



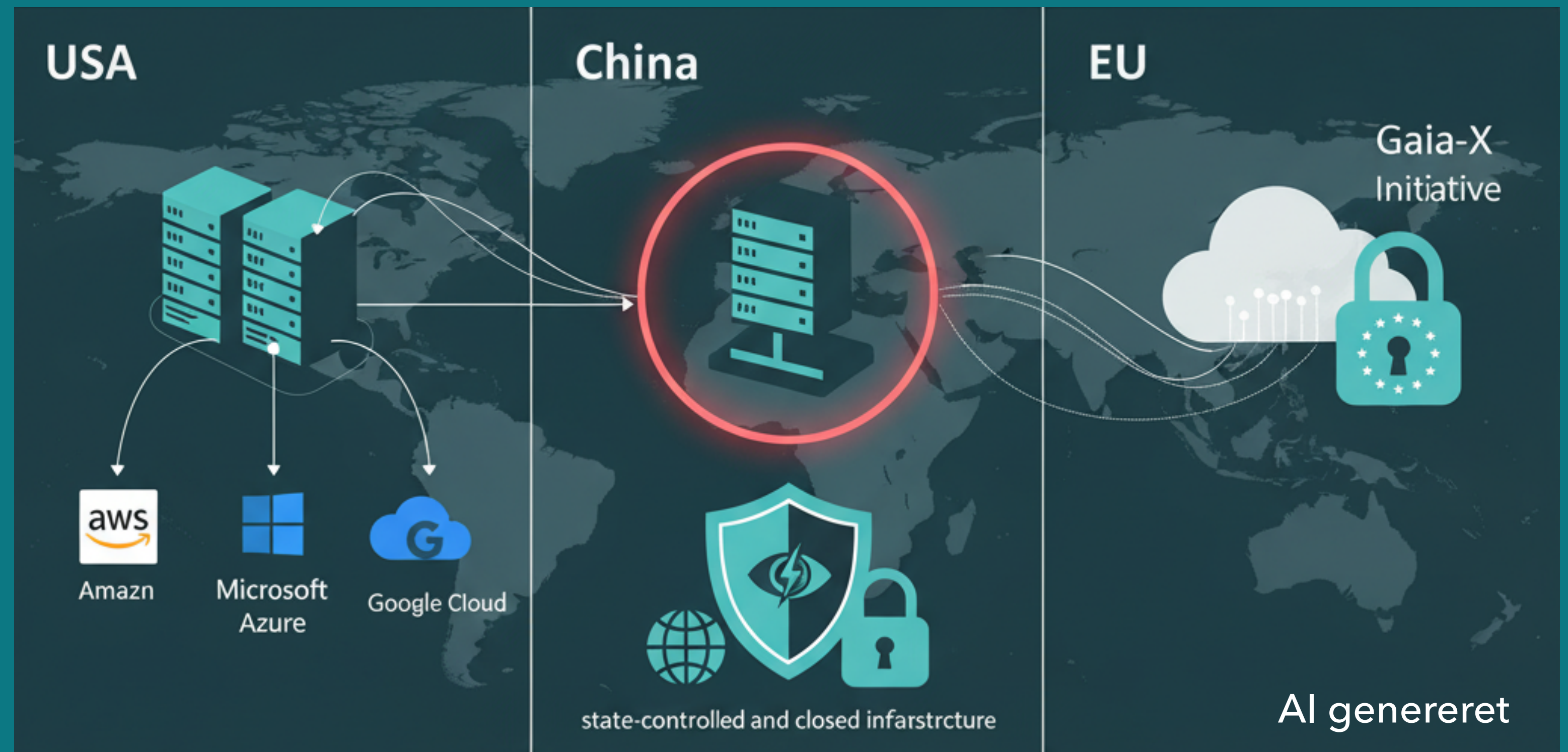
AI genereret

EN GEOPOLITISK SLAGMARK

DIGITALISERING

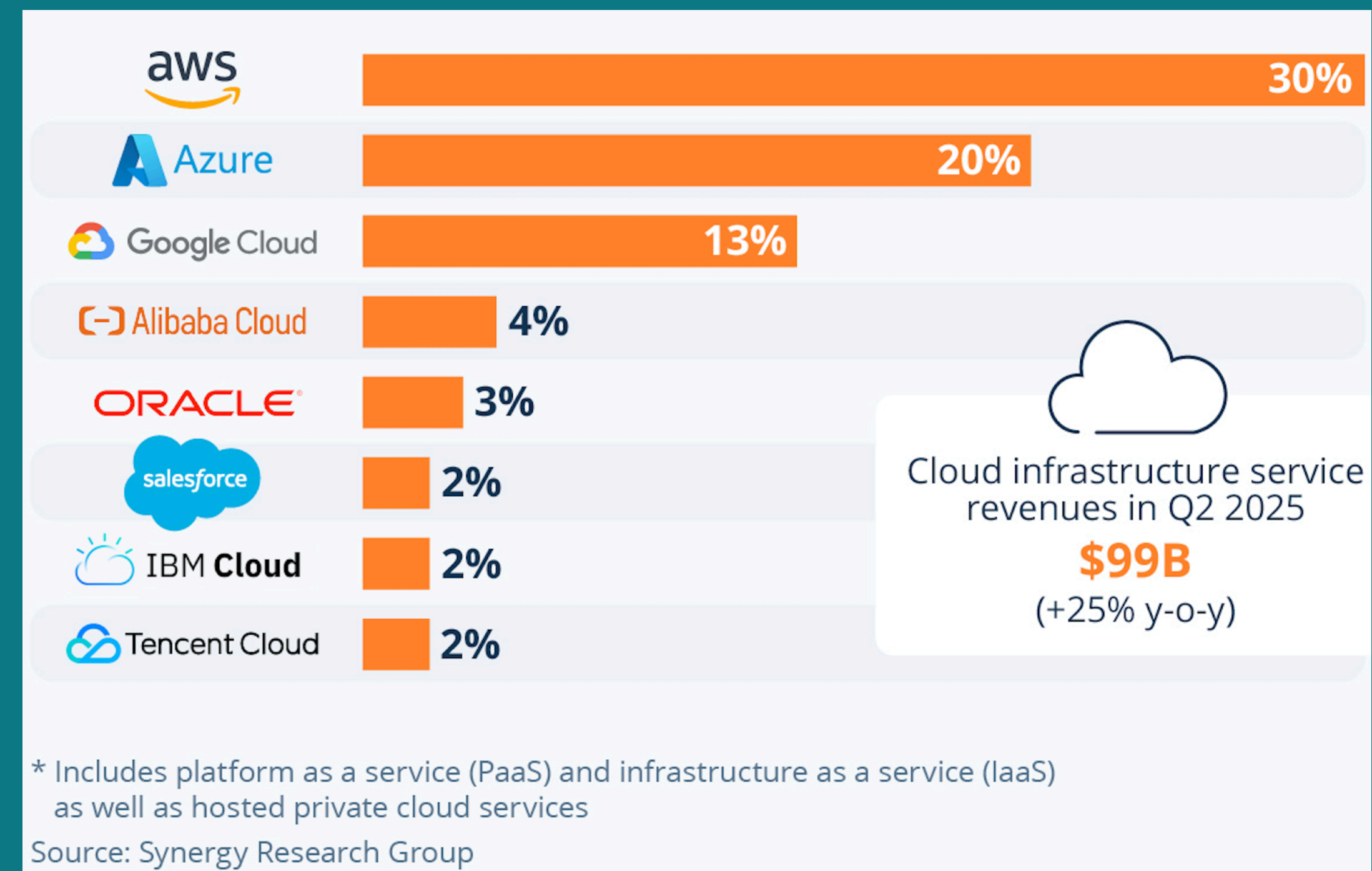
DIGITALISERING SOM GEOPOLITISK SLAGMARK

- ▶ Infrastrukturen
- ▶ Datasuverænitet
- ▶ Sikkerhed



HVEM EJER INFRASTRUKTUREN

- ▶ Infrastruktur = datacentre, netværk, servere og cloud-platforme.
- ▶ USA dominerer markedet med 3 store spillere: Amazon (30%), Microsoft Azure (20%) og Google Cloud (13%). [Ref](#)
- ▶ Kina har en statsstyret og lukket infrastruktur med stærk regulering. [Ref](#)
- ▶ EU arbejder på selvforsyning med initiativer som Gaia-X, men er stadig afhængig af USA og Kina. [Ref](#)
- ▶ Ejerskab = kontrol over data, adgang og påvirkning af, hvad vi får adgang til. [Ref](#)



HVAD BETYDER DATASUVERÆNITET?

- ▶ Data skal opbevares og bruges efter nationale/ regional love.
- ▶ Datasuverænitet handler om, hvem der bestemmer over vores data.
- ▶ Udfordring: Teknologi er global, men lovgivning er lokal.



“SIKKERHED” HANDLER I DAG IKKE KUN OM ANTIVIRUS MEN OM MAGT, VIDEN OG KONTROL

- ▶ Digital sikkerhed er mere end virusbeskyttelse.
- ▶ Det handler om, hvem der styrer data og information.
- ▶ Kontrol over netværk og platforme betyder magt til at påvirke samfundet. Det betyder...
- ▶ Cyberangreb, misinformation og overvågning er strategiske våben.
- ▶ Derfor er digital sikkerhed også et spørgsmål om politik, økonomi og demokrati.



