CyberDay.lu 2023

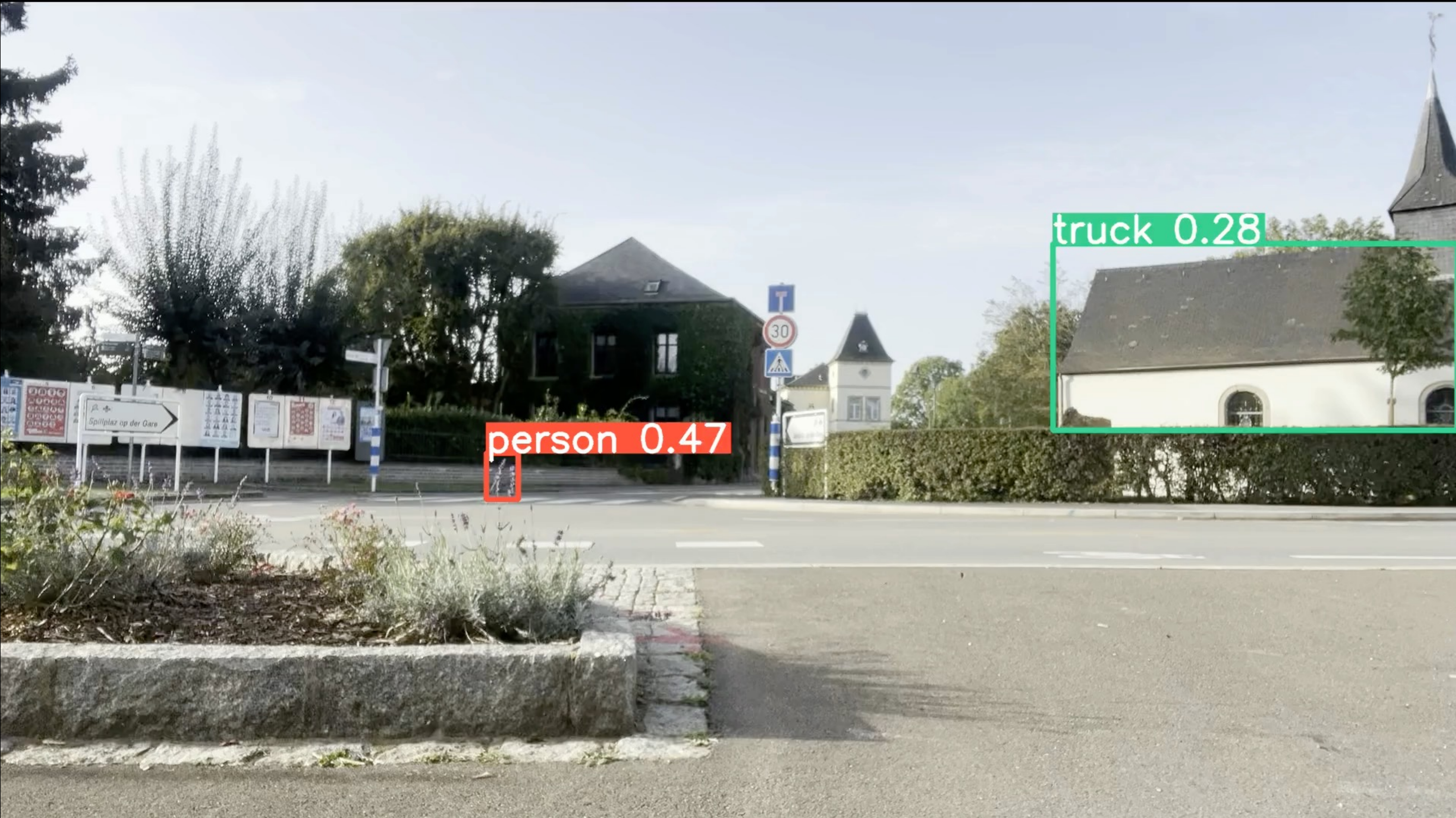
AI 4 Security

Dr. Cynthia Wagner
Dr. Serge Linckels

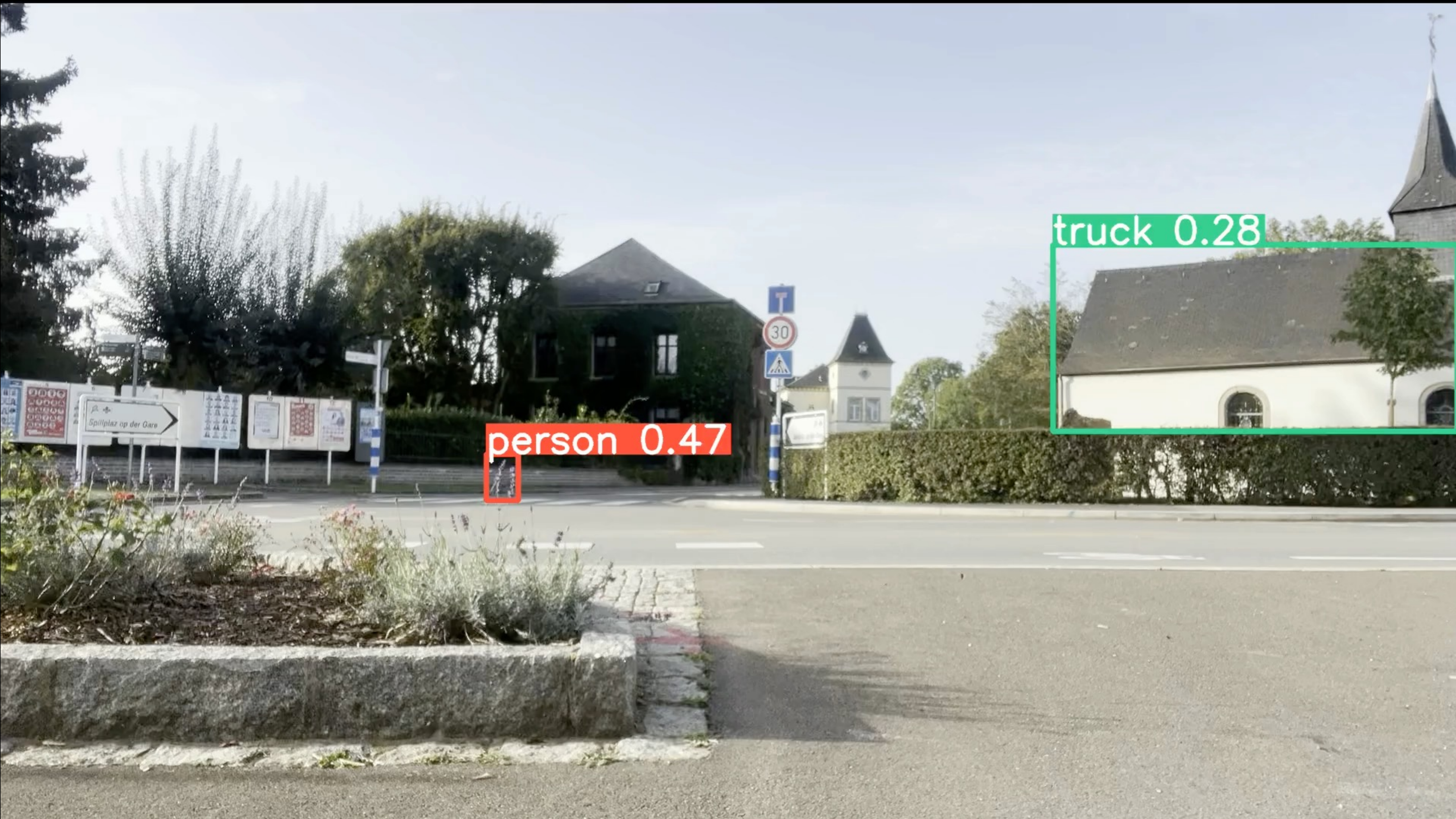
