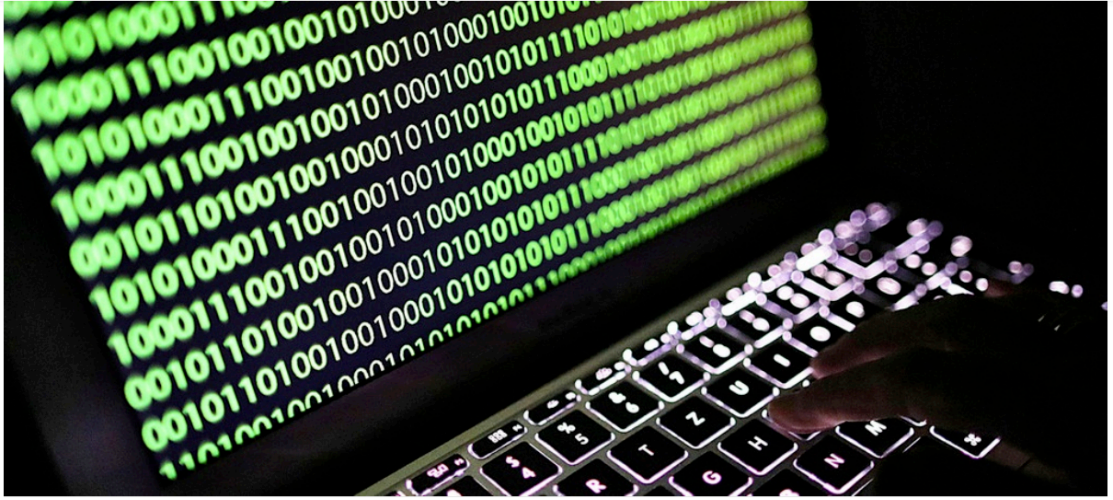
Cyber goes Sicherheitspolitik

Was Tech-Nerds über Security-Nerds wissen sollten

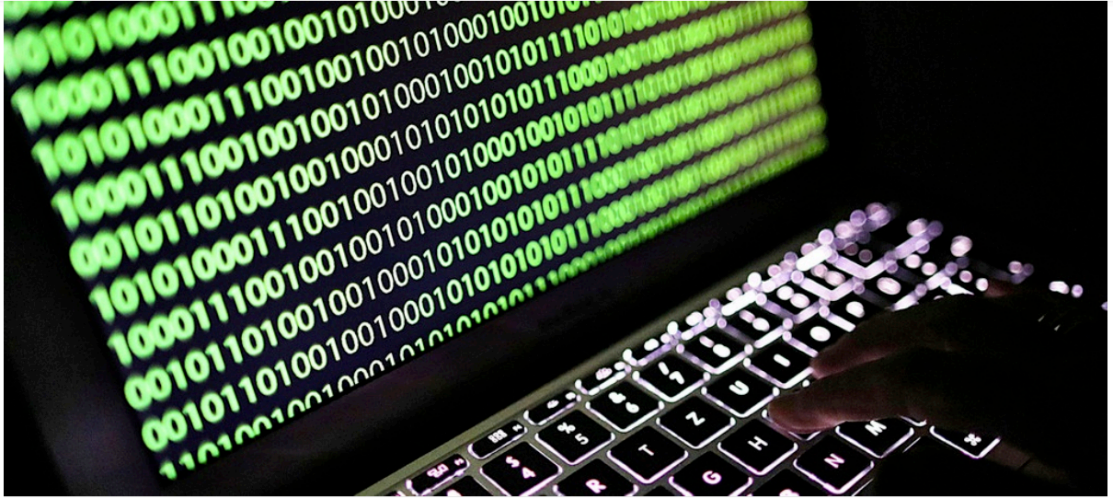


EXKLUSIV Überwachungssoftware

Der Bundestrojaner, den keiner nutzt

Stand: 25.10.2019 16:52 Uhr

Das Bundesinnenministerium will, dass neben der Polizei künftig auch der Verfassungsschutz den umstrittenen "Bundestrojaner" nutzen darf. Dabei wird nach *WDR*-Informationen die Überwachungssoftware schon jetzt kaum eingesetzt.



