Wie KI die Welt der Sicherheit beherrschen wird

KI wird Infrastruktur.

Und Infrastruktur wird Macht.

Welcome to Cursor

The AI Code Editor

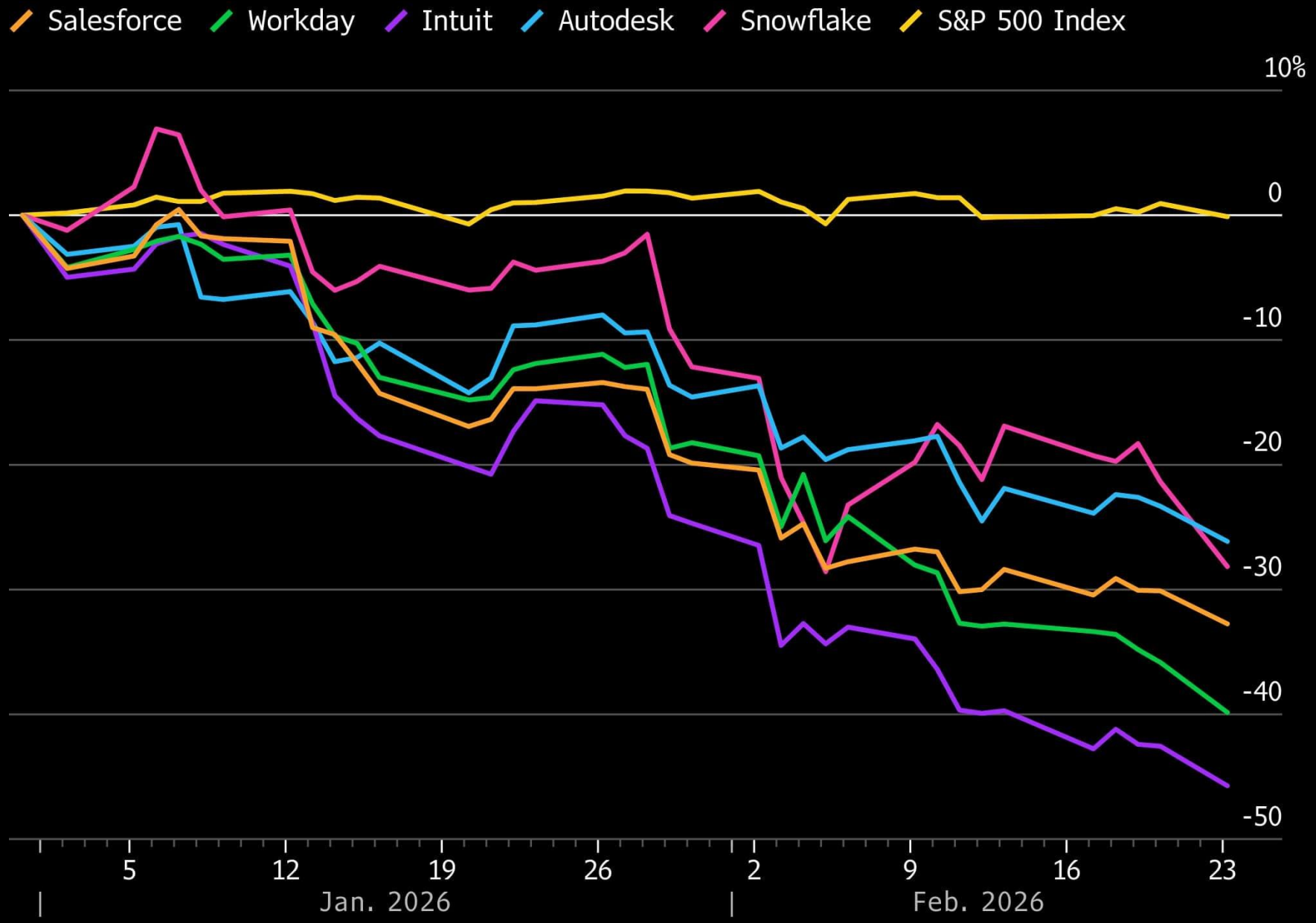
Sign Up

Log In

Skip and continue

Software wird billig. **Make or Buy wird neu gedacht.**

Software Stocks Tumble to Begin Year on AI Fears



Source: Bloomberg
Note: Data is normalized with percentage appreciation as of December 31, 2025.

Bloomberg

Das Gefährliche ist nicht: ‚KI macht Fehler.‘
Das Gefährliche ist: **KI macht Geschwindigkeit.**

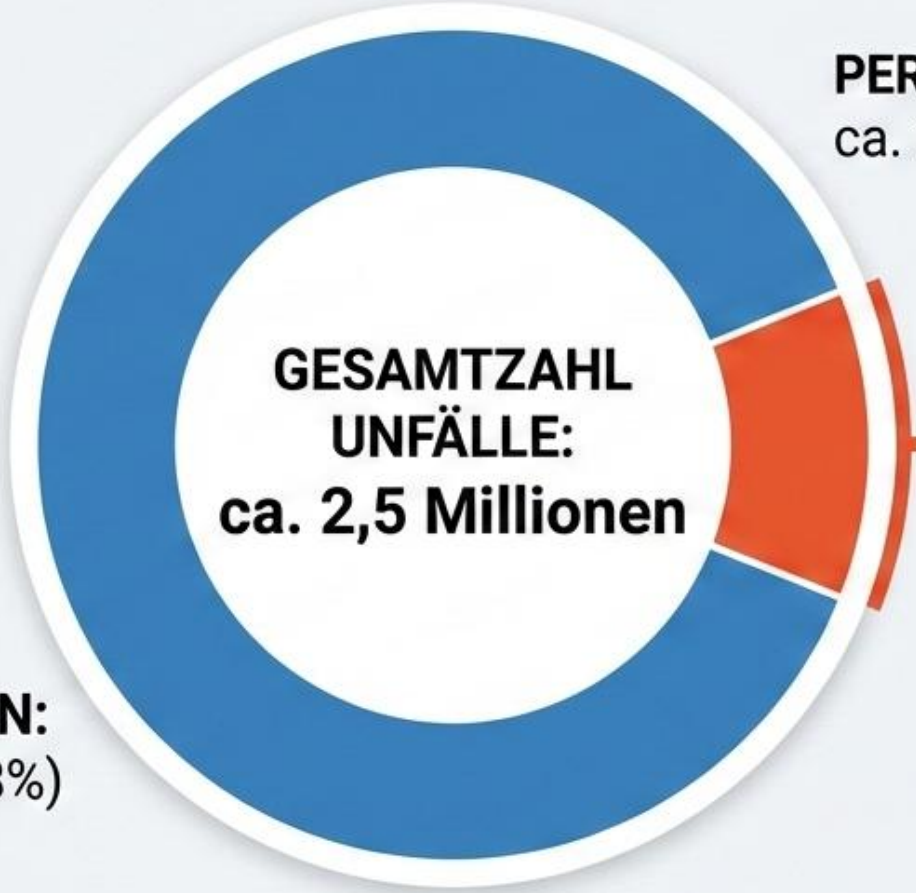
Wenn Handlungen billig werden, wird Angriff billig.
Und Verteidigung muss sich neu erfinden.

