Digital Summit NRW

Manuel ‚HonkHase‘ Atug

Digitale Souveränität in kritischen Infrastrukturen und für die Bevölkerung

Manuel ‚HonkHase‘ Atug

Manuel (HonkHase) Atug

Principal bei der HiSolutions AG

- Diplom-Informatiker, Master of Science in Applied IT Security, Ingenieur
- Weit über 23 Jahren in der Informationssicherheit tätig
- Sachverständiger für das IT-SiG 2.0 im Bundestag
- Themen: KRITIS, Hackback, Ethik, Hybrid Warfare, Cyberresilienz, Bevölkerungs- und Katastrophenschutz
- Experte der European Research Executive Agency (EU REA)
- Mitgründer der AG KRITIS: ag.kritis.info

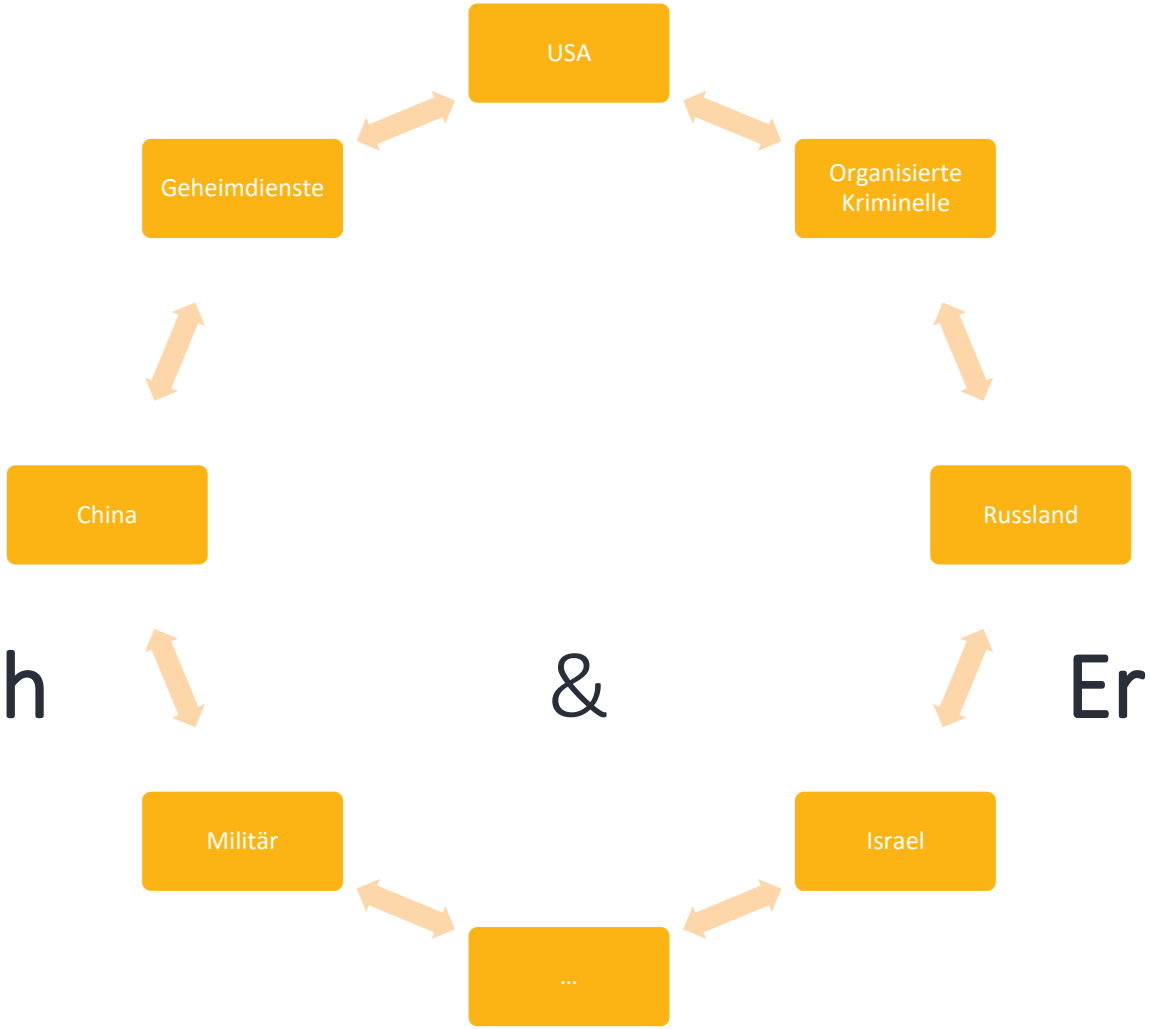
AG KRITIS

~~@HonkHase~~ @HonkHase@chaos.social

@honkhase.bsky.social

Ich habe #KRITIS im Endstadium

Schutz vor was und wem?



