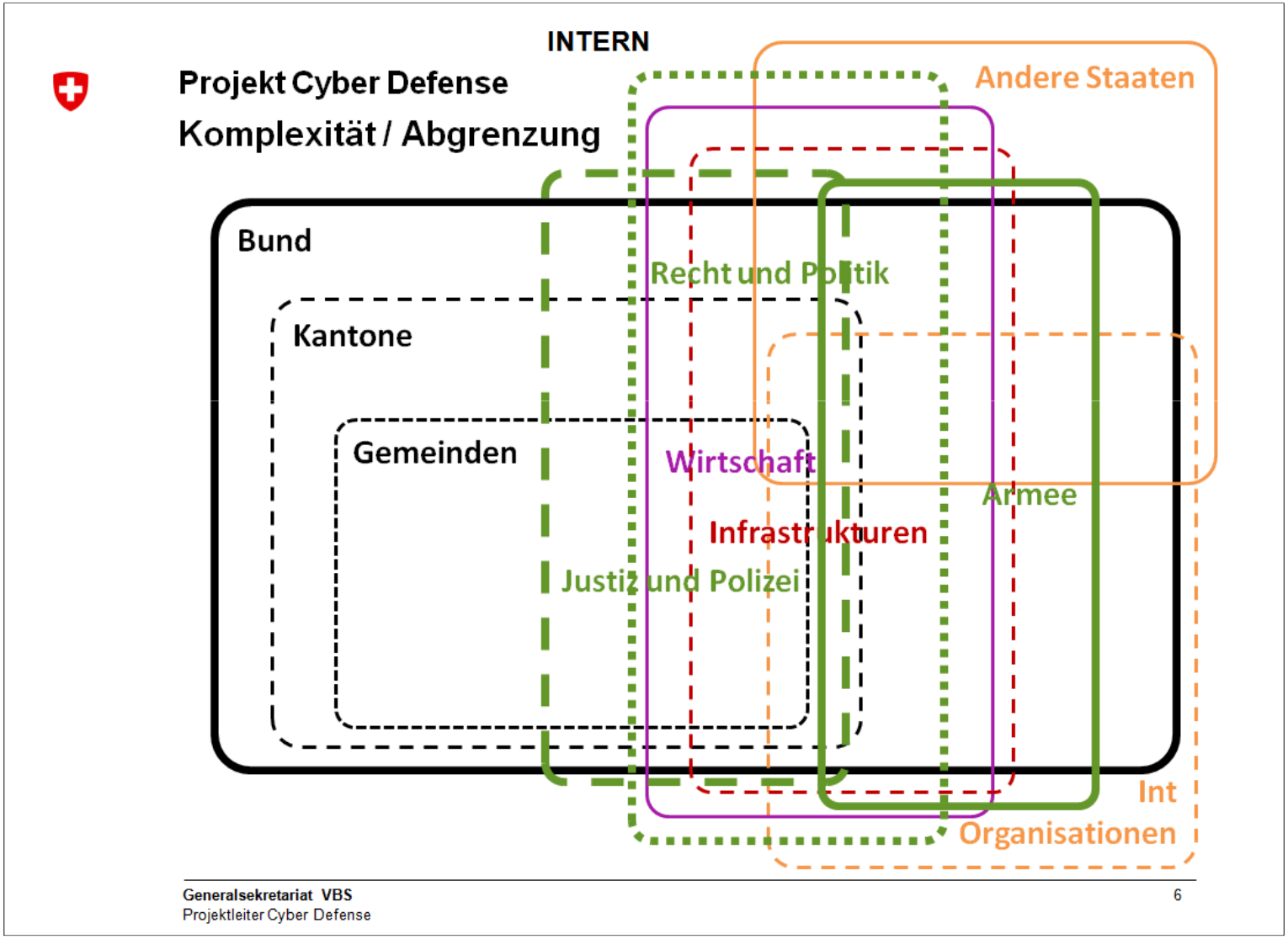


Generalsekretariat VBS
Projektleiter Cyber Defense

7

Komplexität

Originalfolie Stand 31. März 2011

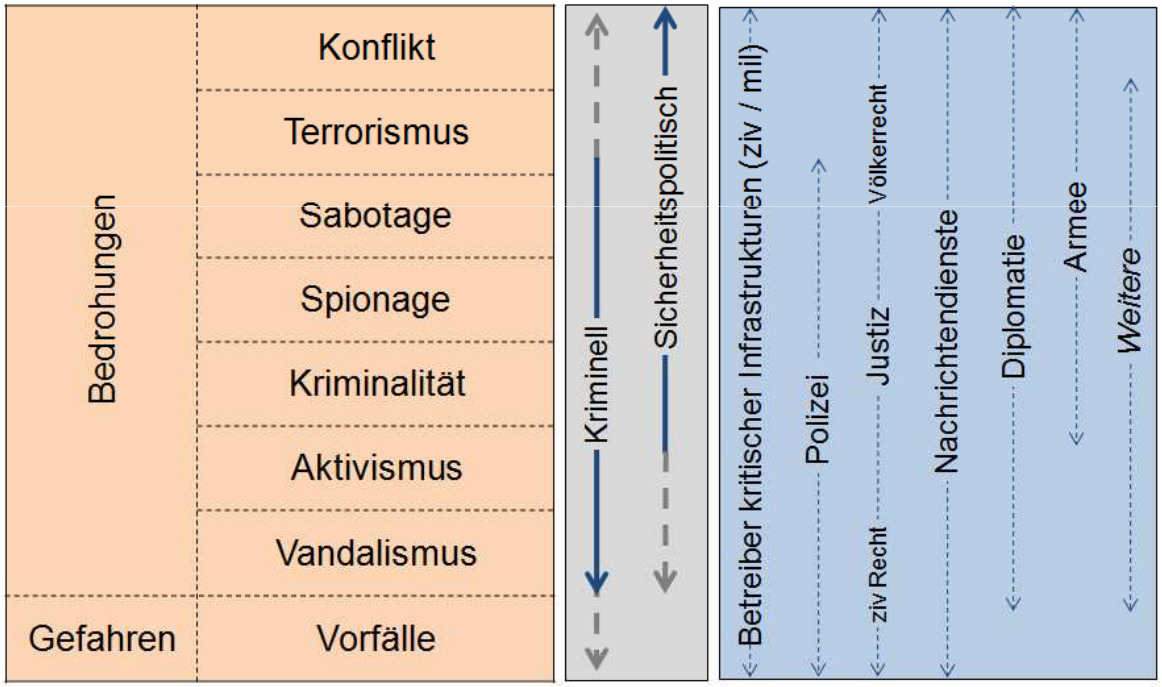


„Der Scope“

Originalfolie Stand 02. November 2011

Projekt Cyber Defense

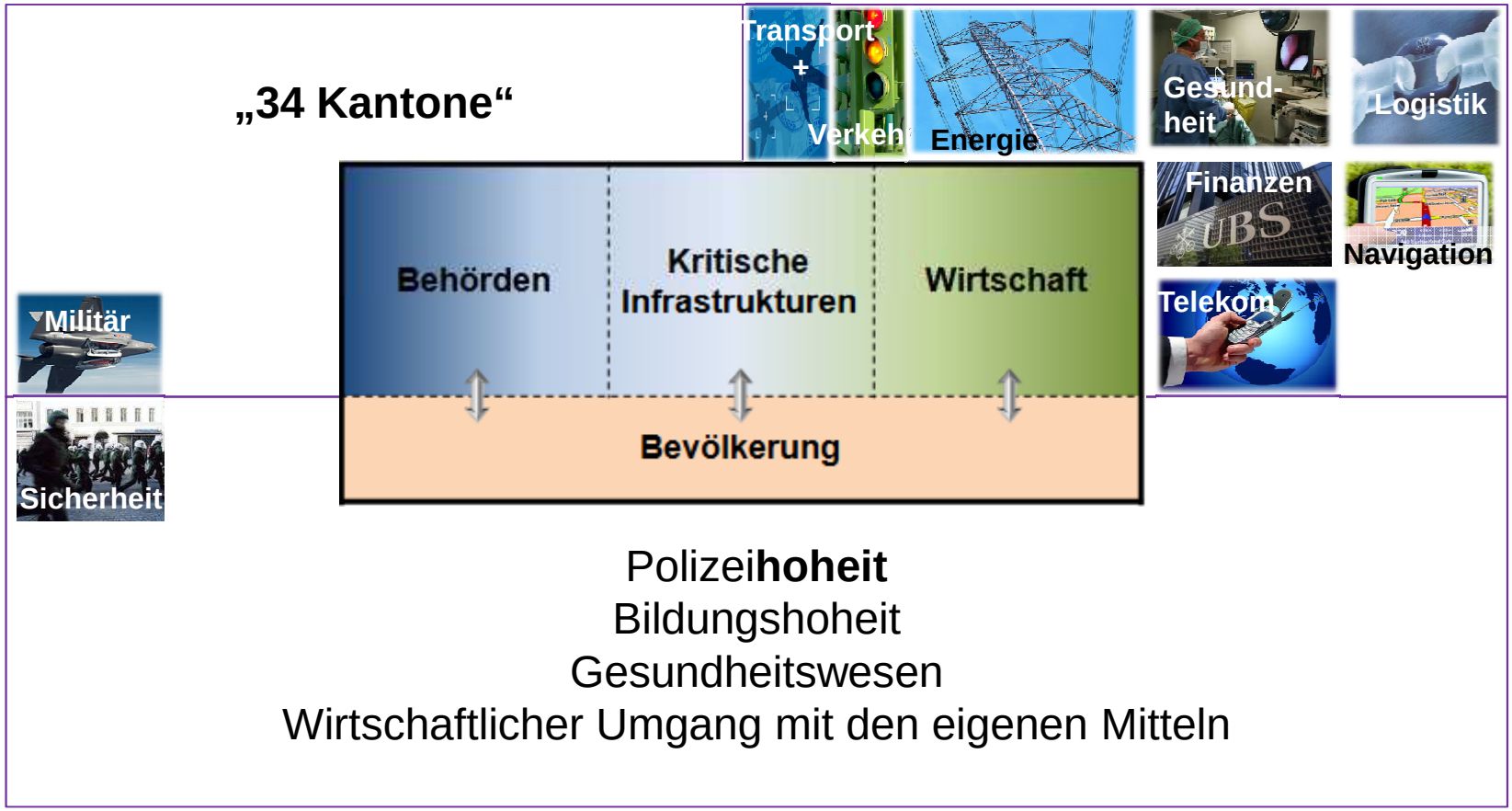
Klassifikation der Cyber-Risiken



Generalsekretariat VBS
Stv Projektleiter Cyber Defense

1

Anwendungsbereich



Polizei**hoheit**
Bildungshoheit
Gesundheitswesen
Wirtschaftlicher Umgang mit den eigenen Mitteln

Warum haben Cyberangriffe Erfolg?

Warum haben Cyberangriffe Erfolg?

1. **Das Ziel der Internet-Architektur war nie der Schutz** der persönlichen Privatsphäre.
2. **Keine Kontrolle / Steuerung** des Internets.
3. **Wachsende Komplexität** der Technologien, Dienstleistungen und Schnittstellen (z.B. Web 2, Datenbanken, VoIP,...).