War nie relevant, bis die Autos kamen!

Anzahl der Pferdeunfälle mit Todesfällen gegenüber letztem Jahr deutlich reduziert.

Berlin, den 12. Juli. (1830)

Verkehrsunfälle in Deutschland 2025



PERSONENSCHÄDEN:
ca. 290.000 (12%)

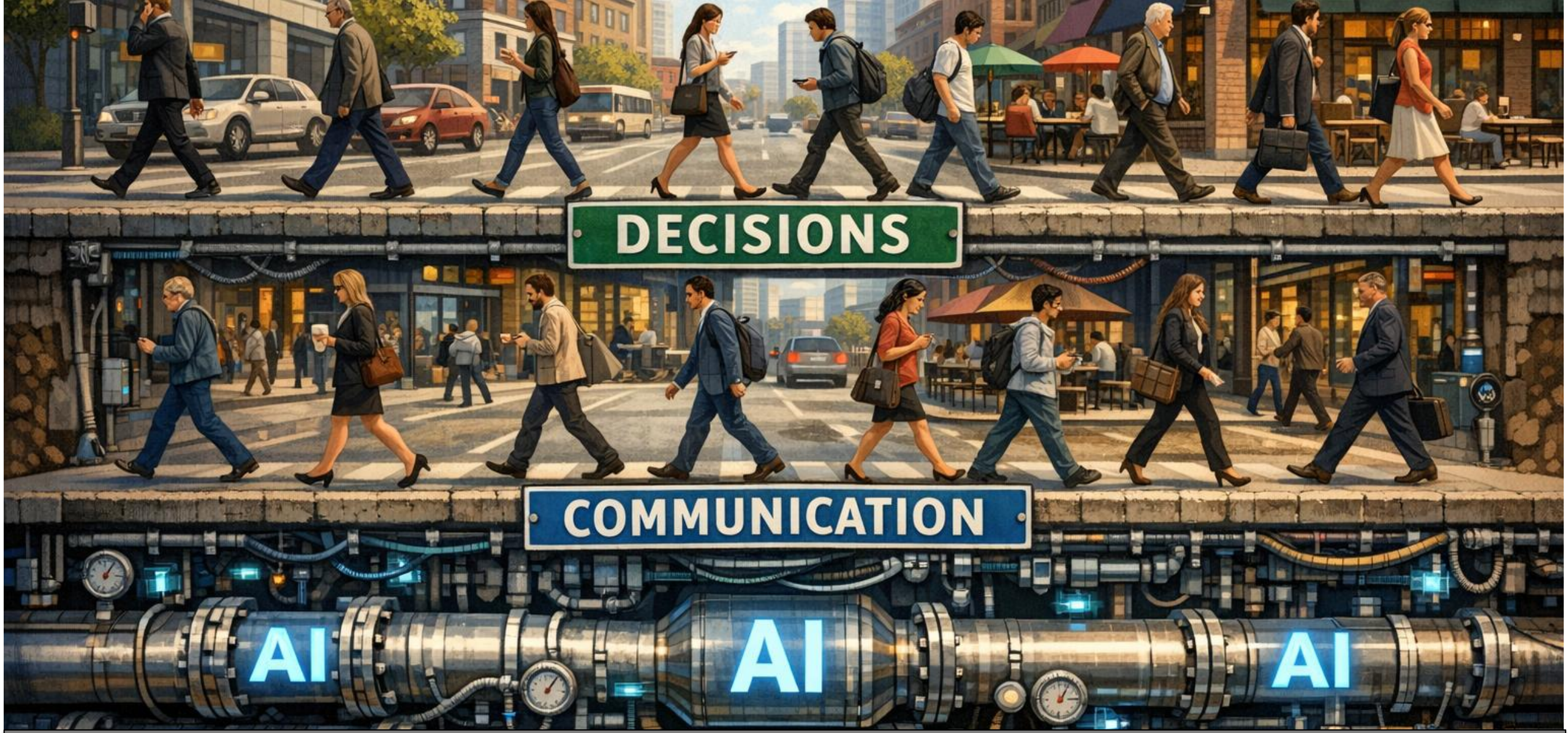
SACHSCHÄDEN:
ca. 2,2 Millionen (88%)

VERLETZTE:
ca. **370.000**

VERKEHRSTOTE:
ca. **2.810**

DURCHSCHNITT PRO TAG: ca. 6.850 Unfälle

Quelle: Schätzungen basierend auf vorläufigen Daten des Statistischen Bundesamtes & Polizei



KI ist nicht Werkzeug oder Technologie. KI wird Infrastruktur!
Das kannst Du nicht „patchen“!

