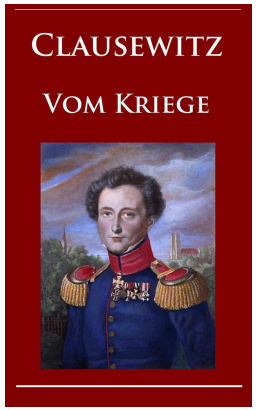
Generalversammlung eCH 2023



Datensouveränität und Standardisierung

Prof. Jean-Pierre Hubaux, EPFL

Gründer und Akademischer Direktor, EPFL Center for Digital Trust

Mitgründer, Tune Insight SA

jean-pierre.hubaux@epfl.ch

Bern, 3. Mai 2023

Datensouveränität

Per Definition: Schweizer Daten unterliegen dem Schweizer Recht

Wie kann dies erreicht werden?

- Sich selbst schützen → Cybersecurity
- Einsatz der richtigen Tools → Kryptographie
- Datenverwaltung → Richtige Nutzung der Cloud
- Vorbereitung der Menschen verbessern → Weiterbildung
- …

Konkretes Beispiel: Cyberangriffe gegen die EPFL

Tagesdurchschnitt:

1.5 Mio
opportunistic scans

>1 M
E-Mails; nur 8% sind sauber und werden an die Mailboxen der EPFL weitergeleitet

5'000
gezielte Angriffe

Opportunistc scan: Versuch, die auf einem exponierten Rechner laufenden Dienste aufzulisten (auf TCP/IP-Ebene, nicht auf Anwendungsebene)

Gezielter Angriff: Versuch, eine bekannte Sicherheitslücke auf Anwendungsebene auszunutzen (z. B. in WordPress)

Cybersicherheit auf einer Folie

- Historische Doktrin: Schutz von Aussen (misstraue dem Draussen, vertraue dem Drinnen)
  - Firewall

Generated by DALL-E

- Heutige Doktrin: Schutz von Aussen **und** von Innen
  - **Defense-in-depth**
  - Micro-segmentation
  - Least privilege
  - Zero trust (Jargon des US National Institute of Standards and Technology)

Micro-segmentation im physischen Umfeld, um seitwärts Bewegeung (lateral moves) zu verhindern

Wie Troja von den Griechen besiegt wurde

“Zieht die Statue zu ihrem Haus”, riefen sie, “und betet zur Erhabenheit der Göttin.”
Wir durchbrachen die Mauer und öffneten die Verteidigung der Stadt. *Buch II der Aeneis*

Das Trojanische Pferd
V.a. beschrieben in Virgils *Aeneis* (29 bis 19 v. Chr.)

Kryptographie:
Eine grosse Erfolgsgeschichte der Standardisierung

- *Kryptographie: “Geheimschrift”*

- Vertraulichkeit
  - Daten sind nur mit dem korrekten Schlüssel zugänglich

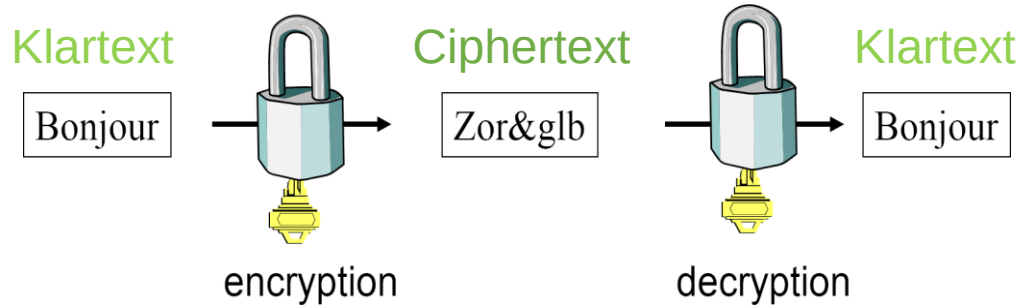
- Integrität
  - Jegliche Veränderung der Daten kann aufgespürt werden

- Authentifizierung
  - Der Autor/Absender einer Nachricht kann eindeutig und als einziger identifiziert werden

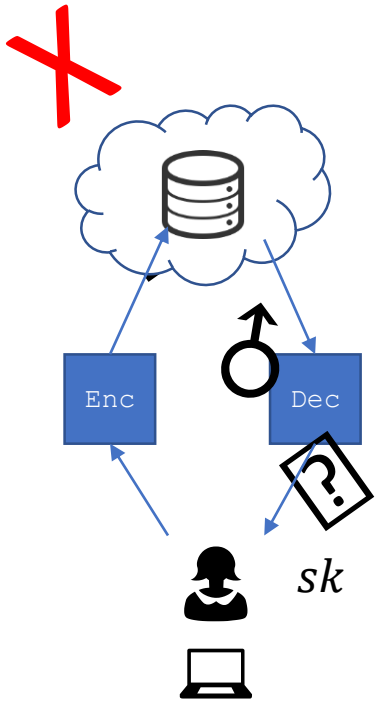
- Non-Repudiation
  - Der Autor/Absender einer Nachricht kann diese nicht verleugnen (digitale Signaturen)