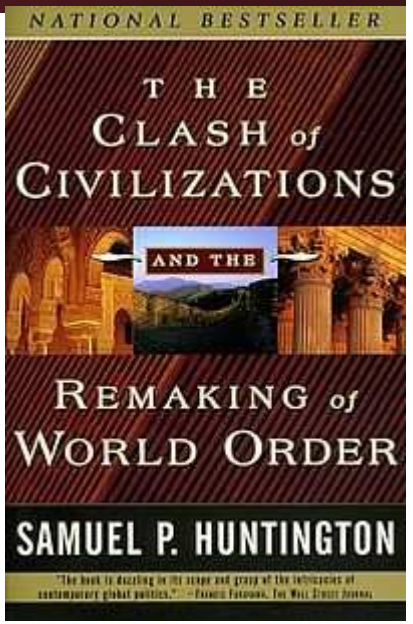
Jeder fünfte Mensch ist online

4. **Monokulturen**: „write once – run everywhere".
5. **Mangelnde Qualität**: „Wichtige Software" hat ca. 3 Fehler pro 1'000 Zeilen Code. Beispiel Windows XP mit 40 Millionen Zeilen
   ➔ 120'000 potentielle Schwachstellen (Vulnerabilities).
6. **Innovations-Druck** immer schneller neue Features bzw. Software auf den Markt zu bringen (der Anwender ist der Beta-Tester).
7. **Sicherheitsbewusstsein** nicht überall vorhanden
   ➔ Updates sind vorhanden, aber werden nicht installiert.

Gefechtsgrundsätze: ICT als Waffe

- Attraktives Kosten-Nutzen Verhältnis (TF: **Ökonomie der Kräfte**)
- Perfekte Überraschung / Täuschung (TF: **Überraschung**)
- Distanzen und Grenzen verschwinden
- Kaum Regeln → Straflosigkeit
- Medien und soziale Medien = Schlüsselakteure
- Vernetzung / Externalisierung & Zentralisierung / Virtualisierung →
  Wachsende (zun. strategische) Abhängigkeiten, Komplexität, Intransparenz
- Informationsumgebung = Waffenarsenal und “Kampfplatz”
- Schwachstelle „Mensch“ – auch als e-Everything-user
- Traditionelle Organisationen werden
  durch Information umgegangen
- Es gibt keinen 100%igen Schutz!

„The clash of Civilizations“



„Der Starke ist am mächtigsten allein“

(Gedanken-) **Freiheit**
Datenschutz
Globale Chancen

„Gemeinsam sind wir stark“

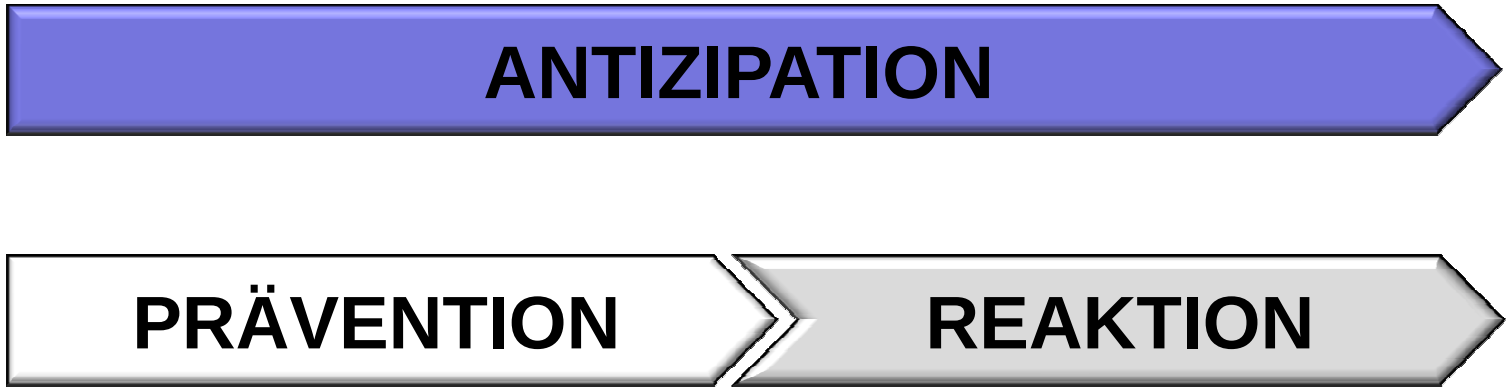
Schutz
„Ruhe und Ordnung“
Recht
Regulierung

„Après Moi, le Déluge!“

(Industrie-) **Spionage**
Erpressung v2.0 (DDoS)
„Proliferation“

Drei grundsätzliche Ziele

Das Richtige rechtzeitig wissen.



Die Anfälligkeit der Schweiz vor Cyber-Risiken reduzieren.

Konsequenzen von Cyber-Risiken beheben und entgegen wirken.