EXKLUSIV Überwachungssoftware

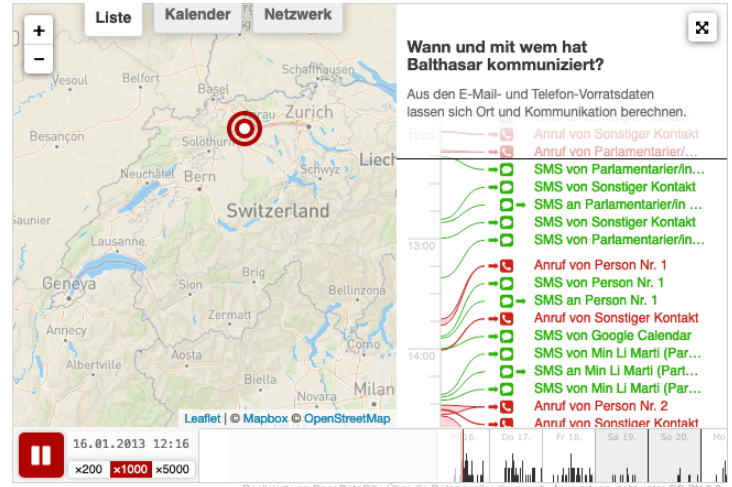
Der Bundestrojaner, den keiner nutzt

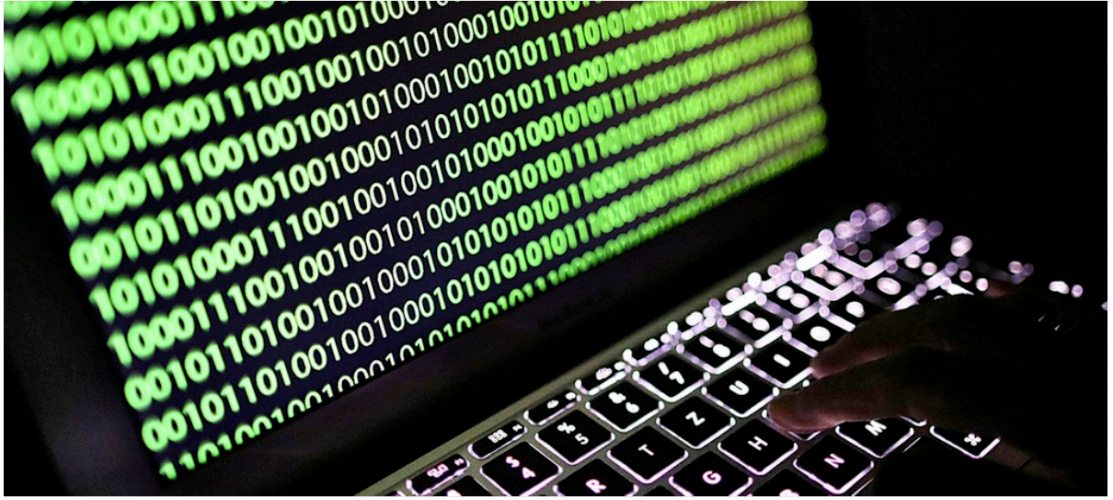
Stand: 25.10.2019 16:52 Uhr

Das Bundesinnenministerium will, dass neben der Polizei künftig auch der Verfassungsschutz den umstrittenen "Bundestrojaner" nutzen darf. Dabei wird nach *WDR*-Informationen die Überwachungssoftware schon jetzt kaum eingesetzt.

Vorratsdatenspeicherung

In der Schweiz müssen Anbieterinnen von Telefon- und Internetdiensten im Auftrag des Staates das Kommunikationsverhalten ihrer KundInnen aufzeichnen, z.B. wer wann wen angerufen hat und wie lange das Gespräch gedauert hat, wer sich wann ins Internet eingeloggt hat und für welche Dauer, wer wann wem ein E-Mail oder SMS geschickt hat und die Standortinformationen des Mobiltelefons. Diese Speicherung von elektronischen Kommunikationsdaten wird im Gesetz als «rückwirkende Überwachung» oder umgangssprachlich als Vorratsdatenspeicherung bezeichnet. Die Daten müssen für 6 Monate abgelegt und auf Verlangen an Strafverfolgungsbehörden oder den Geheimdienst herausgegeben werden.





EXKLUSIV Überwachungssoftware

Der Bundestrojaner, den keiner nutzt

Stand: 25.10.2019 16:52 Uhr

ÜBERWACHUNG

EU-Innenminister wollen Verschlüsselung umgehen

Die Polizei soll an alle Informationen kommen, die sie benötigt - auch wenn sie verschlüsselt sind. Damit würde allerdings die E2E-Verschlüsselung abgeschafft.

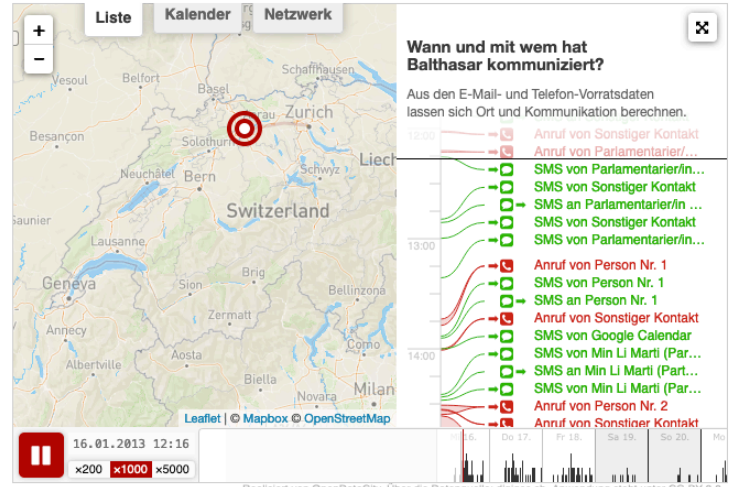
14. November 2020, 14:21 Uhr, Moritz Tremmel

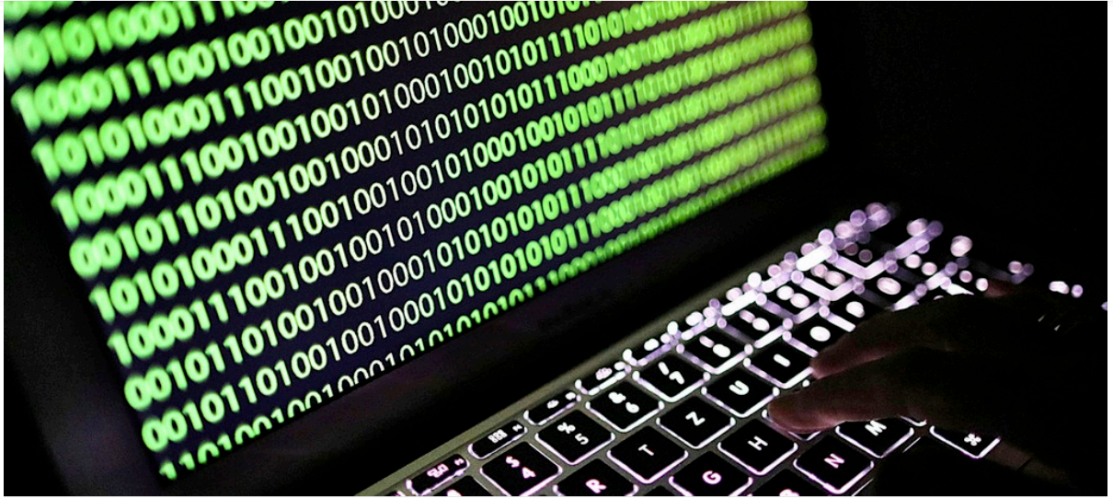
(Bild: Mahesh Patel/Pixabay)

Ein Schlüssel für die Polizei?