Verschlüsselungstechniken: Symmetrische Verschlüsselung

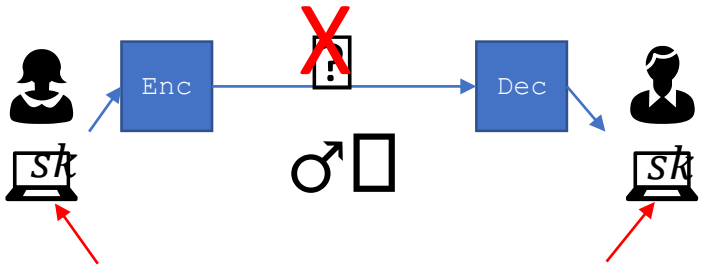
Derselbe Schlüssel wird für die Ver- und Entschlüsselung verwendet.



Im Ruhezustand (Speicherung)



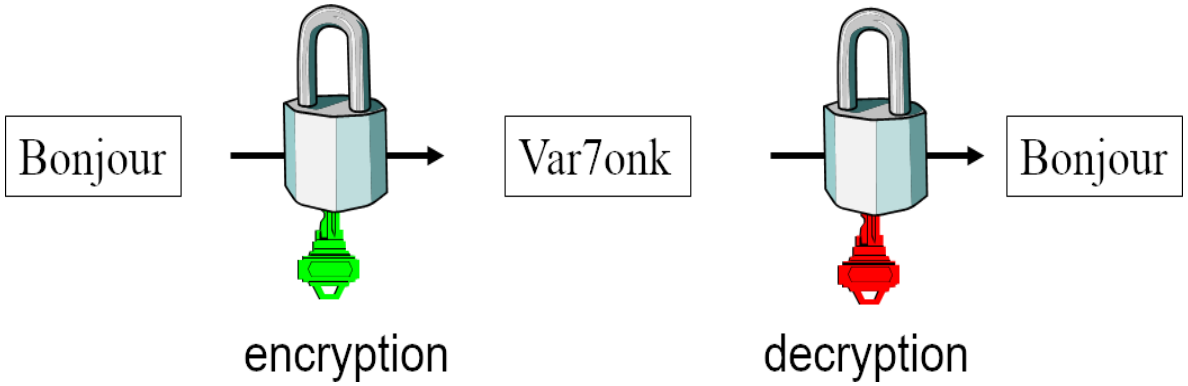
Im Transit (Übermittlung)



sk muss irgendwie umgetauscht werden

Verschlüsselungstechniken: Asymmetrische Verschlüsselung

Löst das Problem sich auf einen zuvor geteilten symmetrischen Sicherheitsschlüssel einigen zu müssen und zwar durch die Nutzung einen öffentlichen und privaten Schlüsselpaars.

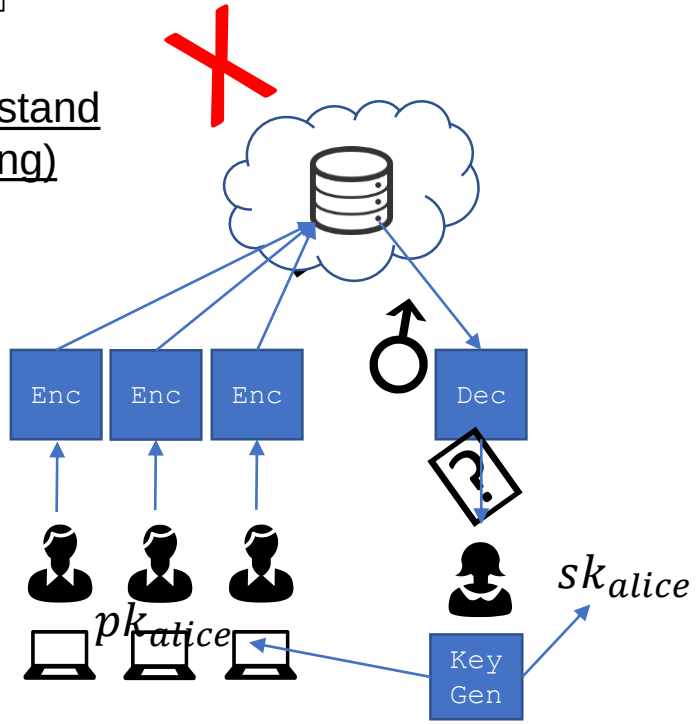


Verschlüsselung mit dem öffentlichen Schlüssel (*pk*)