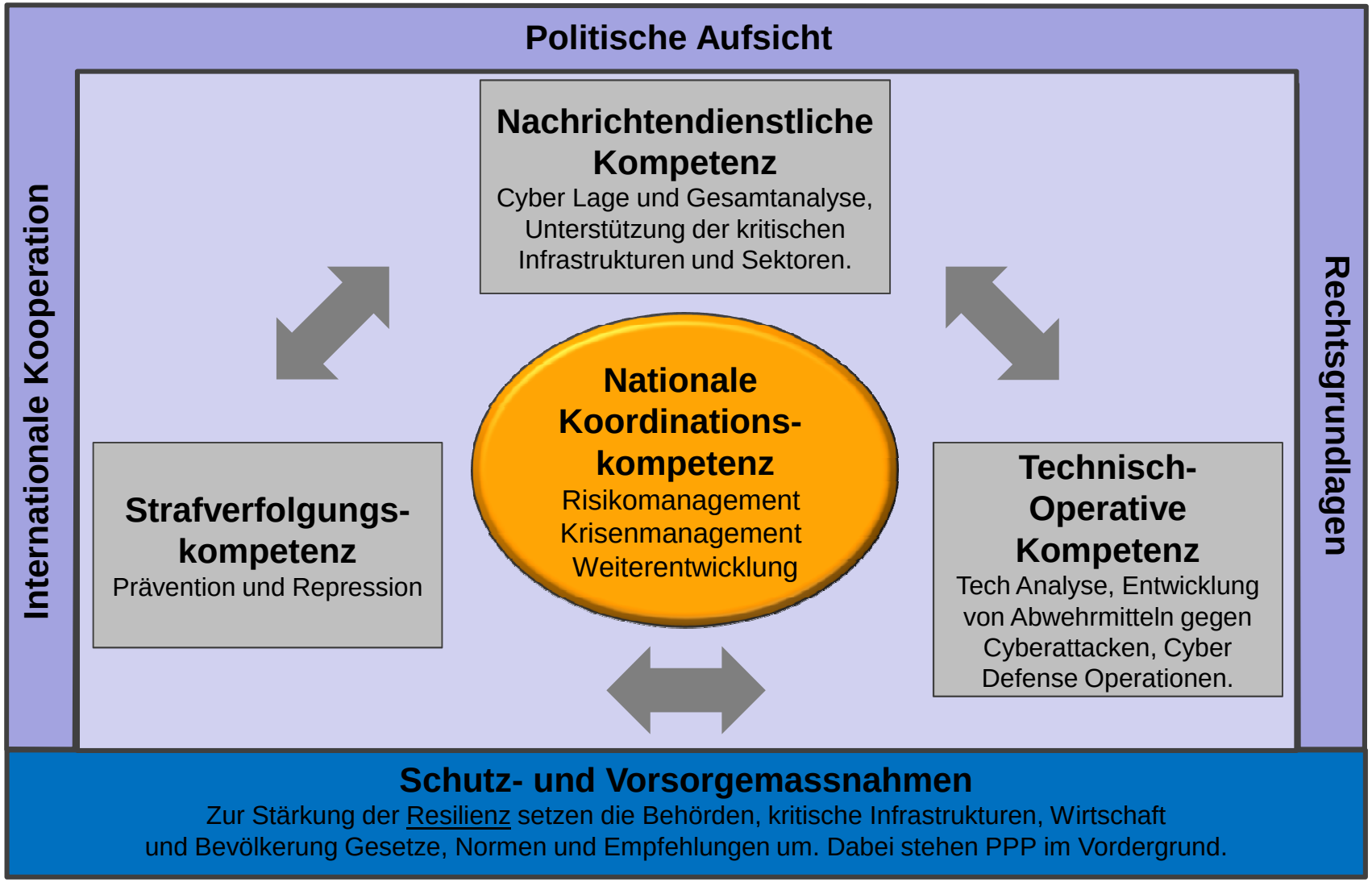
Sektoren-Treffen: z.B. Polizei

Ad hoc AG: Fünf Postulate

1. **Technische / Forensische Kompetenzzentren**
   - Unterstützung für komplizierte(re) Ermittlungen
   - Können virtuell bleiben
   - Zusammenarbeit mit Wirtschaft, Forschung & Lehre sowie Bundesstellen
2. **Ad hoc Arbeitsgruppen zu neuen Phänomenen**
   - Überkantonal, koordinierend
   - Greift auf Kompetenzzentren zurück
3. **Lagezentren / Lagebilder**
   - Quellen: Regionale Lagezentren, Lagebilder der Arbeitsgruppen und Kompetenzzentren, Lagebilder aus dem internationalen Interessenraum
   - Fernziel: Internationales Cybercrime-Observatorium
4. **Kompetenzregelung / Führung**
   - Wer macht was warum in einer ao Lage oder einer Krise?
5. **Grundschutz / Regulatoren**
   - ICT-Fitness
   - ICT-Grundschutzpflicht
   - Zulassungspflicht nach Sicherheitskriterien für ICT-Dienstleister