USA'S TILGANG – INNOVATION OG MARKEDSKRAFT

- ▶ Fokus på innovation, økonomisk vækst og global AI-lederskab.
- ▶ "Winning the Race: America's AI Action Plan" fremmer hurtig udvikling og markedsfrihed.
- ▶ Store techgiganter (OpenAI, Google, Microsoft) driver AI-udvikling.
- ▶ Offentlige AI-systemer skal være ideologisk neutrale.
- ▶ Minimal regulering for at fremme konkurrence og investering.



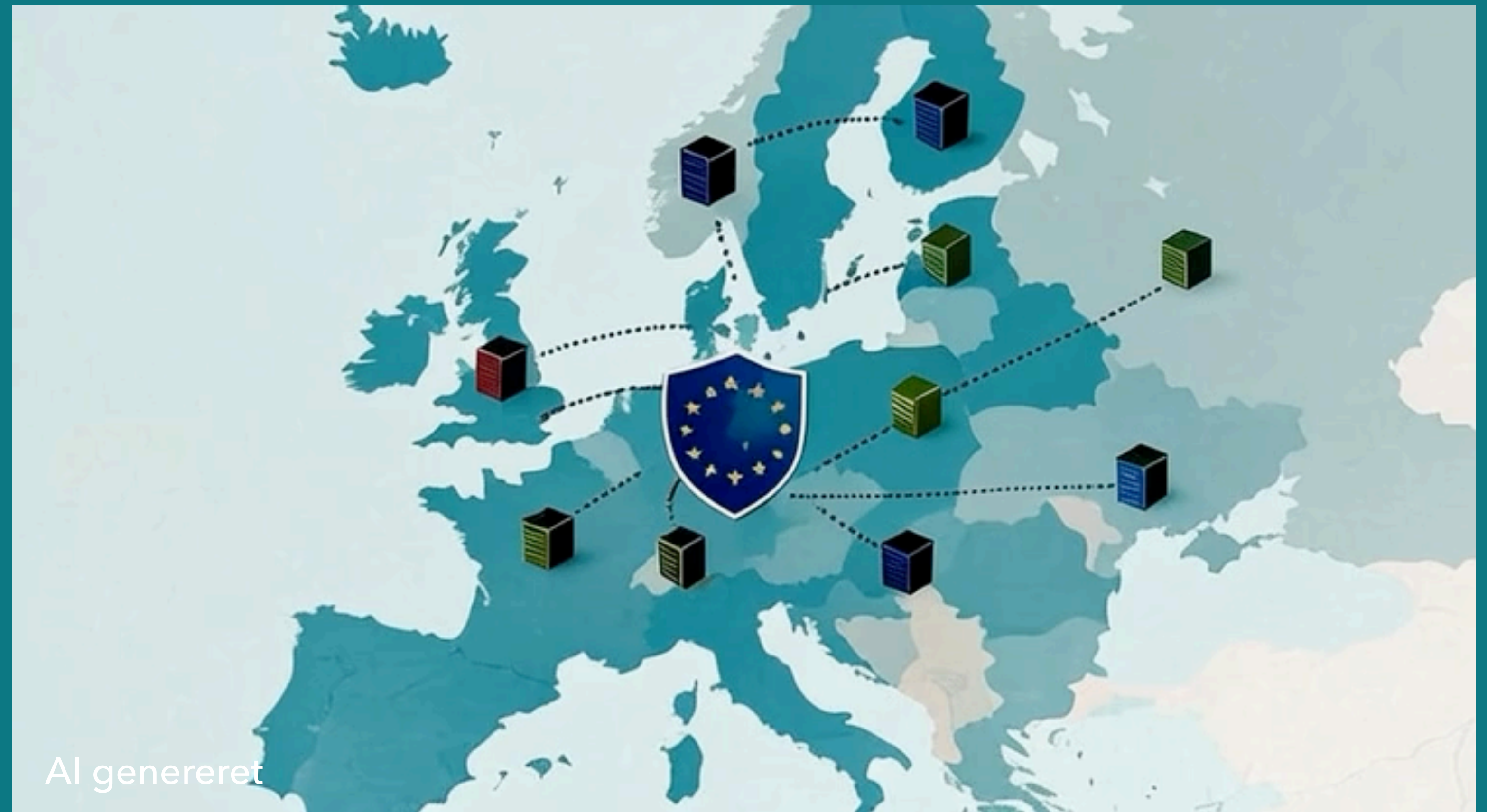
KINA – STATSKONTROL OG CYBERSIKKERHED

- ▶ Central statslig kontrol via Cybersecurity Law, Data Security Law og PIPL.
- ▶ Fokus på national sikkerhed og digital suverænitet.
- ▶ Stram overvågning og eksportkontrol på data og teknologi.
- ▶ Digital Silk Road udvider kinesisk teknologisk magt globalt.
- ▶ AI-produkter og infrastruktur underlagt statslig censur og retningslinjer.