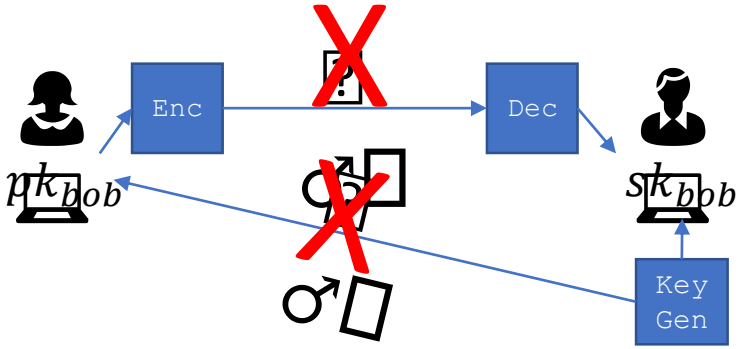
stellt sicher, dass nur der private Schlüssel (*sk*)

zur Entschlüsselung genutzt werden kann.

Im Ruhezustand (Speicherung)



Im Transit (Übermittlung)



Der Schutz von Daten im Ruhezustand und im Transit

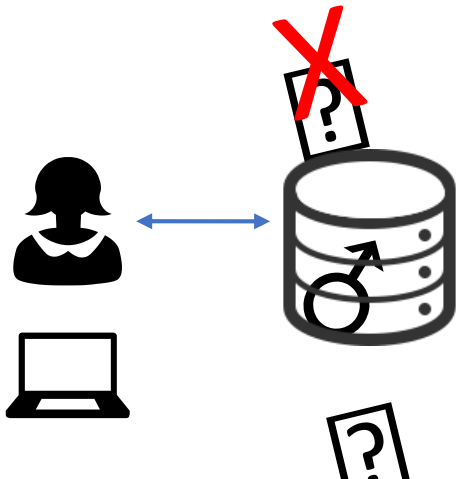
- Kryptographie wird verwendet, um **Datensicherheit** herzustellen.
- Alle geläufigen Verschlüsselungsalgorithmen sind standardisiert.

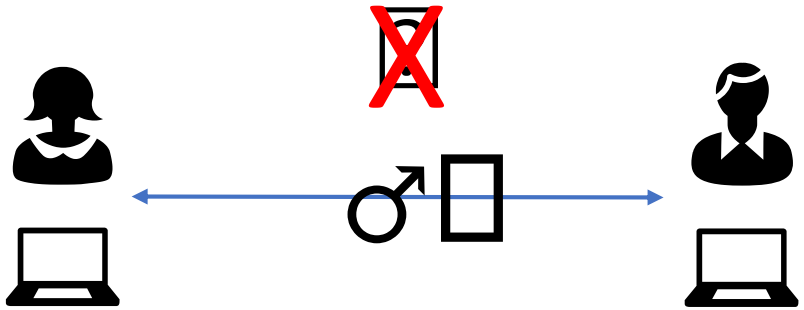
  - Vertraulichkeit
    - ✓ Verschlüsselung
  - Integrität & Nachweisbarkeit
    - ✓ Hash-and-sign

Reicht das aus?

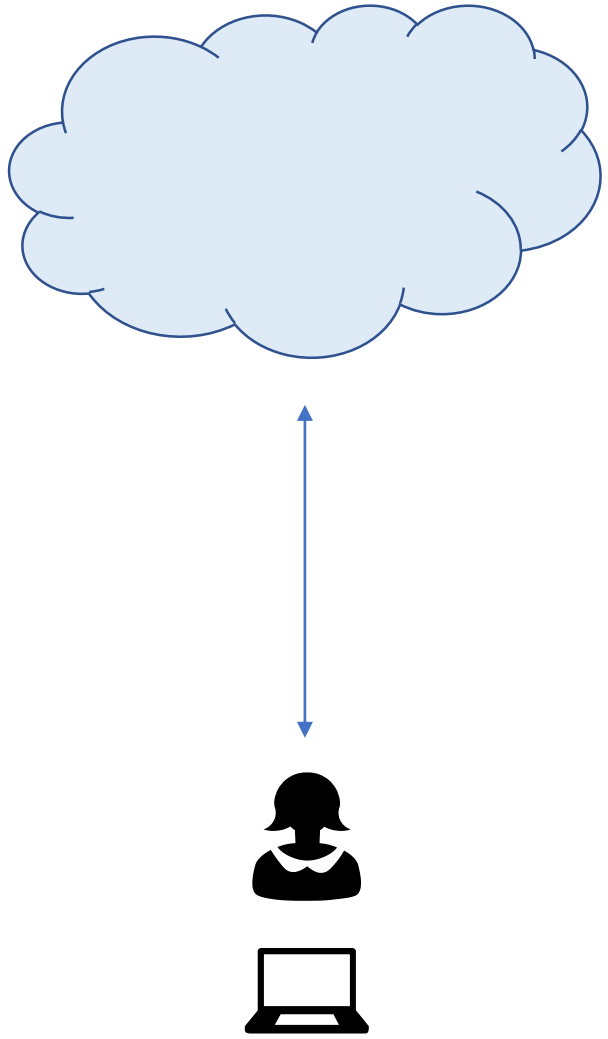
Nein! Daten müssen auch während der Verarbeitung geschützt werden! (for computation)