SPIK Präsentation 7. Nationale IT-Ermittler Tagung / 2011 Seite 10

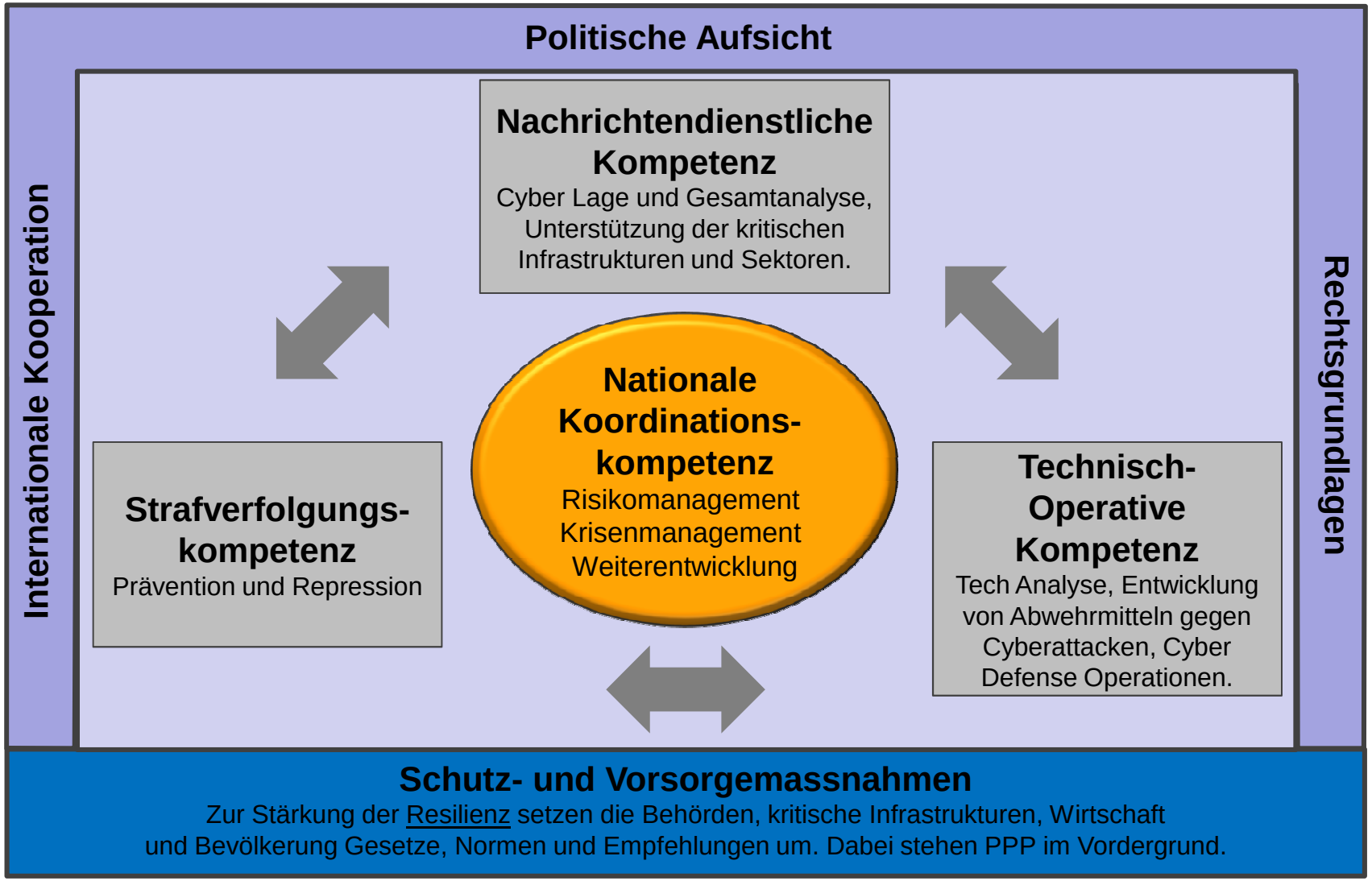
CYD-Konstrukt



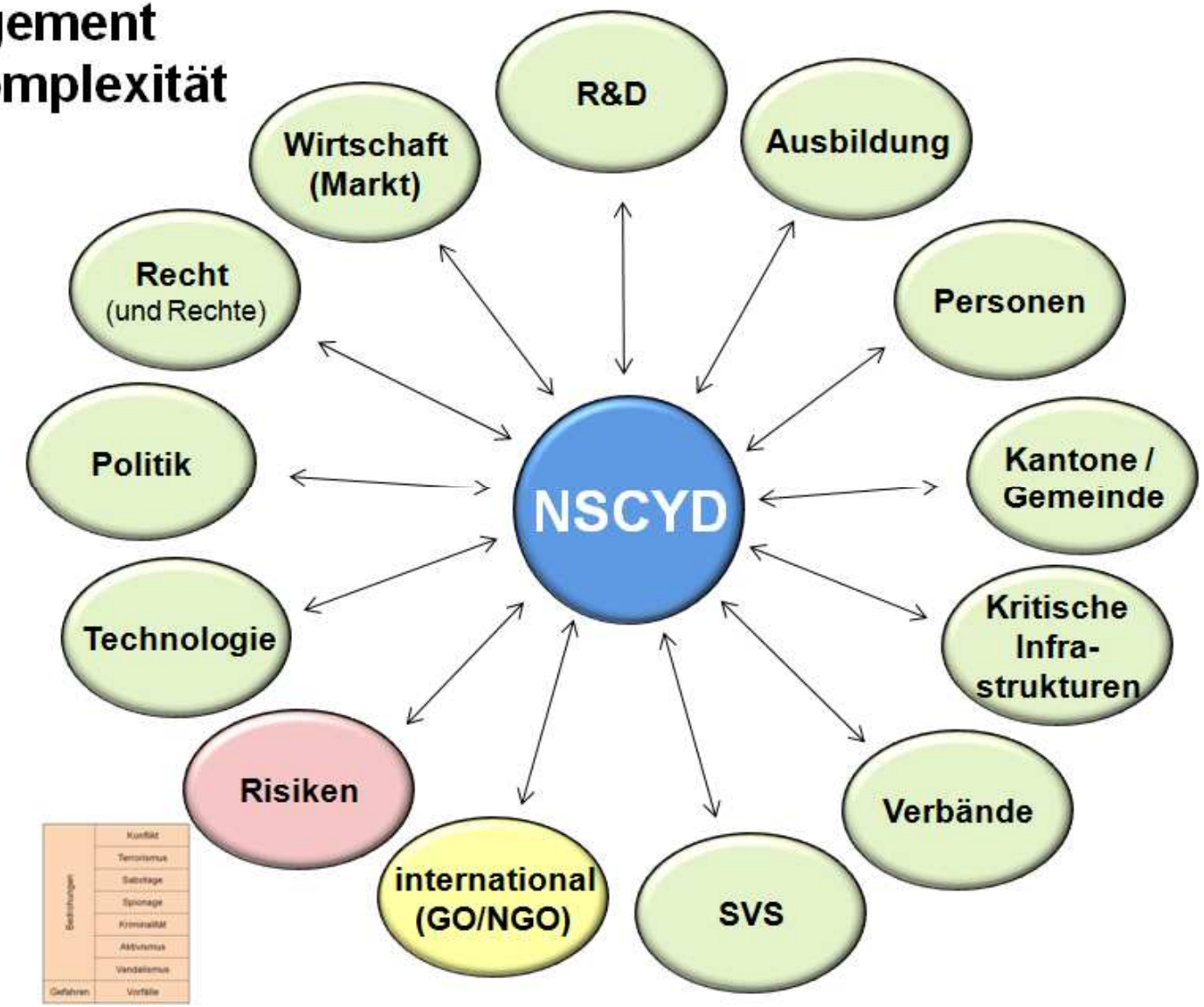
Strafverfolgung, Grundsätze

- Grundsätzlich Sache der Kantone
- Die Schnittstellen zwischen dem (eidgenössischen) Strafprozessrecht und dem (kantonalen) Polizeirecht sind vertieft zu untersuchen
- Das Recht der Polizei zum Zugriff auf Daten, die ein Verdächtiger auf ausländischen Servern gespeichert hat ist neu klar zu definieren.
- Zentrale Elemente der Strafverfolgungskompetenz im Rahmen von CYD sind :
  - die koordinierende Instanz wenn mehr als ein Kanton oder (mehr als) ein Kanton und ein ausländischer Staat betroffen sind sowie
  - die Koordination zwischen den Prozessen und Bedürfnissen der Strafverfolgung und der technischen Instanzen (maximale Beweissicherung!).