Vorratsdatenspeicherung

In der Schweiz müssen Anbieterinnen von Telefon- und Internetdiensten im Auftrag des Staates das Kommunikationsverhalten ihrer KundInnen aufzeichnen, z.B. wer wann wen angerufen hat und wie lange das Gespräch gedauert hat, wer sich wann ins Internet eingeloggt hat und für welche Dauer, wer wann wem ein E-Mail oder SMS geschickt hat und die Standortinformationen des Mobiltelefons. Diese Speicherung von elektronischen Kommunikationsdaten wird im Gesetz als «rückwirkende Überwachung» oder umgangssprachlich als Vorratsdatenspeicherung bezeichnet. Die Daten müssen für 6 Monate abgelegt und auf Verlangen an Strafverfolgungsbehörden oder den Geheimdienst herausgegeben werden.





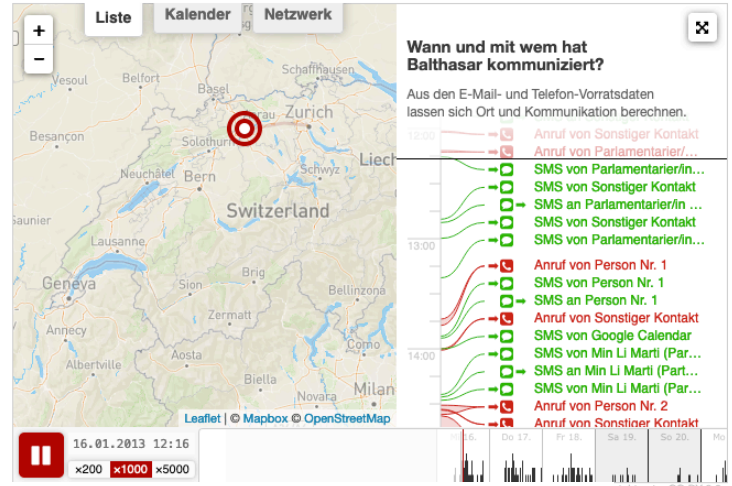
EXKLUSIV Überwachungssoftware

Der Bundestrojaner, den keiner nutzt

Stand: 25.10.2019 16:52 Uhr

Vorratsdatenspeicherung

In der Schweiz müssen Anbieterinnen von Telefon- und Internetdiensten im Auftrag des Staates das Kommunikationsverhalten ihrer KundInnen aufzeichnen, z.B. wer wann wen angerufen hat und wie lange das Gespräch gedauert hat, wer sich wann ins Internet eingeloggt hat und für welche Dauer, wer wann wem ein E-Mail oder SMS geschickt hat und die Standortinformationen des Mobiltelefons. Diese Speicherung von elektronischen Kommunikationsdaten wird im Gesetz als «rückwirkende Überwachung» oder umgangssprachlich als Vorratsdatenspeicherung bezeichnet. Die Daten müssen für 6 Monate abgelegt und auf Verlangen an Strafverfolgungsbehörden oder den Geheimdienst herausgegeben werden.



ÜBERWACHUNG

EU-Innenminister wollen Verschlüsselung umgehen

Die Polizei soll an alle Informationen kommen, die sie benötigt - auch wenn sie verschlüsselt sind. Damit würde allerdings die E2E-Verschlüsselung

Cybersicherheit

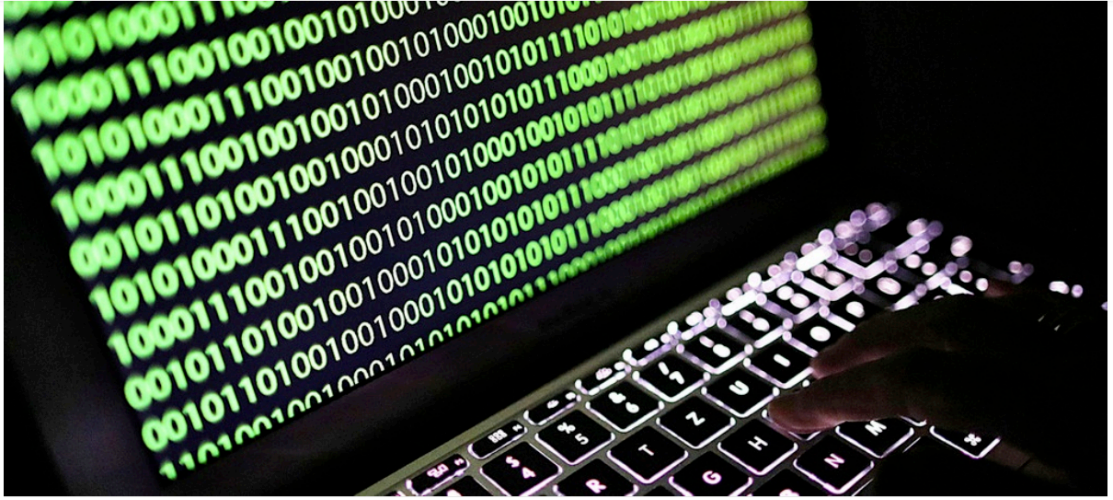
14. November 2020, 14:21 Uhr

Ein Schlüssel für die Polizei?

Gutachten warnt Bundesregierung vor Hackback

Sollte Deutschland bei einem digitalen Angriff zurückschlagen? Davon rät der Wissenschaftliche Dienst des Bundestages ab. Zu groß sei die "Eskalationsgefahr".

