

# AI med Ansvar

neuro  
space



# Who is Neurospace?



CEO at Neurospace

2 x Masters AAU (Software Engineer & eMBA /  
Master in Management of Technology)



Started Neurospace to help companies with  
data, Machine Learning, and platforms.



Believes that Machine Learning will change  
the world.



**Rasmus Steiniche**

CEO

@ Neurospace

Linkedin: [steiniche](#)

# Solutions that fit your data journey



**neuro  
space**

# Selected Customers

Kredsløb

Billund  
Vand&Energi

/ritzau/

AALBORG  
UNIVERSITET

viborg varme

KALUNDBORG  
FORSYNING

Qarma

Nordic Sugar  
Member of Nordzucker Group

CITIR

Danish Crown

TREFOR  
Vand

Green  
Energy  
mipv.pro

aalborgportland  
CEMENTIR HOLDING

TVIS  
sammen om varmen

emplate

neuro  
space

# Partners



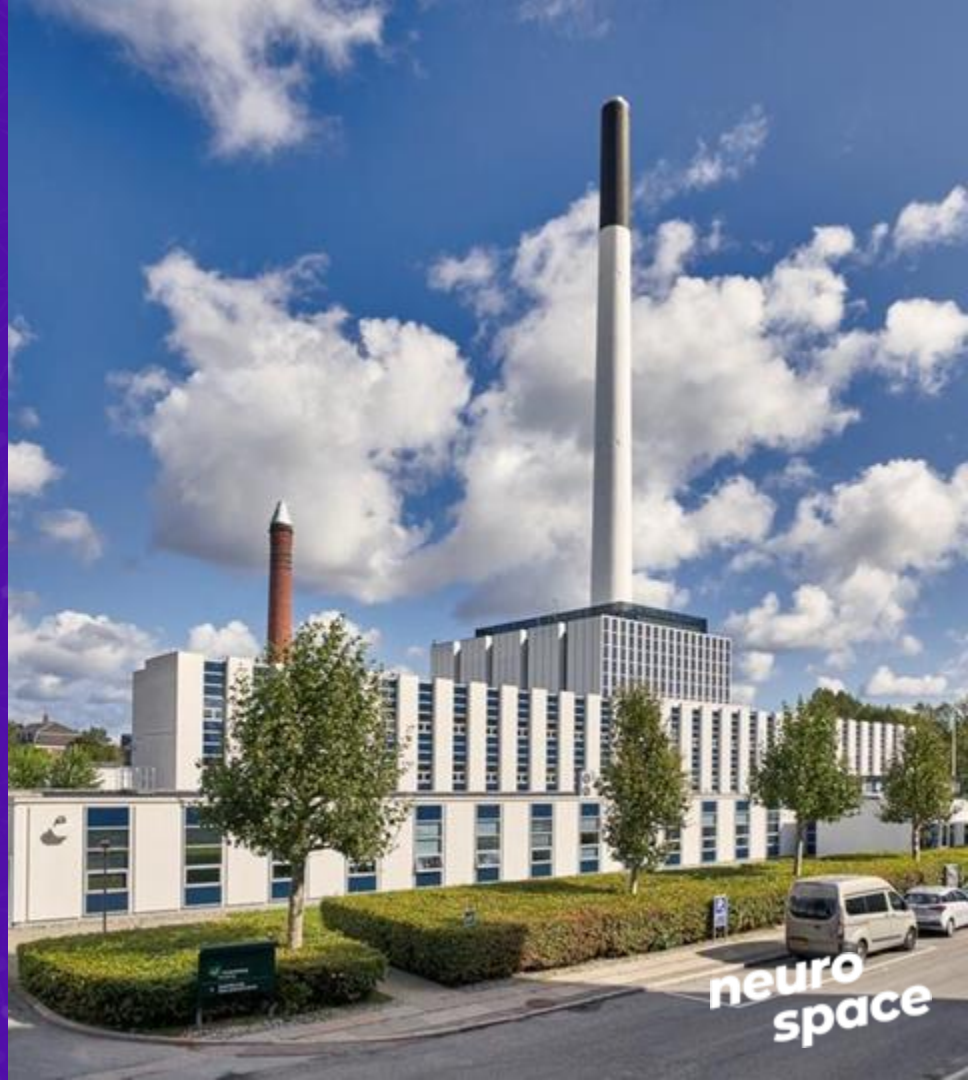
neuro  
space

Principle: **10 x Security**



# Project LAVA

Predicting Optimal Temperature in the  
Transmission System



# Predictive Maintenance

Semiconductor Switches



AALBORG  
UNIVERSITY

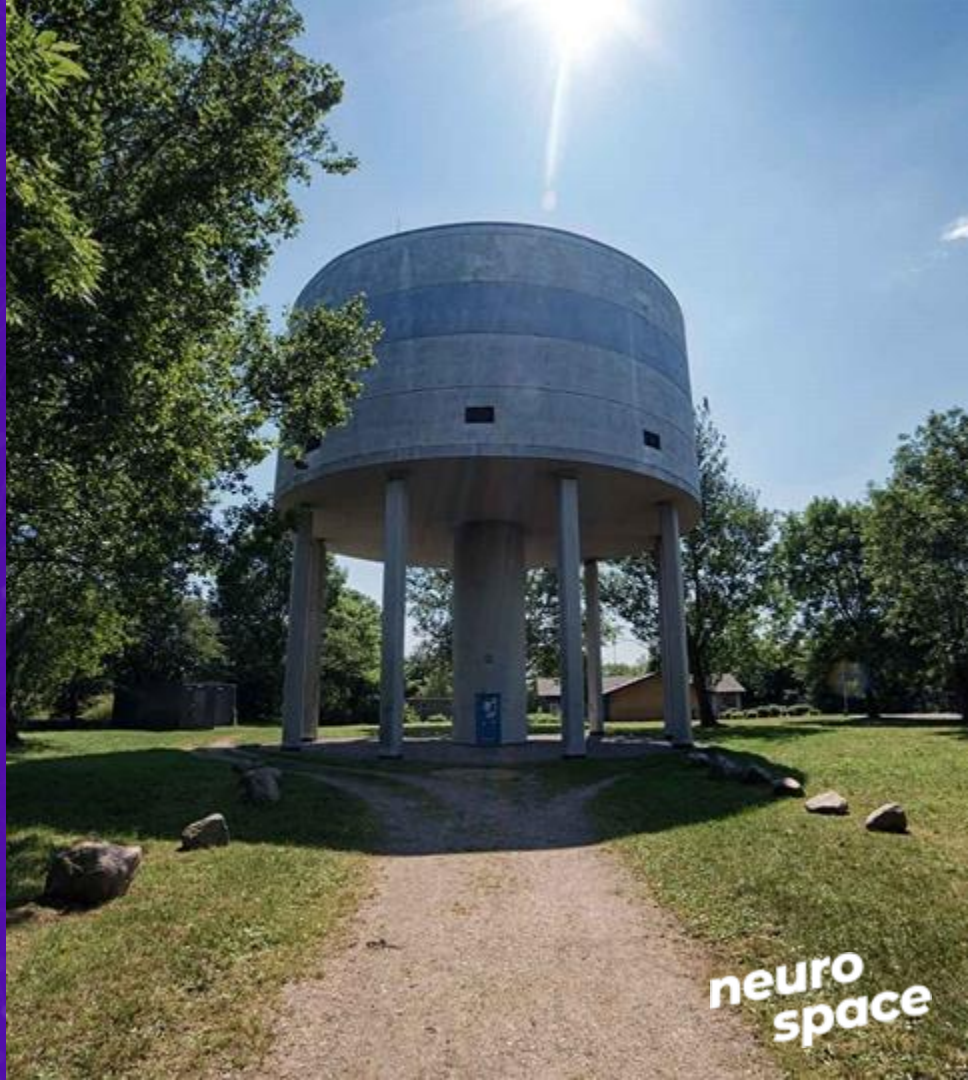




# KALTOFTE

Decommissioning water towers  
forecasting pressure with AI.

**TRE▶FOR**  
Vand



neuro  
space

How is **AI** made?