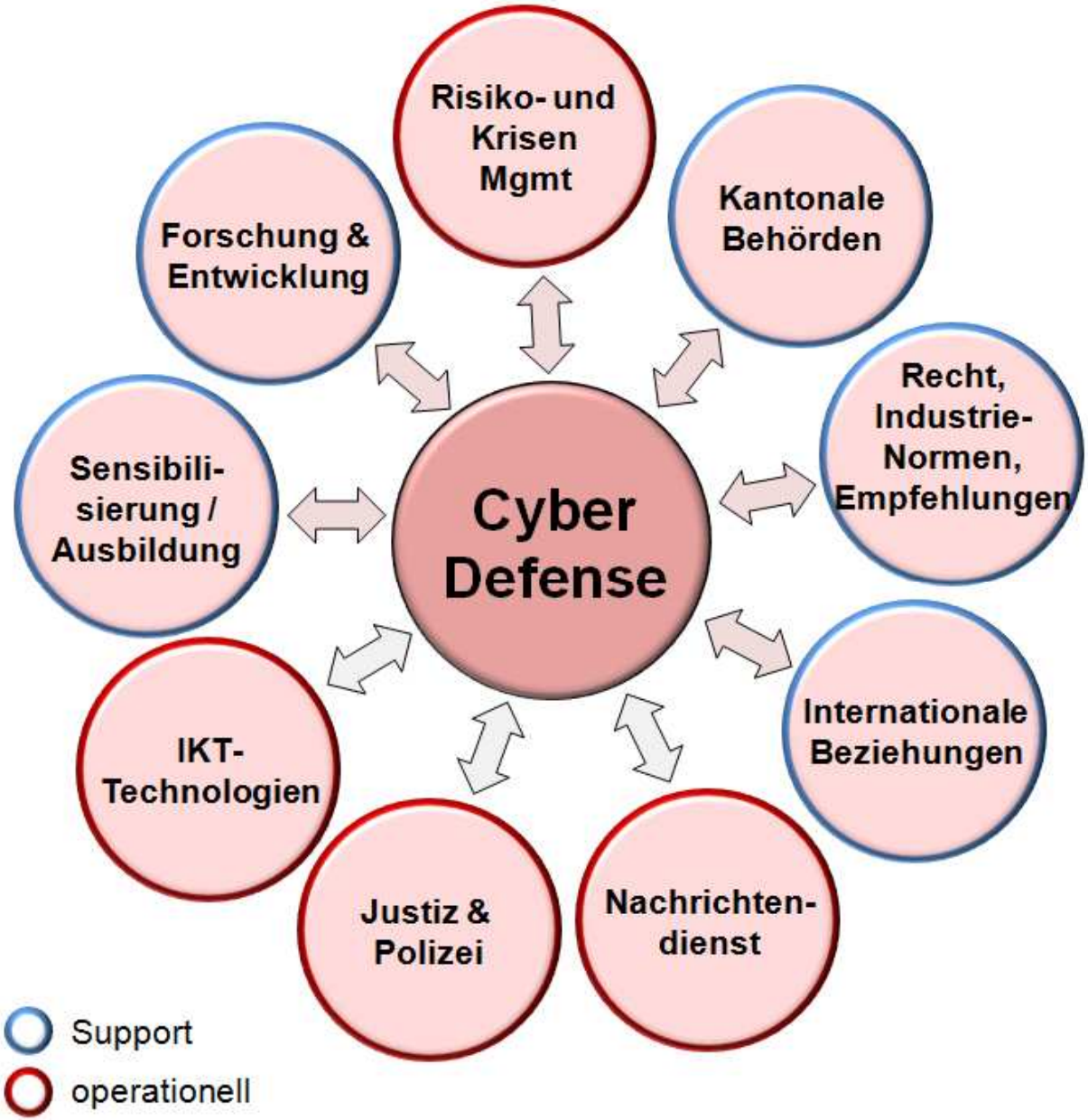
CYD-Konstrukt



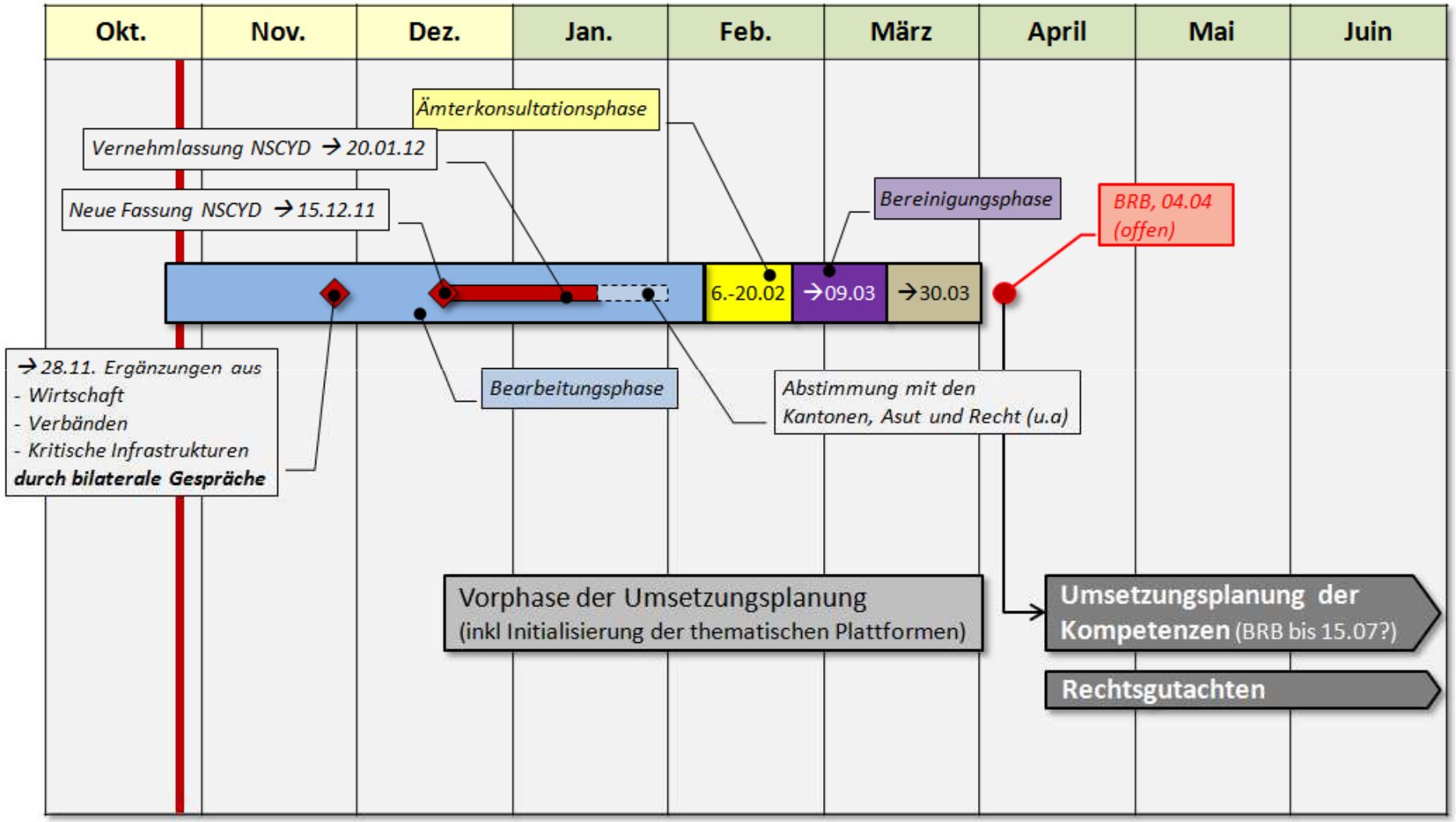
Management der Komplexität



