Cyber Security - aus der Sicht eines Bundesparlamentariers

- Konflikte finden zunehmend im Cyber-Raum statt.
- Die grösste Gefahr geht von professionell agierenden Akteuren wie kriminellen Organisationen, terroristischen Gruppen oder Staaten aus.
- Gefahrenpotenzial: Cyber-Kriminalität, Spionage, Manipulation von Information, gezielte Desinformation, Propaganda, Cybervandalismus und -terrorismus
- Exponiert sind Behörden, militärische Einrichtungen, kritische Infrastrukturen, Firmen, aber auch Privatpersonen.

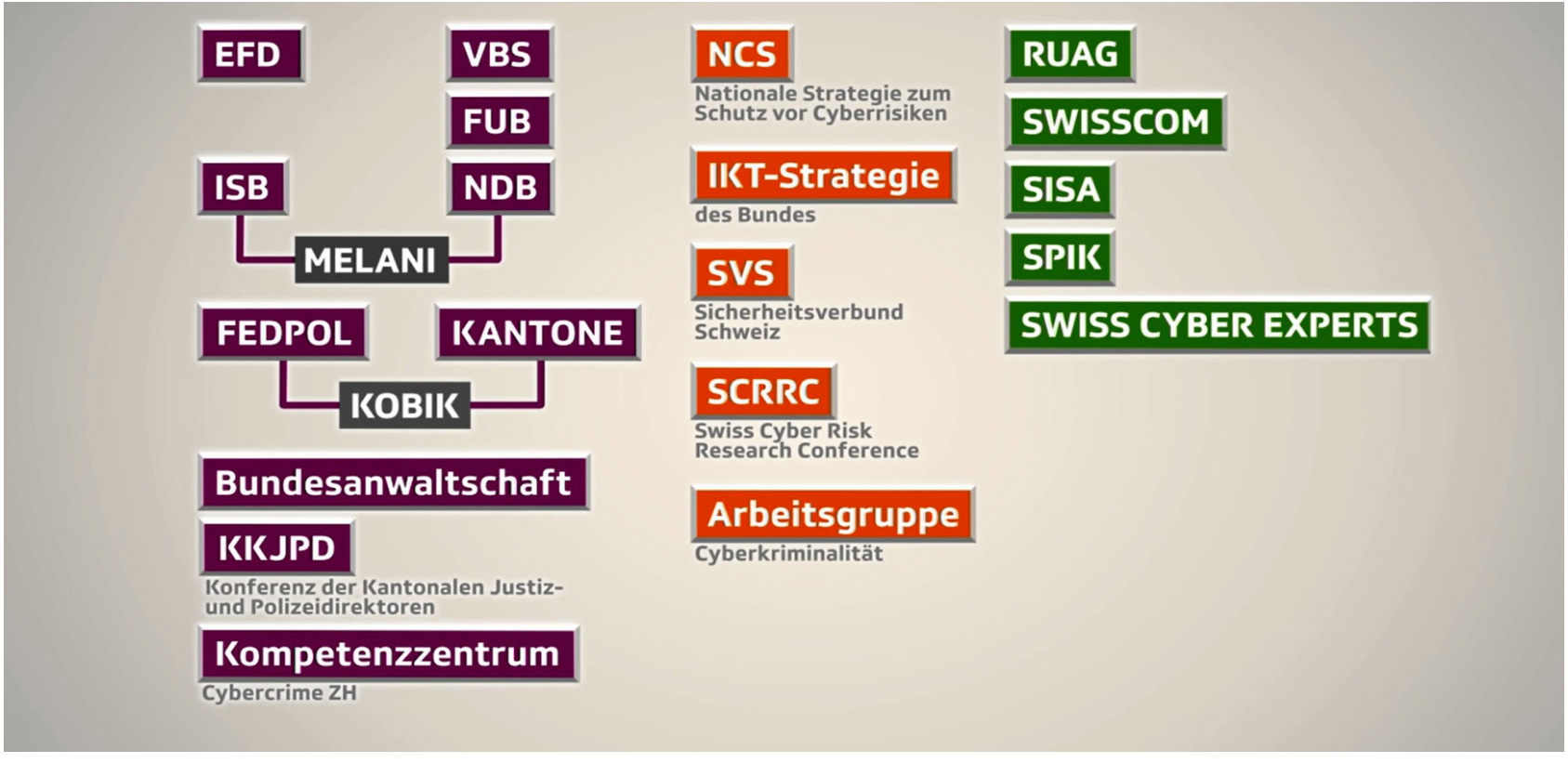
Zur Abwehr von Cyber-Angriffen braucht es Strukturen, Ressourcen und ein klares Gesamtkonzept.