3. September 2019, 18:25 Uhr / Quelle: ZEIT ONLINE, dpa, ml / 40 Kommentare /



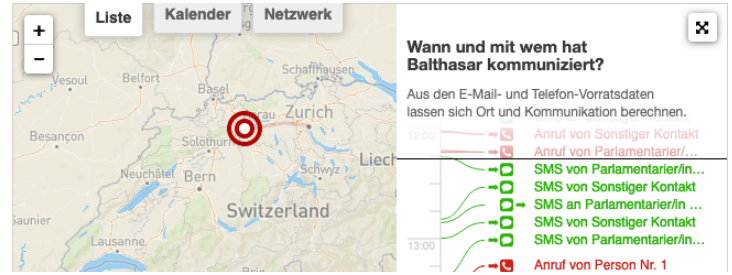
EXKLUSIV Überwachungssoftware

Der Bundestrojaner, den keiner nutzt

Stand: 25.10.2019 16:52 Uhr

Vorratsdatenspeicherung

In der Schweiz müssen Anbieterinnen von Telefon- und Internetdiensten im Auftrag des Staates das Kommunikationsverhalten ihrer KundInnen aufzeichnen, z.B. wer wann wen angerufen hat und wie lange das Gespräch gedauert hat, wer sich wann ins Internet eingeloggt hat und für welche Dauer, wer wann wem ein E-Mail oder SMS geschickt hat und die Standortinformationen des Mobiltelefons. Diese Speicherung von elektronischen Kommunikationsdaten wird im Gesetz als «rückwirkende Überwachung» oder umgangssprachlich als Vorratsdatenspeicherung bezeichnet. Die Daten müssen für 6 Monate abgelegt und auf Verlangen an Strafverfolgungsbehörden oder den Geheimdienst herausgegeben werden.



ÜBERWACHUNG

EU-Innenminister wollen Verschlüsselung umgehen

Die Polizei soll an alle Informationen kommen, die sie benötigt - auch wenn sie verschlüsselt sind. Damit würde allerdings die E2E-Verschlüsselung

Cybersicherheit

14. November 2020, 14:21 Uhr

Ein Schlüssel für die Polizei?

Former spy chief calls for military cyber attacks on ransomware hackers

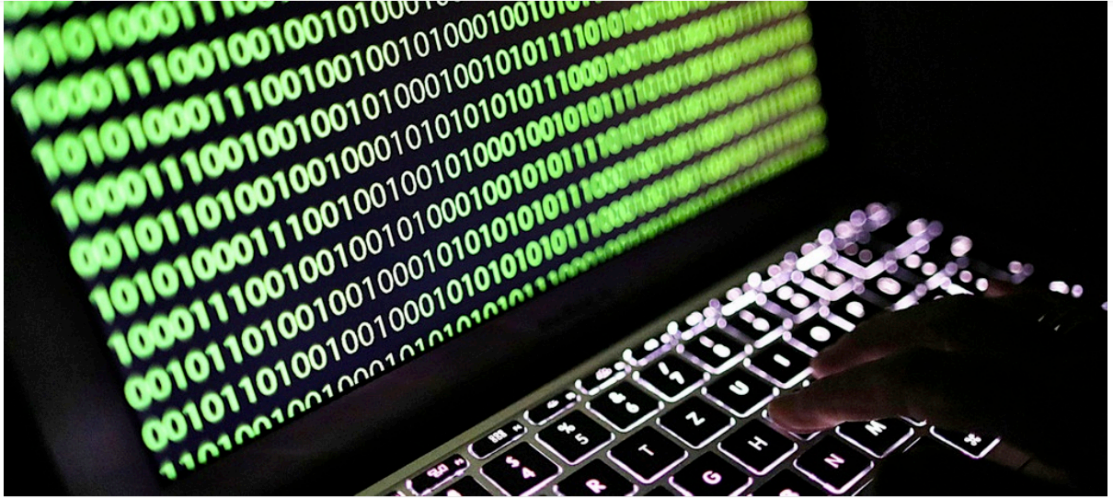
The most serious ransomware groups should be the target of cyber attacks to disrupt their operations, Ciaran Martin has said

By James Cook
15 February 2021 • 8:00pm

Gutachten Bundesreg

Sollte Deutschland bei einem digitalen Angriff zurückschlagen? Davon rät der Wissenschaftliche Dienst des Bundestages ab. Zu groß sei die "Eskalationsgefahr".

3. September 2019, 18:25 Uhr / Quelle: ZEIT ONLINE, dpa, ml / 40 Kommentare /



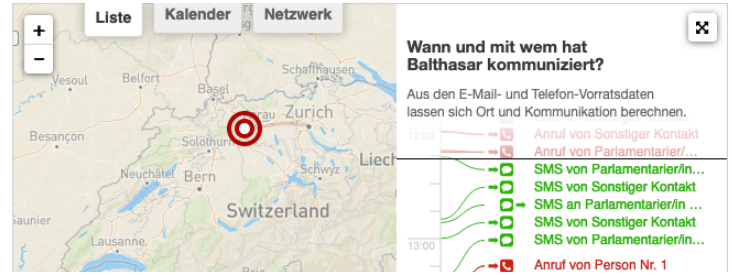
EXKLUSIV Überwachungssoftware

Der Bundestrojaner, den keiner nutzt

Stand: 25.10.2019 16:52 Uhr

Vorratsdatenspeicherung

In der Schweiz müssen Anbieterinnen von Telefon- und Internetdiensten im Auftrag des Staates das Kommunikationsverhalten ihrer KundInnen aufzeichnen, z.B. wer wann wen angerufen hat und wie lange das Gespräch gedauert hat, wer sich wann ins Internet eingeloggt hat und für welche Dauer, wer wann wem ein E-Mail oder SMS geschickt hat und die Standortinformationen des Mobiltelefons. Diese Speicherung von elektronischen Kommunikationsdaten wird im Gesetz als «rückwirkende Überwachung» oder umgangssprachlich als Vorratsdatenspeicherung bezeichnet. Die Daten müssen für 6 Monate abgelegt und auf Verlangen an Strafverfolgungsbehörden oder den Geheimdienst herausgegeben werden.



ÜBERWACHUNG

EU-Innenminister wollen Verschlüsselung umgehen

Die Polizei soll an alle Informationen kommen, die sie benötigt - auch wenn sie verschlüsselt sind. Damit würde allerdings die E2E-Verschlüsselung

Cybersicherheit

14. November 2020, 14:21 Uhr

Ein Schlüssel für die Polizei?