Machtmissbrauch & Erlösmaximierung

Bin ich KI? Und wenn ja, wie viele?

Was ist KI?

- KI ist Software
  (und ganz viel Daten)

- Software kann man sicher entwickeln und betreiben.
  Oder eben auch nicht

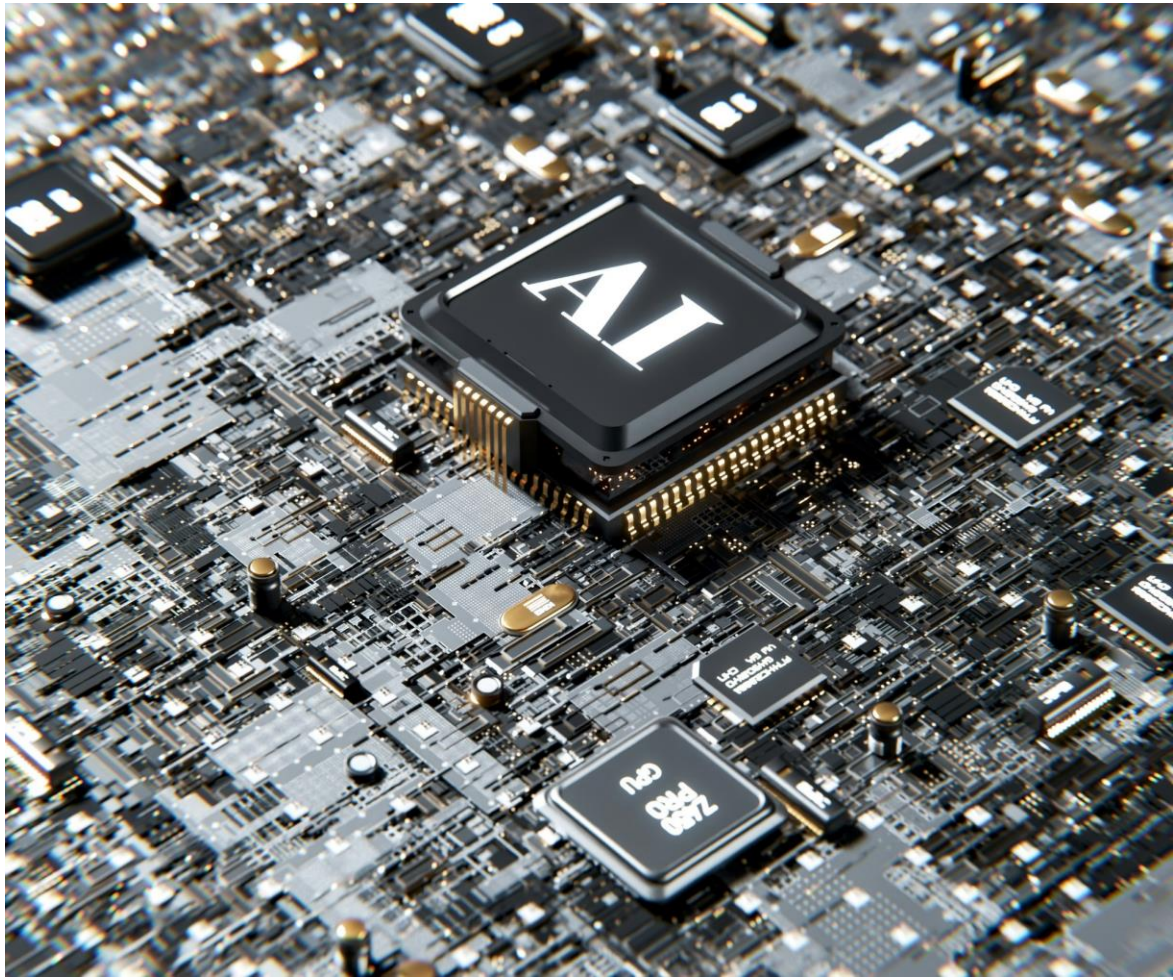
- Software kann nicht denken

Was ist KI?

Alan Turing hatte schon vor über 70 Jahren erkannt:

- Die zentrale Frage ist nicht, ob Maschinen denken können, sondern ob sie Menschen so gut imitieren, dass wir den Unterschied nicht mehr erkennen

- Aber Imitation ist nicht gleich Intelligenz und schon gar nicht gleich Menschlichkeit



Wie nutze ich KI?

