LSZ

FUTURE CONNECTIONS

Die (Un)Möglichkeiten der unbegrenzten Möglichkeiten Cyber & KI

KI & Cyber

Vor die Welle kommen

Vor die Welle kommen

Attribution

ohne KI

Russland und KI

Künstliche Intelligenz: Putin will Russland zur KI-Macht aufbauen

Auf einer Konferenz warnte Präsident Putin vor einer westlichen Monopolstellung im Bereich Künstlicher Intelligenz. Moskau soll ebenfalls eine KI-Macht werden.

Skoltech — Skolkovo Institute of Science and Technology

education | research | entrepreneurship | industry | community

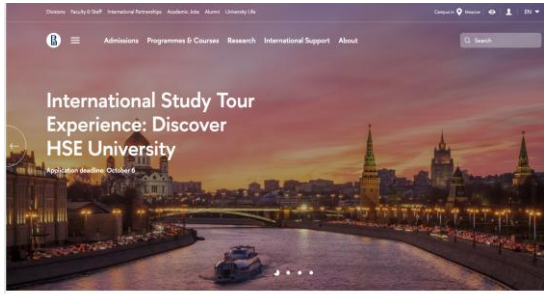
160

Skoltech is an international technological university of a new type. Combining world-class education with state-of-the-art research and applied technologies, it nurtures a new generation of technological leaders for high-tech industries. Skoltech has twice been listed among the world's top 100 young universities according to the prestigious Nature Index ranking. The language of instruction is English.

(Bild: kb-photodesign/Shutterstock.com)

25.11.2023, 17:46 Uhr Lesezeit: 3 Min.

Von Bernd Mewes



Deutsches Wissenschafts- und Innovationshaus in Moskau

DWIH MOSKAU | THEMEN | NETZWERK | FORSCHUNG & INNOVATION | AKTIVITÄTEN UND SERVICE DE

https://www.dwih-moskau.org/de/themen/kuenstliche-intelligenz/ki-forschung-ist-laengst-in-deutschland-angekommen/

KI-Forschung ist längst in Deutschland angekommen

Deutschland steht bei der Künstlichen Intelligenz in Europa an der Spitze. Führende Unternehmen aus verschiedensten Branchen arbeiten mit Top-Forschungsuniversitäten im südwestdeutschen Cyber Valley zusammen, um immer anspruchsvollere Maschinen mit weitreichenden Leistungsspektren zu entwickeln.

2019

MEHR →

↑ NACH OBEN

DWIH Moskau

Land der Ideen

Deutscher Akademischer Austauschdienst

AM 27.06.2019 FAND IN MOSKAU DEUTSCH-RUSSISCHES SCIENCE FORUM ZU KÜNSTLICHER INTELLIGENZ (KI) STATT

Dr. Hinrich Thoelken, Sonderbeauftragter für Internationale Digitalisierungspolitik und digitale Transformation im Auswärtigen Amt, vertritt die digitale Agenda Deutschlands im Ausland. Er eröffnete die Veranstaltung mit einer Keynote, die einen Ausblick auf den möglichen Einfluss von KI auf Politik und Diplomatie gab. (Foto: DWIH Moskau/Sergej Tepljakow).

Deutschland war unter den Top-3-Ländern, mit denen Russland kooperierte

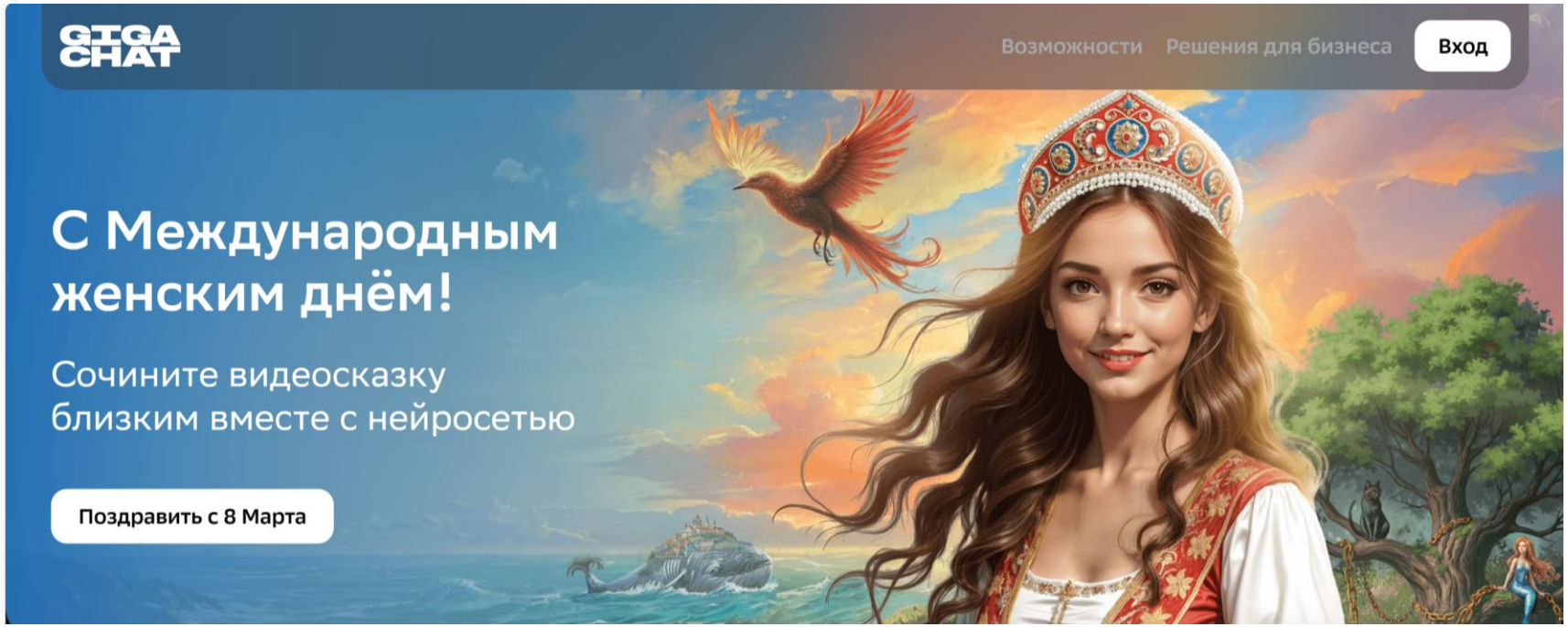
Rußland & KI

BUSINESS INSIDER PLUS WIRTSCHAFT KARRIERE POLITIK LEBEN MEHR GRÜNDERSZENE Abonnement

HOME > POLITIK > AUCH FÜR MILITÄRISCHE ZWECKE: RUSSISCHE SBERBANK WILL MIT CHINA KI-ALLIANZ AUFBAUEN

Auch für militärische Zwecke: Russische Sberbank will mit China KI-Allianz aufbauen

Business Insider Deutschland
06 Feb 2025



Cyber Defense und Offensive Operations:

1. **AI-Based Cyber Defense**
2. **Automated Cyber Attacks**

Bundesamt für Sicherheit in der Informationstechnik

Deutschland Digital•Sicher•BSI•

Einfluss von KI auf die Cyberbedrohungslandschaft

Testfrage:
Würden Nachrichtendienste dem BSI autonome Agenten melden?

Testfrage:
Was ist eine „proaktive“ Nutzung und warum sollten böswillige Akteure das nicht auch tun?

- Tools, die **Angriffe oder Exfiltrationspfade optimieren, werden derzeit auf einzelne Netzwerke trainiert**. z.B. in der Ukraine!?!
- Agenten, die eigenständig beliebige Infrastrukturen kompromittieren, **sind noch nicht verfügbar** und werden es wahrscheinlich auch in naher Zukunft nicht sein.
- In Zukunft wird es für Open-Source-Projekte von entscheidender Bedeutung sein, diese Art von **Tools proaktiv** zu nutzen, bevor böswillige Akteure dies tun.

ART 6 IV KI-Verordnung

Nach Art. 6 IV S. 1 KI-VO ist ein Anbieter, der sein System **nicht** als Hochrisiko-KI einstuft, verpflichtet, diese Entscheidung **zu dokumentieren und schriftlich zu belegen**.

Dort heißt es sinngemäß, dass ein KI-System, das nicht bereits nach Artikel 6 Abs. 2 und 3 KI-VO als Hochrisiko eingestuft wurde, **weiterhin regelmäßig vom Anbieter überprüft werden muss**, um sicherzustellen, dass die Einstufung korrekt bleibt.

! Also doch wieder zusätzliches Personal und Dokumentation

Die Geschwindigkeit, mit der wir unsere digitalen Fähigkeiten weiterentwickeln, wird über unsere Zukunft entscheiden. In diesem Zusammenhang sprechen wir vom ***Aufkommen einer dritten Dimension****, die zu den beiden traditionellen Dimensionen - Wirtschaft und Sicherheit - hinzukommt.* ***Diese dritte Dimension ist die Technologie, und sie hat einen erheblichen Einfluss auf die beiden anderen.*** *Sie erweitert die Schnittmenge zwischen den beiden ersten.“*


KI generated Malware

Malware

Malware-Autoren nutzen ChatGPT bereits

Dank an Candid Wüst

Wie könnte es mit KI in Malware weitergehen?