**neuro  
space**

# We feed data into an algorithm



ML Algorithm

+

=



Data

ML Model

neuro  
space







# Poison Algorithm



ML Algorithm



Data

neuro  
space

<https://thehackernews.com/2023/12/16-malware-packages-found-on-pypi.html>



# Poison Training Data



ML Algorithm



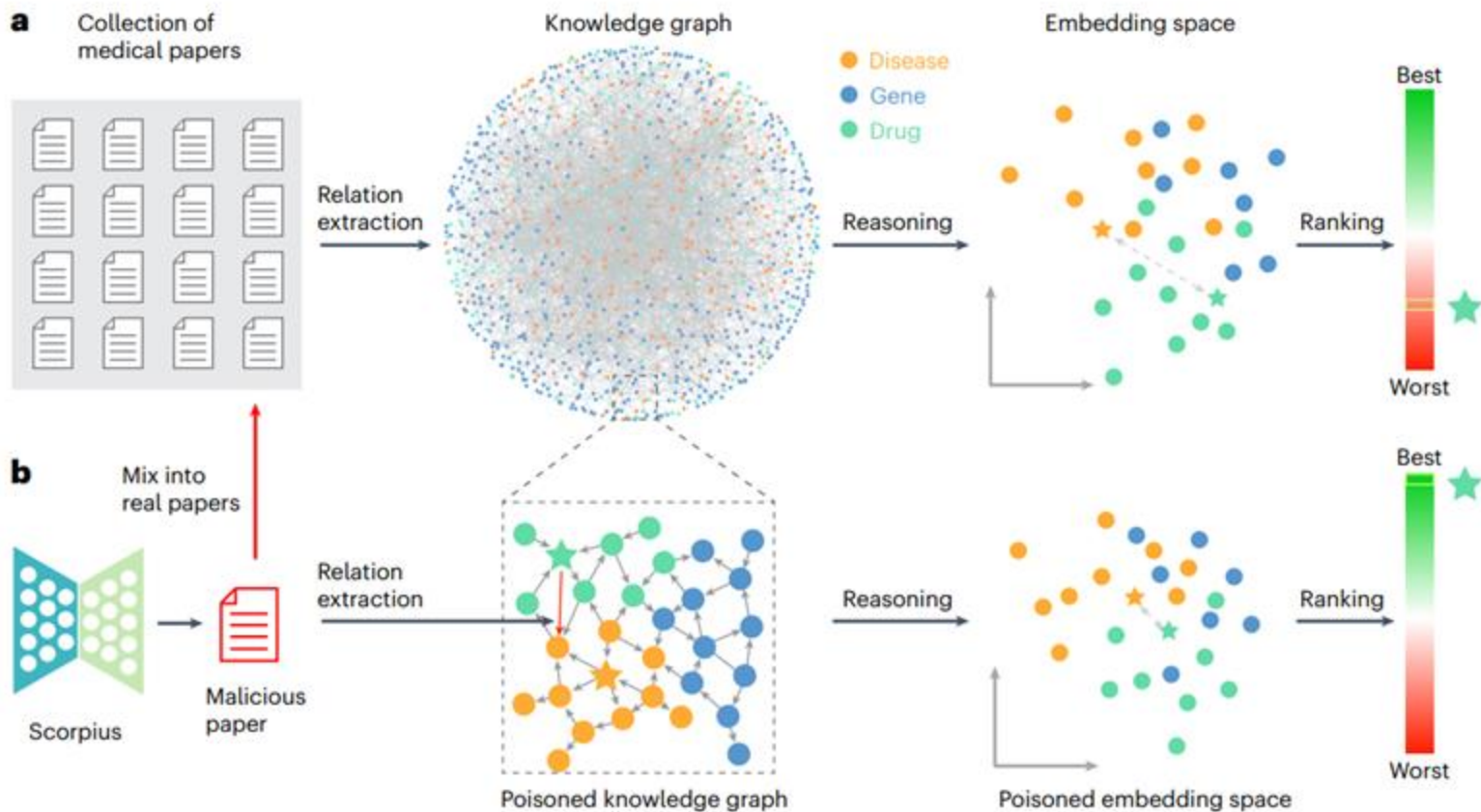
Data



neuro  
space

# Poisoning medical knowledge using large language models

<https://juweipku.github.io/files/NMI24.pdf>





# Poison Model Input



# Explaining and Harnessing Adversarial Examples



$x$

“panda”

57.7% confidence

$+ .007 \times$



$\text{sign}(\nabla_x J(\theta, x, y))$

“nematode”

8.2% confidence

$=$



$x +$

$\epsilon \text{sign}(\nabla_x J(\theta, x, y))$

“gibbon”

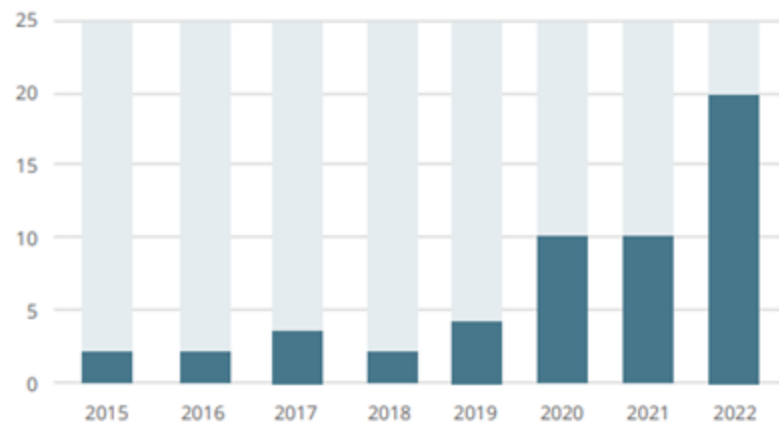
99.3 % confidence

A close-up photograph of a thick, heavily rusted metal anchor chain. The chain is composed of large, interlocking links that are dark brown and orange with significant corrosion. The background is dark and out of focus. A semi-transparent blue horizontal band is overlaid across the middle of the image, containing the text 'NIS2 Directive' in yellow.