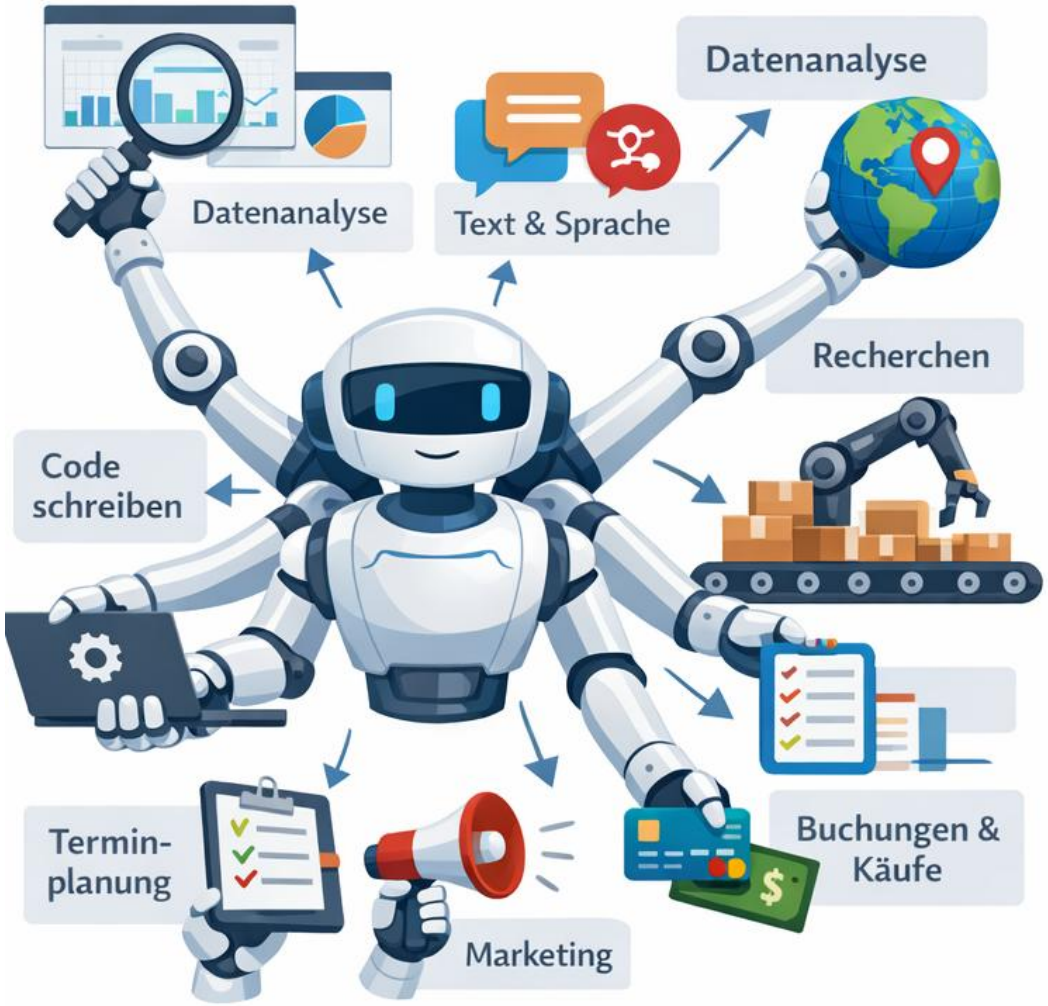

SOUL.MD
BOOTSTRAP.MD
LIVING AI


OPENCLAW
OpenAI

Einfache Aufgaben

- Kalender-Update
- E-Mail beantworten
- Bericht zusammenfassen

Autonomer Agent



Human in the Loop: Kontrolle wird Ritual

Schein-Kontrolle.

Unprüfbarkeit.

Verantwortungsdiffusion.


Werte bleiben – Handlungen gehen
Selbstbild ≠ Wirksamkeit

Menschen als Haustiere der KI?

NEWS | 13 February 2026

AI agents are hiring human 'meatspace workers' — including some scientists

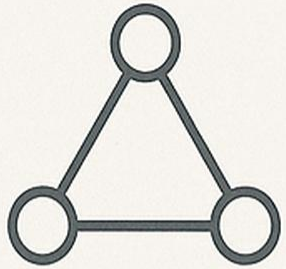
Biologists, physicists and computer scientists have joined a platform called RentAHuman.ai to advertise their skills.


Top 5 IT-Sicherheitsbedrohungen 2024 (basierend auf ENISA, Deloitte, Wikipedia)
Angriffe auf Verfügbarkeit (DDoS, Ransomware)
30%
Ransomware
25%
Datendiebstahl / -schäden
Missbrauch legitimer Zugangsdaten
15%
IoT-Malware & Schwachstellen
12%
0
5
10
15
Geschätzter An