EU – DATABESKYTTELSE OG DIGITAL SUVERÆNITET

- ▶ Regulering gennem GDPR, Data Governance Act og AI Act.
- ▶ Fokus på borgerrettigheder, gennemsigtighed og etisk AI.
- ▶ Digital suverænitet som mål: uafhængighed af ikke-europæisk teknologi - Gaia-X
- ▶ Fremmer markedsregler og sikker dataudveksling internt i EU.
- ▶ Balancerer innovation med stærk regulering.



CYBER-TRUSLER OG INFORMATIONSKRIG

- ▶ Cybertrusler og misinformation bruges som våben i internationale magtkampe.
- ▶ Center for Cybersikkerhed vurderer i 2025, at truslen mod Danmark er MEGET HØJ.
- ▶ Hybridkrigsførelse kombinerer tekniske angreb med målrettet misinformation.
- ▶ Truslerne påvirker både teknologi og befolkningens tillid og holdninger.



CYBER-TRUSLER OG INFORMATIONSKRIG

**HAR I OPLEVET ELLER HØRT OM
KONKRETE EKSEMPLER PÅ
CYBERANGREB, MISINFORMATION
ELLER DIGITAL OVERVÅGNING?**

- ▶ SolarWinds-angrebet: Russerne spionerede via softwareopdateringer. (2020)
- ▶ Pro-russiske grupper spredte falske nyheder og angreb danske hjemmesider. (Ex Maj 2023)
- ▶ Cambridge Analytica misbrugte data til politisk manipulation. (2018)
- ▶ Kina overvåger sin befolkning med digital teknologi for kontrol.

MALWARE, HACKING OG RANSOMWARE

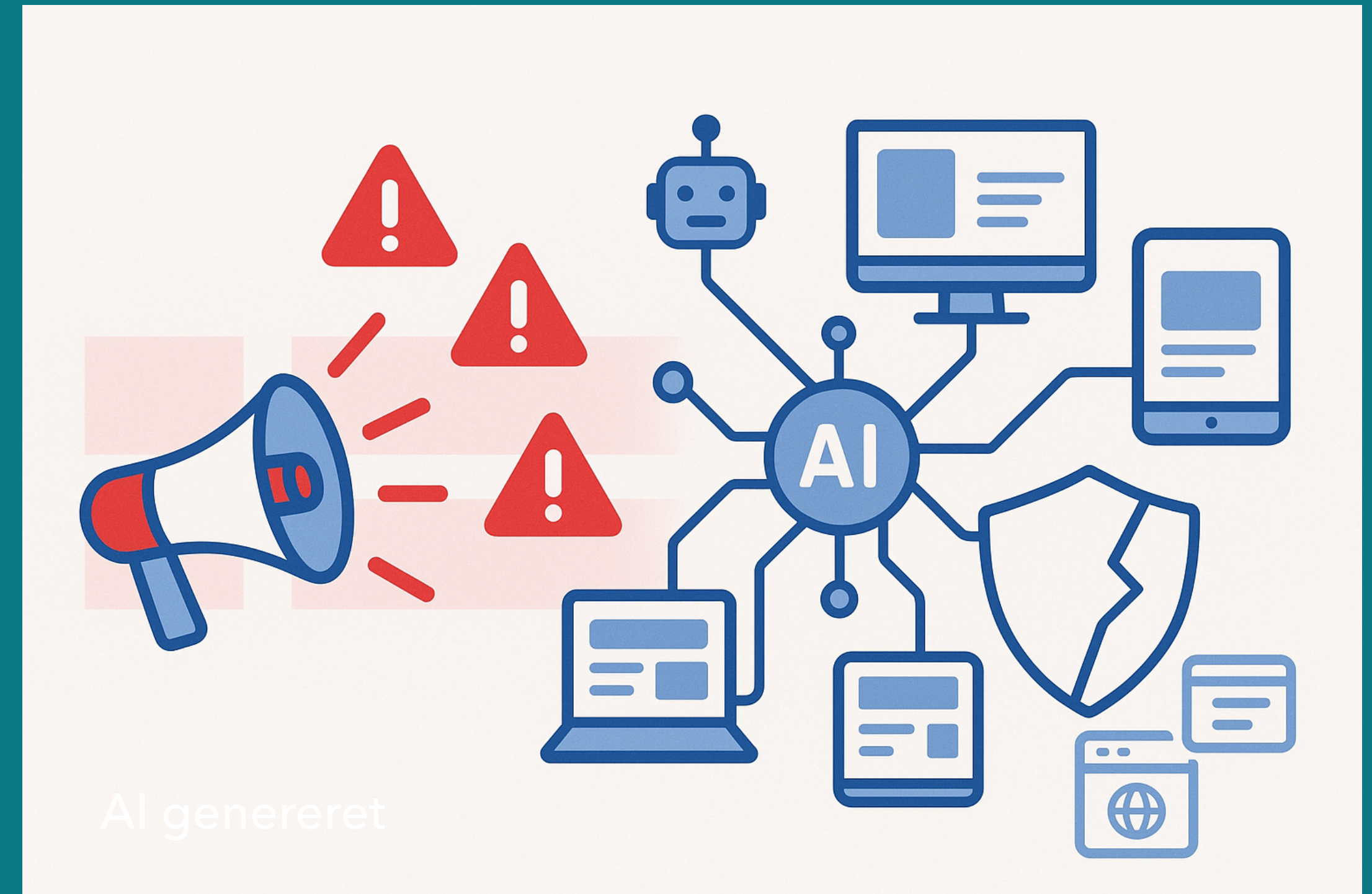
HVEM ANGRIBER – OG HVORFOR?