Gutachte Bundesr

Sollte Deutschland
der Wissenschaftlic
"Eskalationsgefahr"

3. September 2019, 18:25

Former spy chief calls for military cyber attacks on ransomware hackers

The most serious ransomware groups should be the target of cyber attacks to disrupt

NATIONAL SECURITY

Biden Pledges Tough Response To Cyberthreats. Experts Say It Won't Be Easy

February 12, 2021 · 5:06 AM ET

Heard on Morning Edition

GREG MYRE

Vorratsdatenspeicherung

In der Schweiz müssen Anbieterinnen von Telefon- und Internetdiensten im Auftrag des Staates das Kommunikationsverhalten ihrer KundInnen aufzeichnen, z.B. wer wann wen angerufen hat und wie lange das Gespräch gedauert hat, wer sich wann ins Internet eingeloggt hat und für welche Dauer, wer wann wem ein E-Mail oder SMS geschickt hat und die Standortinformationen des Mobiltelefons. Diese Speicherung von elektronischen Kommunikationsdaten wird im Gesetz als «rückwirkende Überwachung» oder umgangssprachlich als Vorratsdatenspeicherung bezeichnet. Die Daten müssen für 6 Monate abgelegt und auf Verlangen an Strafverfolgungsbehörden oder den Geheimdienst

ÜBERWACHUNG

EU-Inn
umgeh

Die Polizei s
verschlüssel

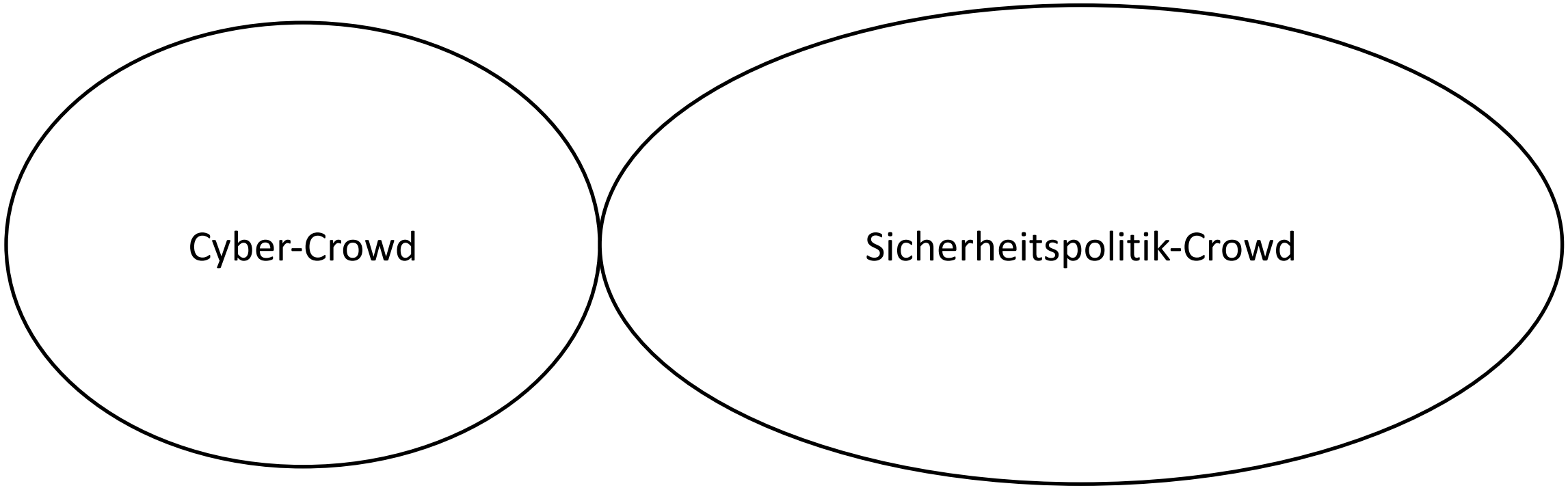
Ein Schlüssel für die Polizei?

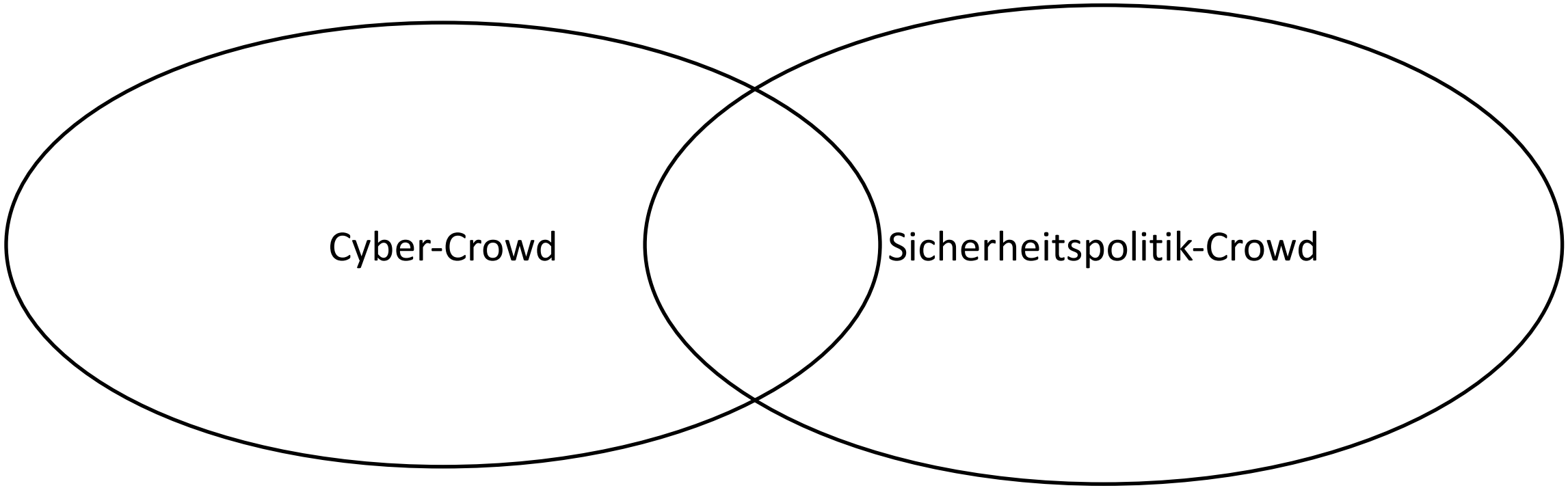
3. September 2019, 18:25 U

February 12, 2021 · 5:06 AM ET

Heard on Morning Edition

GREG MYRE


Cyber-Crowd
Sicherheitspolitik-Crowd


Cyber-Crowd
Sicherheitspolitik-Crowd

Was ist Sicherheitspolitik?

