



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Generalsekretariat VBS
Projekt Cyber Defense

Nationale Strategie Cyber Defense

Herbstveranstaltung STA, 03.11.2011, Bern

Dominik Schwerzmann, Projekt Cyber Defense



Thema

- Sicht aus dem Projekt Cyber Defense
- Methode der Strategieschöpfung
- Stand der Arbeiten



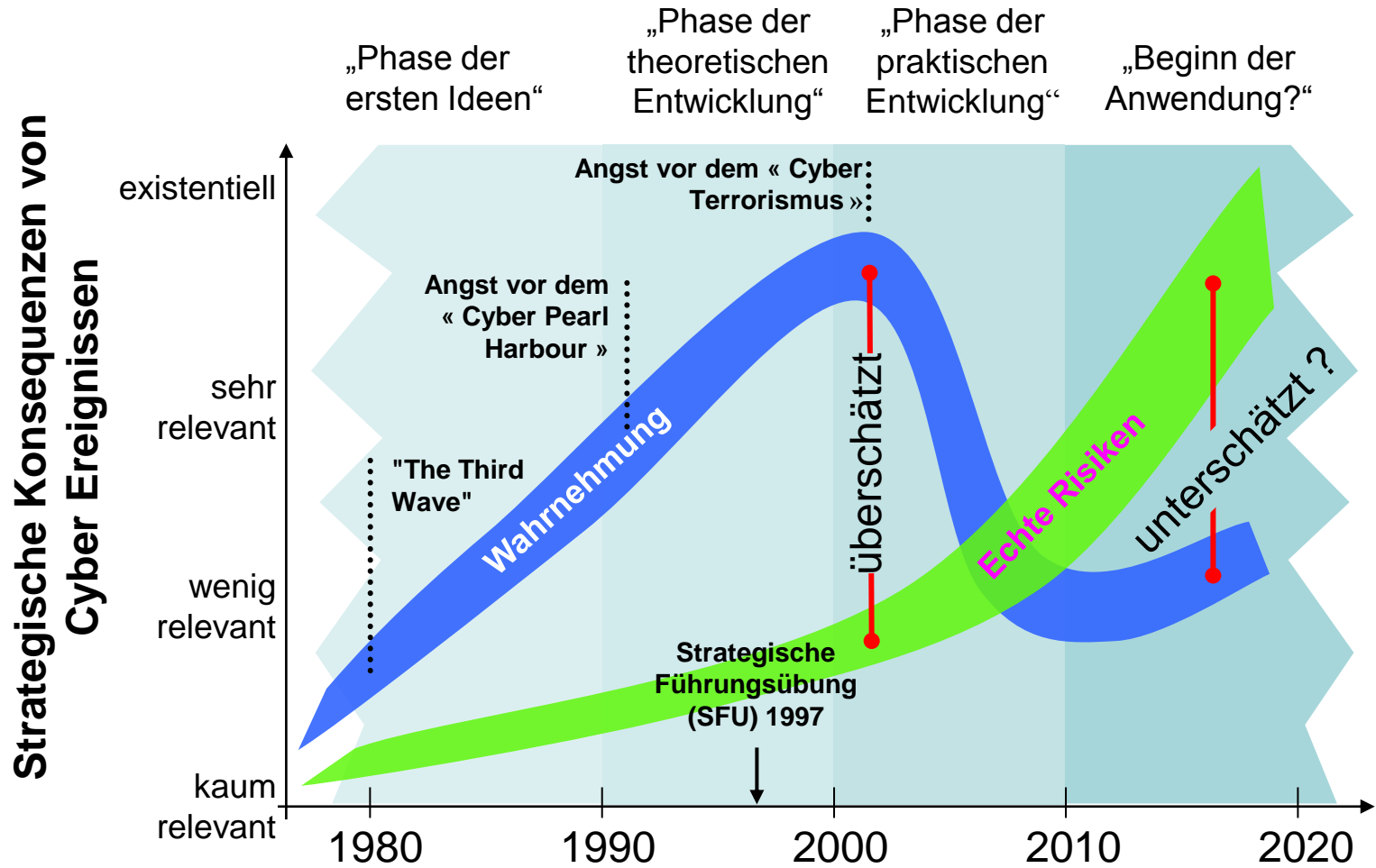
Umfeld

- Wahrnehmung Cyber-Risiko
- Politik
- Auftrag des Bundesrates
- Wer wird mit einbezogen?
- Anwendungsbereich
- Herausforderungen
- Sicherheitspolitische Situierung
- Angriffsmöglichkeiten
- Warum Cyber-Angriffe?