…im Ruhezustand und ***im Transit***



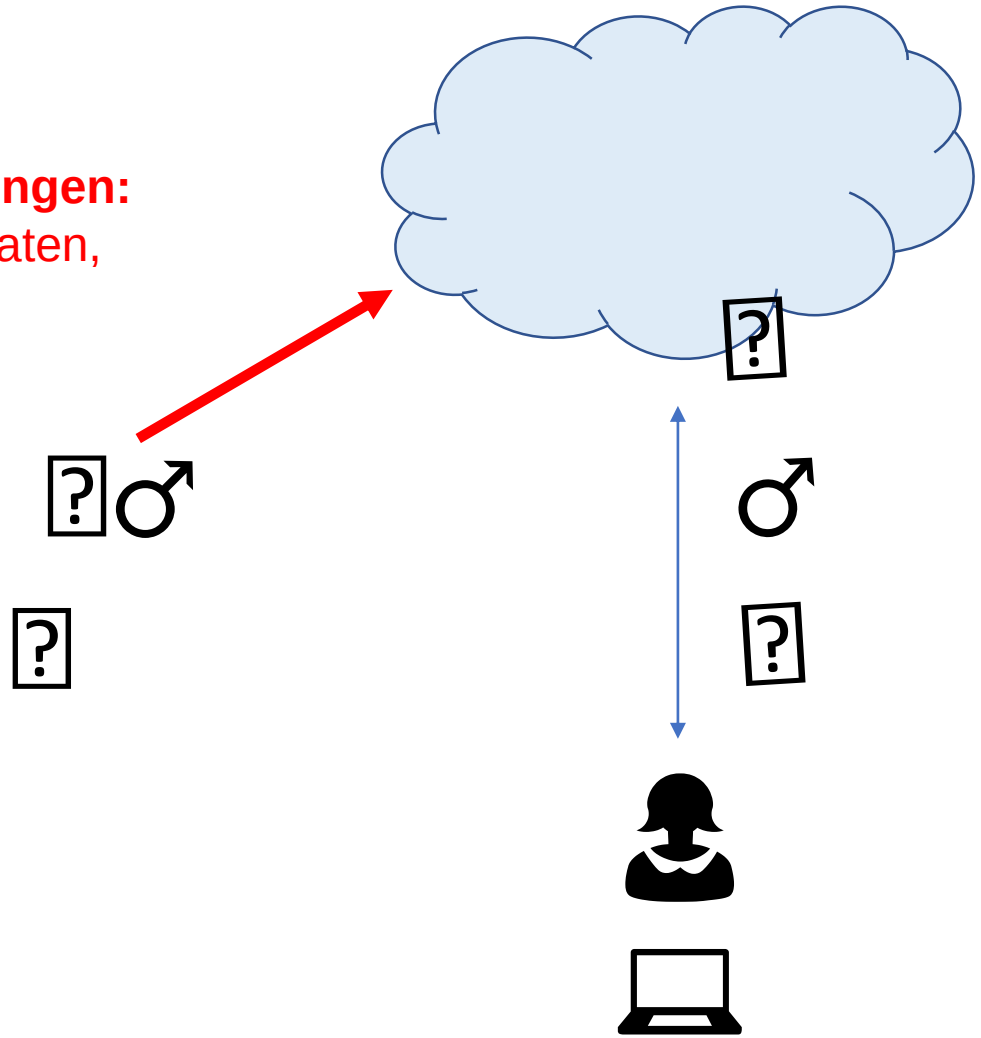


Cloud Computing



Sicherheits- und Privacy Herausforderungen des Cloud Computings

Sicherheitsbedrohungen:
Hacking von Nutzerdaten,
Aktivitätsmonitoring,
denial of service