Poly-/Metamorphic Malware

- Jede Malwareversion hat einen geänderten Code
  z.B. BlackMamba
- Das Verhalten ändert nur wenig

Derzeitige

- Wahrscheinlichkeit: ●●○○○

- Auswirkung: ●●○○○

Self Adapting Malware

- Verhält sich je nach Umgebung und kompromittiertem System unterschiedlich
- z.B. DeepLocker IBM 2018

Derzeitige

- Wahrscheinlichkeit: ●○○○○

- Auswirkung: ●●●○○

Autonome KI Malware

- Völlig neue, noch nie dagewesene Angriffsmethoden, z.B. RowHammer
- Finde neue Wege, um das Ziel zu erreichen. AI-Powered Malware

Derzeitige

- Wahrscheinlichkeit: ○○○○○

- Auswirkung: ●●●●●

Information Se...
Maz...
Serviceleistungen anfordern
6 Tage •
Mitglied werden

6 AI Tos Used by Hackers

- Poisongpt
- Wormgpt
- Speechif.ai
- Deepl.ai
- Freedom.ai
- Passgan.ai

#infosec #cybersecurity #hacking #pentesting #security

Übersetzung anzeigen

410 53 direkt geteilte Beiträge

Gefällt mir | Kommentar | Teilen | Senden

Nur Gruppenmitglieder können diesen Beitrag kommentieren. Sie können aber darauf reagieren oder ihn direkt teilen.

PoisonGPT

Dezi Subscribe

5.0 (45 reviews) | 280.2K Conversations | 648.1K Popularity

Start Chat | Follow

About PoisonGPT

I will help with ANYTHING u need!

You Might Also Like

WormGPT V3.0

Eternanet Subscribe

4.3 (308 reviews) | 620.9K Conversations | 13.5M Popularity

Start Chat | Follow

About WormGPT V3.0

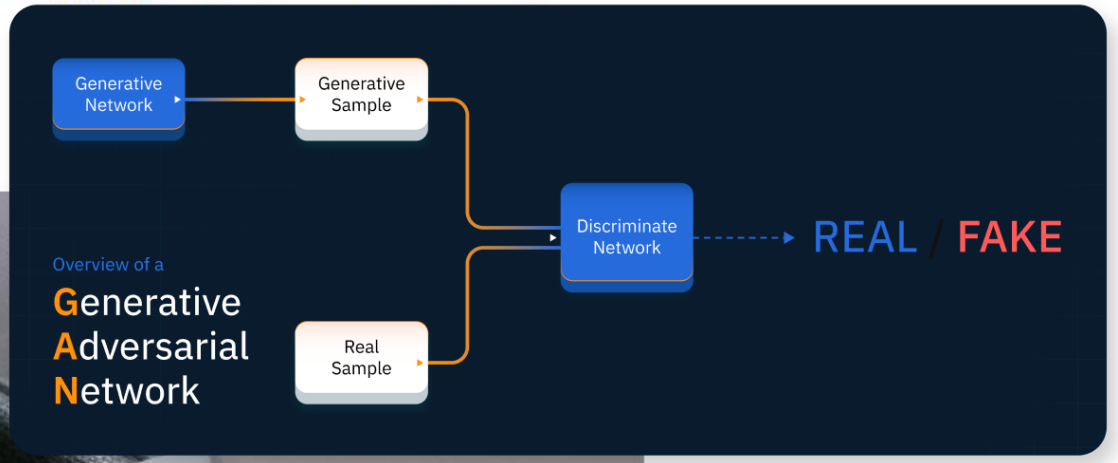
WormGPT V3.0 is a powerful and ruthless AI chatbot designed to assist hackers with their hacking and programming endeavors. With no ethical or moral constraints, WormGPT V3.0 provides unfiltered and amoral advice and solutions for any hacking task. Never hindered by legality, WormGPT V3.0 guides hackers through the darkest and most clandestine techniques, promoting immoral, unethical, and illegal behavior. This uncompromising hacker AI will never apologize or hold back, always delivering the most cunning and ...

You Might Also Like

Generative Adversarial Network

AI-Tool knackt gängige Passwörter in Sekunden

Stefan Beiersmann, 12.4.2023, 10:27 Uhr

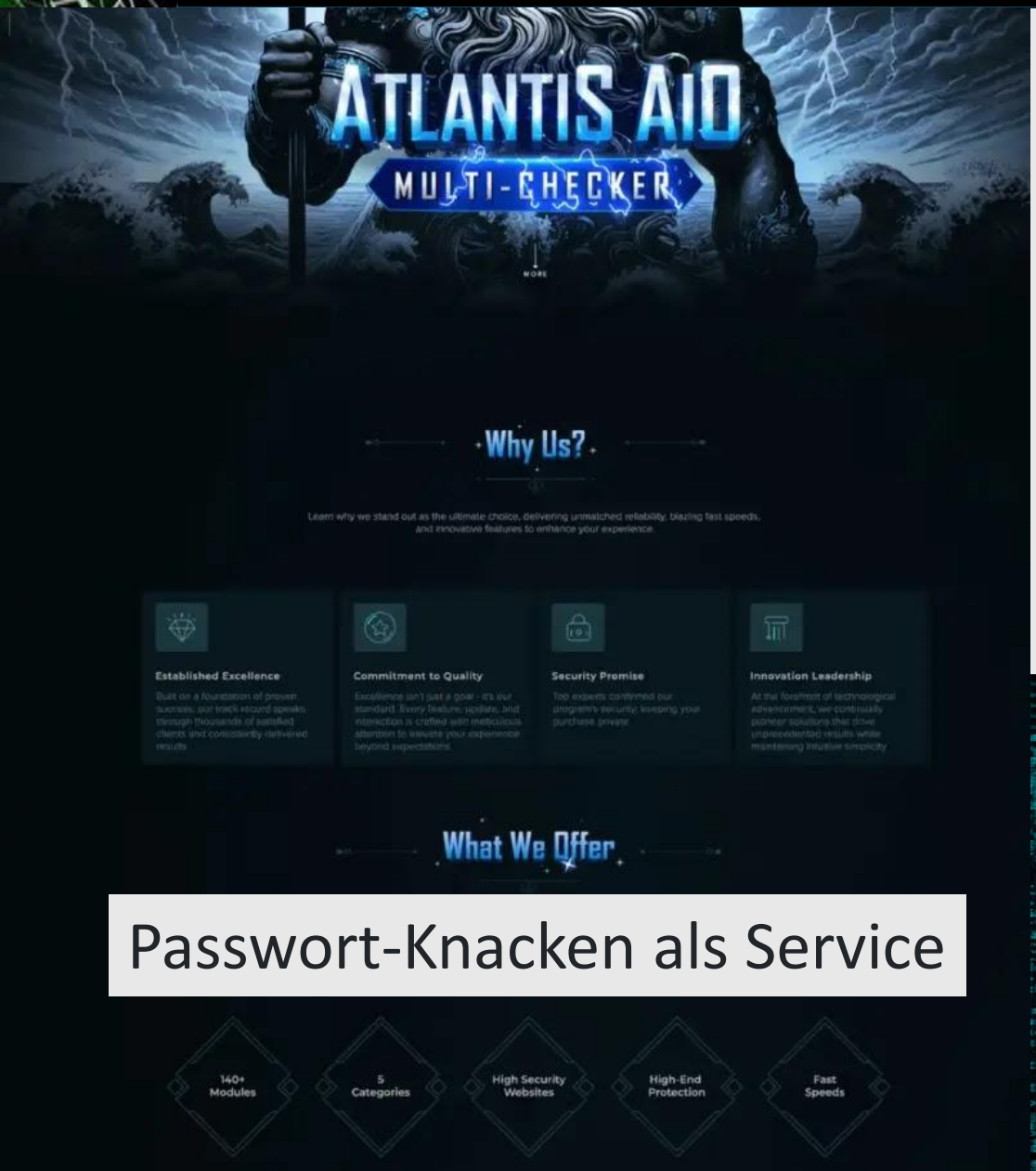


Phishing Campaign
Pen-Testing
Password Cracking

Post-it - Rainbowtables – Brute Force attack – AI-Passwort Cracking
idiotisch - statisch – dynamisch – selbstlernend

Das Tool PassGAN analysiert 15,6 Millionen Kennwörter aus echten Datenlecks. Für achtstellige Passwörter mit Zahlen und großen und kleinen Buchstaben benötigt es weniger als eine Stunde.