Wahrnehmung Cyber-Risiko





Politik



Geschäft Nr.	Titel
07.3509	Rechtssicherheit für Anbieter von Internetdienstleistungen
07.3510	Strafrechtliche Schritte gegen Cyberkriminalität
07.3689	Internetkriminalität
07.3750	Internetkriminalität. Aufstockung ...
07.3751	Kampf dem Terrorismus
08.3100	Nationale Strat. für die Bekämpfung Internetkriminalität
08.3101	Die Schweiz wirksamer gegen Cybercrime schützen
08.3618	Schaffung eines nationalen Kompetenzzentrums
08.418	Mehr Rechtssicherheit bei Netzwerkkriminalität
09.3266	Sicherheit des Wirtschaftstandortes Schweiz
09.4222	Rechtliche Verantwortlichkeit Internetprovider
10.3466	Effektivität und Effizienz im Bereich... Internetkriminalität
10.3541	Schutz vor Cyberangriffen
10.3625	Massnahmen gegen Cyberwar
10.3910	Leit- und Koordinationsstelle im Bereich der Cyber-Bedrohung
10.4020	MELANI für Alle
10.473	Effektivität und Effizienz im Bereich ... Internetkriminalität



Auftrag des Bundesrates

- Der Bundesrat hat das VBS beauftragt, eine Strategie gegen Cyber-Risiken zu erarbeiten. Sie muss Auskunft darüber geben:
 - wie die Bedrohungslage im Cyberspace aussieht,
 - wie der Bund und die Schweiz bzw. die Betreiber der Kritischen Infrastrukturen dagegen gerüstet sind,
 - wo die Mängel liegen und
 - wie diese Mängel am effektivsten und effizientesten zu beheben wären.





Wer wird mit einbezogen?



- **Wirtschaft:** als Nutzer und Versorger kritischer Infrastrukturen, als Dienstleister, Hersteller und Lieferanten sowie als Betreiber privater Forschungs- und Entwicklungseinrichtungen.



- **Betreiber kritischer Infrastrukturen:** als Erbringer von Leistungen mit einer übergeordneten und sicherheitsrelevanten öffentlichen/staatlichen Bedeutung.



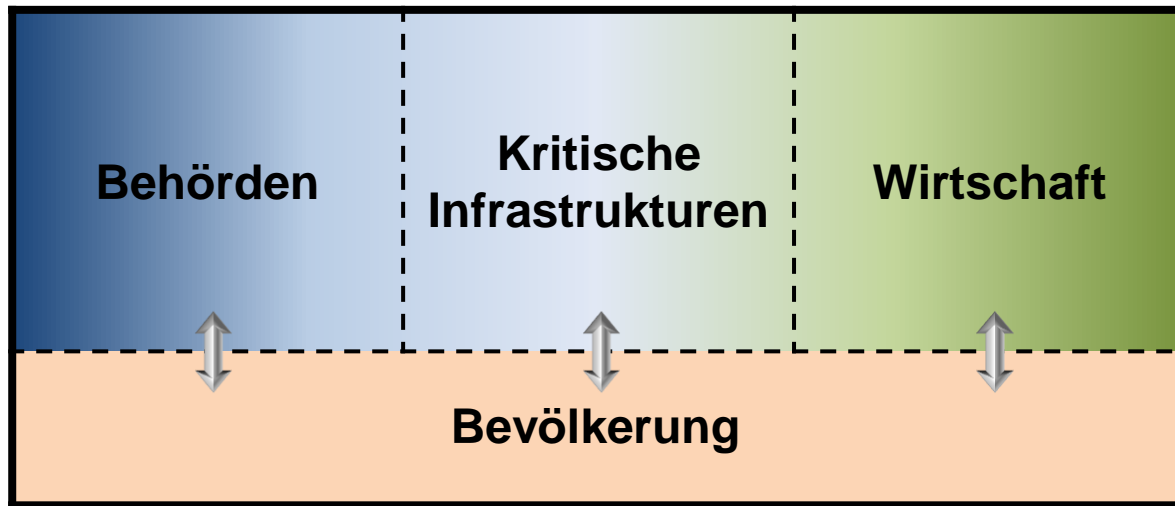
- **Behörden (Bund und Kantone):** als Betreiber und Nutzer kritischer Infrastrukturen, als Gesetzgeber und Richter, Exekutive (inkl. Strafvollzug), Aufsichtsbehörden und Dienstleister, als Risiko- und Krisenmanagementorgane sowie als Betreiber von Forschungs- und Entwicklungseinrichtungen.