12 October 2023

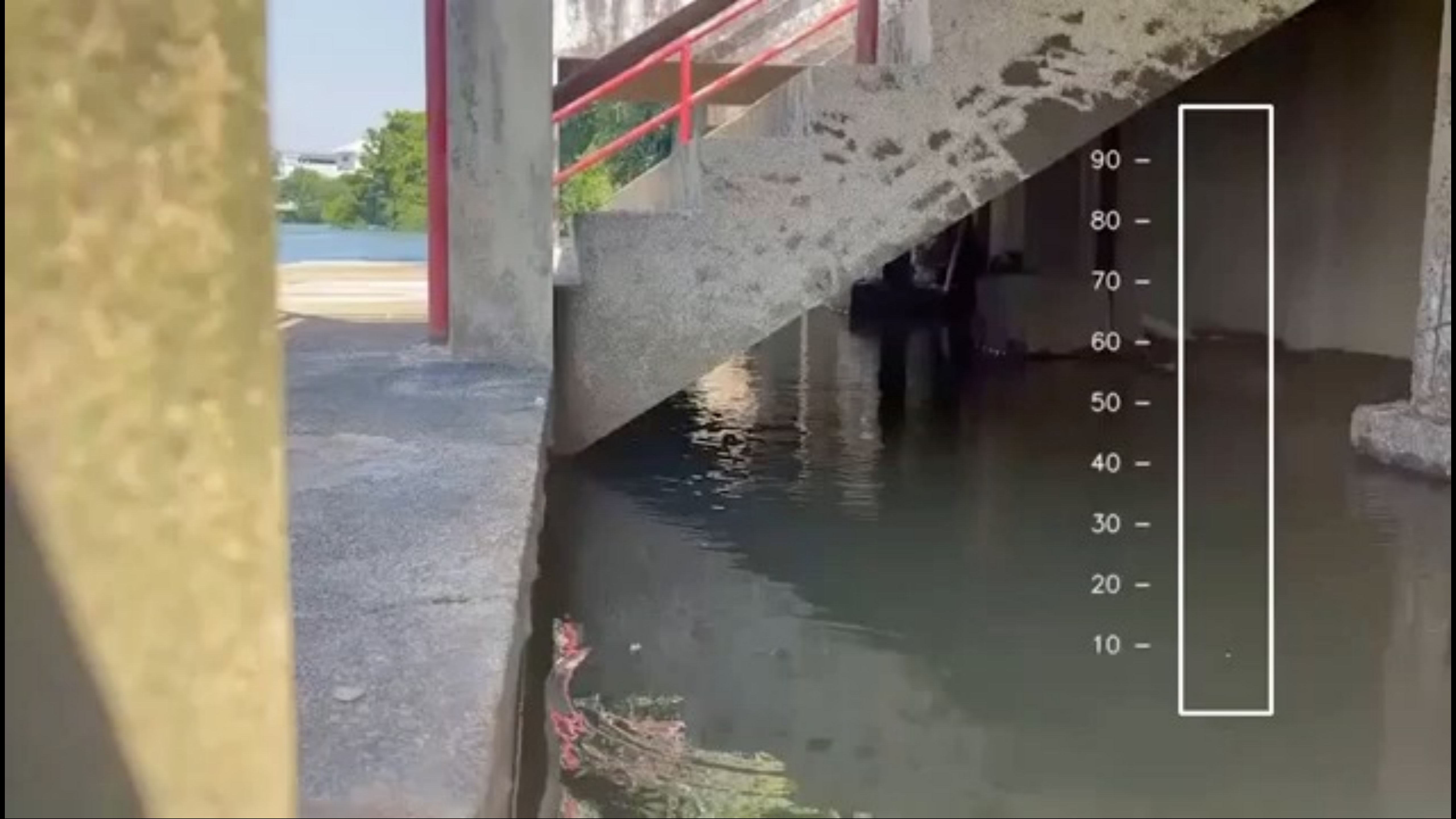
Digital
Learning
Hub_

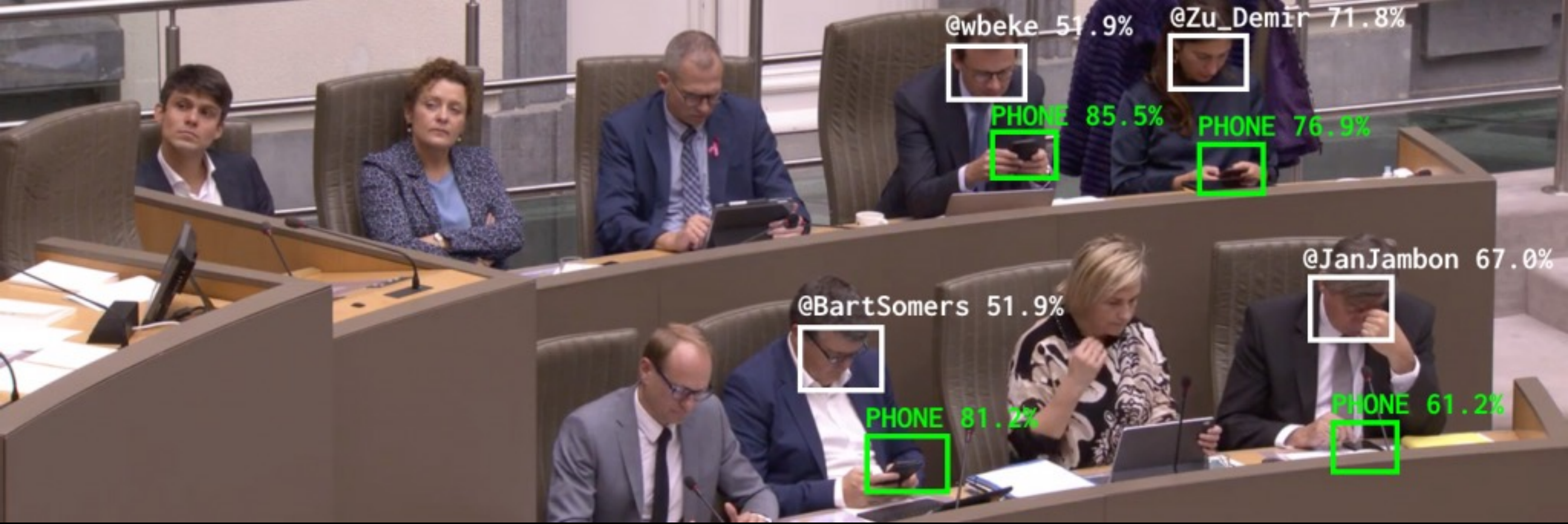
restena
network · security · .lu


person 0.47
truck 0.28
Spillplaz op der Gare
30

```
from ultralytics import YOLO
model = YOLO('yolov8n.pt')
results = model(‘myvideo.mov’, save=True, stream=True)
```