- Massnahmen zur Schaffung und Wahrung des kollektiven Gutes Sicherheit (eines Staates)
  - Forschung
  - Doktrin
  - Gesetze
  - Fähigkeiten
  - Organisationen
    - Nachrichtendienste
    - Strafverfolgung
    - Militär

Sicherheitspolitik und Technologien

- Technologie hat Einfluss auf eigene Möglichkeiten und Fähigkeiten

Sicherheitspolitik und Technologien

- Technologie hat Einfluss auf eigene Möglichkeiten und Fähigkeiten
- Technologie hat Einfluss auf fremde Möglichkeiten und Fähigkeiten

Sicherheitspolitik und Technologien

- Technologie hat Einfluss auf eigene Möglichkeiten und Fähigkeiten
- Technologie hat Einfluss auf fremde Möglichkeiten und Fähigkeiten
- Technologie muss

Sicherheitspolitik und Technologien

- Technologie hat Einfluss auf eigene Möglichkeiten und Fähigkeiten
- Technologie hat Einfluss auf fremde Möglichkeiten und Fähigkeiten
- Technologie muss
  - Verstanden werden: was ist es und was kann es?

Sicherheitspolitik und Technologien

- Technologie hat Einfluss auf eigene Möglichkeiten und Fähigkeiten
- Technologie hat Einfluss auf fremde Möglichkeiten und Fähigkeiten
- Technologie muss
  - Verstanden werden: was ist es und was kann es?
  - Entwickelt/beschafft werden: wie kriegen wir bzw. unsere Gegner es?

Sicherheitspolitik und Technologien

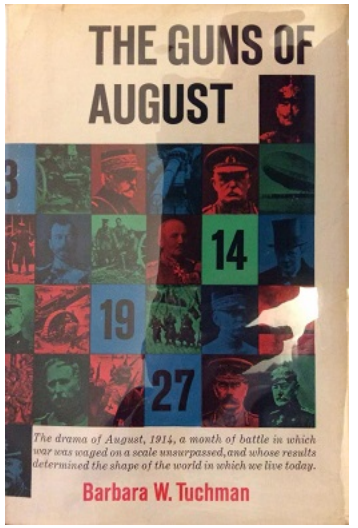
- Technologie hat Einfluss auf eigene Möglichkeiten und Fähigkeiten
- Technologie hat Einfluss auf fremde Möglichkeiten und Fähigkeiten
- Technologie muss
  - Verstanden werden: was ist es und was kann es?
  - Entwickelt/beschafft werden: wie kriegen wir bzw. unsere Gegner es?
  - Genutzt werden: wie kann man es nutzen und wollen/können wir das?

Sicherheitspolitik und Technologien

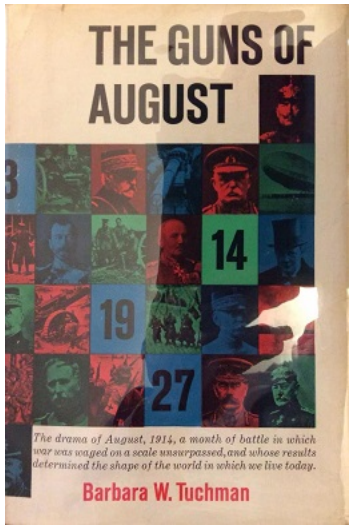
- Technologie hat Einfluss auf eigene Möglichkeiten und Fähigkeiten
- Technologie hat Einfluss auf fremde Möglichkeiten und Fähigkeiten
- Technologie muss
  - **Verstanden werden: was ist es und was kann es?**
  - Entwickelt/beschafft werden: wie kriegen wir bzw. unsere Gegner es?
  - Genutzt werden: wie kann man es nutzen und wollen/können wir das?

Herausforderung durch “Neuland“

- Denkweise geprägt vom letzten grossen “Neuland“
  - WWI -> Kavallerie, dafür Grabenkampf nicht berücksichtigt
  - WWII -> Grabenkampf, dafür Panzer nicht berücksichtigt
  - „*More of the same?*“ / Innovationsblindheit



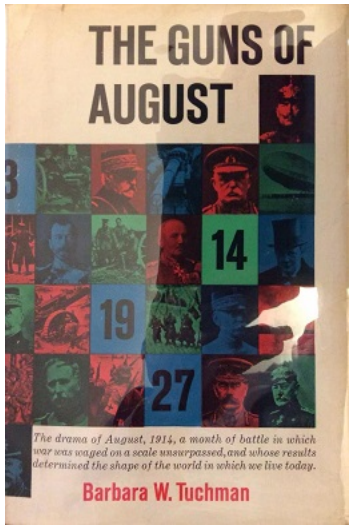
Herausforderung durch “Neuland“



- Denkweise geprägt vom letzten grossen “Neuland“
  - WWI -> Kavallerie, dafür Grabenkampf nicht berücksichtigt
  - WWII -> Grabenkampf, dafür Panzer nicht berücksichtigt
  - „*More of the same?*“ / Innovationsblindheit

- Neue Ereignisse werden in bekannte „Boxen“ gedrängt
  - Bekannte Konzepte werden neuen Realitäten übergestülpt, obwohl sie vielleicht zu falschem Schluss führen

Herausforderung durch “Neuland“



- Denkweise geprägt vom letzten grossen “Neuland“
  - WWI -> Kavallerie, dafür Grabenkampf nicht berücksichtigt
  - WWII -> Grabenkampf, dafür Panzer nicht berücksichtigt
  - „*More of the same?*“ / Innovationsblindheit

- Neue Ereignisse werden in bekannte „Boxen“ gedrängt
  - Bekannte Konzepte werden neuen Realitäten übergestülpt, obwohl sie vielleicht zu falschem Schluss führen

➢ „*You are always planning for the last war*“
(*Cyber Pearl Harbor, Cyber 9/11*)

Gedankliche „Boxen“ Sicherheitspolitik

- Konflikt als „game“
  - Gegner?
  - Ziele?
  - Fähigkeiten?
  - Räume?
  - „Regeln“?