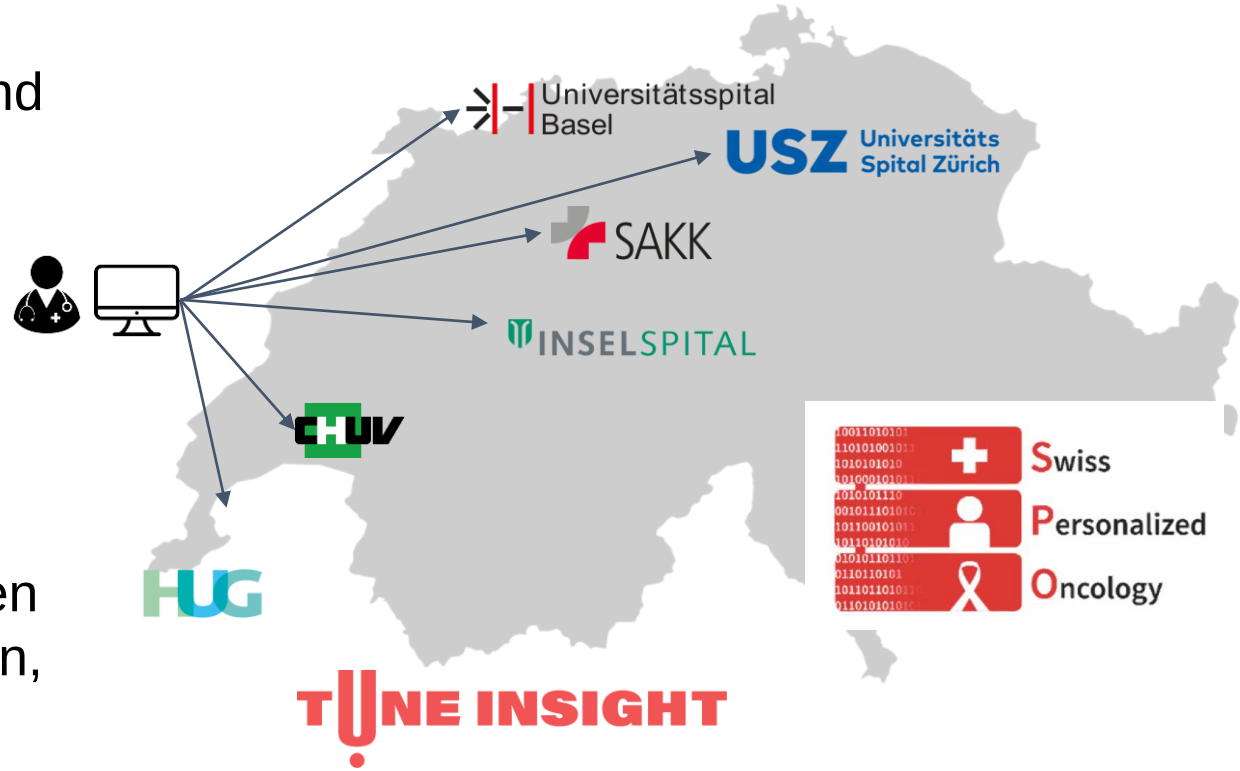


Privacy Bedrohungen:
Der Cloudbetreiber nutzt seinen Zugang zu Nutzerdaten aus, z.B. zu politischen oder wirtschaftlichen Zwecken

Das Bundesamt für Informatik hat eine breite Konsultation zur vorgeschlagenen Cloud Strategy des Bundes begonnen.

Wir haben eine Lösung für das Problem der datenschutzfreundlichen föderierten Analytise entwickelt

- Wir sind in der Lage Daten zu verarbeiten und sie gleichzeitig dezentral zu halten
- Tune Insight nutzt die Werkzeuge der (homomorphen) Kryptographie, um dies zu erreichen
- Die Lösung funktioniert im großen Masstab – und das ohne Präzisionsverlust
- Dies eröffnet beispiellose Möglichkeiten für datenschutzbewusste Datenkooperationen im Gesundheitswesen und darüber hinaus
- Wir haben die Lösung auch in anderen vertikalen Anwendungsbereichen eingesetzt (Finanzwesen, Versicherungsektor, Cybersicherheit,…)



Nationale Cyberstrategie

- Brandneu! (April 2023)
- Liste der Hauptbedrohungen
- 17 konkrete Massnahmen, z.B.:
  - Bildung, Forschung, Innovation
  - Analyse von Trends
  - Krisenmanagement
  - Internationale Regeln im Cyberraum
  - …