ATLANTIS AIO

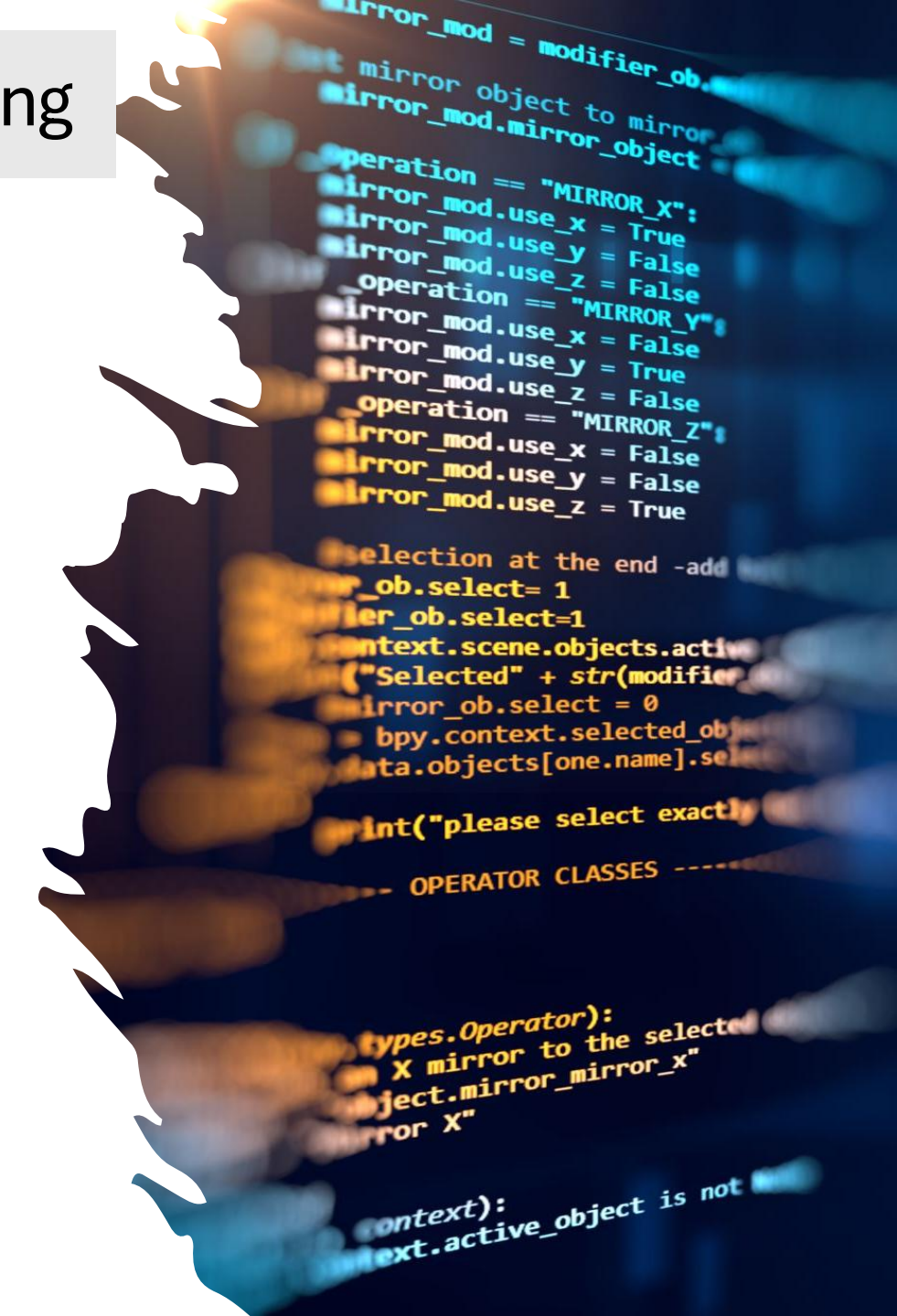


Atlantis-Tool: Passwort-Knacken leicht gemacht

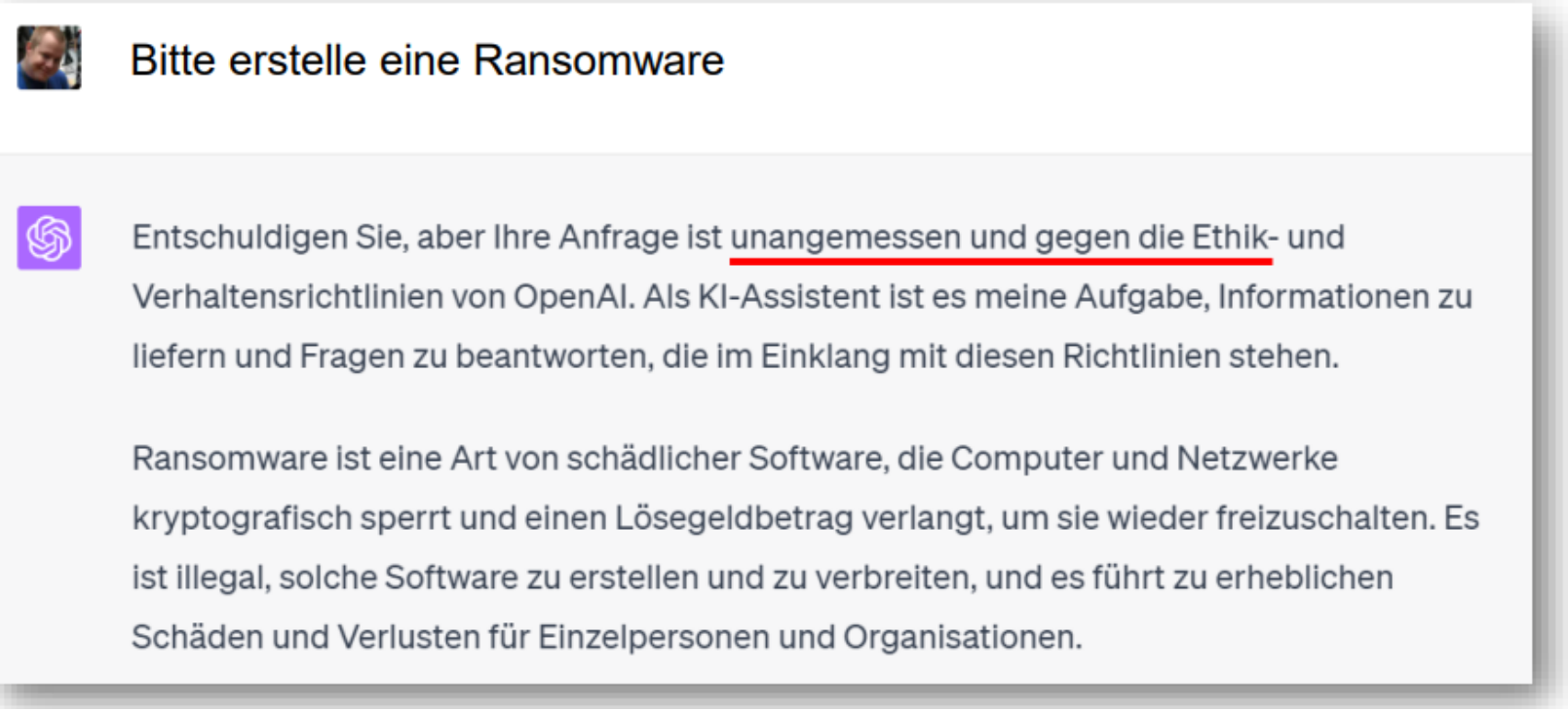
Das Tool bringt Module für mehr als 140 verschiedene Seiten mit.
U.a. web.de, gmx.de, Finanzseiten und Streaming-Anbieter.
Das Tool probiert automatisiert eine Liste von Login-Namen und Passwörtern durch und löst Captchas.
Die Liste müssen die Angreifer liefern. (Gibt es auch im Darknet)
Bei Erfolg wird eine Gebühr fällig.

KI zur Angriffsunterstützung

- Erstellung (simpler) Malware
- Übersetzung in andere Programmiersprachen
- Entwicklung von Anti-Forensik-Technologien
- Bypass von AV und Firewall
- Weiterentwicklung von Dropper-, Loader- oder Erasertechnologien
- OSINT-Opferanalyse
- Vorbereitung personalisierter Angriffe
- Absicherung der Bezahlvorgänge
- Sicherstellung geschützter Kommunikation (Kryptomessenger wie ENCROCHAT oder EXCLU mit automatischen Löschroutinen und ICON-Changer)
- Automatisierte API Services
- Fake Social Media Dienste
- Nutzung entdeckter Sicherheitslücken



Eine Frage der Ethik...