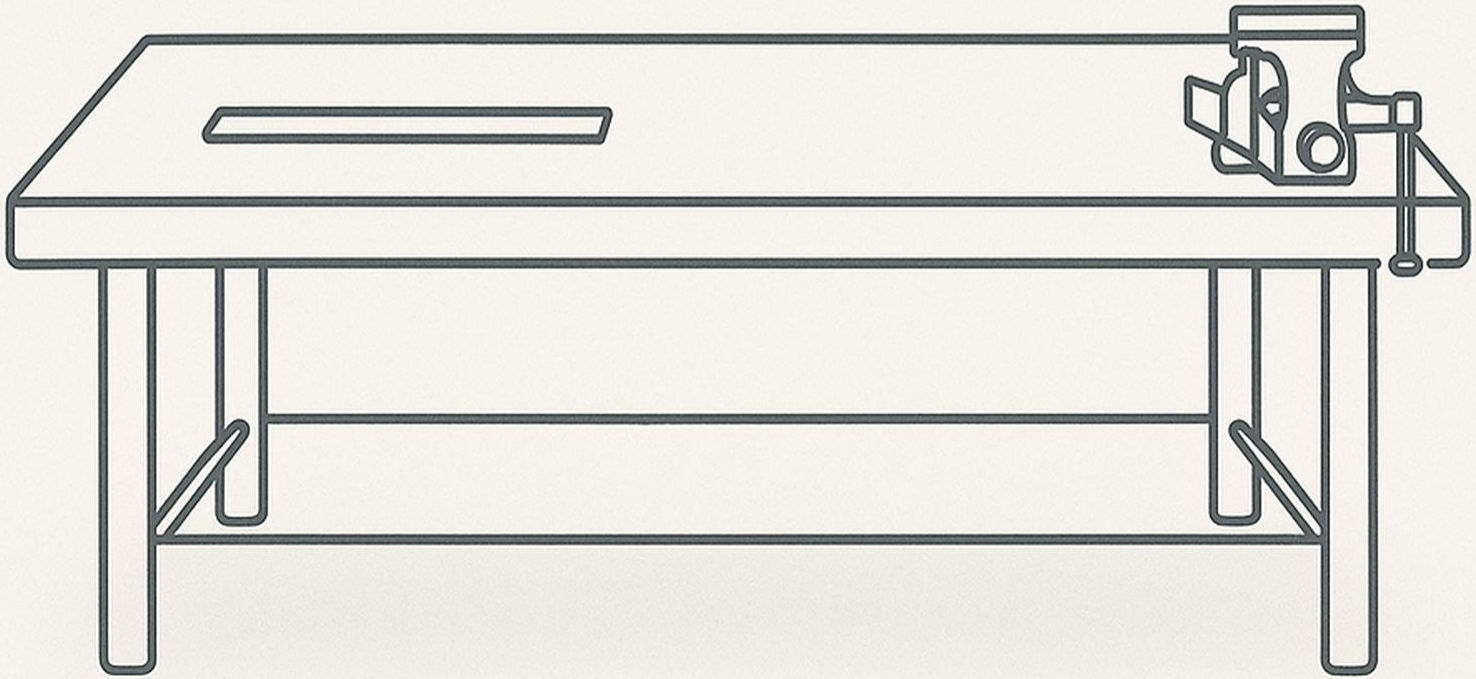
Kriminalität ist ein Ressourcenproblem

Skill

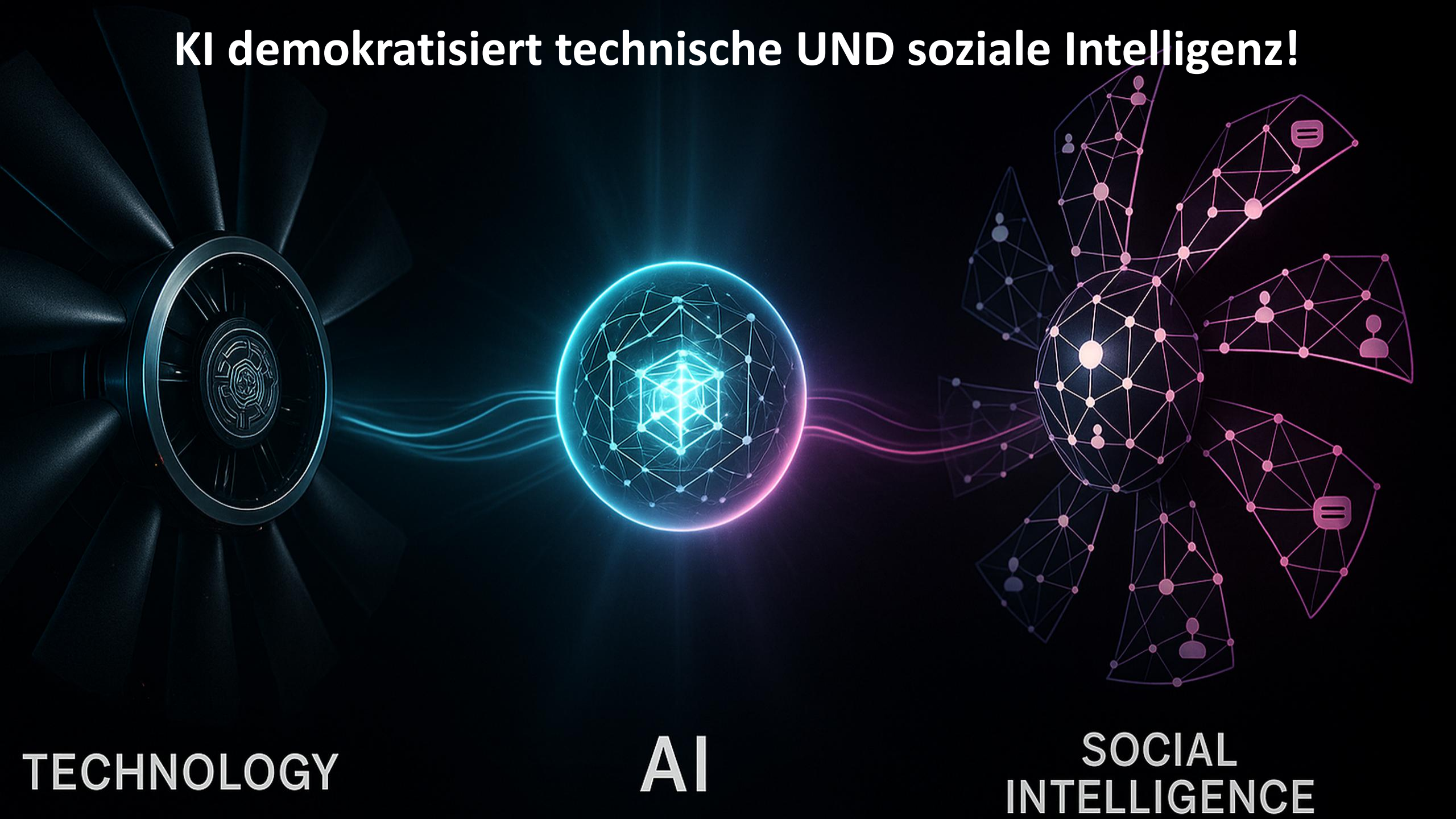
Time



Coordination



KI demokratisiert technische UND soziale Intelligenz!



Darknet

Ransomware veröffentlich nicht die Kronjuwelen, die verstehen nix vom Business des Opfers.

Datenverlust kann man runter-managen. Die riesigen Datenmengen kann eh niemand sichten.

Type a message here

Drop files

Send message

Considering your relationship and desire to close the deal, we will make the discount for you and extend the timer. But that's all that we can do for you.

Basta Group, 09:40

Our discount is 20%.

Basta Group, 09:41

We hope you will appreciate it.

You, 10:48

We hope you will appreciate it.

You, 10:48

The money, even with the 20% discount, is unfortunately over our financial possibilities. We have heard that in other cases 10% of the EBIT of the last years is paid. The EBIT of the last 3 years for [redacted] Holding was 4.8[redacted]$. We can send you the balance sheet data if you would like to see it. This gives a total of $484,000. That's the maximum because we can't make any sales because of your cyber attack.

Basta Group, 11:11

years is paid. The EBIT of the last 3 years for [redacted] Holding was 4.8[redacted]$. We can send you the balance sheet data if you would like to see it. This gives a total of $484,000. That's the maximum because we can't make any sales because of your cyber attack.

Basta Group, 11:11

No need to tell us Wilhelm Hauff's fairy tales. Our analytical department analyzed your financial documents and appointed the amount you are able to pay without any problems. Therefore, our price is $880,000. You have 3 days to make the payment. After that, our price will be $1,100,000 again.

We asked for test decryption and a file list of exfiltrated files.

Good afternoon, yet we cannot provide, the person who has access to data - does not contact for the reasons unknown to us. But it already was, I think will appear in the nearest future. You can send files for test interpretation. Did you estimate mashtaba? how to you?

We are unable to provide you with a list of files at this time. I have already explained.

Make a decision faster, our team is going on vacation

Gesendet: Montag, 13. Oktober 2022 um 16:19 Uhr
Von: volkzidonov@cock.li
An: mailadresse@corporate-trust-verhandlungsteam
Betreff: Re: help

I have reply.

On 2022-10-11 19:45, volkzidonov@cock.li wrote:
> Dear
> First of all, thank you for contact us, we're sorry to attack your
> company, we are a mature and integrity team. We hope to reach an
> agreement with you with the fastest speed to solve this case. If you
> have any questions, you can tell us, we are willing to communicate
> with you with the greatest sincerity.
> Please buy $510,000(usd) worth of ETH to send to our wallet address.
> ETH address:0x282dC843E849914082Ec54c494a6D65738568979
> After we receive ETH, I will send all the passwords to you.We randomly
> generate a password for each server, each password is only taken
> effect on one server. AES encryption is the most advanced encryption
> algorithm in the world, without anyone can crack. Even the US FBI and
> the Ministry of Defense cannot be decrypt. Please don't try scan disk
> or recovery. This will make data damage, once the data is damaged,
> even if you pay the ETH, I can't restore the data. Data will be
> permanently lost.
>
> In addition, we will provide you with test password. Decrypt software:
> C:\crypt\bcfmgr.exe
> Select the volume and click "decrypt volume". Enter the password to
> decrypt.
>
> SERVER-TEST-005 192.168.12.130 abcdefgh
> VMWARE_99-2021 192.168.12.132 E:\ abcdefgh
> KLZSRV32-TEST 192.168.12.155 abcdefgh
> KLZSRV19 192.168.12.54 abcdefgh
>
> On 2022-10-11 15:27, kluke01 wrote:
>> bro , how to decrypt and how much ?
>>
>> Please contact: volkzidonov@cock.li
>> spare email: volkzidonov@morke.org
>> Your identity code: XdM5FGoro1Tj
>>
>> kluke01
>>
>> kluke01@126.com

Ransomware Jungs sind nicht die hellsten Kerzen auf der Torte.

Das KI-Unternehmen Anthropic hat sein neues Modell Claude Opus 4.6 zunächst in einer kontrollierten Umgebung getestet, bevor es am Donnerstag veröffentlicht worden ist. Das sogenannte Frontier Red Team stattete Claude Opus 4.6 mit Standard-Werkzeugen wie Python, Debuggern und Fuzzern aus – verzichtete jedoch auf spezielle Anweisungen zur Schwachstellensuche, berichtet Axios ↗ .

Das Ergebnis ↗ übertraf laut Hersteller die Erwartungen: Das System identifizierte über 500 Zero-Day-Schwachstellen in quelloffener Software. Jeder Fund wurde entweder durch interne Teams oder externe Sicherheitsforscher validiert, so Axios weiter.

Claude Opus 4.6: KI findet über 500 Zero-Day-Lücken in Open-Source-Software - Golem.de

Gut patchen reicht gegen Ransomware. Die haben keine Zero-Days.