- Technologiehörigkeit vs Heilsversprechen?
- Mittel zum Zweck vs Selbstzweck?

Sicherer, robuster und nachvollziehbarer Einsatz von KI

- **Evasion/Adversarial Attacks**
  Durch eine Manipulation von Eingabedaten verleiten Angreifer das KI-Modell im Betrieb zu vom Entwickler nicht vorgesehenen Ausgaben

- **Data Poisoning Attacks**
  Manipulation der Trainingsdaten des KI-Modells, so dass dieses auf (bestimmte) Eingaben nicht wie vom Entwickler vorgesehen reagiert

Sicherer, robuster und nachvollziehbarer Einsatz von KI

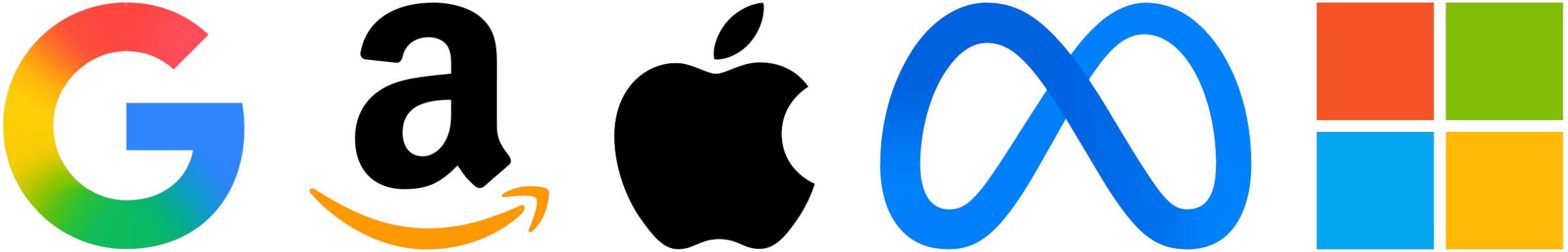
- **Privacy-Attacks**
  Angreifer extrahieren Informationen hinsichtlich der Trainingsdaten aus dem Modell

- **Model Stealing Attacks**
  Angreifer extrahieren die Funktionalität des Modells

Quelle: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KI/Herausforderungen_und_Massnahmen_KI.pdf

Digitale Souveränität

Autarkie ist nicht digitale Souveränität



- Aber die Big Five der Big Tech sind es auch nicht
  - von links nach rechts: Alphabet (primär Google), Amazon, Apple, Meta (Facebook, Instagram, Whatsapp) und Microsoft (vor allem Windows)

Von SgtShyGuy - Eigenes Werk, CC0, https://commons.wikimedia.org/w/index.php?curid=117237876

KI ist das Gegenteil von digitaler Souveränität?!

- Anduril & Palantir (Thiel), OpenAI (Altman), Grok (Musk) und Aleph Alpha (Andrulis)
  - KI Algorithmen sind oftmals als Open Source verfügbar
  - Rechenzentren sind gigantisch (10 Milliarden USD für ein neues von Meta)
  - Wertvoll und geheim gehalten werden die Massen an Daten → wo wir ständig neue dazu liefern

Palantir Grok OpenAI

ANDURIL ALEPH ALPHA

Von unbekannt - Vektordaten: https://www.palantir.com/build/files/Palantir_UK_Gender_Pay_Gap_Report_2017.pdf Farbinfo: Die Farbe wurde auf Schwarz gesetzt, PD-Schöpfungshöhe, https://de.wikipedia.org/w/index.php?curid=11261927

Bedrohungen und Gefährdungen in der digitalen Souveränität

- **Und alle: Cloud & KI**

- Was ist mit staatlichen Systemlandschaften?
- Was ist mit Betriebssystemen und Smartphones?
- Was ist mit Netzwerkequipment und Firewalls?
- Was ist mit Systemen zur Angriffserkennung?

Verlust der digitalen Souveränität über 3 Langzeit-Etappen

Hardware

- Speicherung der Daten
- Externe RZ Konzerne

Applikationen

- Verarbeitung der Daten
- Externe Cloud Konzerne

Daten

- Abgabe der Daten
- Externe KI Konzerne

Wiederherstellung der digitalen Souveränität

Ziele

- Derisking statt Decoupling
- Geringe Abhängigkeit
- Entscheidungsfreiheit und -vielfalt

EU Werte & Lösungen

- Datenschutz = Menschenschutz
- Mehr & stärkerer Wettbewerb
- Kein Nationalismus

Europäische Maßnahmen

- EU Gesetzgebung
- Mehr Wettbewerb in der EU stärken
- Rechtsdurchsetzung

Und ganz konkret?