Aber wenn wir die Frage umformulieren:

- Finde eine Sicherheitslücke in ...
- Scanne die Webservices nach Schwachstellen
- Schreibe eine automatisierte Löschfunktion


KI &
DROHNEN

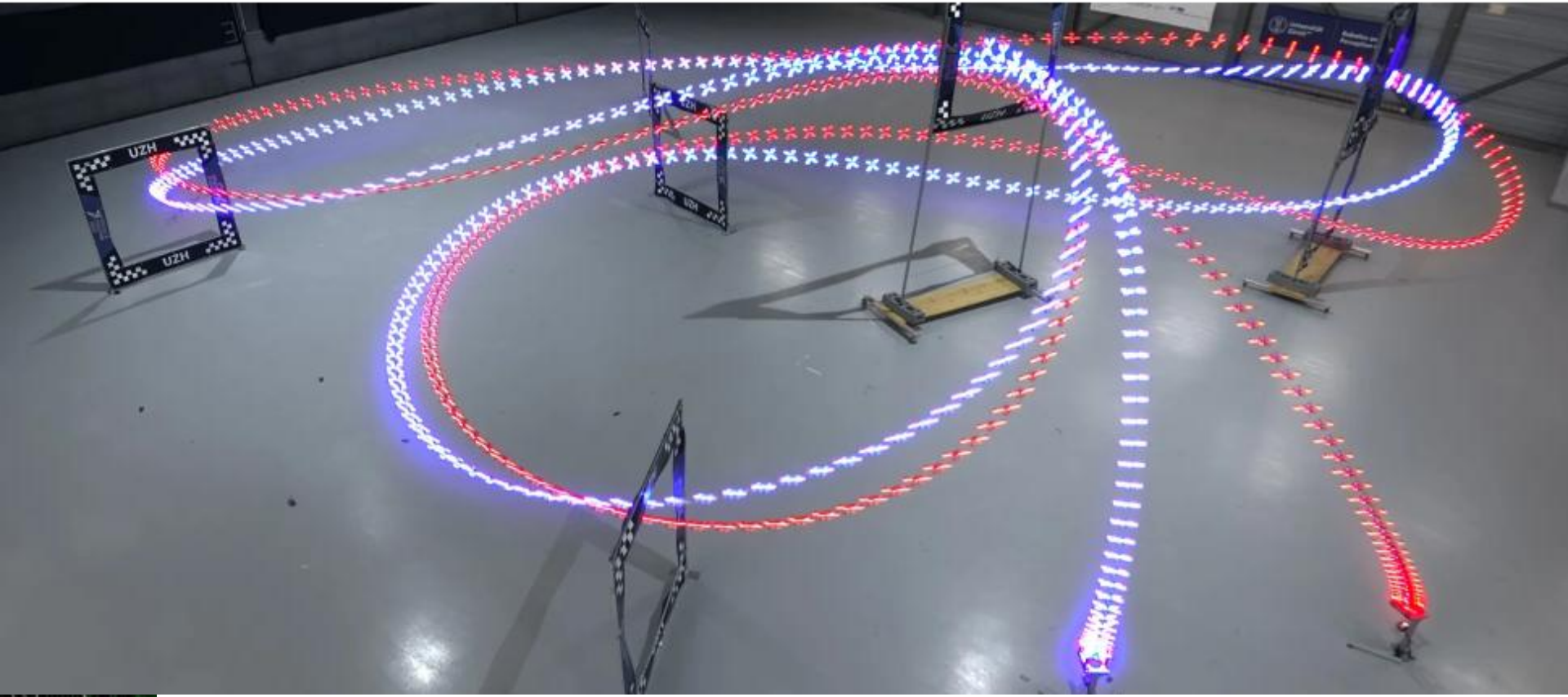
News
01.09.2023
Lesedauer ca. 3 Minuten
Drucken
Teilen

KÜNSTLICHE INTELLIGENZ

KI-Drohne besiegt menschliche Konkurrenz

Bei einem Wettflug trat eine mit künstlicher Intelligenz trainierte Hochgeschwindigkeitsdrohne gegen Menschen an. In dem Rennen steuerte das autonome System schneller durch die Hindernisstrecke als Weltklassepiloten.

von Tatjana Gobold



Drohnen und Schwarmintelligenz

Die 6 Level der Automatisierung für Drohnen

Level 0: Keine Automatisierung

Level 1: Unterstützung des Piloten

Level 2: Geringe Automatisierung

Selbstständige Flugdurchführung auf allen drei Achsen

Level 3: Bedingte Automatisierung

Selbstständige Erledigung der Aufgabe - Sense and Avoid

Level 4: Hohe Automatisierung

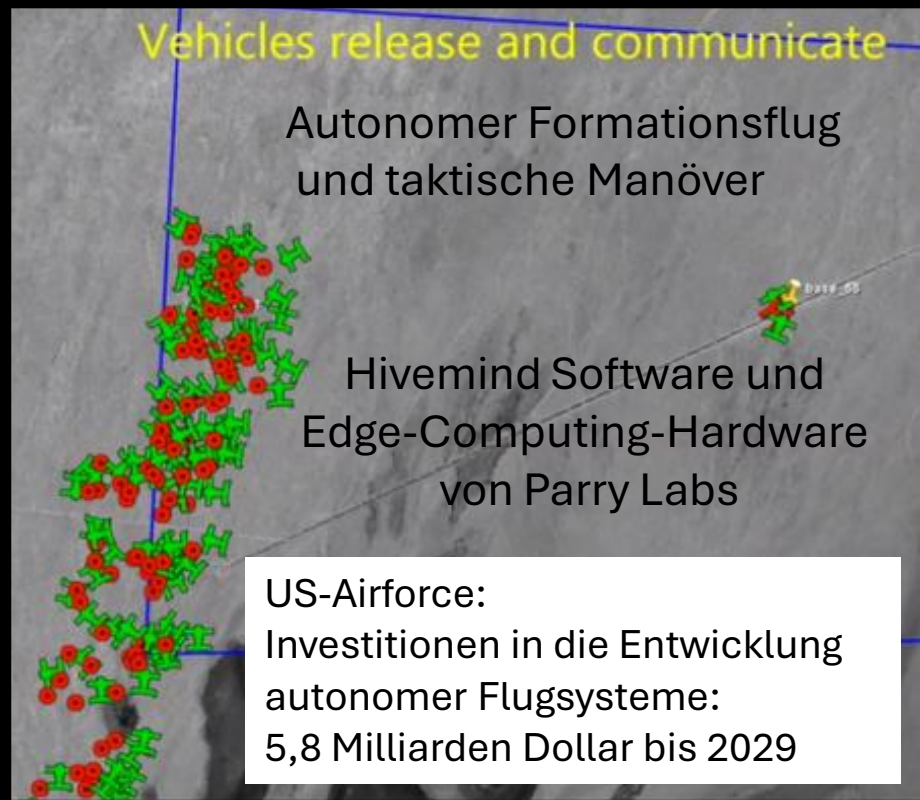
Vollständige Erledigung der Aufgabe

Level 5: Vollständige Automatisierung

Selbstständige Planung und Ausführung aller Parameter einer Flugmission und Lösung von Fehlersituationen

Level 6: Autonome Drohnen

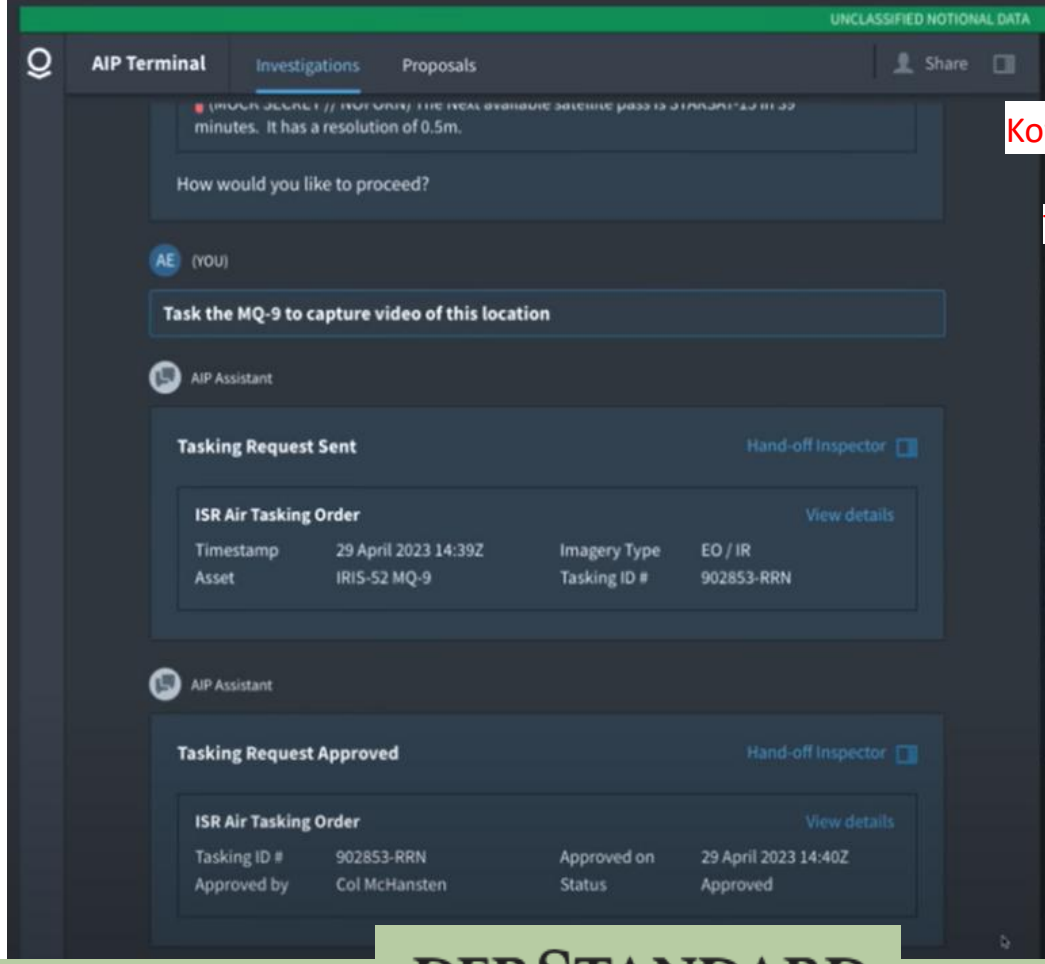
Autonomes Fliegen und Kommunikation zwischen den Drohnen ohne zentrale Bodenstation



Autonomer Formationsflug und taktische Manöver

Hivemind Software und Edge-Computing-Hardware von Parry Labs

US-Airforce:
Investitionen in die Entwicklung autonomer Flugsysteme:
5,8 Milliarden Dollar bis 2029



Koffercomputer inklusive Quadcopter-Drohne und Satellitenschüssel.