- **Bevölkerung:** als Nutzer der Infrastrukturen und Dienstleistungen, als Betreiber und Anwender privater IKT Systeme und der IKT-Systeme am Arbeitsplatz.



Anwendungsbereich





Herausforderungen

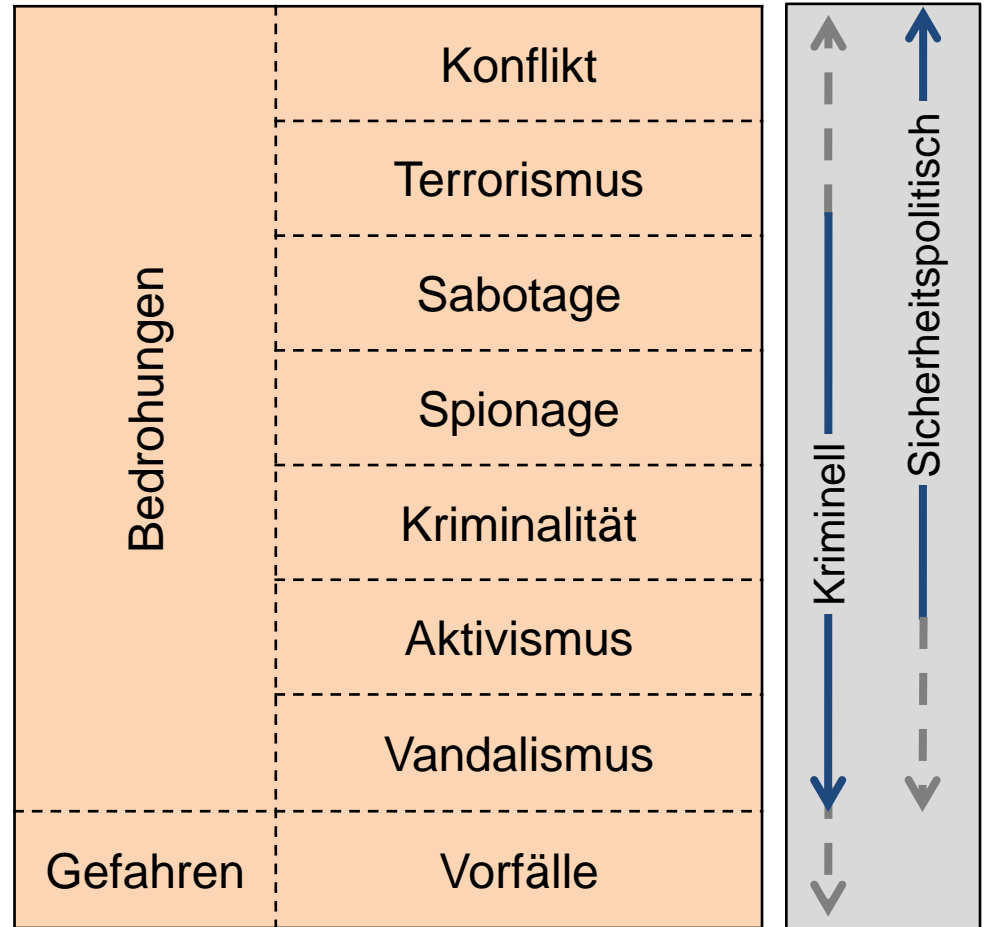
- Die „kleine“ Schweiz – Hightech/Finanzplatz/Universitäten
- Globalisierung, sieben Departemente, 26 Kantone und weitere Akteure
- Organisation dezentral versus zentral
- Kollision staatlicher Sicherheitsinteressen mit marktwirtschaftlichen Interessen und persönlichen Interessen
- richtige und falsche Anreize zum Handeln
- Verordnete versus freiwillige Zusammenarbeit
- Wer trägt die Verantwortung und die Kosten?
- Recht, vergleichbare/faire Normen
- Die neutrale Schweiz – Selbstverteidigung?