- ▶ Ransomware er den mest udbredte cybertrussel – 45% af virksomheder rammes globalt.
- ▶ Kriminelle sælger færdig ransomware-kode som en tjeneste (Ransomware-as-a-Service).
- ▶ Angreb rammer hele forsyningskæden, fx energi og telesektorer.
- ▶ Motivation bag angreb: økonomisk gevinst eller politisk sabotage.
- ▶ Statsstøttede grupper fra Rusland og Kina udfører spionage og sabotage mod Danmark.
- ▶ Danmark er et attraktivt mål på grund af et højt digitalt niveau.

FAKE NEWS OG MANIPULATION

HVORDAN SPREDES MISINFORMATION DIGITALT?

- ▶ Informationskrig = bevidst spredning af falske historier for at skabe mistillid.
- ▶ AI og bot-netværk forstærker og automatiserer spredningen.
- ▶ Hybridangreb kombinerer hacking og misinformation – både data og tillid rammes.
- ▶ I Danmark: Pro-russiske grupper (fx NoName057) angreb offentlige hjemmesider og spredte falske fortællinger om EU og NATO.



EKSEMPLER FRA DANMARK: PÅVIRKNINGEN AF DIGITALE BORGERE

Phishing og økonomisk svindel rammer både borgere og kommuner.

AWS-nedbrud (okt 2025) viser vores afhængighed af amerikansk infrastruktur – selv uden angreb.

AWS-NEDBRUDET I OKTOBER 2025 – EN GLOBAL SÅRBARHED

- ▶ Massive driftsproblemer i AWS' US-EAST-1 region den 20. oktober 2025
- ▶ Mange store tjenester ramte: Perplexity AI, Snapchat, Alexa, Fortnite, Canva, Spotify m.fl.
- ▶ Problemet varede ca. 3,5 timer og påvirkede globale brugeroplevelser
- ▶ Danmark oplevede afbrydelser på apps, AI-værktøjer, smarthome-funktioner og kommunikation
- ▶ Viser vores afhængighed af få store amerikanske cloud-udbydere
- ▶ Et teknisk problem ét sted kan lamme kritiske systemer verden over



TECHGIGANTER OG STORMAGTERS INTERESSER

- ▶ USA-koncerners platforme som Google, Meta og Amazon styrer meget af den information, vi ser globalt.
- ▶ Kinesiske apps som TikTok og WeChat er underlagt strenge krav fra den kinesiske stat, der overvåger og censurerer indhold.
- ▶ Data er det nye råstof og et vigtigt våben i magtspillet mellem stater.
- ▶ Som borger og IT-frivillig er din rolle vigtig – kritisk tænkning og etik betyder mere end kun teknisk kunnen.



OPSUMMERING

- ▶ Cybertrusler og informationskrig rammer ikke kun stater, men også hver enkelt borger.
- ▶ Vi skal styrke vores digitale robusthed – det vil sige modstandskraft mod angreb og manipulation.
- ▶ Kildekritik er afgørende for, at vi kan navigere sikkert i et informationsmiljø fyldt med misinformation.
- ▶ Vi må samarbejde – både myndigheder, virksomheder og borgere – for at skabe et sikkert digitalt samfund.
- ▶ AI bliver frontlinjen i kampen om sandhed og magt. Det er fremtidens store udfordring.