Politische Forderungen

Cyber-Bedrohungen

- Militärische Cyberverteidigung
- Zivile Cybersicherheit (insbesondere Cyber-Kompetenzzentrum)
- Fachübergreifende Zusammenarbeit

Cyber hat in unserem Land bisher kein Gesicht



Was Bundesrats-Mitglieder sagten (1)

- Bundespräsidentin Doris Leuthard am 7.6.2017 im Ständerat (anlässlich der Beratung des Geschäftsberichtes des Bundesrates): **«Das Thema Cybersicherheit wurde vielleicht eine Zeitlang unterschätzt oder nicht auf Stufe Gesamtbundesrat eingehend diskutiert.»**
- Der Bundesrat in seiner Antwort vom 30.8.2017 auf meine Motion: **«Der Bundesrat teilt die Ansicht des Motionärs, dass die zur Sicherstellung der Cyber-Security notwendigen Kompetenzen zu verstärken und bundesweit zu koordinieren sind.»**

Was Bundesrats-Mitglieder sagten (2)

- Bundesrätin Doris Leuthard am 23.4.2018 (im Umfeld einer GPK-Sitzung): **«Die Schweiz hinkt bezüglich Cyber-Sicherheit im internationalen Vergleich hinterher – eine Aufrüstung ist unumgänglich.»**

- Bundesrat Guy Parmelin am 19.9.2018 anlässlich des 2. Forums «Cyber-Souveränität»: **«Ich glaube, dass die Schweiz gut aufgestellt ist. Sie hat die nötigen akademischen, institutionellen und wirtschaftlichen Voraussetzungen.»**

Was der Bundesrat konkret entschieden hat

- Er genehmigte im Dezember 2017 die **Strategie für den Schutz kritischer Infrastrukturen.**
- Er verabschiedete im April 2018 die neue **Strategie zum Schutz vor Cyberrisiken.**
- Er fällte im Juli 2018 Grundsatzentscheide zum Aufbau eines **Kompetenzzentrums Cybersicherheit** (Ansiedelung im Finanzdepartement, Leitung durch einen oder eine «Mr./Mrs. Cyber», Klärung der Details bis Ende 2018; u.a. Mandat des «Mister Cyber», Organisationsform, Budget und Personalbedarf).
- Er verabschiedete am 5. September 2018 die **Strategie Digitale Schweiz**.
- Er baut in der **Armee** gezielt Kompetenzen auf**: Cyber-Lehrgang** (wird ab 2019 zweimal jährlich durchgeführt).

NCS 2018 – 2022 (18.4.2018)

- Mit der **Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken 2018-2022** trägt der Bundesrat der gestiegenen Bedeutung von Cyber-Risiken Rechnung.
- Die Strategie zeigt auf, wie der Bund **gemeinsam mit der Wirtschaft, den Kantonen und den Hochschulen** den Cyber-Risiken begegnen will und welche Massnahmen dazu in den **nächsten fünf Jahren** umgesetzt werden sollen.

– ***7 Ziele, 10 Handlungsfelder, 29 Massnahmen***
– *Gestützt auf die Überprüfung der Strukturen im Bereich Cyber-Risiken wird der Bund gemeinsam mit den Kantonen, der Wirtschaft und den Hochschulen den **Umsetzungsplan zur NCS erarbeiten.***
– *Wer übernimmt für welche Massnahmen **die Verantwortung?** Welche **Mittel werden eingesetzt? Bis wann sollen welche Schritte abgeschlossen** sein?*

Was machen andere Staaten?