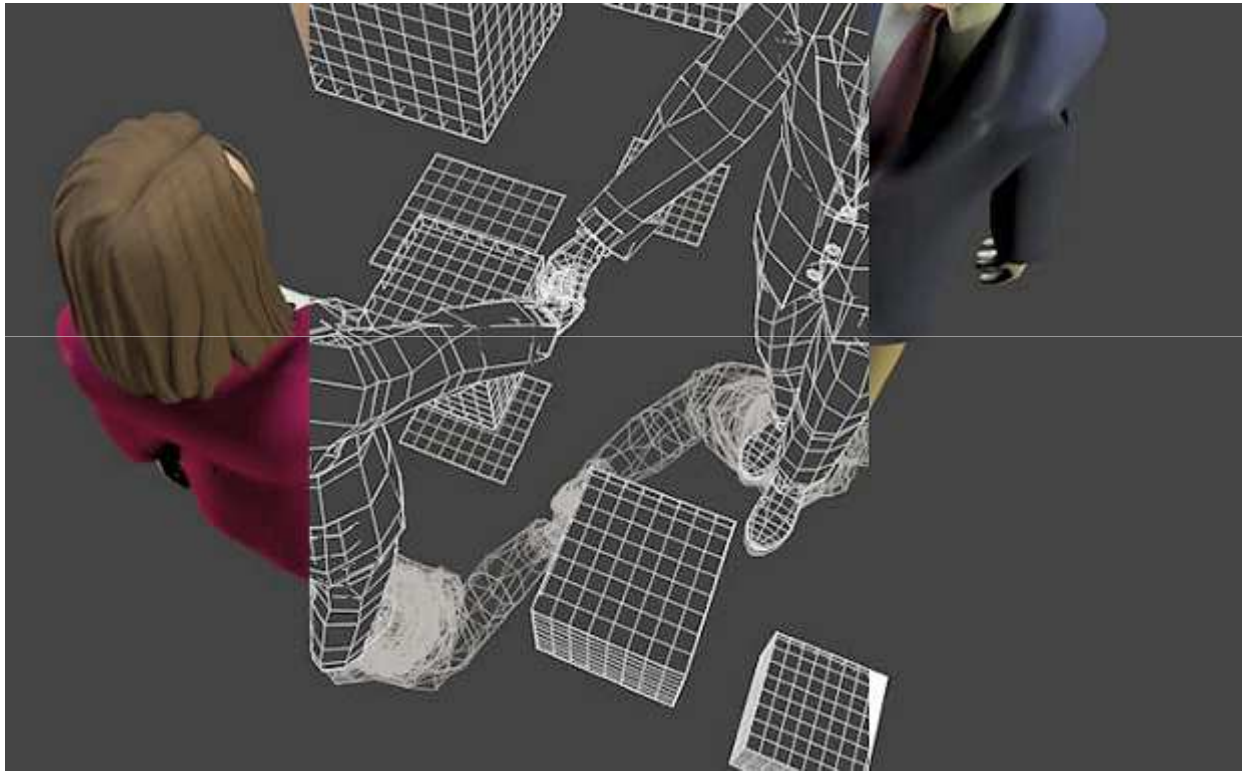
Thematische Plattformen



Allgmeiner Zeitplan



Vielen Dank für Ihre Aufmerksamkeit!