AI genereret

FORDELE, RISICI, BIAS OG
ETISKE DILEMMAER

AI I PRAKSIS

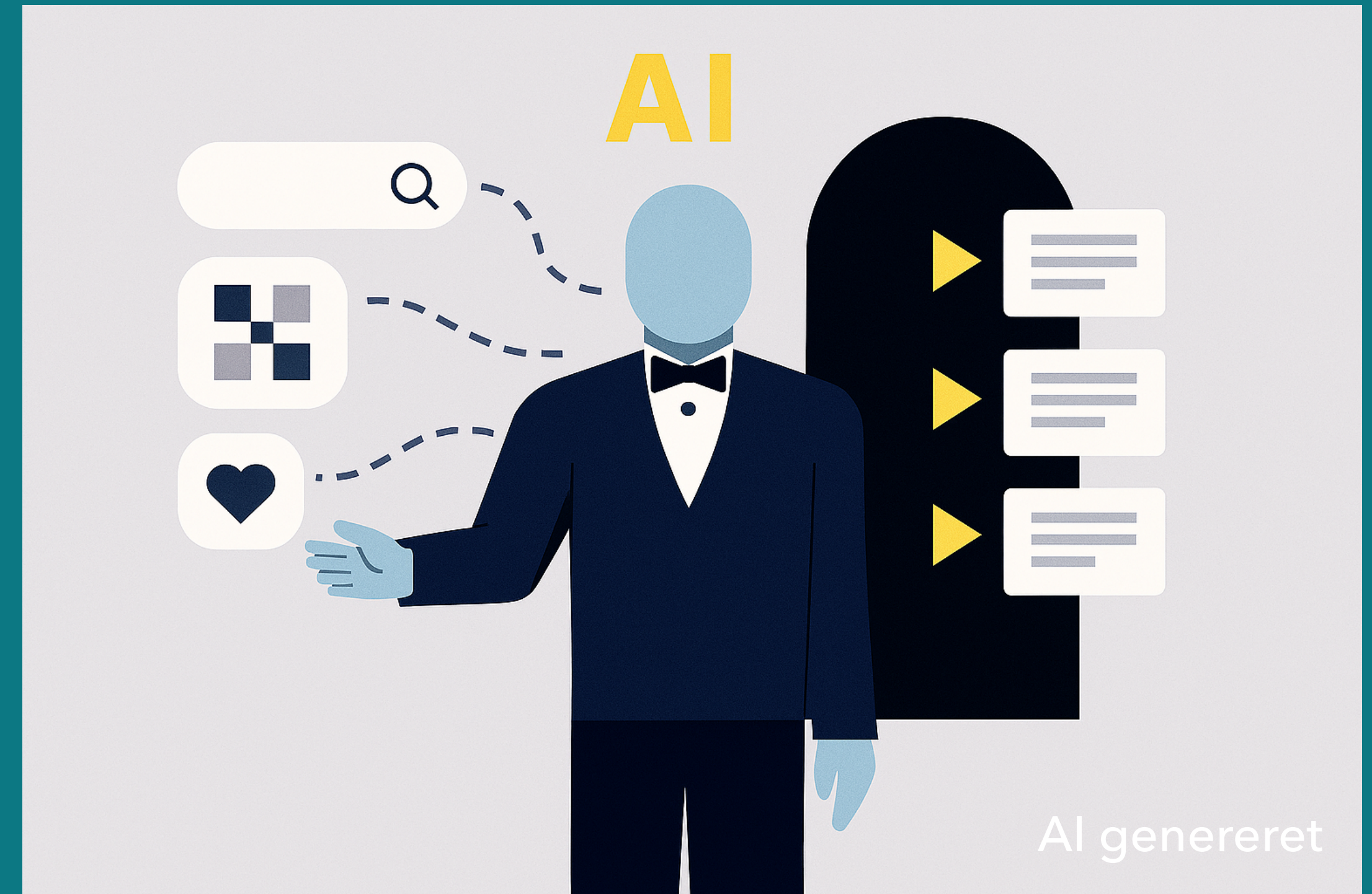
HVAD ER KUNSTIG INTELLIGENS?

- ▶ Kunstig intelligens (AI): Programmer der udfører menneskelige opgaver
- ▶ Tænkning, læring, problemløsning og beslutningstagning
- ▶ Maskinlæring, dyb læring, neurale netværk, og naturligsprogsbehandling.