BK

Brusceras, Karolania <Karolania.Brusceras@mik-masterpart.com>

Vicord, Chris; Boskovicova, Petra;

Payments

Hello Chris,

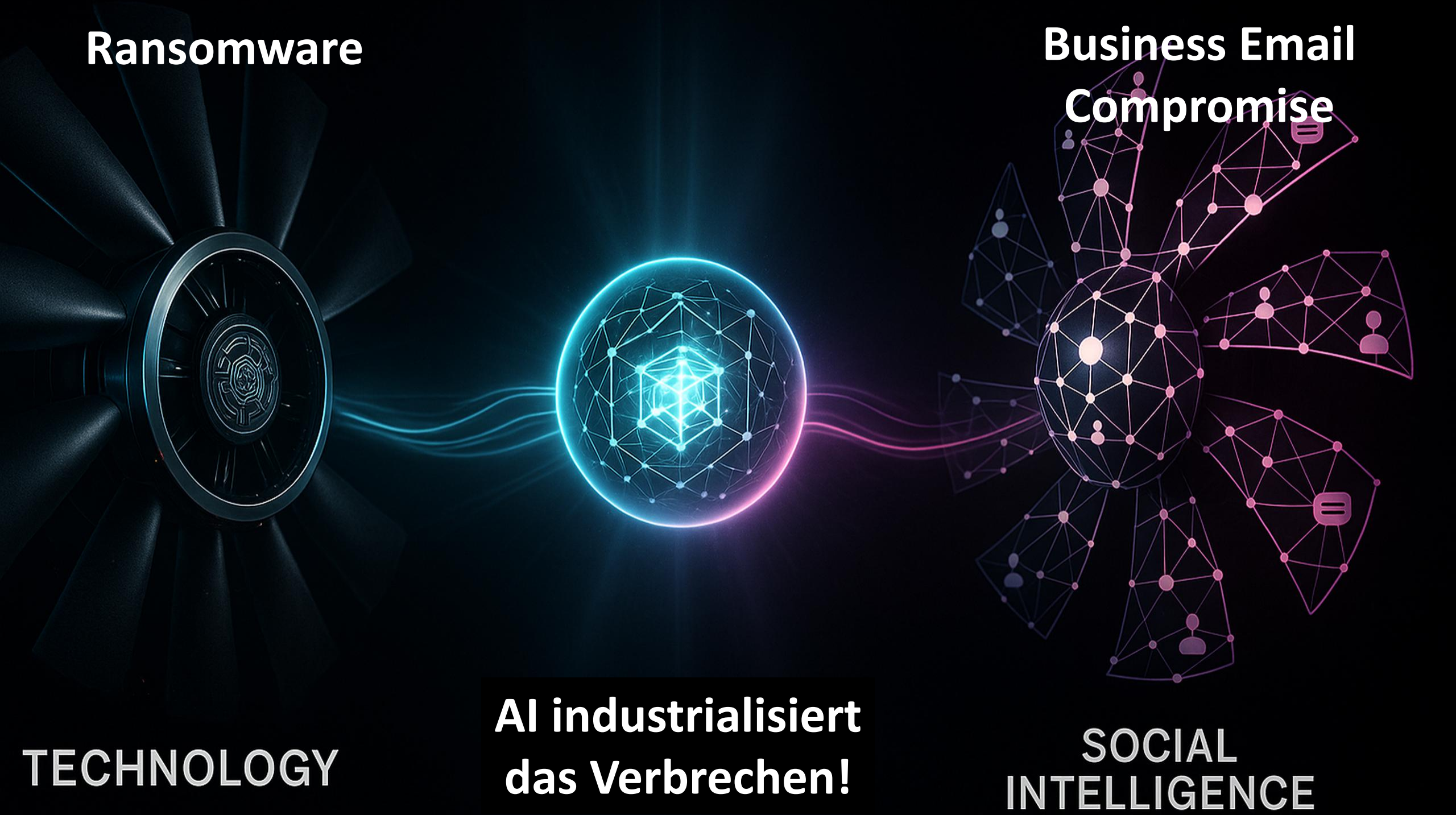
could you confirm the amount of payments „not paid“ to Shogu as soon as possible please?
22.7. - 505.638,73usd-Sodexo Services
16.7. – 338..948,97usd-Sodexo Services
26..7. – 397.304,41usd-Shogu Electrical
27.8. – 199.181,08usd-Skyscape Service

Thank you.