Sicherheitspolitische Situierung

- Sipol B 2010
- Risikoannahmen als „Messlatte“ für die zu entwickelnden Konzepte





Angriffsmöglichkeiten

- Angriffe worauf?
 - Kommunikationswege
 - Rechner
 - Daten

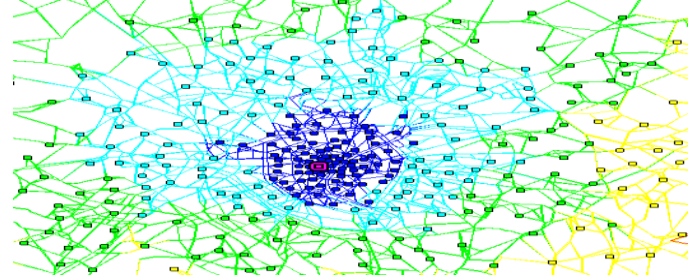
- Was ist bedroht?
 - Verfügbarkeit (online?)
 - Integrität (Verlässlichkeit)
 - Vertraulichkeit (Informations- und Datenschutz)
 - Authentizität (sichere Identität / Herkunft / Verbindlichkeit)

- Ereignisse durch: Fehlkonstruktion, Ermüdung, Unterlassung, Drittwirkung, höhere Gewalt (...)





Warum Cyber-Angriffe?



- Attraktives Kosten-Nutzen Verhältnis
- Ein Werkzeug, viele Einsatzmöglichkeiten
- Zunahme der Fähigkeiten
- Täuschung / Anonymität
- Distanzen und Grenzen überwinden
- laufend neue Chancen / Möglichkeiten
- Gelegenheit macht Diebe
- Zunahme der technischen Leistungsfähigkeit
- Zunahme der Nutzungsmöglichkeiten
- Wachsende Abhängigkeiten, Vernetzung, Komplexität, Intransparenz
- Schwachstelle Mensch
- Schwachstelle Sicherheitsmassnahmen
- Kein 100% Schutz möglich



Die nationale Strategie





Bestandesaufnahme

- Vorhandene Fähigkeiten **unzureichend** koordiniert und verstreut (keine kritische Grösse / Durchhaltefähigkeit)
- Konzeptionelle Antworten auf die „**normale Situation**“ und Cyber-Kriminalität ausgerichtet und keine SIPOL-Sicht
- Wenig Verständnis und Wissen über die Komplexität (Gesellschaft-Systeme); die meisten Konzepte befassen sich nur mit der eigentlichen **Computer-Sicherheit**
- Problem der **Sicherheitskultur** (Faktoren: Bewusstsein, Komfort, Konkurrenz, Mensch)



Was macht ein CYD-Dispositiv effektiv

- ständige Risikobeurteilung
- politische und rechtliche Grundlagen
- Anpassungs- und Durchhaltefähigkeit
- Vertrauensbasis
- Kooperation öffentlich / privat, national / international
- Fokus auf bedeutsame Verwundbarkeiten (die kritischen Infrastrukturen)
- fördern der Eigenverantwortung
- Koordination von Information und Fähigkeiten