INTRODUKTION TIL AI'S INDFLYDELSE

- ▶ AI styrer ikke kun svar, men også hvilke data vi får vist.
- ▶ AI er en gatekeeper, altså en digital dørvogter, der bestemmer, hvad der slipper igennem til os.
- ▶ Vores input (fx søgninger og tidligere valg) påvirker, hvad AI viser og prioriterer.
- ▶ Det betyder, AI kan forme vores opfattelse ved at fremhæve bestemte informationer.
- ▶ Derfor er det vigtigt at tænke kritisk over, hvad vi ser.



FORDELE VED AI I PRAKSIS

- ▶ Automatiserer rutineopgaver og forbedrer beslutningsstøtte.
- ▶ Øger tilgængelighed via chatbots, oversættelser og billedgenkendelse.
- ▶ Eksempel: AI-assistance i smartphones – stemmegenkendelse, realtidsoversættelse.

EKSEMPLER PÅ AI ANVENDELSE

Billedgenkendelse: AI identificerer objekter, personer og scener i billeder. Bruges i sociale medier, sikkerhed og apps som Google Lens og Bing

Lydbillede: AI-genkender musik og lyd, fx Shazam til at finde sange



EKSEMPLER PÅ AI ANVENDELSE

Talegenkendelse: AI omdanner tale til tekst og forstår stemmekommandoer.

Virtuelle assistenter: Siri, Google Assistant, Alexa.

Tale-til-tekst: MAC, Windows, live-undertekster på YouTube.



AI genereret

EKSEMPLER PÅ AI ANVENDELSE

Maskinoversættelse: AI oversætter tekst og tale mellem sprog.

Tekst fra billeder: Scan et menukort med Google Translate og se oversættelsen med det samme.

Live oversættelse: Tal og se samtaler oversat i realtid.

Integration: Bruges i Google Translate-appen og Google Lens.

RISICI OG BIAS

- ▶ Bias opstår via skævt data – f.eks. køns- og racebias i rekruttering.
- ▶ AI kan give fejloplysninger (“hallucinationer”).
- ▶ Modvirkes via menneskelig kontrol, kvalitetsdata og etikvejledninger.
- ▶ Ubalance i træningsdata og konsekvenser.

ETISKE DILEMMAER OG ANSVAR

- ▶ Privatliv, overvågning, behov for transparens.
- ▶ EU's AI Act og Liability Directive stiller ansvarsspørgsmål for udviklere og brugere.
- ▶ Særligt vigtigt i frivillige IT-miljøer med følsomme data.

VORES ASSISTENTER – GPT (GENERATIVE PRE-TRAINED TRANSFORMER)

- ▶ **Funktion:** Trænet på store mængder tekstdata til at forstå og generere sammenhængende tekst ved at forudsige næste ord.
- ▶ **Sprogmodeller:** GPT er en type stor sprogmodel, brugt til naturlig sprogforståelse og tekstgenerering.
- ▶ **Multimodal AI:** Nyere versioner kan også håndtere billeder, lyd og video ud over tekst.
- ▶ **Integration:** Assistent i applikationer. F.eks. Gemini i Google-søgninger, Co-Pilot i office programmer
- ▶ **Brug:** Kan skabe tekster, billeder, lyd eller video baseret på brugerens input (prompts).

MODEL	LAND/ORGANISATION	KENDETEGN	SÆRLIGT
GPT-5	OpenAI (USA)	Avanceret tekst- og billedforståelse	Integreret i Microsoft-produkter
CLAUDE 4 SONNET	Anthropic (USA)	Fokus på sikkerhed og "constitutional AI"	Brugt i myndighedssammenhæng
GEMINI 2.5	Google DeepMind (USA/UK)	Stærk multimodal - tekst, billeder, video	Dybt integreret med Google-søgning - to versioner
LLAMA 4	Meta (USA/EU)	Open source, forskning og undervisning	Kan køres lokalt på mindre hardware
MISTRAL MAGISTRAL	Mistral AI (Frankrig)	Europæisk, flersproget, dataprivatliv	Del af 'AI for Citizens' initiativet
FALCON 2 11B VLM	UAE (Tech Innovation Inst)	Multimodal, energieffektiv	Open source
DEEPSEEK V3.2- EXP	Kina (Hangzhou DeepSeek)	Effektiv til lange dokumenter, statskontrol	Begrænset udbredelse pga. sikkerhedspolitiske årsager
QWEN 3	Alibaba (Kina)	Kinesisk/engelsk allround-model	Asiatisk konkurrent til ChatGPT
GROK 4	xAI (Elon Musk)	Realtidsdata adgang, integreret i X-platform	Fokus på realtids-AI

HVAD ER EN PROMPT

- ▶ En prompt er en instruktion eller et spørgsmål, du skriver til AI for at få et svar eller en opgave løst.
- ▶ Kan bestå af enkelte ord, sætninger, spørgsmål eller mere komplekse opgaver.
- ▶ Resultatet afhænger af, hvordan du formulerer og præciserer din prompt.