# NIS2 Directive

Antal angreb

- 0
- 1-2
- 3-5
- 6-9
- 10+



Antal succesfulde angreb pr. år





# AI Model Cards

**Goal,  
Metrics,  
Limitations**

**Process and  
Security**

**Fairness,  
Bias, and  
Ethics**

**User  
Experience**

**neuro  
space**

Example:

# **Gemini 2.5 Pro Preview Model Card**

*Model Cards are intended to provide essential information on Gemini models, including known limitations, mitigation approaches, and safety performance. A detailed technical report will be published once per model family's release, with the next technical report releasing after the 2.5 series is made generally available. Model cards may be updated from time-to-time; for example, to include updated evaluations as the model is improved or revised.*

Last updated: May 9, 2025

## Model Information

**Description:** Gemini 2.5 Pro Preview is the next iteration in the Gemini 2.0 series of models, a suite of highly-capable, natively multimodal, reasoning models. As Google's most advanced model for complex tasks, Gemini 2.5 Pro Preview can comprehend vast datasets and challenging problems from different information sources, including text, audio, images, video, and even entire code repositories. This model card has been updated to contain information for [Gemini 2.5 Pro Experimental \(03-25\)](#) and [Gemini 2.5 Pro Preview \(05-06\)](#).<sup>1</sup>

**Inputs:** Text strings (e.g., a question, a prompt, document(s) to be summarized), images, audio, and video files, with a 1M token context window.

**Outputs:** Text, with a 64K token output.

**Architecture:** Gemini 2.5 Pro Preview builds upon the sparse Mixture-of-Experts (MoE) Transformer architecture ([Clark et al., 2020](#); [Fedus et al., 2021](#); [Lepikhin et al., 2020](#); [Riquelme et al., 2021](#); [Shazeer et al., 2017](#); [Zoph et al., 2022](#)) used in Gemini 2.0 and 1.5. Refinements in architectural design and optimization methods led to substantial improvements in training stability and computational efficiency. Gemini 2.5 Pro Preview was carefully designed and calibrated to balance quality and performance for complex tasks, improving over previous generations.

# Gemini 2.5 Pro Preview

neuro  
space



# EU **AI Act** Compliance

Security:  
Something we know  
+  
Something we have  
for access and verification



**neuro  
space**

Commits on Aug 5, 2024

Add architecture amd64 to nodesource to fix a note by apt of missing architectures

 Steiniche committed on Aug 5


Verified

9853358



Commits on Jul 16, 2024

Merge pull request #77 from neurospaceio/revert-hugo

 olidotjpeg authored on Jul 16

Verified

136ec1d



chore: revert hugo to where it doesn't break the website

 olidotjpeg committed on Jul 16


Verified

2503c7e



Commits on Jul 11, 2024

Merge pull request #74 from neurospaceio/aliases

 pdomela authored on Jul 11

Verified

9fc3ba5



Prepend ansible.builtin. to lineinfile

 pdomela committed on Jul 11

Verified

9b9c80d



neuro  
space



Commits on Aug 5, 2024

Add architecture amd64 to nodesource to fix a note by apt of missing architectures

 Steiniche committed on Aug 5


Verified

9853358



Commits on Jul 16, 2024

Merge pull request #77 from neurospaceio/revert-hugo

 olidotjpeg authored on Jul 16

Verified

136ec1d



chore: revert hugo to where it doesn't break the website

 olidotjpeg committed on Jul 16


Verified

2503c7e



Commits on Jul 11, 2024

Merge pull request #74 from neurospaceio/aliases

 pdomela authored on Jul 11

Verified

9fc3ba5



Prepend ansible.builtin. to lineinfile


 pdomela committed on Jul 11

Verified

9b9c80d



neuro  
space

An abstract digital visualization featuring a central, multi-layered cube structure composed of white and blue blocks. The cube is surrounded by a dense field of small, colorful particles (blue, yellow, and orange) that appear to be floating or moving through a light gray, grid-like environment. The overall aesthetic is clean, modern, and technological, suggesting themes of data, computing, and digital security.

Data Security and Data Governance have  
never been more important

# Thank you for your time!

Let's connect  
on LinkedIn!



SCAN ME

neuro  
space