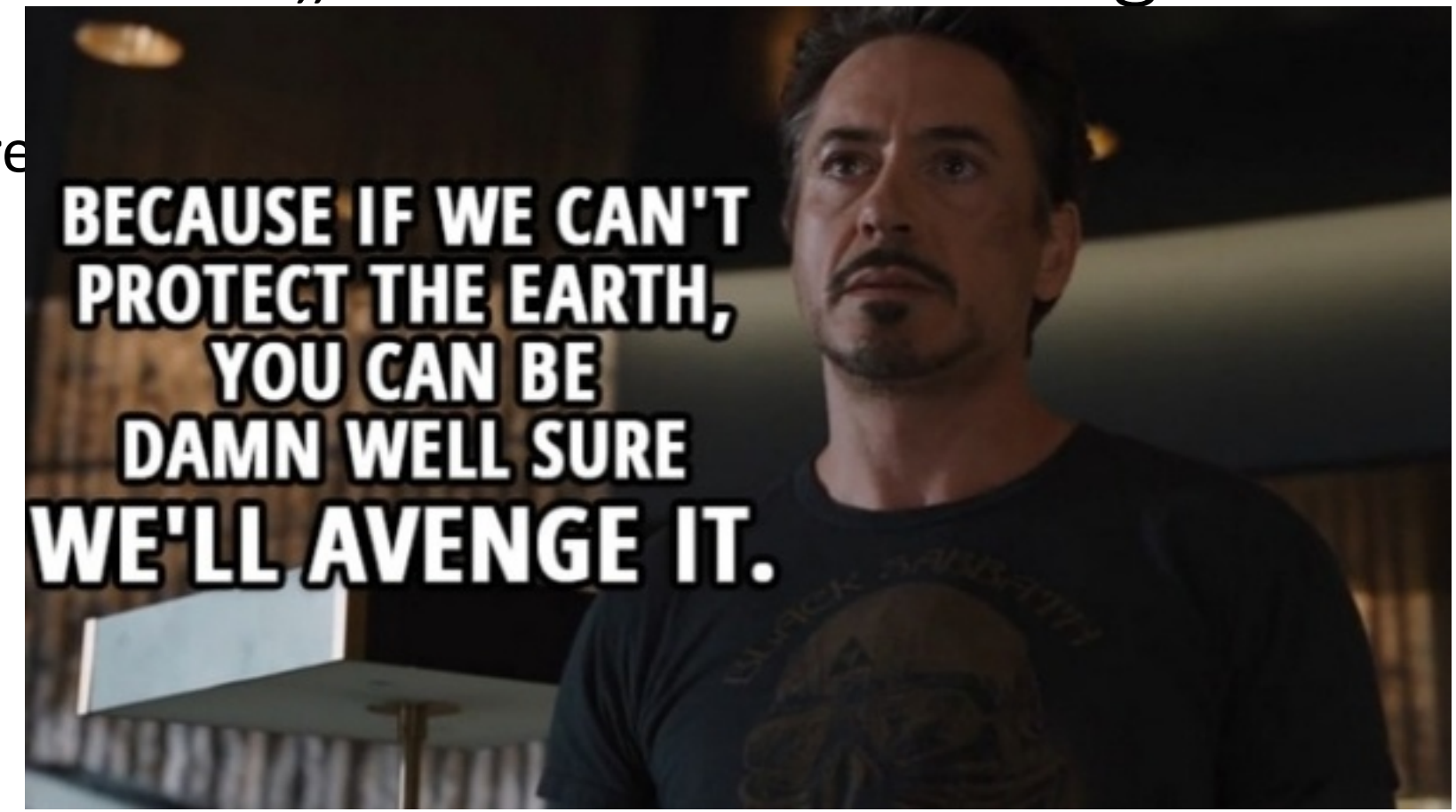
- Sicherheitspolitik als Forschungsfeld: Theorien, „Weltsichten“

Bestehende „Boxen“: Kalter Krieg

- Abschreckung: *Mutually assured destruction*

Bestehende „Boxen“: Kalter Krieg

- Abschre



Bestehende „Boxen“: Kalter Krieg

- Abschreckung: *Mutually assured destruction*
- Eskalation: Kubakrise
- Technologiewettkampf: Sputnik, *missile gap* und co.
- Spionage: verlässliche Information über Fähigkeiten und Intentionen, Desinformation

„Cyber“ ist tricky

- Konflikt als „game“
  - Gegner?
    - Staatlich, nicht-staatlich, gemischt, schwer zu eruieren (*attribution*)
  - Ziele?
    - Vielzahl an möglichen Motiven, von kommerziell über Terrorismus bis Machtpolitik
  - Fähigkeiten?
    - Schwierig zu quantifizieren und überhaupt zu erkennen, wirft ganze neue Fragen zu Rüstungskontrolle auf (*dual-use* / Proliferation)
  - Räume?
    - Neuer Raum? Verwendung in den bekannten Räumen? Mischformen?
  - „Regeln“?
    - *Lol*