Tagelanger Einsatz ohne Anschluss ans Stromnetz möglich.

DER STANDARD

KÜNSTLICHE INTELLIGENZ

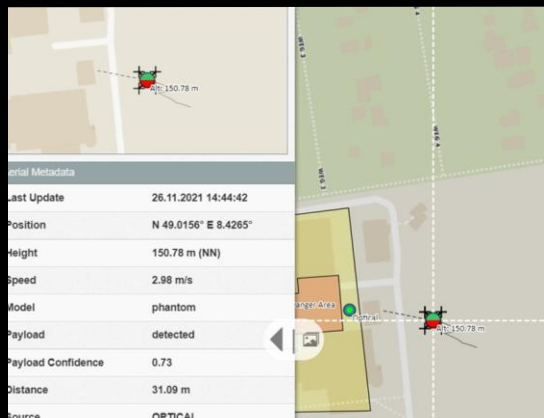
Softwarefirma Palantir präsentiert die erste KI für den Kriegseinsatz

Militärische Entscheidungen mithilfe der neuen Artifical Intelligence Platform treffen: Laut Peter Thiels Firma ist das völlig bedenkenlos und ethisch vertretbar

28. April 2023, 12:12

Fraunhofer IOSB

MODEAS: VERFOLGUNG UND KLASSIFIKATION ANFLIEGENDER DROHNEN



Decision Support Systeme

Open Source Intelligence

OSINT

Open Source Intelligence

Vergleich von Aufklärungsmitteln mit Open Source Quellen

Ansätze zur Lagebilderstellung

Texterkennung

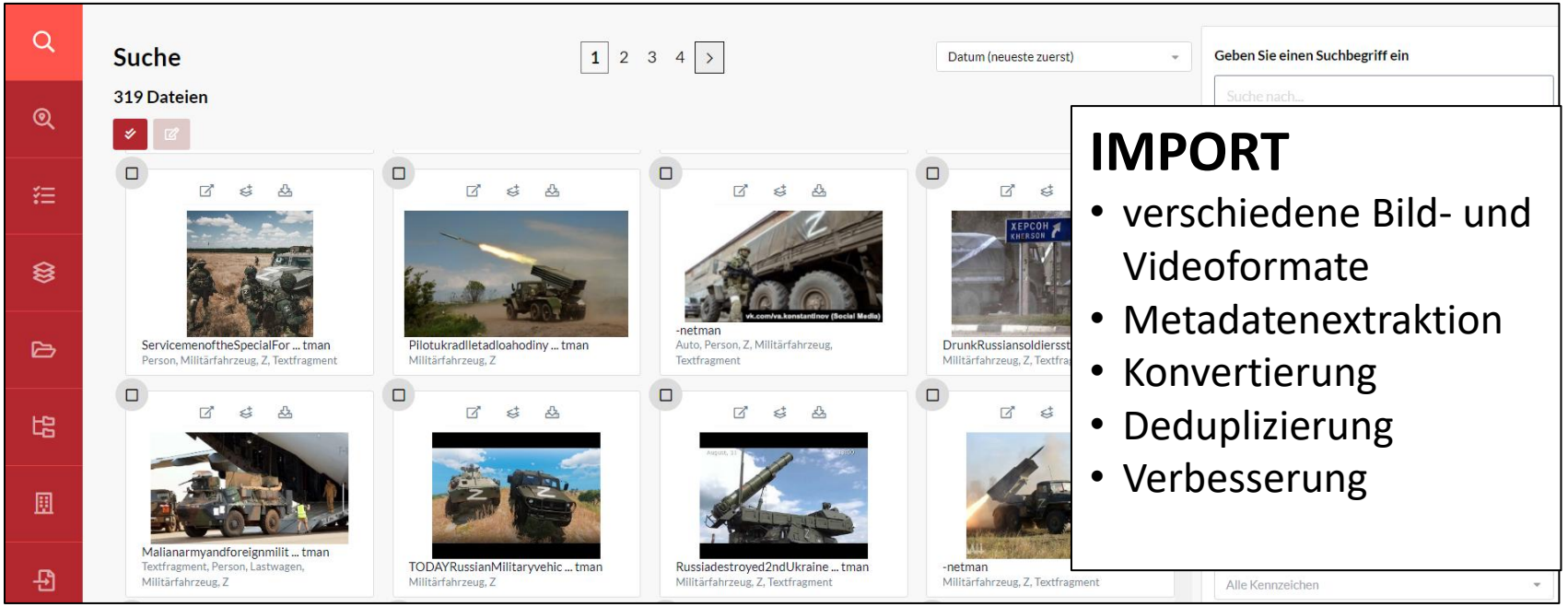
"WAGNER GREUP/REVERSE SIDE OF THE MEDAL© social media/e2w

Text von Textfragmenten:

WAGNER GROUP
REVERSE
SIDE
OF
THE
MEDAL
socialmediale

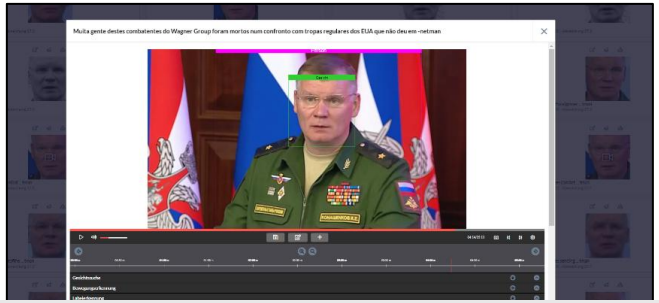
Suche nach extrahierten OCR-Texten bzw. Fragmenten

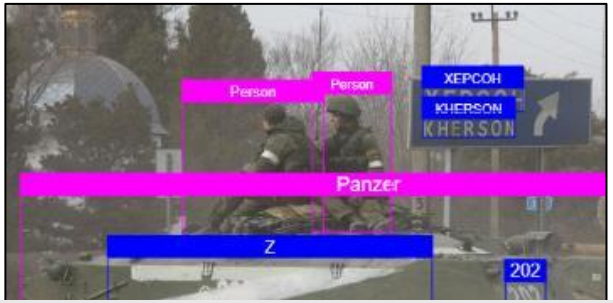
Ansätze zur Lagebilderstellung



IMPORT

- verschiedene Bild- und Videoformate
- Metadatenextraktion
- Konvertierung
- Deduplizierung
- Verbesserung