Dokumentenstruktur der NSCYD

- Einleitung
- Bestandesaufnahme
 - Wirtschaft, Kritische Infrastrukturen, Behörden und Bevölkerung
 - manches wird getan, wenig ist koordiniert
- Soll / Ambition
 - Grundszenarien als Massstab
 - Rechtsgrundlagen, Robustheit, Anpassungsfähigkeit, Informationsaustausch, Kompetenzvermittlung, Eigenverantwortung, Subsidiarität



Der Massstab



Basisbedrohungen

Cyber-Bedrohungen, denen **die Schweiz täglich ausgesetzt** ist und die das Funktionieren von Wirtschaft, Gesellschaft und Institutionen **permanent und nachhaltig beeinträchtigen** können. Diese Bedrohungen nehmen laufend an Intensität und Komplexität zu und werden durch fahrlässiges Verhalten, fehlerhafte technische Entwicklungen und unzureichende Sicherheitskonzepte begünstigt. Die zunehmende Komplexität und Unübersichtlichkeit der Systeme und die damit einhergehenden Abhängigkeiten können auch bei vermeintlich kleineren Bedrohungen **unvorhersehbare Eskalationspotenziale** schaffen.



Existenzielle Bedrohung

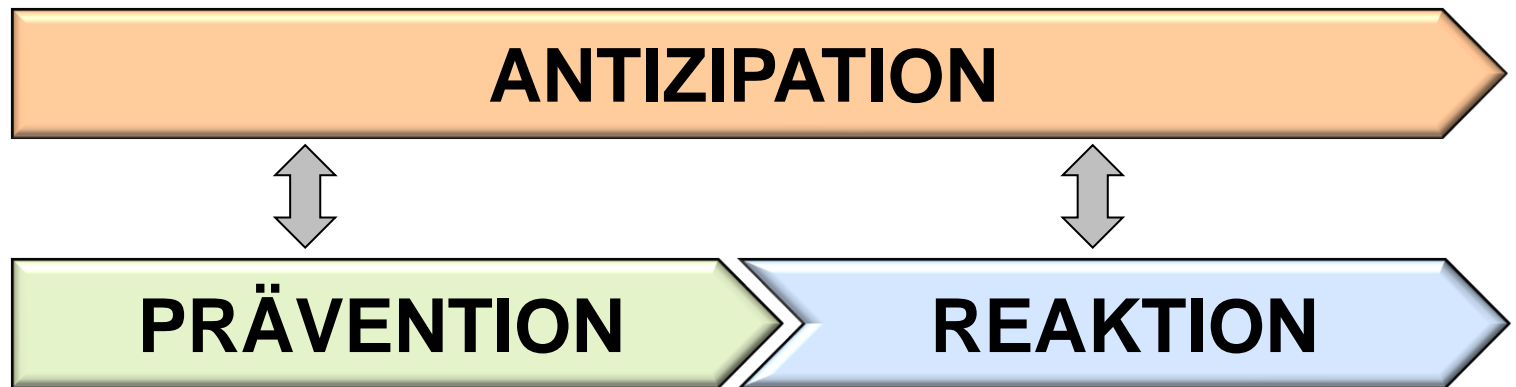
Cyber-Angriffe, die weniger wahrscheinlich sind, aufgrund ihrer Motivation und Intensität (u.a. Gleichzeitigkeit, Komplexität und Dauer, Anvisierung mehrerer Ziele, schwer kriminelle oder terroristische Absichten) aber **gravierende Schäden für das Gesamtsystem Schweiz verursachen** können. Bis heute sind Angriffe dieser Dimension unterblieben. Dennoch muss ein nationales Schutzkonzept auch derartigen Angriffen Rechnung tragen, weil sie in einem technologisch hochentwickelten Land wie der Schweiz nicht ausgeschlossen werden können und weil die **potenziellen Schäden enorm** sein könnten.