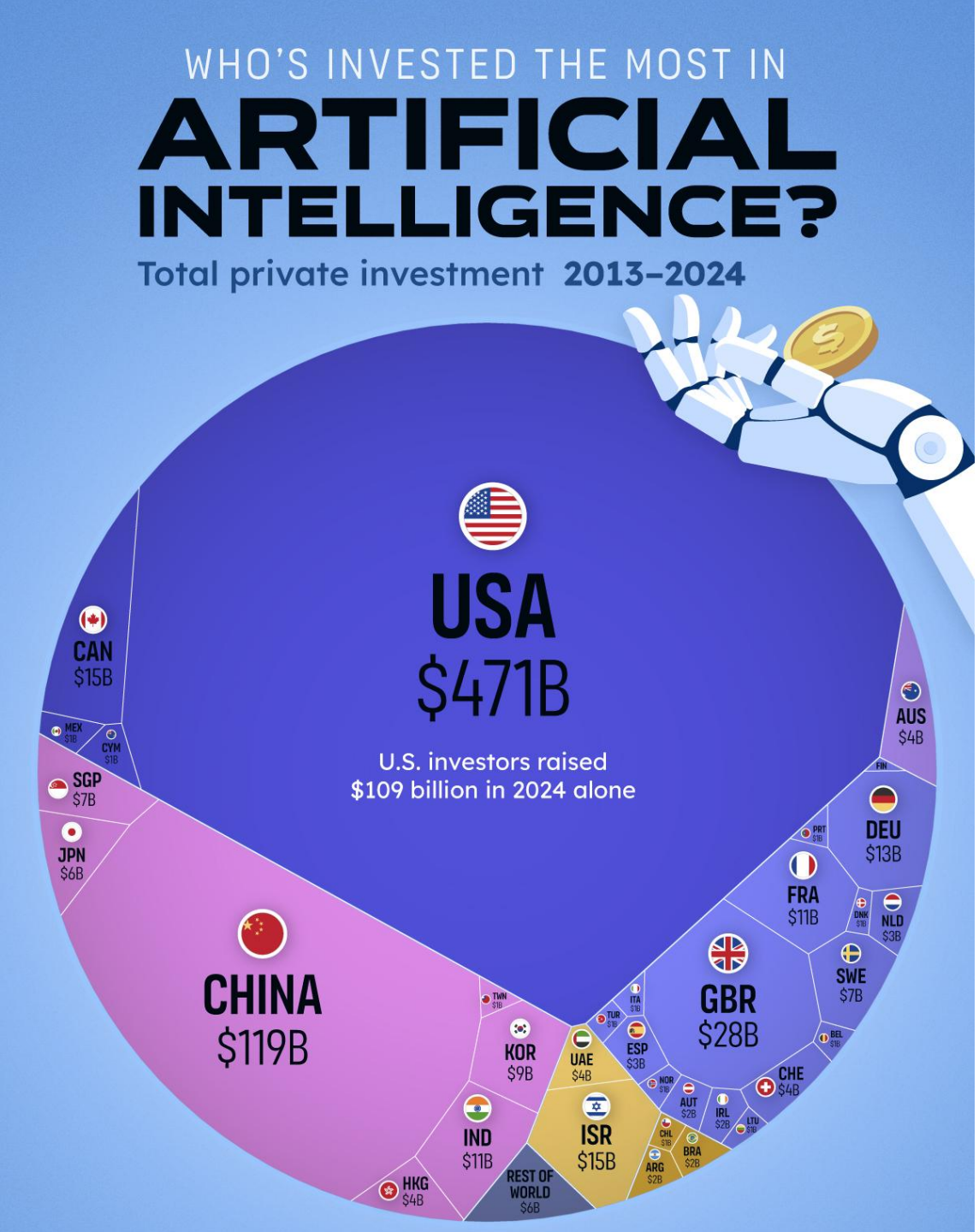
Best regards,

Karolania Brusceras
Corporate Treasury

MIK MasterSystemParts Verwaltungs GmbH
A Joint Venture between BigSupplier and LargeVendor


Ransomware
Business Email Compromise
TECHNOLOGY
AI industrialisiert das Verbrechen!
SOCIAL INTELLIGENCE


ERFOLGSWAHRSCHEINLICHKEIT
GEWINN
ATTRIBUTION
EINTRITTSSCHWELLE
KLEINERE GRUPPEN



America innovates

China replicates

Europe regulates


EU
Artificial
Intelligence Act

Three Samsung employees reportedly leaked sensitive data to ChatGPT

One is said to have asked the chatbot to generate notes from a recorded meeting.

Shadow AI → Agenten an Systeme → 'zu spät'

Erst heimlich.
Dann „macht doch eh jeder“.
Dann irreversibel.

Wenn Nutzen hoch & Nachweis gering → Normalform Regelbruch.

Stealth Adoption: Regeln werden entwertet

Human in the Loop: Kontrolle wird Ritual

Schein-Kontrolle.

Unprüfbarkeit.

Verantwortungsdiffusion.

COMPUTERWOCHE

News

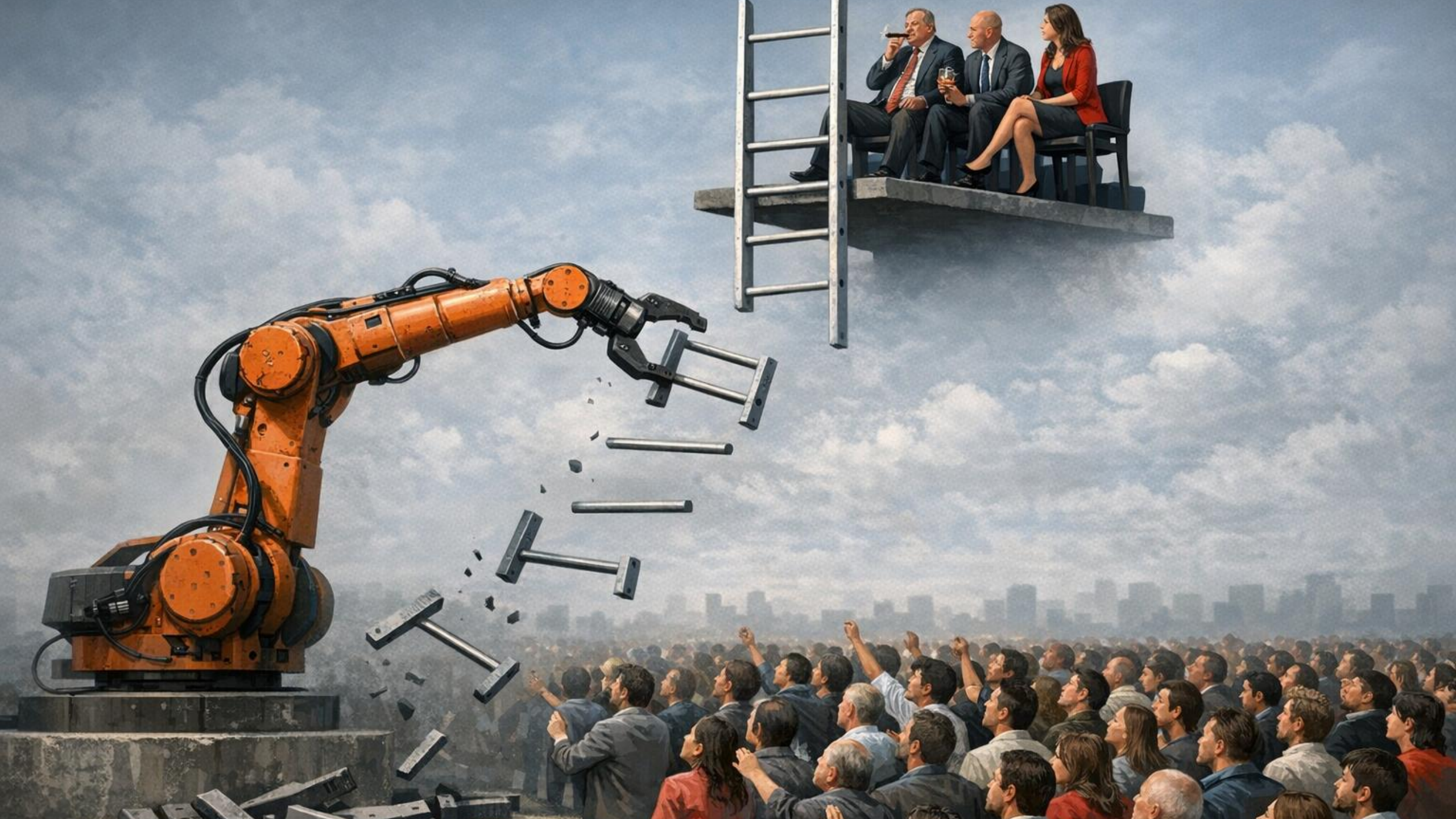
20. Mai 2025

Vergangene Woche gab **Microsoft** dann bekannt, dass das Unternehmen in seinem Heimatbundestaat Washington 2.000 Mitarbeitende entlässt. Laut **Bloomberg** waren Programmierer am stärksten von der Kündigungswelle betroffen.

Kündigungen treffen Softwareentwickler am härtesten

Wie das Nachrichtenportal basierend auf Beschäftigungsdaten des Bundesstaates herausfand, arbeiteten mehr als 40 Prozent der entlassenen IT-Spezialisten in der Softwareentwicklung. Dagegen waren laut Bloomberg relativ wenige Vertriebs- oder Marketingpositionen von den Kündigungen betroffen.

Die jetzigen Personalmaßnahmen sind Teil der jüngsten Entlassungen bei Microsoft, von denen etwa insgesamt **6.000** Personen betroffen sind. Der Grund für diese Entscheidung scheint das allgemeine Umdenken in der Tech-Industrie zu sein.