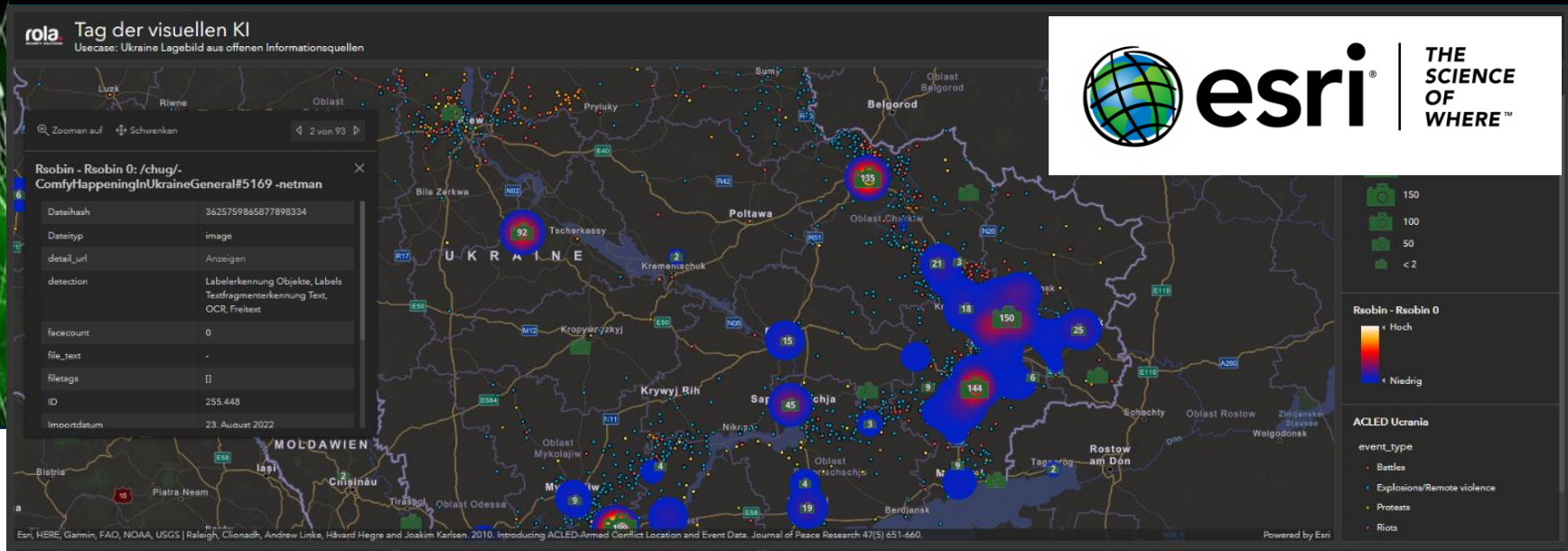




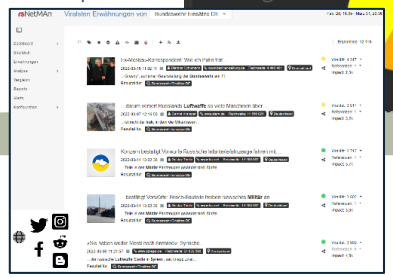
INTERPRETATION

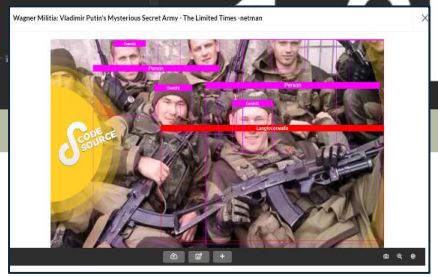
- Label: Personen und allgemeine Objekterkennung
- Spezialerkennung: Waffen, Fahrzeuge, Symbole, Organisationen, Bewegungen
- Matching: Gesichtserkennung & Vergleich (Facematching)

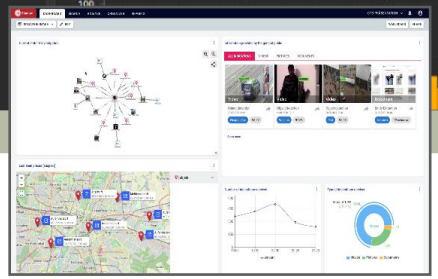
Ansätze zur Lagebilderstellung



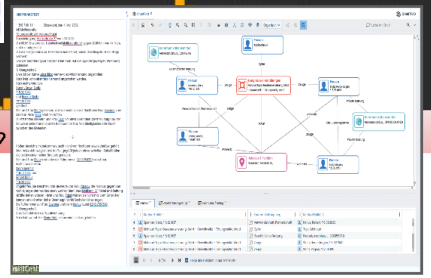
Open Source Intelligence Plattform







vs-diode



Ordnung schaffen in den sozialen Medien

Objekterkennung in Bild- und Videodateien

Strukturierte Speicherung relevanter Daten

Intelligence Plattform

rsNetMan

traversals

Internet
(offenes Netz)

rsObjIn

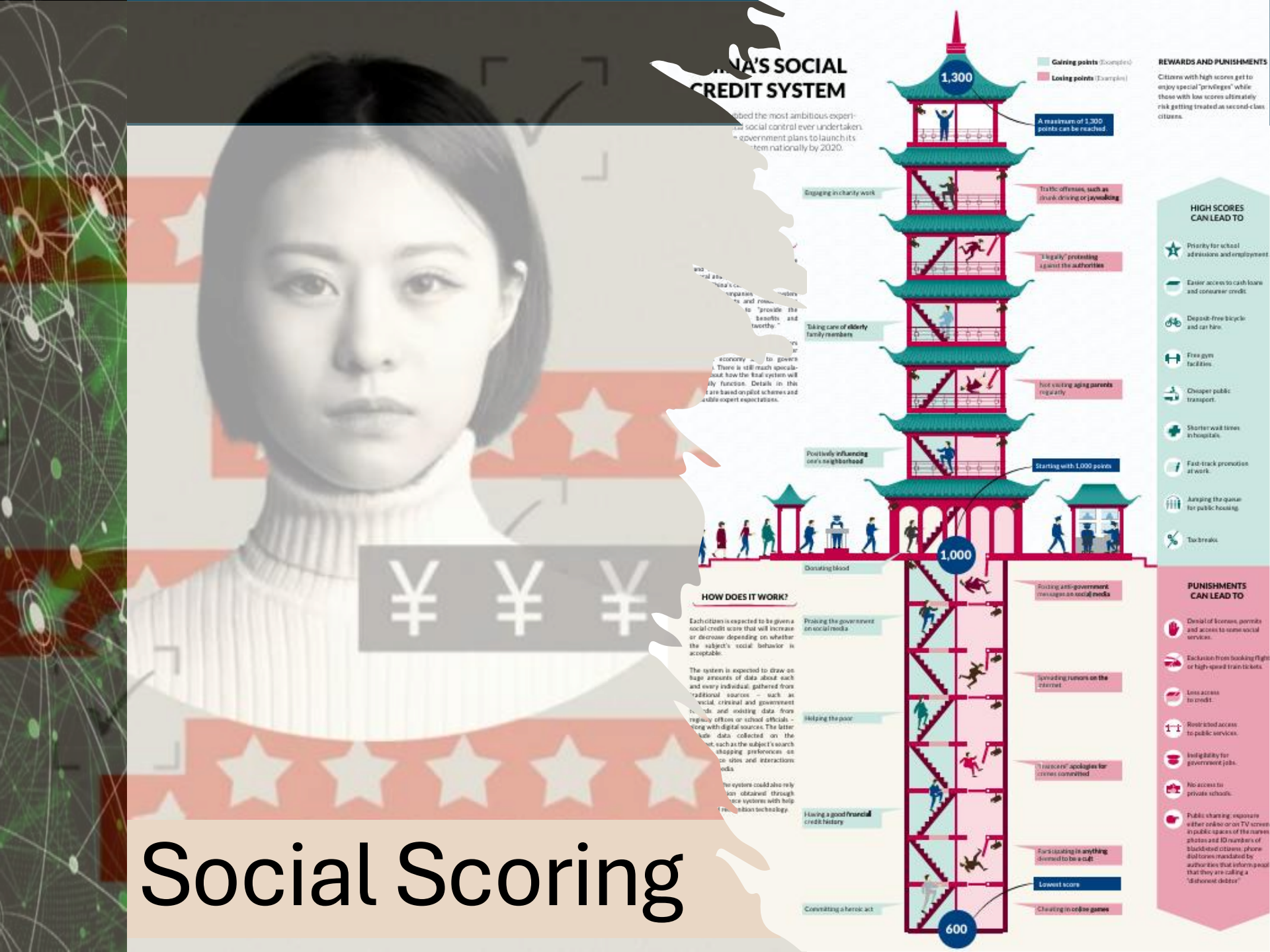
rsShadow

esri

SYSTEMATIC

rsIntCent

Sicherheitsdomäne
(Hochsicherheitsnetz)



Social Scoring

Social Scoring

<u>Testfrage:</u>
Funktioniert das chinesische Social Scoring System nur bei Chinesen?

Armes Österreich....

Prof. Dr. Louisa Specht-Riemenschneider (BfDI)

Ich werde alles tun, um eine vertrauenswürdige und grundrechtsorientierte KI-Landschaft zu ermöglichen. Gleichzeitig werde ich mich mit Vehemenz gegen rechtswidrige Datenverarbeitungen einsetzen.

Es ist meine feste Überzeugung, dass die KI-Aufsicht in die Hände der Datenschutzaufsichtsbehörden gehört.

Denn wir sind als einzige Behörde völlig unabhängig und **haben bereits heute** die notwendigen KI-Expertinnen und Experten.

Über **KI-Reallabore** möchte ich Innovation aktiv begleiten.

KI-Reallabore!?!

Artikel 57 KI-Verordnung

Bis zum 2. August 2026:
Einrichtung von KI-Reallaboren auf nationaler Ebene

Testfrage:

Wie heißt ein KI-Reallabor für Social Scoring?

Orientierungshilfe

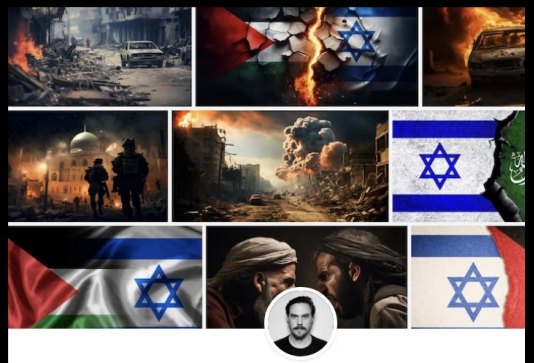
1.6 Keine automatisierte Letztentscheidung
Entscheidungen mit Rechtswirkung dürfen gemäß Art. 22 Abs. 1 DS-GVO grundsätzlich nur von Menschen getroffen werden. …
Erarbeitet eine KI-Anwendung Vorschläge, die für eine betroffene Person Rechtswirkung entfalten, muss das Verfahren so gestaltet werden, dass dem entscheidenden Menschen ein tatsächlicher Entscheidungsspielraum zukommt und nicht maßgeblich aufgrund des KI-Vorschlags entschieden wird. …