Fähigkeiten



**1. Das Richtige
rechtzeitig wissen.**



**2. Die Schweiz
resilienter gegen Cyber-
Risiken zu machen.**

**3. Konsequenzen von
Cyber-Risiken beheben
und entgegen wirken.**



Ansprechpartner



- Wirtschaft / KI
 - Finanzwesen
 - Telekommunikation
 - Energie
 - (...)
- Verbände (...)
 - asut
 - SPIK
 - SBVg
 - SKO
- Politik
 - (...)
- Bundesverwaltung
 - EDA
 - fedpol
 - NDB
 - RD (VBS, EJPD)
 - EDÖP
 - EFD (Risk Management)
 - ISB
- Kantone (...)
 - KKJPD
 - KKPKS
 - Hochschulen (UNIL, HEIG VD)



Erhebung vorhandener Schutzmassnahmen bezüglich Cyber-Risiken (→ IST-Zustand)

- Was wird **heute** zu Gunsten der Sicherheit getan?
- Welche Probleme, Mängel, Lücken usw. werden dabei festgestellt?





Erhebung künftig möglicher Schutzmassnahmen bezüglich Cyber-Risiken (→ SOLL-Zustand)

- Was soll **künftig** zusätzlich zu Gunsten der Sicherheit getan werden?
- Was können Bedingungen dazu sein (Umgebungsvariablen, Finanzierung, Rechtsgrundlagen, Zusammenarbeitsformen...)?
- Was sind die Erwartungen an die Nationale Strategie?