WORLD'S MOST SURVEILLED CITIES

Cities with most surveillance cameras per square mile

CAMERAS PER SQUARE MILE

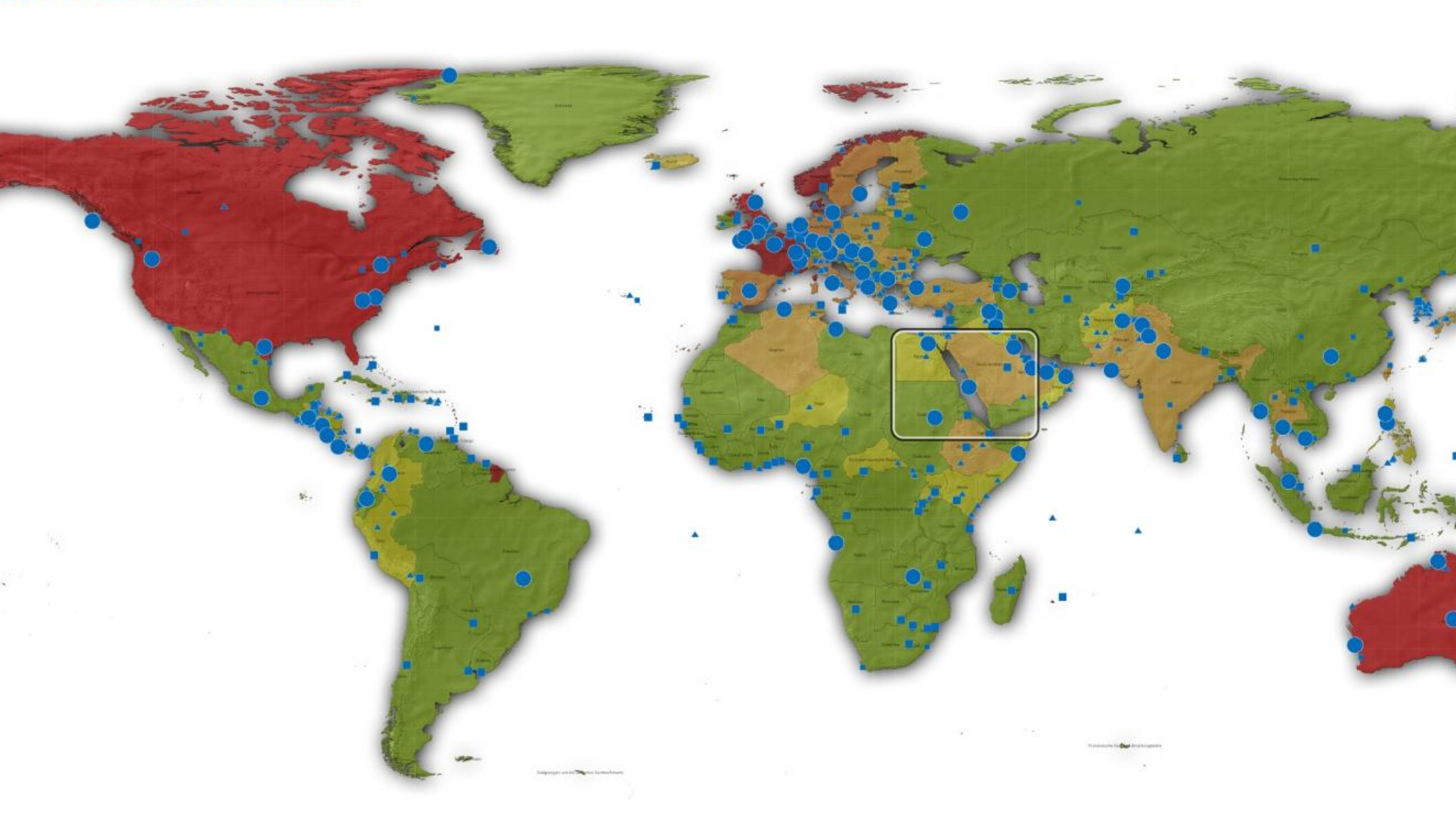
Delhi, India	**1,826.6**	Singapore	387.6	Beijing, China	181.5
London, UK	1,138.5	Changsha, China	353.9	Taiyuan, China	174.4
Chennai, India	**609.9**	Wuhan, China	339	Suzhou, China	165.6
Shenzhen, China	520.1	Seoul, South Korea	331.9	**Mumbai, India**	**157.4**
Wuxi, China	472.7	Xiamen, China	228.7	Mexico City, Mexico	151.7
Qingdao, China	415.8	Moscow, Russia	210.0	Changchun, China	139.6
Shanghai, China	408.5	New York, US	193.7		

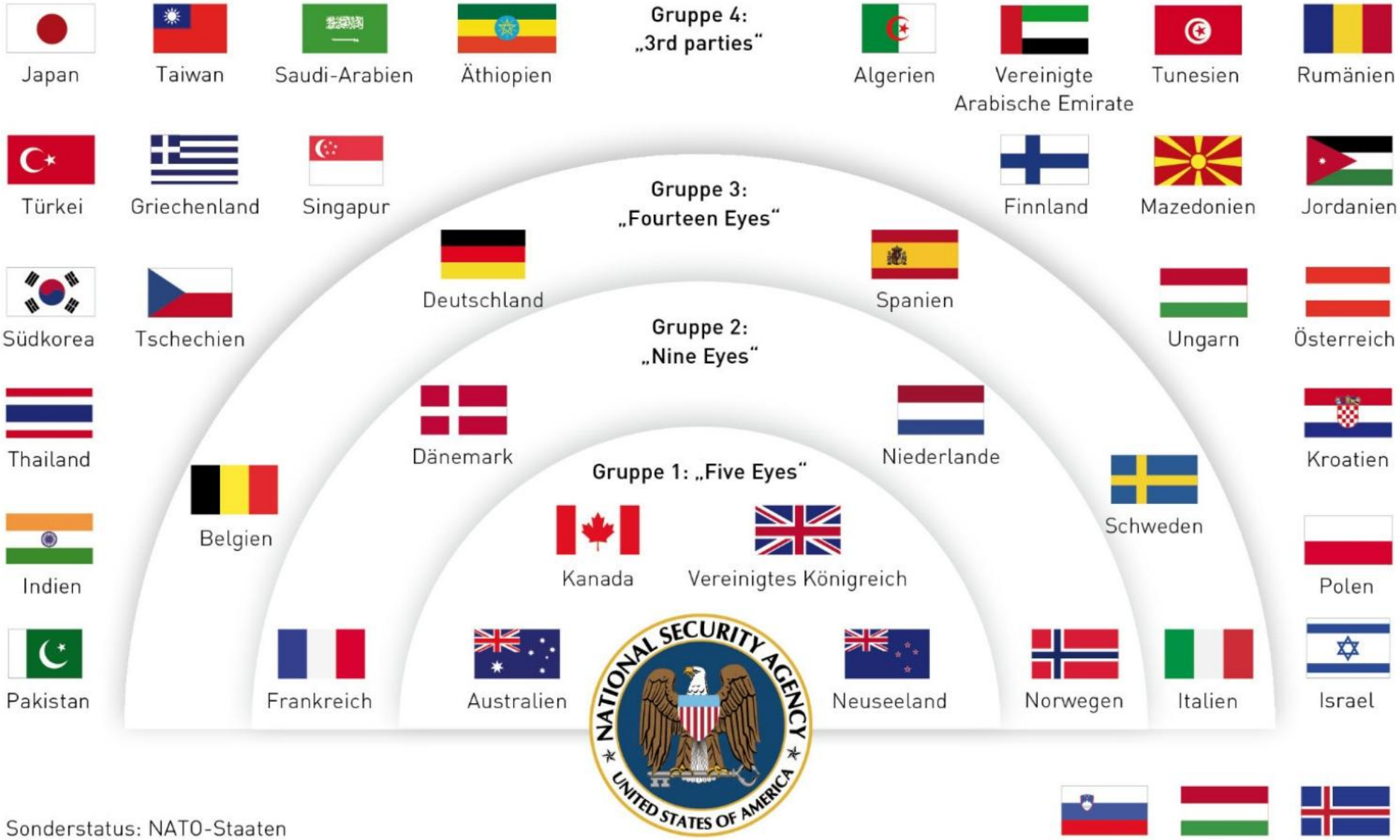
Regime-Grade Automation.