„Cyber“ ist tricky

- Konflikt als „game“
  - Gegner?
    - Staatlich, nicht-staatlich, g … *ttribution*)
  - Ziele?
    - Vielzahl an möglichen Mo … rrorismus bis Machtpolitik
  - Fähigkeiten?
    - Schwierig zu quantifiziere … wirft ganze neue Fragen zu Rüstungskontrolle auf (*du*
  - Räume?
    - Neuer Raum? Verwendun … Mischformen?
  - „Regeln“?
    - *Lol*

„Cyber“ ist tricky

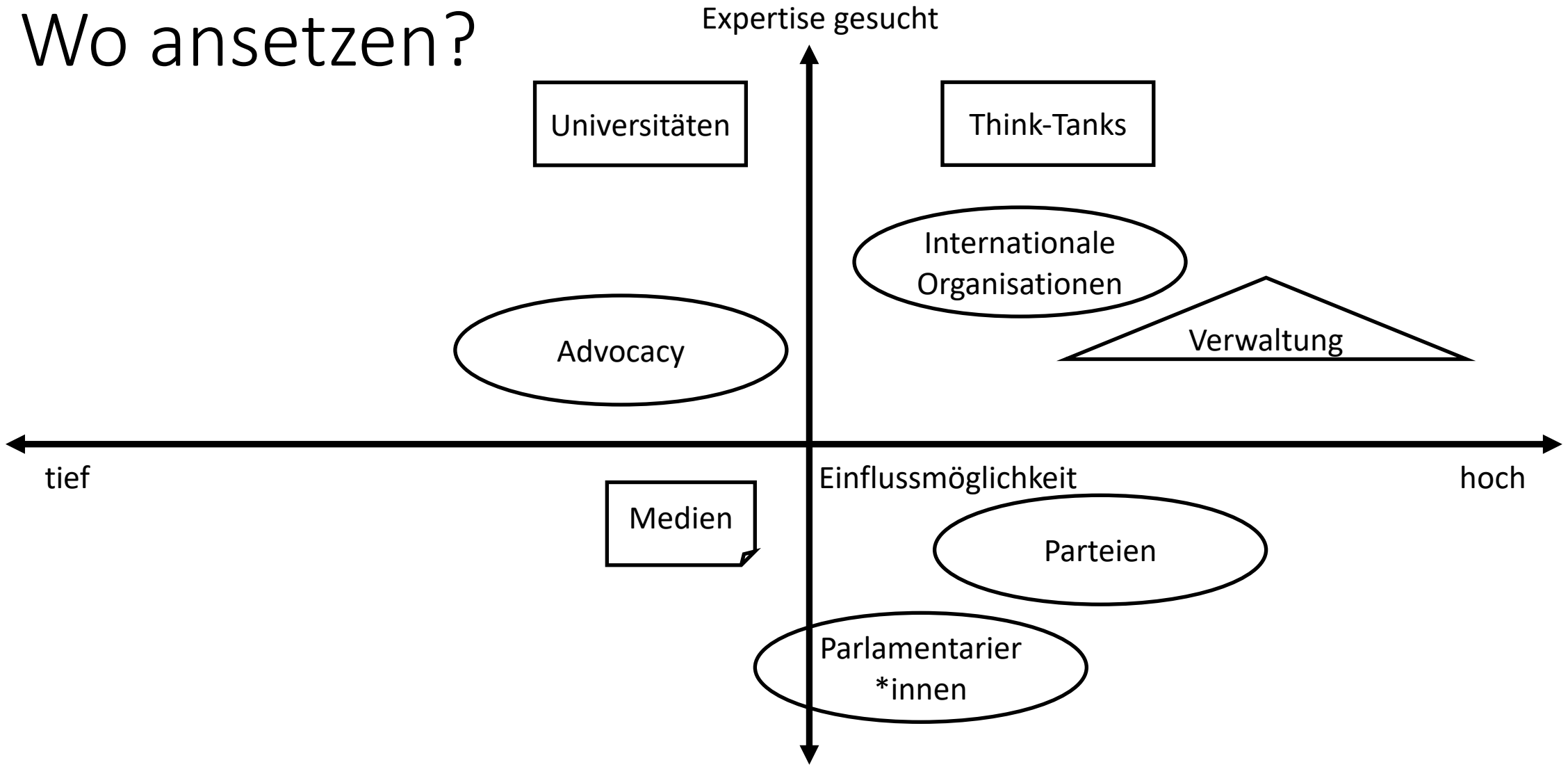
- Konflikt als „game“
  - Gegner?
    - Staatlich, nicht-staatlich, gemischt, schwer zu eruieren (*attribution*)
  - Ziele?
    - Vielzahl an möglichen Motiven, von kommerziell über Terrorismus bis Machtpolitik
  - Fähigkeiten?
    - Schwierig zu quantifizieren und überhaupt zu erkennen, wirft ganze neue Fragen zu Rüstungskontrolle auf (*dual-use* / Proliferation)
  - Räume?
    - Neuer Raum? Verwendung in den bekannten Räumen? Mischformen?
  - „Regeln“?
    - *Lol*
    - Abhängigkeit von anderen Akteuren, z.B. USA mit aktuellem Ansatz *persistent engagement / defending forward*

- Sicherheitspolitik als Forschungsfeld: Theorien, „Weltsichten“
  - *Work in progress* aber fehlende Einsatzerfahrungen
  - Was Sicherheit ausmacht muss ebenfalls neu gedacht werden (Desinformation, *Hacking Democracy* etc.)

Cold war = mostly cold coffee

- Abschreckung: Funktioniert für Cyber sehr schlecht, bzw. ist kompliziert
- Eskalation: ganz neue Eskalationsleitern und Cyber schlecht geeignet, aber aktuell „Wettrüsten“ (AI Arms Race etc.)
- Technologiewettkampf & Spionage: immer noch relevant

Wo ansetzen?



Politik

Forschung

Verwaltung

Medien

Weiterführende Quellen und Fragen?

- Percepticon Podcast
- Sicherheitspolitischer Bericht (SiPol)
- Myriam Dunn Cavelty; Florian J. Egloff, “The Politics of Cybersecurity: Balancing Different Roles of the State.” St Antony’s International Review 15 no.1 (2019):37-57