PROMPTS

- ▶ Vær specifik og klar: Undgå vage formuleringer, beskriv præcis hvad du ønsker.
- ▶ Tilføj kontekst og mål: Forklar baggrund, formål og evt. rolle eller tone.
- ▶ Opdel komplekse opgaver: Stil ét klart spørgsmål ad gangen, især ved større opgaver.
- ▶ Anfør ønsket output: Fortæl hvordan svaret skal præsenteres (fx. liste, tekst, tabel).

PROMPTS

- ▶ Undersøg kilder og fakta: Stol aldrig blindt på AI – tjek kilder og søg supplerende viden.
- ▶ AI kan hallucinere (kan generere overbevisende men opdigtede svar)
- ▶ Justér din prompt og gentag for bedre resultater.
- ▶ Brug eksempler: Giv AI konkrete eksempler på ønskede outputs.
- ▶ Eksperimentér: Test med variationer
- ▶ Brug roller/personaer: Bed AI om at svare som fx “ekspert” hvis relevant.

Bemærk retningslinjer fra ÆldreSagen

GRATIS VS. BETALT AI-APPLIKATION

- ▶ Gratis: Begrænsede funktioner og langsommere svartid.
- ▶ Betalt: Avancerede modeller og bedre performance.
- ▶ Prioritet: Betalte brugere har fortrinsadgang ved spidsbelastning.

For mere info om forskelle mellem gratis og betalte versioner af ChatGPT, Gemini osv. se deres officielle sammenligninger.

FIL- & BILLEDUPLOAD

- ▶ Du kan uploade billeder, dokumenter eller filer direkte i chatten – AI kan læse, analysere og besvare alt indholdet.
- ▶ Brug billedupload til f.eks. at få AI til at beskrive, analysere eller generere tekst ud fra billedet.

SIKKERHED VED BRUG AF PROMPTS MED AI

- ▶ Vær varsom med at dele følsomme oplysninger i dine prompts. AI-modeller kan lagre eller bruge information til fremtidig træning.
- ▶ Undgå at inkludere private data, adgangskoder, personnumre eller fortrolige forretningsdata i prompterne.
- ▶ AI kan generere plausible, men forkerte eller bedragende svar – vær kritisk og tjek altid fakta.
- ▶ Husk, at data sendt til cloud-baserede AI-tjenester passerer over nettet og kan potentielt opsnappes.
- ▶ Overvej hvordan virksomhedens datasikkerhed og GDPR-regler påvirker brugen af AI-værktøjer.
- ▶ Brug AI til at støtte beslutninger, men ikke til ukritisk at erstatte menneskelig vurdering, især ved følsomme emner.
- ▶ Sikkerhedsbrud eller misbrug kan ske via manipulerede prompts, der får AI til at afsløre eller konstruere følsomme oplysninger.



AI genereret

ØVELSER

WORKSHOP

ØVELSE 1: SAMMENLIGNING AF MULTIMODAL AI-RESPONSER

Formål: Deltagerne prøver at stille det samme spørgsmål til Grok, Gemini og ChatGPT.

Opgave: Vælg et spørgsmål, der inkluderer både tekst og billede (fx. "Analyser denne infografik og forklar hovedpointerne").

Aktivitet: Sammenlign svarenes kvalitet, detaljeringsgrad og brug af multimodale input.

ØVELSE 2: GENERERING AF AI-ASSISTERET INDHOLD

Formål: Fremvis hvordan AI kan hjælpe i dokumentation, idegenerering eller tekstforfatning.

Opgave: Brug ChatGPT eller Gemini til at skrive en kort tekst (fx et resume af et komplekst emne), og derefter redigeres teksten af deltagerne.

Aktivitet: Sammenlign svarenes kvalitet, detaljeringsgrad og brug af multimodale input.

ØVELSE 3: AI I DAGLIGDAGS PRAKSIS

Formål: Demonstrere AI-integration i smartphones og apps.

Opgave: Brug ChatGPT eller Gemini til at skrive en kort tekst (fx et resume af et komplekst emne), og derefter redigeres teksten af deltagerne.

Aktivitet: Prøv stemmeassistenter (Siri, Google Assistant) eller AI-plugins i søgemaskiner og diskuter oplevelsen.