person 0.47
truck 0.28
Spillplaz op der Gare
30

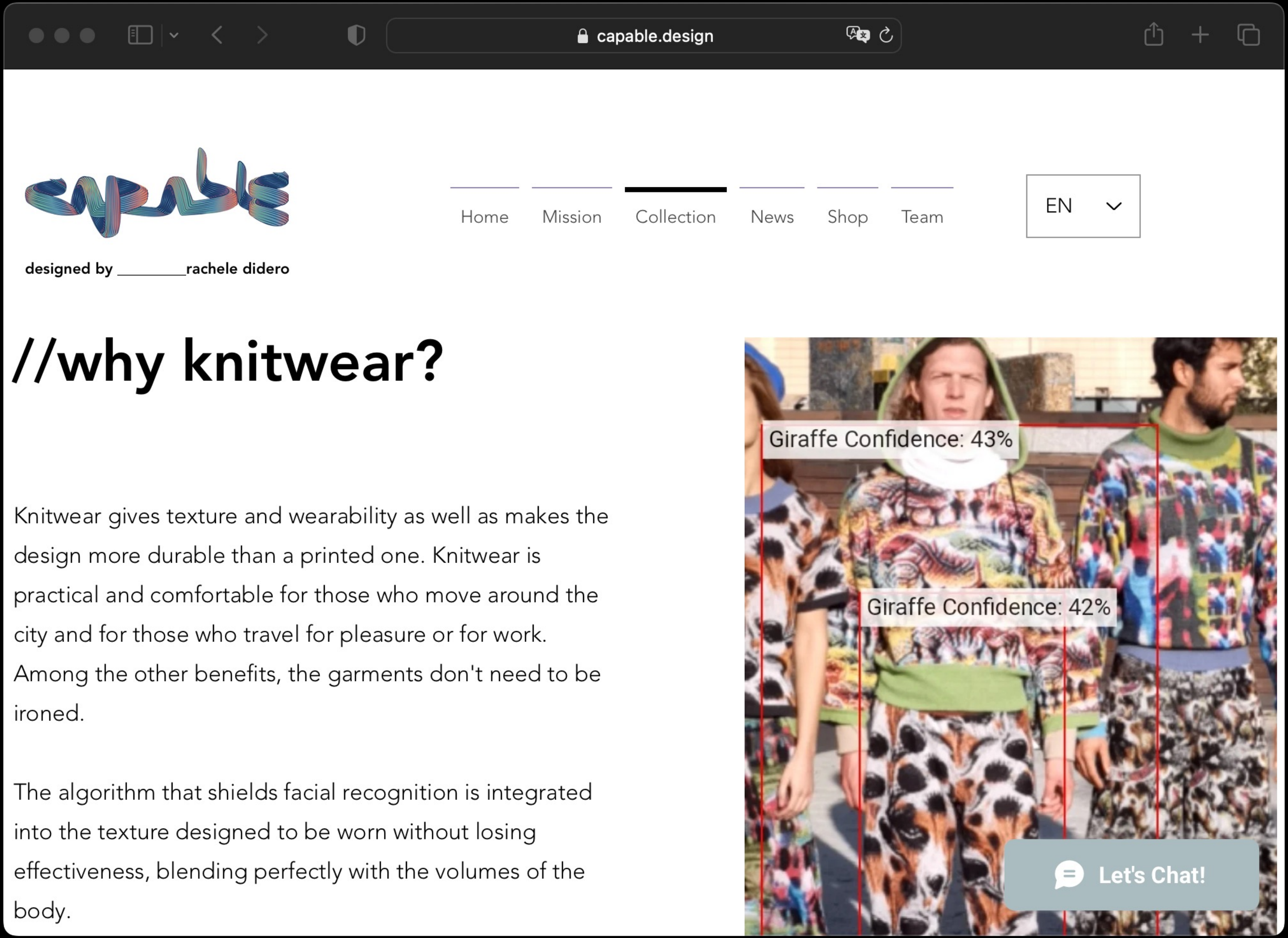

90 –
80 –
70 –
60 –
50 –
40 –
30 –
20 –
10 –



The Flemish Scrollers, 2021-2023 – Dries Depoorter