Information Security Society Switzerland

Die ISSS vernetzt Security Professionals

COMPASS Bier-Talk
3. November 2011, Jona

Dr. Thomas Dübendorfer
Präsident, ISSS

https://www.isss.ch/

Eindrücke der ISSS Berner Tagung 2010

Peter Fischer

Dr. Ursula Widmer

Stephan Klapproth

„Unbegrenzte Mobilität – Chancen und Risiken"

Nächste Berner Tagung:
24.11.2011 „Cloud Computing – Chancen und Risiken“

Vernetzung mit Security Professionals

Direkte Kontakte und Erfahrungsaustausch mit Security Professionals in der Schweiz auf diversen Fach- und Führungsebenen.

- **ISSS Events**
  - Drei grosse Fachtagungen pro Jahr
  - Zehn regionale Security Lunches pro Jahr
- **Task Forces** und **Special Interest Groups**
- **Privates XING-Forum mit ISSS-Badge**

Eindrücke vom ISSS Security Lunch «Security Theatre» 2010

Bruce Schneier

Weiterbildung zum Vorzugspreis

ISSS-Mitglieder erhalten grosszügige Rabatte von ca. 15% auf folgende Angebote:

- **Über 80 Security Kurse unserer Partner**
- **Über 20 Security Events pro Jahr**
- **Fachliteratur (u.a. digma, IT-Security)**

Weitere Angebote zum Vorzugspreis:

- **Software von Microsoft, Adobe etc. um 10% günstiger**
- **Kombimitgliedschaft SwissICT**

Wie werde ich Mitglied?

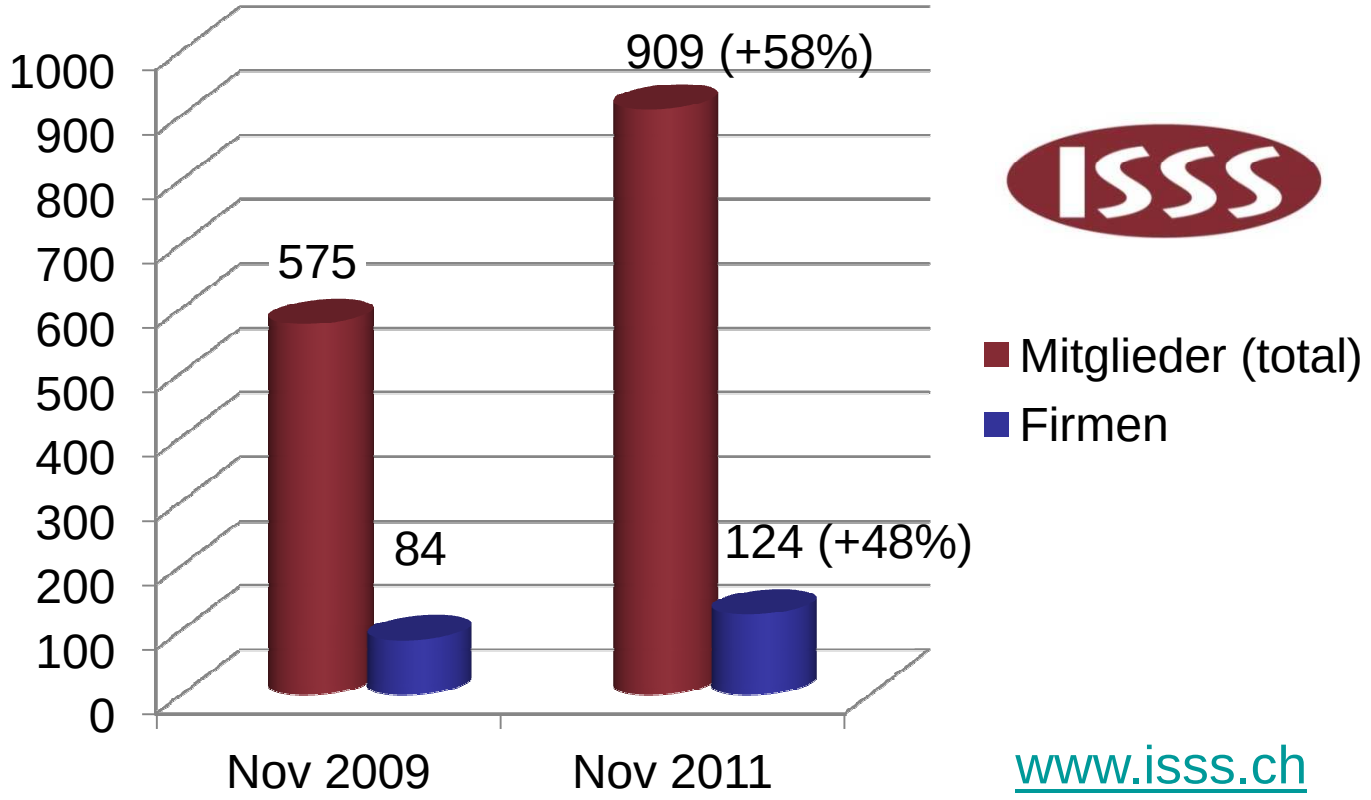
- **So einfach wie nie**
  - Heute Abend Visitenkarte an ISSS-Präsident Thomas Dübendorfer oder an Mark Saxer abgeben.
  - Oder: Auf www.isss.ch den Mitgliedsantrag ausfüllen.

- **Überzeugende Vorteile**
  - Mitgliedschaft bis Ende 2011 geschenkt
  - Überraschungsgeschenk im Welcome Package
  - Immer informiert zu ISSS und Partner Security Events
  - Sie profitieren von den attraktiven ISSS-Benefits

- **Minimale Kosten (Jahresgebühr 2012):**
  - CHF 20.- (Studierende), CHF 60.- (Einzelmitglieder), CHF 250.- (Firmen inkl. 5 Vertreter)

Mitgliederwachstum der ISSS

Die Information Security Society Switzerland vernetzt über 900 Security Professionals. Sind auch Sie dabei?



www.isss.ch

Vielen Dank für Ihre Aufmerksamkeit!

Mehr zur ISSS: https://www.isss.ch/

BY-NC-ND Rachel Young

BY Phil Parker

Danke an Compass Security AG für Organisation, Steaks & Bier!