- Der Vergleich mit Europa fällt unterschiedlich aus: **Deutschland ist an der Spitze**, gefolgt von den skandinavischen Staaten und UK. Osteuropa und die südlichen Länder hinken hinten nach. **Die Schweiz ist etwa im Mittelfeld** anzusiedeln.
- Was die Welt anbelangt, stehen die VR China, die Russ. Föderation, aber auch die USA gut da. Vor allem **in der VR China sind Angriffe praktisch unmöglich**, weil die Regierung das gesamte Internet engmaschig kontrolliert, und zwar mit mehreren hunderttausend «Beamten».

Land	Militärische Mittel für CYBER	Zivile Mittel
DEU	Kdo Cyber und Informationsraum: 14'000 Soldaten, davon ca. 1'000 im Bereich Cyber-Schutz und Cyber-Operationen. Abschirmdienst (Bestand klassifiziert).	BSI (Bundesamt für Sicherheit in der Informationstechnik; ca. 550 FTE + 100 in Beschaffung gem. neuer Gesetz ITSEC) Abwehrzentrum: 15 FTE BND (Bundesnachrichtendienst; Bestand klassif.)
AUT	Cyber-Verteidigungszentrum (Abwehramt) : 40 FTE. Kommando Führungsunterstützung und Cyber-Defence: ca. 50 FTE.	Verschiedene Dienste (zB govCERT, CERT.at, Heeresnachrichtendienst, CERTs der kritischen Infrastrukturen. Cyber Security Steering Board und Cyber Security Plattform (Kooperation zwischen Regierung und Wirtschaft)
ESP	Mando conjunto de ciberdefensa: 300 FTE Ende 2018; jede Streikraft (Luft, Marine, Heer) verfügt zus. über einen eigenen CERT (=Cyber Emergency Response Team).	National Cyber Security Council (Prime Minister), Comité Especializado de Situación, Centro Criptológico Nacional, CCN (inkl.CCN.CERT)
FRA	COCYBER (Centre des opérations cyber): 3'200 FTE (1'000 wurden zus. geplant) mit bis 4'000 Personen (dafür 80 FTE um dieses zu unterstützen) in der "Réserve citoyenne" (Miliz).	ANSSI (Agence nationale de la sécurité des systèmes d'information): ca. 600 FTE +130 in einem Kompetenzzentrum Cyber-Defence). Direction générale de l'armement (DGA): 450 FTE in verschiedene Labors.
SUI	VBS (insgesamt) ca. 65 FTE (vorgesehen ca. 165 bis Ende 2020) + 400-600 Milizsoldaten bis Ende 2025. Diese Bestände wurden von der Motion 17.3507 legitimiert.	Ca. 20 FTE im EJPD (gegen Cyber-Kriminalität), 10 FTE im EFD (MELANI und Koordinationsstelle NCS), 2 FTE in der Abt. Sicherheitspolitik, 2 FTE im WBF und 2 FTE im UVEK).

Fazit (1)

- Der Handlungsbedarf ist unbestritten, speziell im Bereich der wirkungsvollen **Koordination und Zusammenarbeit**.
- Der Bund [Bundesverwaltung heisst 37 000 Mitarbeitende in 100 Ländern; 90 Bundesämter (BR Maurer am 7.12.2017 im NR)] hat **zu wenig Spezialisten**, die wirklich etwas verstehen von der Sache.
- Die Cyberangriffe nehmen immer mehr zu, aber die **Departemente haben noch keine Routine**, wie sie damit umgehen sollen; es wird deshalb noch zu viel improvisiert.

Fazit (2)

- Das **Thema «Cyber» muss beim Bund ein «Gesicht» erhalten**; das ist wichtig, gerade auch für die Öffentlichkeit.
- Der Kampf gegen und der Schutz vor Cyberrisiken ist eine **gemeinsame Verantwortung von Staat, Gesellschaft, Wirtschaft und Wissenschaft.**
- Die Landesregierung erhielt von uns **klare politische Aufträge**. Diese sind nun umzusetzen, denn die technische Entwicklung ist bedeutend schneller als die politischen Entscheide. Unsere Cyber-Abwehr braucht **mehr finanzielle und personelle Ressourcen**.

Das Parlament wird die Umsetzung hartnäckig begleiten – Halbheiten dulden wir nicht!