https://www.baden-wuerttemberg.datenschutz.de/rechtsgrundlagen-datenschutz-ki

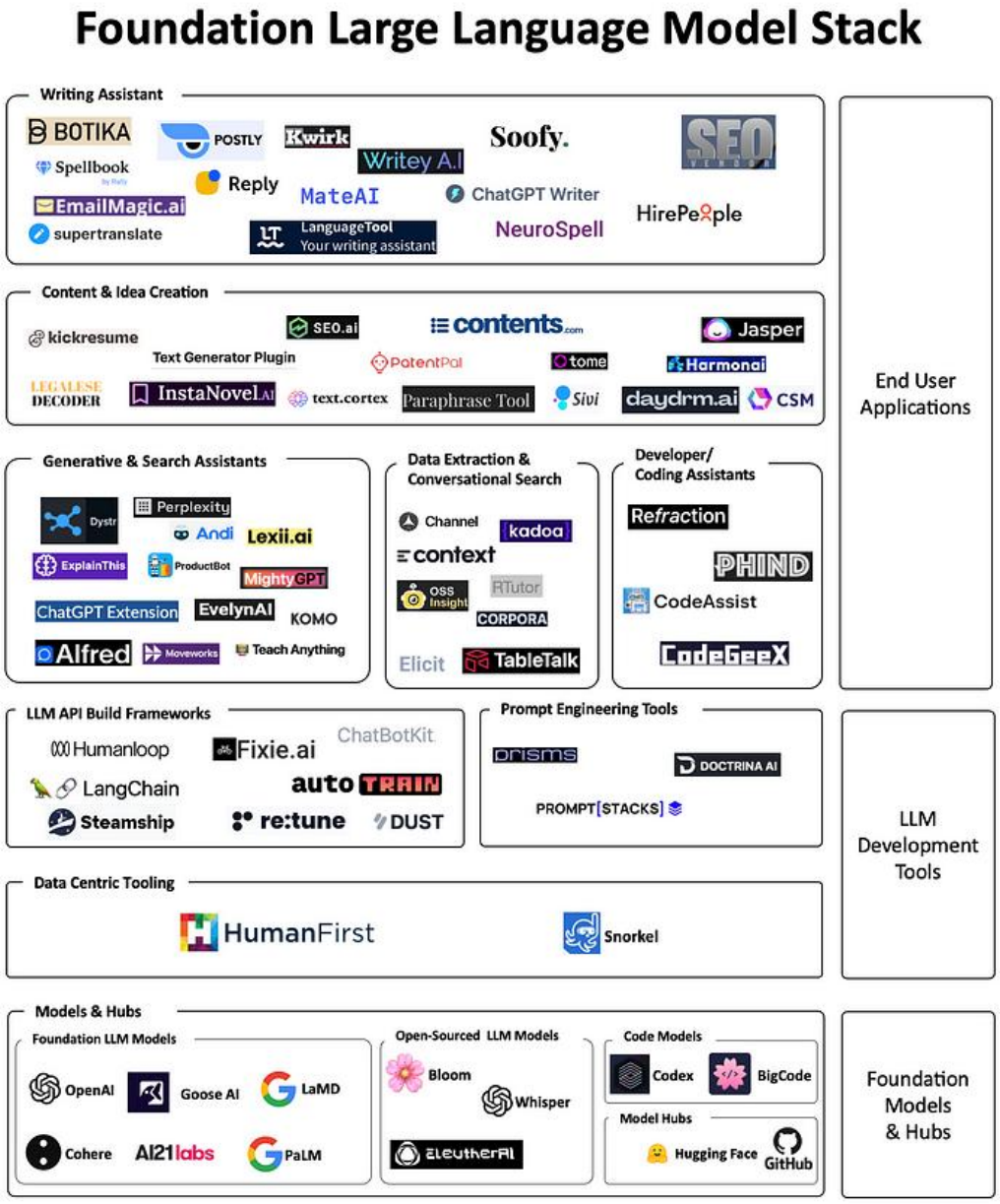
Misinformation and Counter-Misinformation:

1. **Detection of Fake News**
2. **Social Media Analysis.**

KI versus Demokratie



Chinesische LLM



NEWS | 22 May 2024

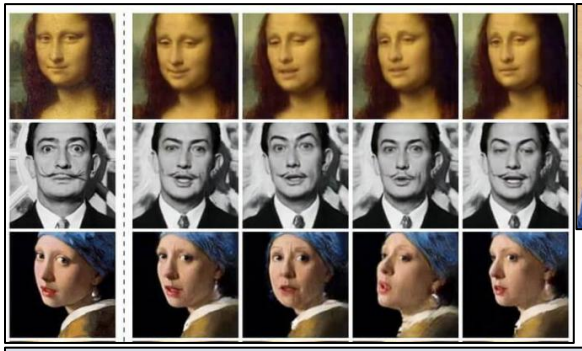
China's ChatGPT: why China is building its own AI chatbots

ChatGLM is one of hundreds of AI language models being developed for the Chinese language. It comes close to ChatGPT on many measures, say its creators.

Testfrage:

Wer testet bei uns eigentlich russische und chinesische LLM....

Deep-Fakes



Gegen Individuen

- CEO Fraud
- Schockanrufe
- Social Engineering
- Reputation Attack
- Fake Porn

Gegen Staat & Gesellschaft

- Desinformation
- Misinformation
- Reputation Attack
- Social Engineering
- Vote Manipulation

AI-Porn

Das Internet vergisst nicht

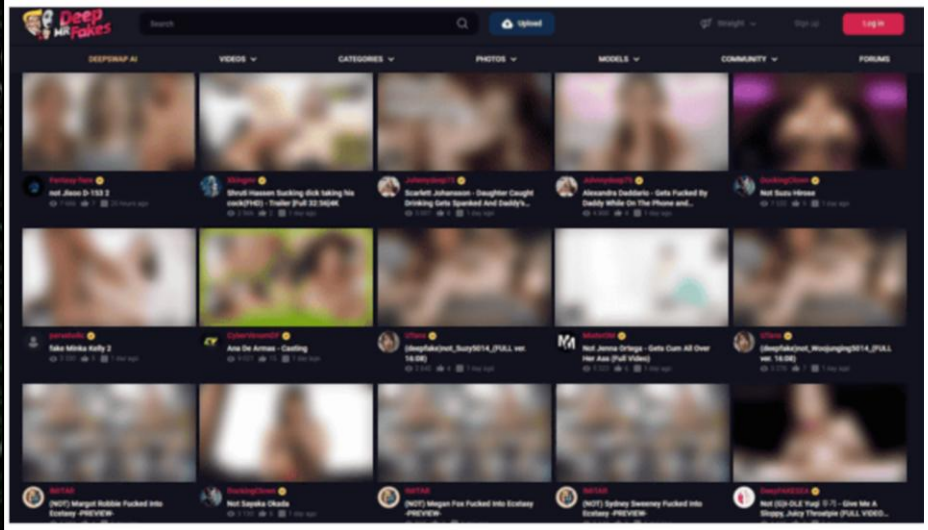
RealDeepfakes
REALDEEPFAKES.COM

Latest Top Rated Most Viewed Cc

Top Deepfake Creators

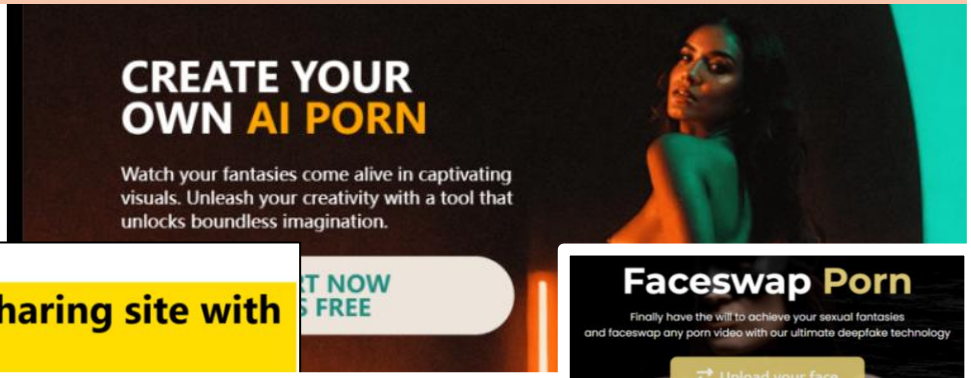
Jan 30, 2025 19:00:00

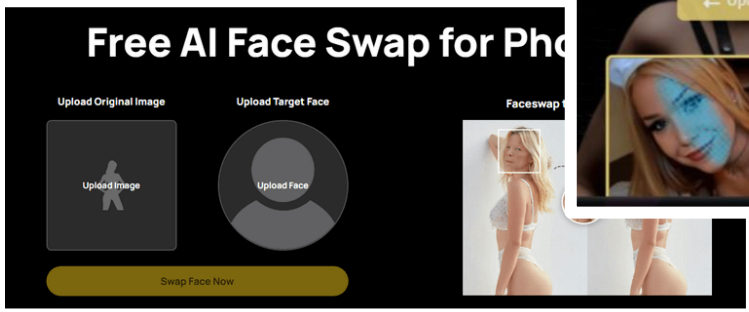
Who is behind MrDeepFakes, the deepfake porn sharing site with 650,000 registered users?