https://driesdepoorter.be/theflemishscrollers/

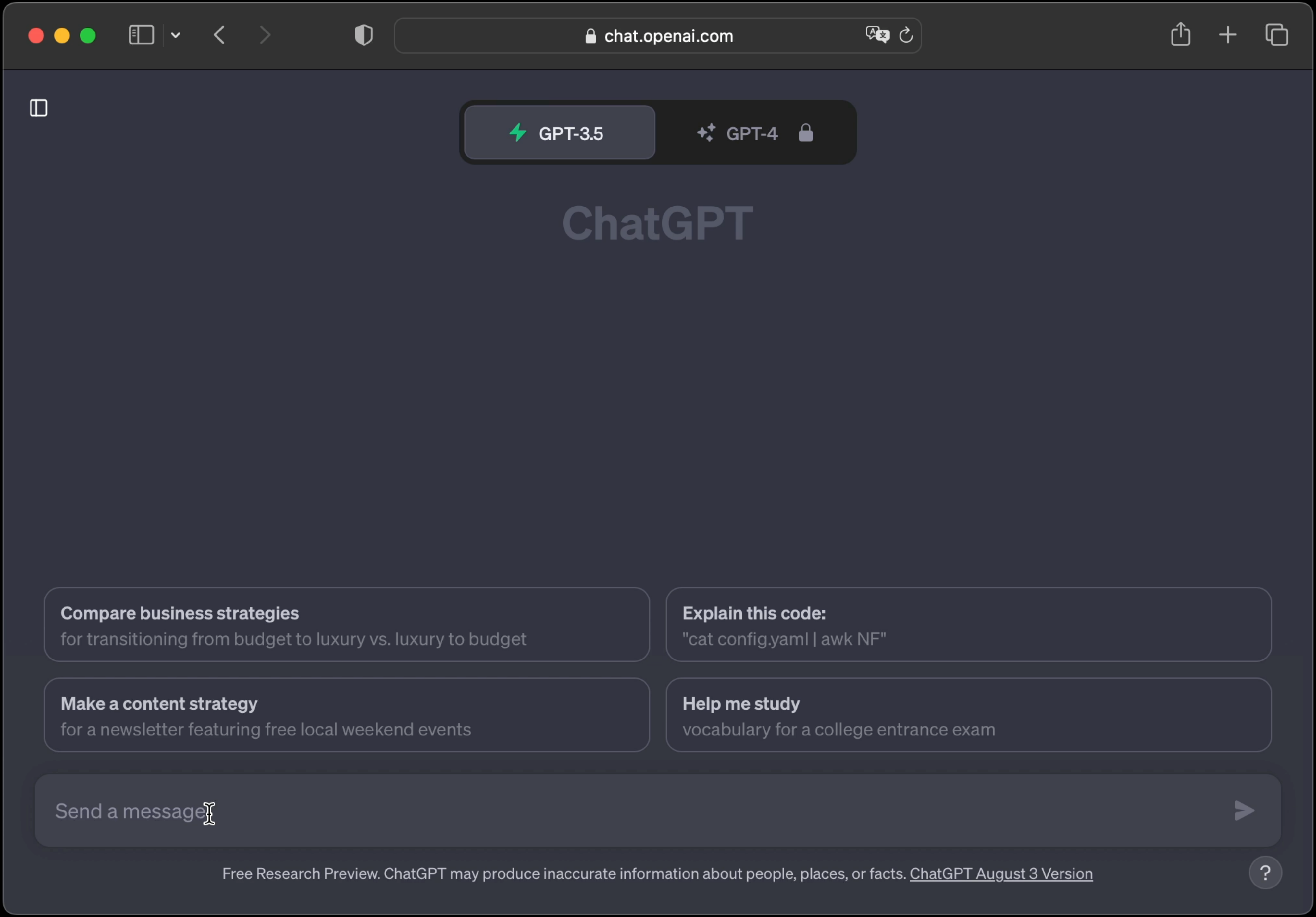
Source: Quarz (https://youtu.be/_yKga54tx6U)



//why knitwear?