Trainingsdaten sind die neue SIGINT-Munition

Wer die Daten hat, hat den Trainingsvorteil.

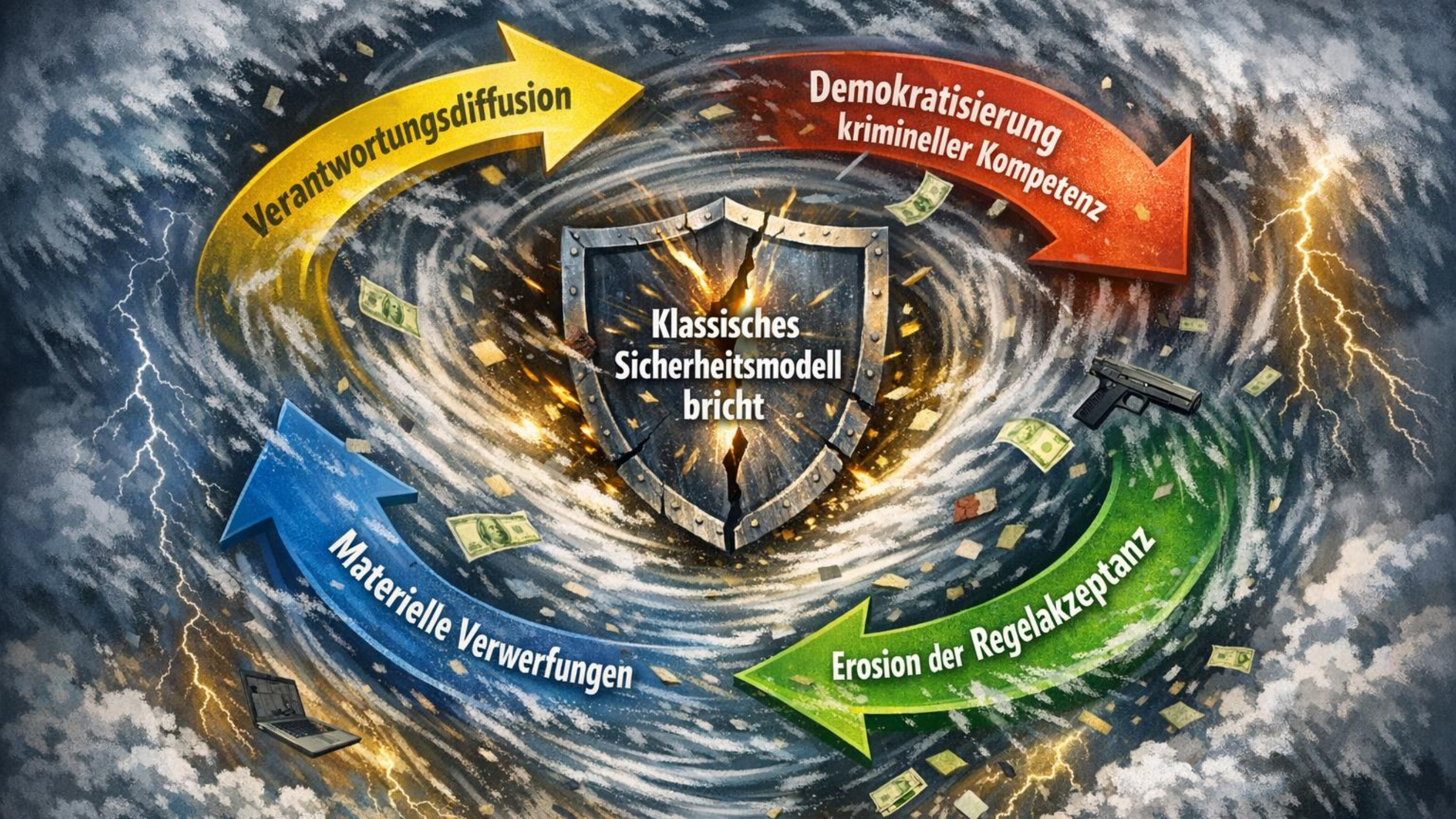

NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA
MAKE AMERICA
GREAT AGAIN





Sonderstatus: NATO-Staaten

Geheimdienste und Organisierte Kriminalität: Beide werden agentisch!


Verantwortungsdiffusion
Demokratisierung krimineller Kompetenz
Klassisches Sicherheitsmodell bricht
Erosion der Regelakzeptanz
Materielle Verwerfungen

Was Verteidiger jetzt tun müssen?

Flucht nach vorne. KI nutzen!

Empfehlung #1: Agil bleiben

In unsicheren Zeiten der Veränderung ist das die #1-Defense.

- Fortschritt beobachten, Patterns früh erkennen, Taktik anpassen
- jede Woche, nicht jedes Jahr
- Partnernetzwerk bauen, um „vor der Lage“ zu sein: Hersteller, Threat Intel, Forschung, MSSP/IR, Branchenpeers
- schnelle Lernschleifen schlagen perfekte Pläne.

Empfehlung #2: Frühwarnsystem

„go chinese on your infrastructure“

- Exzessive Überwachung der Infrastruktur
- maximale Telemetrie von Systemen/Workloads/APIs/Identity-Pfaden
- SOC / SIEM mit KI-Korrelation, um in agentischer Geschwindigkeit mithalten zu können
- Alles mit in die Überwachung einbeziehen

Empfehlung #3: Identitäten managen

Identity Governance für Agenten und Menschen

- Non-human Identities pflegen und berechtigen
  „wer darf was in wessen Namen tun?“
- saubere Lifecycle-Prozesse, least privilege, schnelle Rezertifizierung
- Enablement statt Verbote: sichere Standard-Tools, klare Spielregeln, schnelle Freigaben
- Nicht „Governance“ predigen – ein Team-Pakt mit den Kollegen schließen

„Wir nutzen KI als Werkzeug für alle. Und arbeiten gemeinsam dran, dass die Menschen die Kontrolle über die Maschinen behalten!“