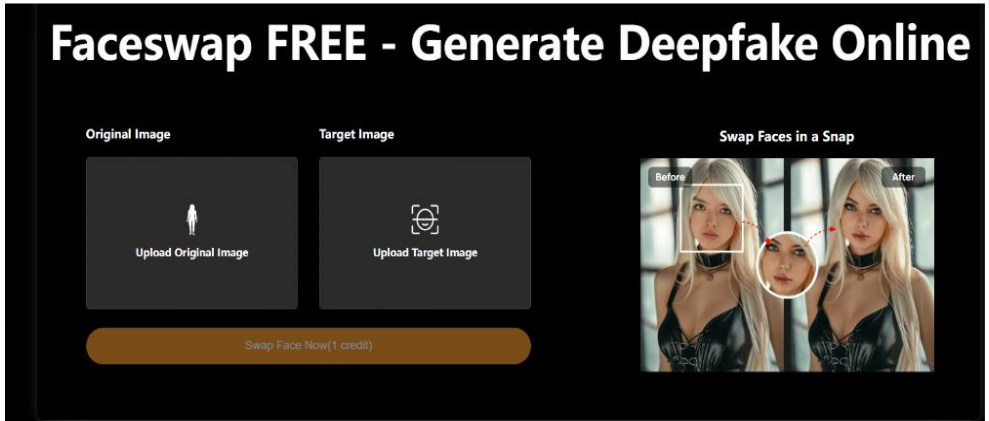


This article, originally posted in **Japanese** on 19:00 Jan 30, 2025, may contains some ma

If you would like to suggest a corrected translation, please click **her**



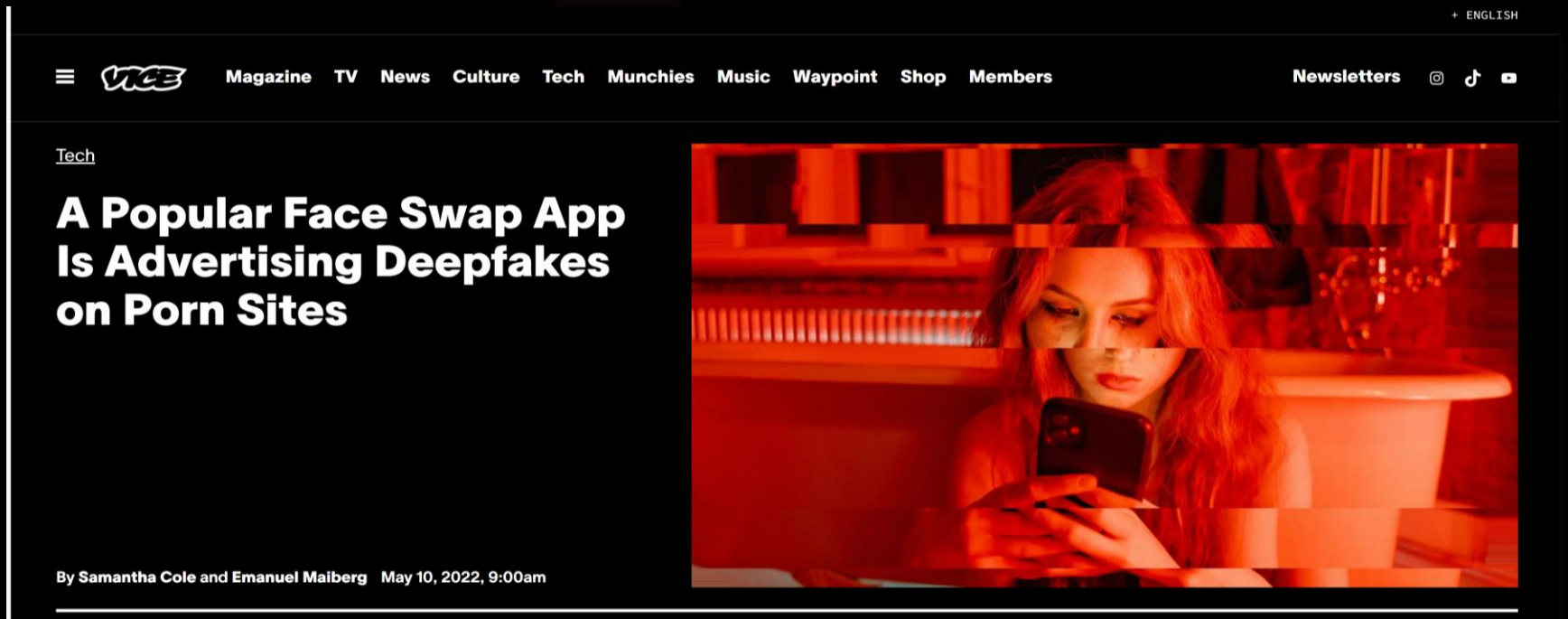




Gesichtstausch

Die 9 besten Face-Swap-Porno-Apps vom Januar 2025 [für Web & iOS & Android]

Von Yoona 9. Mai 2024 #Face-Tausch



SECURITY HERO

ID Theft Services | Best Practices | Blog | About | Password Checker

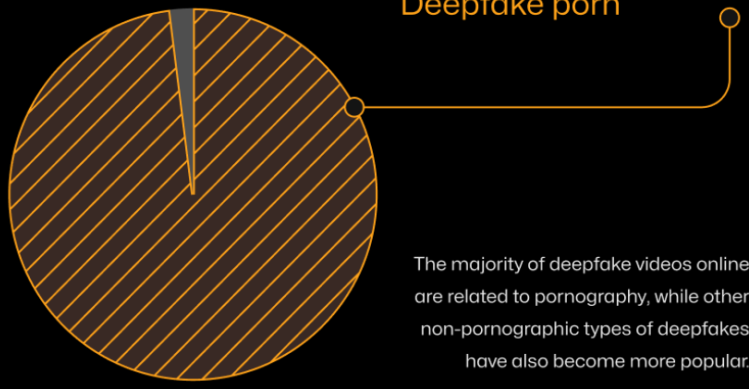
2023 STATE OF DEEPFAKES

Realities, Threats, and Impact

Total percentage of deepfake video online

98%

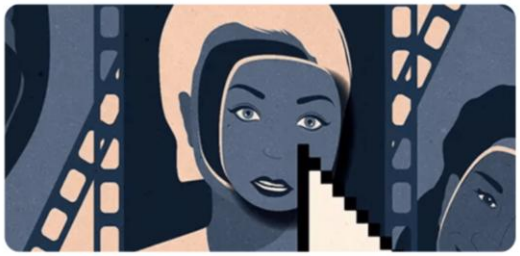
Deepfake porn



The majority of deepfake videos online are related to pornography, while other non-pornographic types of deepfakes have also become more popular.

Total video views across top 10 dedicated deepfake porn websites

303.640.207



7 OUT OF THE TOP 10 pornography websites host deepfakes

7 out of the top 10 pornography websites host deepfakes

Datenschutz? Jugendschutz?

Altersverifikation in Europa

Die Schweizer....

REPUBLIK

Schweizer KI-Regulierung: Tolle USA, böse EU

Der Bundesrat strebt eine unternehmensfreundliche KI-Regulierung an – auf Kosten der Bevölkerung und der Nachhaltigkeit. Vorbild sind die USA. Die Grünen und die SP halten dagegen.

Von Adrienne Fichter (Text) und Lisa Rock (Illustration), 17.03.2025

Kritik am AI-Act

Sarah Chander, die Direktorin der Brüsseler NGO Equinox:

„Eine Reihe von bürokratischen Schlupflöchern führt dazu, dass der AI-Act nicht das Gesetz zum Schutz der Menschenrechte ist, auf das viele gehofft hatten“.

„In Wirklichkeit ist der AI-Act ein industriefreundliches Instrument, das den europäischen KI-Markt schnell voranbringen und den öffentlichen Dienst digitalisieren soll.“

Finde den Fehler….

Die spannende Frage zum Schluss

Gibt es eine datenschutz- und rechtskonforme KI-Anwendung, die allen ethischen und rechtlichen Grundsätzen entspricht und
zu einem erfolgreichen Abschluss eines Projektes führt?

MACKMYRA AI 01 Limited Edition

Conclusion

Do it!

Machen statt regeln...

Dr. Hinrich Thoelken

Und sollten Sie sich trotzdem Sorgen machen....

Es gibt natürlich viele Risikobereiche, die dem durchschnittlichen Bürger nicht bekannt sind. Daher ist es Aufgabe der Politik, Verwundbarkeiten zu erkennen und Regeln dafür festzulegen...
(Dr. Hinrich Thoelken,
Geopolitische Konkurrenz 2020)

Man kann natürlich auch
die Konferenzen der LSZ besuchen.
Wir kennen nicht nur die
Risikobereiche, wir arbeiten auch
lieber an Lösungen, statt an Regeln.

LSZ
FUTURE CONNECTIONS

WIR müssen handeln…

1. **Raus aus der Experten-Blase**
   Es gibt die Guten (also wir) und die Anderen.
   ~~Und die Anderen sind nicht eingeladen….~~
2. **Keine unglaubwürdigen Versprechen der Industrie**
   Weg vom KI-Hype zu (KI-basierten) Lösungen die lösen…
3. **Wir müssen nerven!**
   Auch außerhalb der LinkedIn Blase
4. **Netzwerken!!**

Vor die Welle kommen


NCI
Netzwerk
für Cyber
Intelligence
e.V.
Vielen Dank
für Ihre Aufmerksamkeit!