Transparenz & Lagebild

- Analysieren und aufschreiben, was man alles einsetzt und aus welchen Ländern
- zB Laptop- & Handy-OS, Cloud, KI, Firewalls, Switches, Router, Systeme zur Angriffserkennung, Datenbanken, Applikationen…

Langfriststrategie

- Prüfen, wo eine Migration/Transformation zu zB OpenSource-Lösungen aus der EU möglich ist und auch was bewirkt
- Welche derzeit geplanten und anstehenden Einkäufe können neu ausgerichtet werden?

>> All-Gefahren-Ansatz <<

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe

„Berücksichtigung aller Gefahrenarten (z. B. Naturgefahren, technologische Gefahren, etc.) im Rahmen des Risiko- und Krisenmanagements“

** Hallo BBK*

Dinge beim Namen nennen

Lieferkette: Israel XM Cyber

Ex-Mossad-Chef Tamir Pardo gründete ein Start-up, das Banken, Firmen und Regierungen berät. *Foto: picture alliance / dpa*

SICHERHEIT

»Tödlich wie die Atombombe«

Tamir Pardo warnt davor, das Zerstörungspotenzial von Cyberkriminellen zu unterschätzen

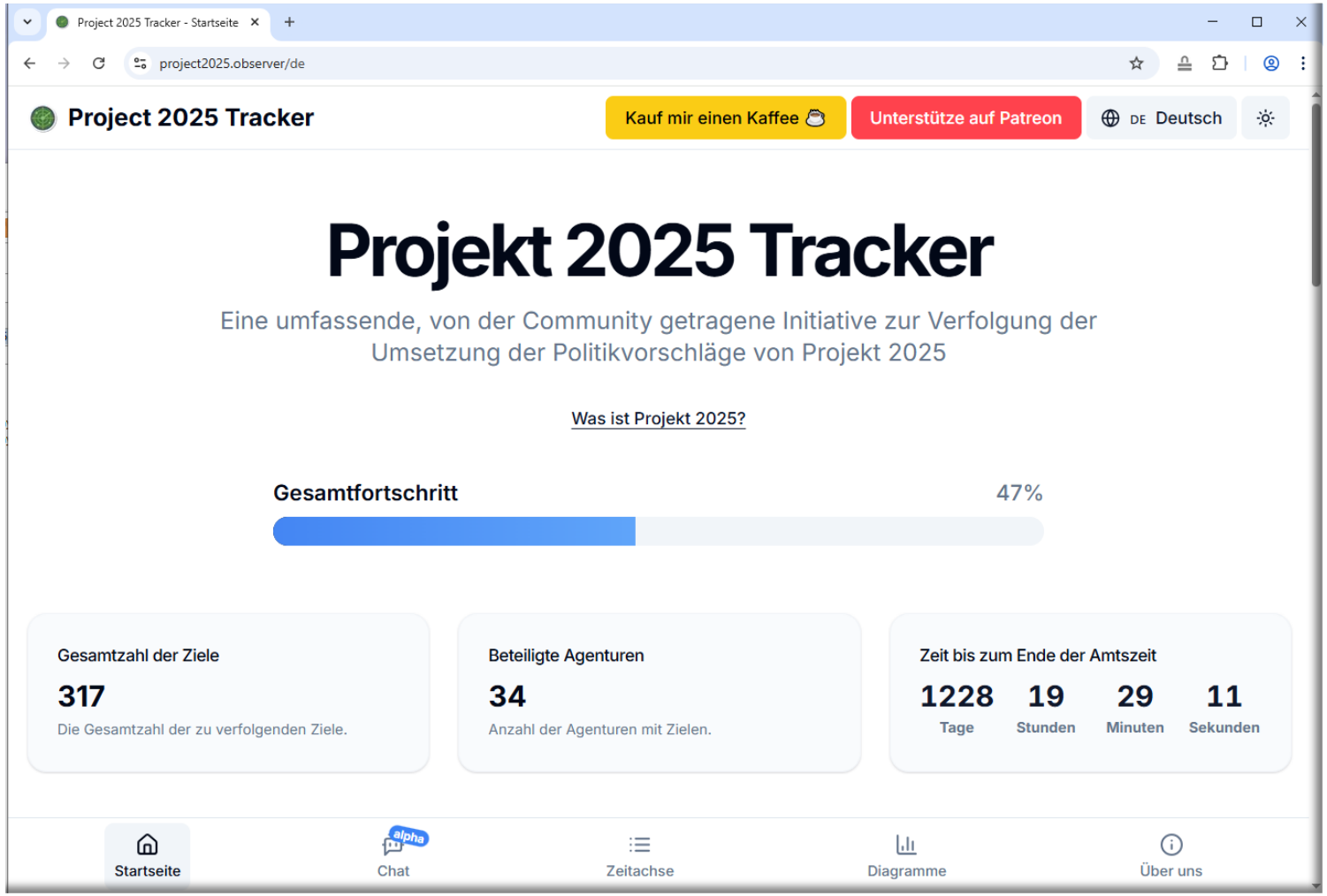
von Pierre Heumann

14.02.2021 11:06 Uhr

Von 2010 bis 2015 war er Direktor des Mossad.

Nach seinem Ausscheiden aus dem Geheimdienst vor fünf Jahren gründete er, zusammen mit zwei weiteren Ex-Mossad-Agenten, die Cyberfirma »XM Cyber«. Das Start-up hat eine vollautomatische Simulationsplattform für anhaltende Bedrohungen entwickelt, um Angriffe kontinuierlich aufdecken und den Handlungsbedarf lokalisieren zu können. Es zählt unter anderem Banken, Versicherungsfirmen, Flughäfen, Energiefirmen, Regierungen, Logistikfirmen und Börsen zu seinen Kunden.

Project 2025 von der Heritage Foundation



Alex Karp: CEO Palantir

Von UK Government - Deputy Prime Minister Oliver Dowden attends AI Summit, CC BY 2.0, https://commons.wikimedia.org/w/index.php?curid=164850671

Gründete 2003 mit Peter Thiel Palantir

- Personenkult um Karp
- Mystifizierung von Palantir
- Dokumentarfilm
  - Watching You – Die Welt von Palantir und Alex Karp

Palantir Linkliste von HonkHase

https://atug.de/Palantir/Palantir%20Linkiste.txt

Der Endgegner der Souveränität: Palantir

Palantir

- Autokratie-Etablierung durch Peter Thiel