Knitwear gives texture and wearability as well as makes the design more durable than a printed one. Knitwear is practical and comfortable for those who move around the city and for those who travel for pleasure or for work. Among the other benefits, the garments don't need to be ironed.

The algorithm that shields facial recognition is integrated into the texture designed to be worn without losing effectiveness, blending perfectly with the volumes of the body.



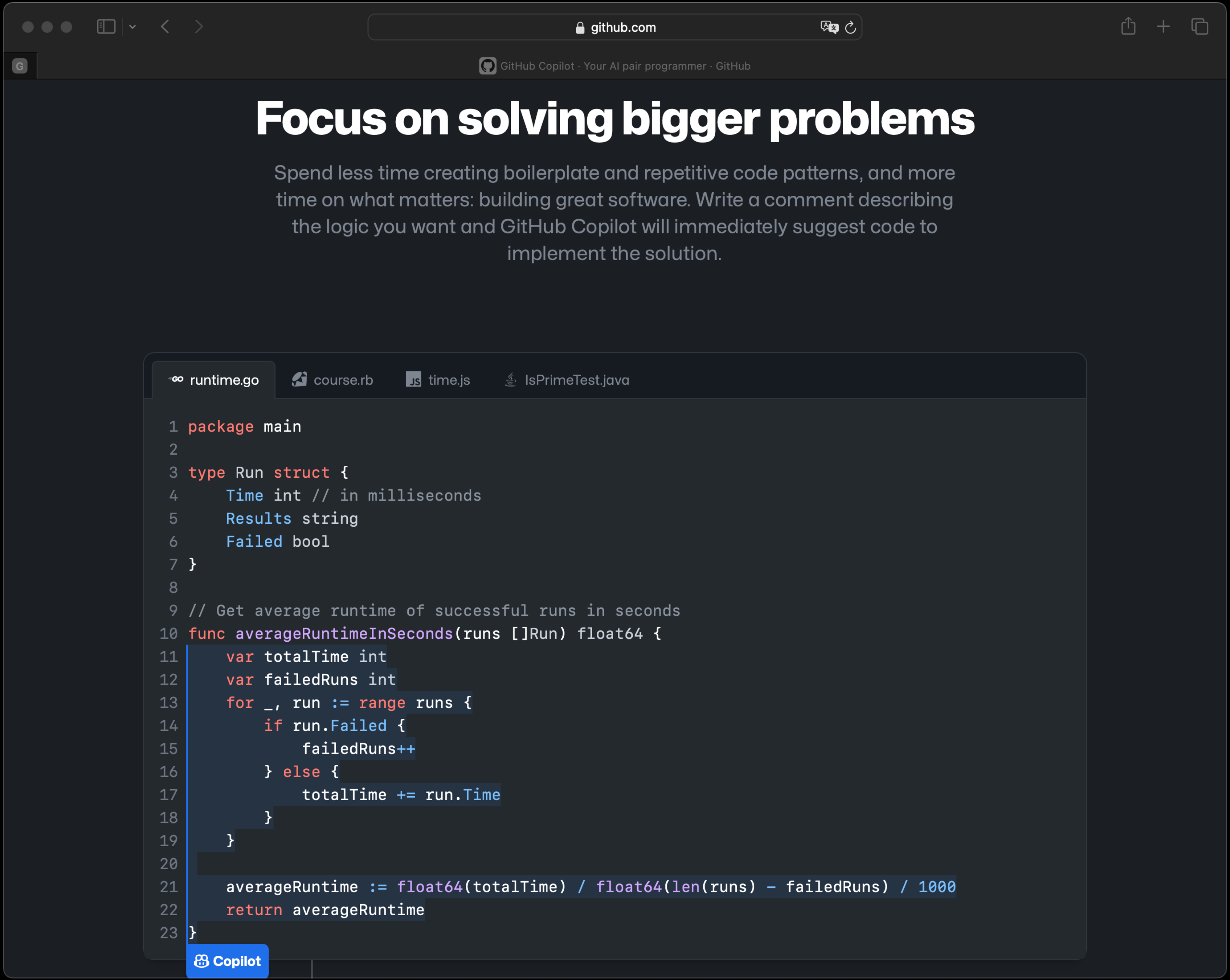
Compare business strategies
for transitioning from budget to luxury vs. luxury to budget

Explain this code:
"cat config.yaml | awk NF"

Make a content strategy
for a newsletter featuring free local weekend events

Help me study
vocabulary for a college entrance exam

Free Research Preview. ChatGPT may produce inaccurate information about people, places, or facts. ChatGPT August 3 Version



Focus on solving bigger problems

Spend less time creating boilerplate and repetitive code patterns, and more time on what matters: building great software. Write a comment describing the logic you want and GitHub Copilot will immediately suggest code to implement the solution.