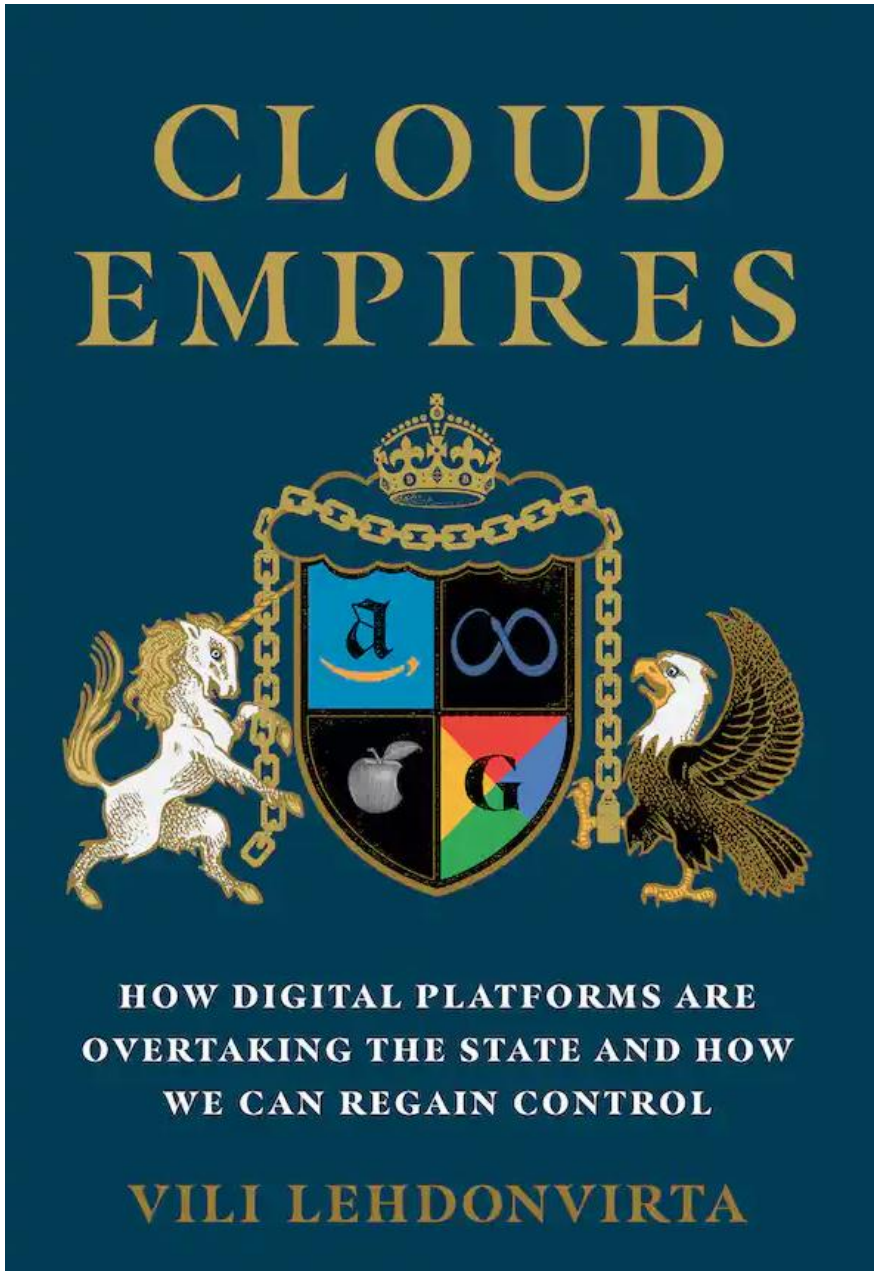
https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-94237.html

Nationale Cyberstrategie (NCS)

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Der Bundesrat

Cloud Imperien



Wie digitale Plattformen den Staat überholen und wie wir die Kontrolle zurückgewinnen können.