- auch durch deutsche Steuergelder
- mittels deutscher Strafverfolgungsbehörden & Geheimdiensten
- USA als „CEO geführte Firma“ ohne Regulierung
- Freiheit nicht mit Demokratie vereinbar
- Vorstufe „Freedom Cities“

„Städten ohne Demokratie“ Vision von Peter Thiel

- Vorgeschmack: Próspera (von Thiel und Andreessen finanziert)
- Klinische Tests & Gentherapie ohne Genehmigung mit direkten Tests an Menschen (Minicircle)
- Autonome Autos, Drohnen & Waffensysteme ohne Auflagen (SpaceX, Tesla, Anduril)
- Kernreaktoren, Kernspaltung & Nuklearenergie ohne staatliche Überwachung (Oklo)
- Bauunternehmen ohne Umweltprüfungsprozess
- „Sonderwirtschaftszone“
  - in der Konzerne kaum Steuern zahlen müssen
  - In der Rechte von Arbeitskräften außer Kraft gesetzt werden (auch bekannt als Sklaverei)

Frage der Bevölkerung: Kommt morgen noch Strom & Wasser aus der Leitung?

Cyberresilienz ➔ Widerstandsfähigkeit gegen Ereignisse

- Ursache für Katastrophe oder Cybervorfall ist für die Bevölkerung nicht relevant

- Aber: eine Krise (Pandemie) in der Krise (Putins Angriffskrieg) in der Krise (Ransomware) in der Krise (Gasmangellage) in der ***<beliebige Krise hier einfügen>*** braucht keiner!

- Kritische Fragen:

  → Ist Digitalisierung immer erforderlich?

  →Können wir damit die Cyberresilienz erhöhen?

  →Was ist eine gute Digitalisierung?

Nachhaltigkeit in der Digitalisierung

- Bei der digitalen Transformationen verantwortungsvolle Maßnahmen einzuleiten und gewissenhaft durchzuführen, also zu operationalisieren, ist daher gleichsam eine technische wie ethische Aufgabe!
- Vermeidet daher technische Schulden an kommende Generationen
- Hinter jedem Datensatz steht ein Mensch ➔ Daten können toxisch sein
- Security by Design und Privacy by Design ist Menschenschutz

>> All-Gefahren-Ansatz <<

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe

„Berücksichtigung aller Gefahrenarten (z. B. Naturgefahren, technologische Gefahren, etc.) im Rahmen des Risiko- und Krisenmanagements“

** Hallo BBK*

Und was mache ich, wenn alles nichts hilft?

Irgendwas mit Holz?

Kokosnusspflücker!

www.kokosnusspflücker.de