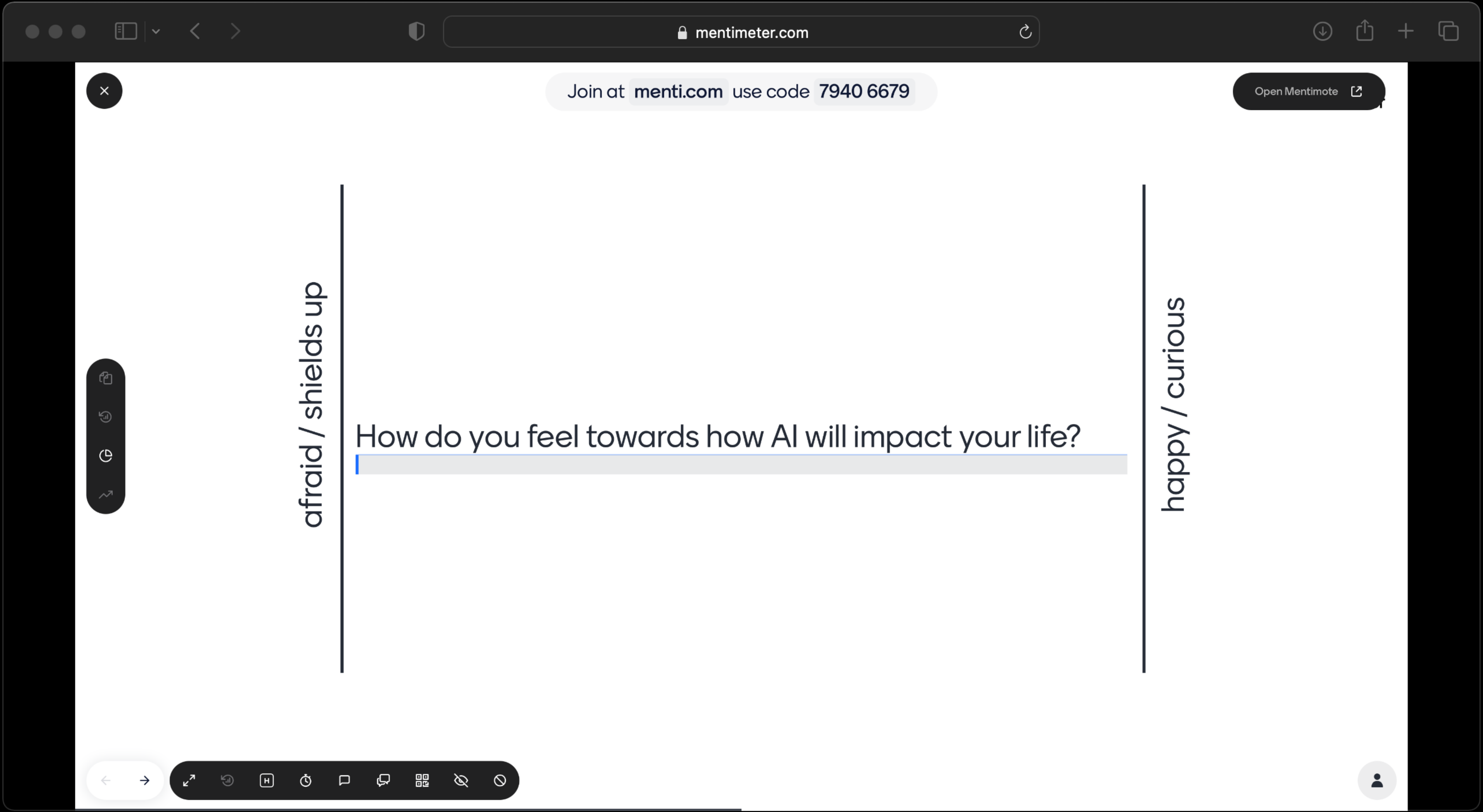
```go
package main

type Run struct {
    Time int // in milliseconds
    Results string
    Failed bool
}

// Get average runtime of successful runs in seconds
func averageRuntimeInSeconds(runs []Run) float64 {
    var totalTime int
    var failedRuns int
    for _, run := range runs {
        if run.Failed {
            failedRuns++
        } else {
            totalTime += run.Time
        }
    }

    averageRuntime := float64(totalTime) / float64(len(runs) - failedRuns) / 1000
    return averageRuntime
}
```