Vili Lehdonvirta, September 2022

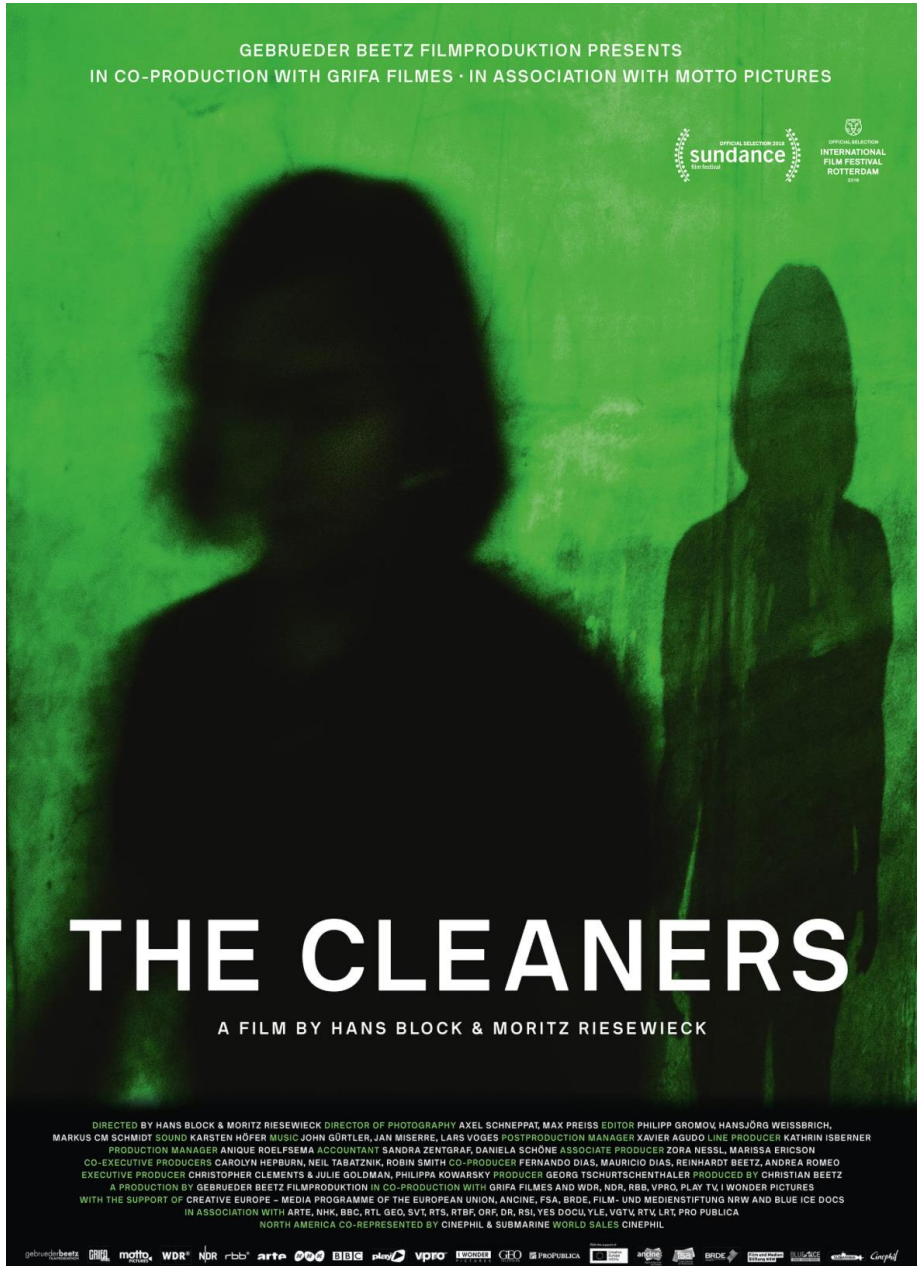
Wird die Demokratie grosse Datenskandale überleben?

Cambridge Analytica verfügte über rund 5.000 Datenpunkte zu jedem Wähler, auf den es abzielte. Zur Verfügung gestellt wurden die Daten von Facebook.

Was, wenn es zu noch mehr Zugang gehabt hätte?

“Es wird immer ein Cambridge Analytica geben.” (ehemaliger Cambridge Analytica Angestellter)

Wie die Zensur privatisiert wurde



- Dokumentarfilm von 2018
- Erklärt, wie Facebook das Hochladen von Bildern zensiert
- Eine Einrichtung mit tausenden von Arbeitern auf den Phlippinen

- Ein weiteres Bespiel: Die Entscheidung, welche Politiker Twitter nutzen dürfen

Schlussbemerkungen

- Standardisierung war im Bereich der Kryptographie enorm erfolgreich und trägt zur Datensouveränität bei
- Trotzdem bleiben Herausforderungen:
  - Cyberangriffe
    - nehmen stetig zu
    - Machine Learning wird die Sache verschlimmern (Deep Fakes)
    - fordern zusätzliche Anstrengungen von allen, um die Cybersicherheit zu verstärken
  - Webgiganten
    - spielen eine immer wichtigere Rolle in nahezu allen Lebensbereichen
    - sind kaum reguliert und schwer zu regulieren
    - GDPR und das neue Schweizer Datenschutzgesetz sind kleine Schritte in die richtige Richtung
  - Cloud computing
    - wird immer beliebter
    - nur die “Hyper-scaler" (Microsoft, Amazon, Google, IBM, Oracle, …) haben die Ressourcen, um vollständige Servicepakete anzubieten
    - Das Bundesamt für Informatik hat eine breite Konsultation zur vorgeschlagenen Cloud Strategie des Bundes begonnen
- **Digitale Souveränität** kann bewahrt werden mit technischen, rechtlichen und organisationellen Massnahmen, inkl. Aus- und Weiterbildungen

C4DT Course on ICT Foundations for Decision Makers

Vermittelt die Grundlagen

- Moderner Informations- und Kommunikationstechnologien
- Cybersicherheit, Privacy und Datenschutz
- Technologischer Entwicklungen: Künstliche Intelligenz und Machine Learning, Blockchain, Quantum Computing, …