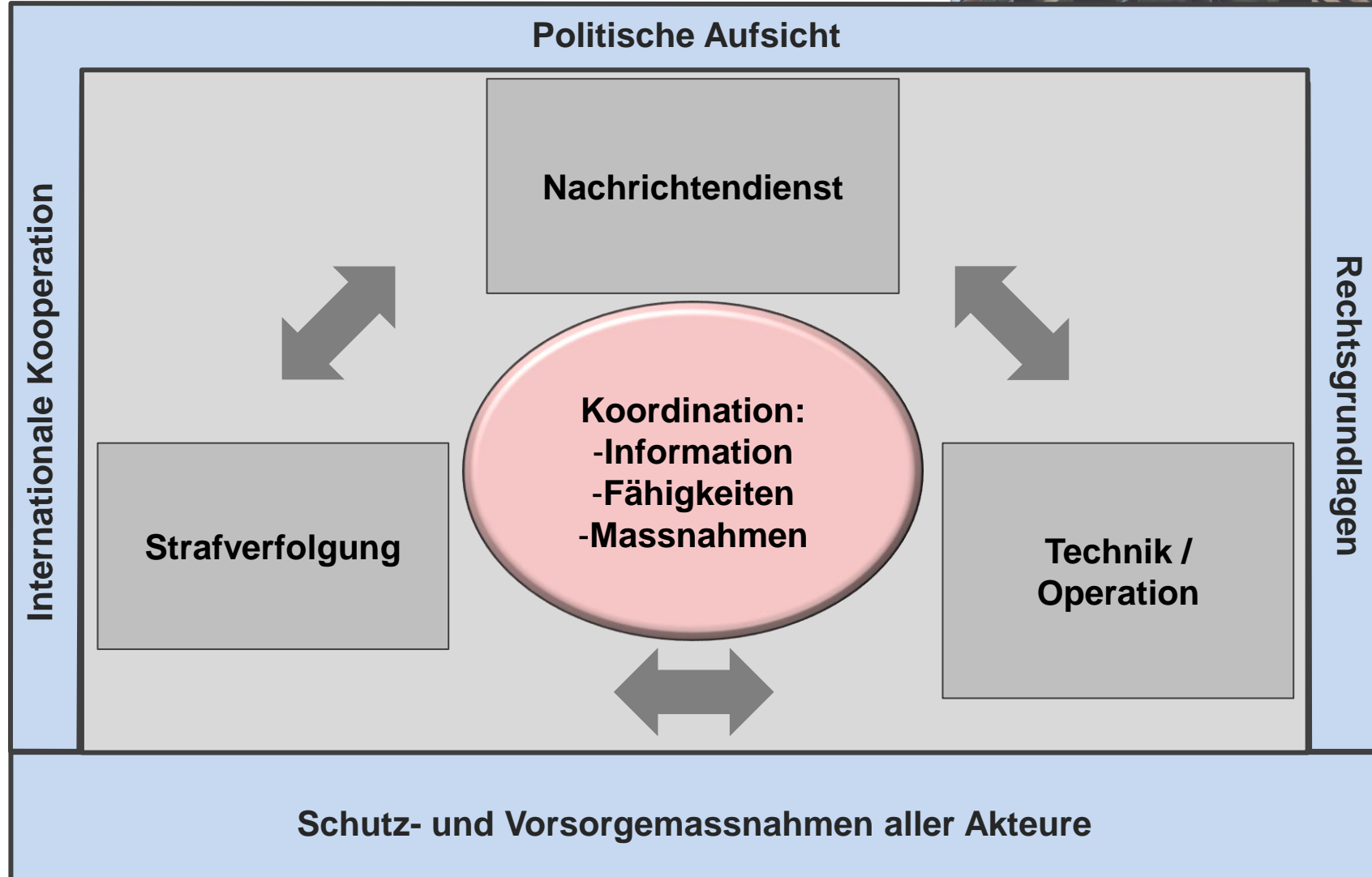
Erhebung der Rechtsgrundlagen

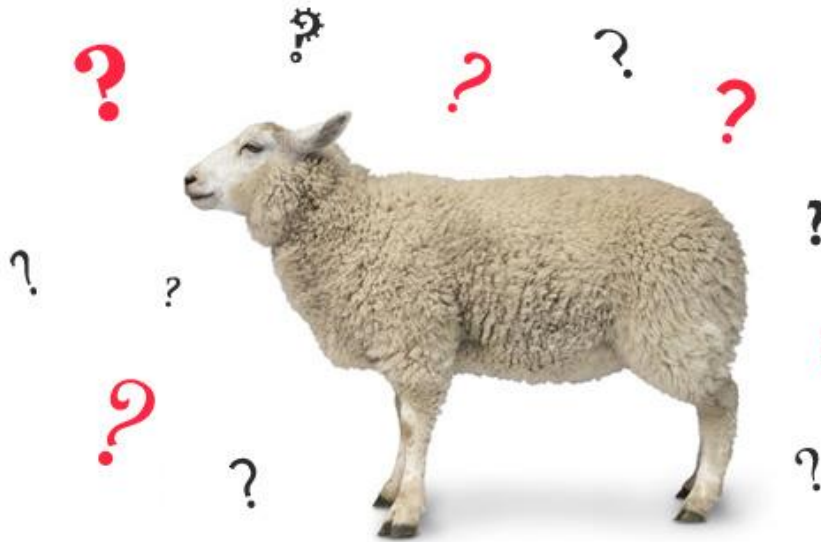
- Welche Rechtsgrundlagen haben wir heute?
- Welche Rechtsgrundlagen müssen in Zukunft angepasst werden?
- Was sind die Kriterien bei der Anpassung / Schaffung von Rechtsgrundlagen?
 - Informationsschutz (insb. Datenschutz)
 - Strafverfolgung
 - Nachrichtendienst (Gerichtsverwendbarkeit)





Woran muss gearbeitet werden?





KONTAKT:

Dominik Schwerzmann, lic. phil. | UZH

Projektteam Cyber Defense, Fachreferent

Eidg. Departement für Verteidigung,
Bevölkerungsschutz und Sport VBS
Generalsekretariat

Schermenwaldstrasse 13, CH-3063 Ittigen

Tel. +41 31 324 00 97

GSM +41 79 264 44 82

Fax +41 31 324 14 82

dominik.schwerzmann@gs-vbs.admin.ch

cyberdefense@gs-vbs.admin.ch