Zielgruppe

- Manager und leitende Angestellte
- Keine technischen Voraussetzungen nötig

Diskutanten

- Erfahrene Spezialisten aus der Industrie und EPFL Professoren

Understand the digital ecosystem

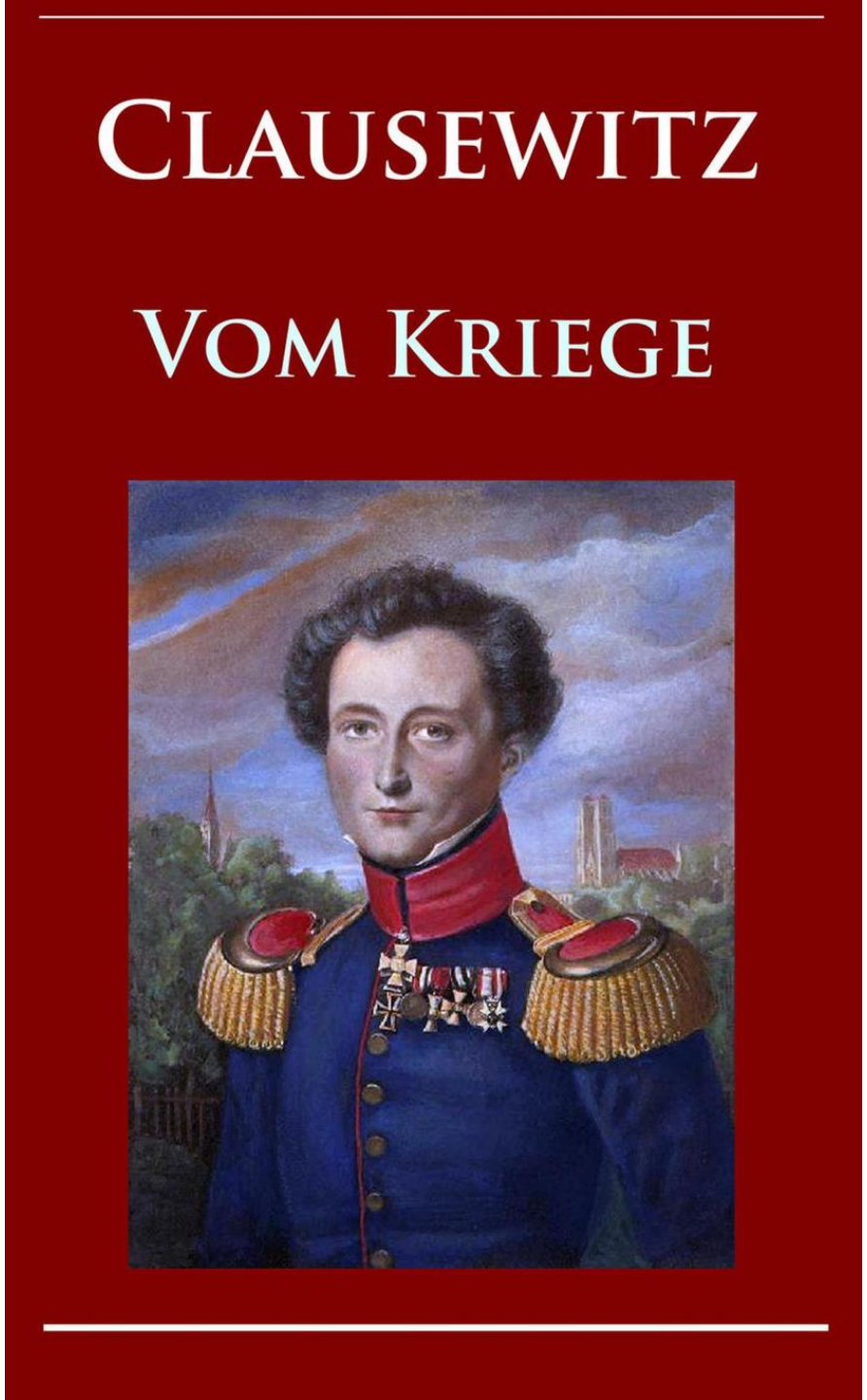
Engage with ICT stakeholders

Lead digital transformation

Der Inhalt kann an spezifische Wünsche und Bedürfnisse angepasst warden.

c4dt@epfl.ch

c4dt.epfl.ch/ictf-2023



Eine Botschaft der Hoffnung:

„Die verteidigende Form des Kriegführens ist an sich stärker als die angreifende.“

Carl von Clausewitz: Vom Kriege, 1832

jean-pierre.hubaux@epfl.ch