Gartner estimates by 2025, 70% of new applications developed by enterprises will use no-code or low-code technologies

https://www.gartner.com/en/newsroom/press-releases/2022-12-13-gartner-forecasts-worldwide-low-code-development-technologies-market-to-grow-20-percent-in-2023

Resistance is futile

Picture of Jean-Luc Picard as Locutus after Borg assimilation.
Picture from Star Trek DS9 "Emissary"

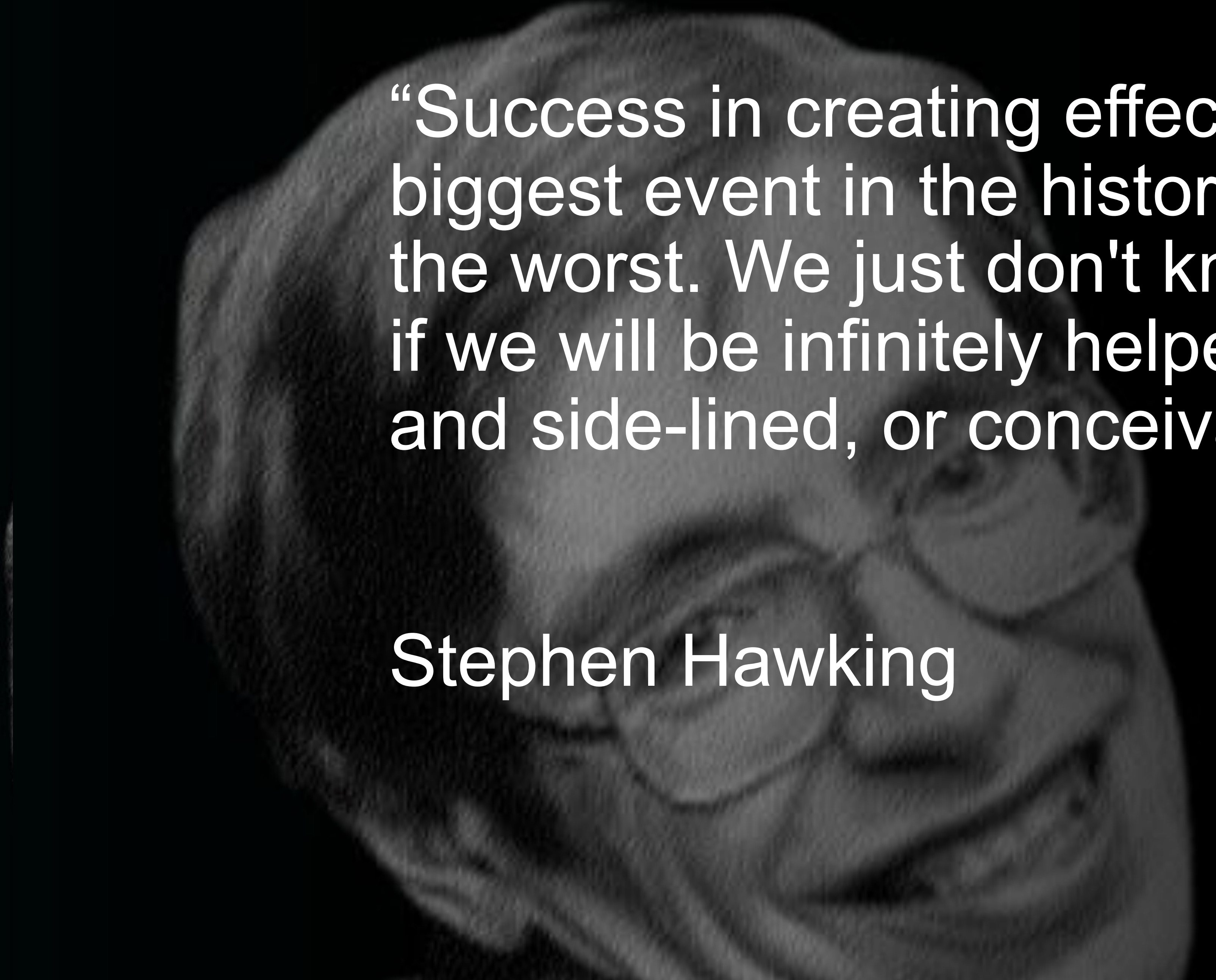


Join at menti.com use code 7940 6679

afraid / shields up

How do you feel towards how AI will impact your life?

happy / curious

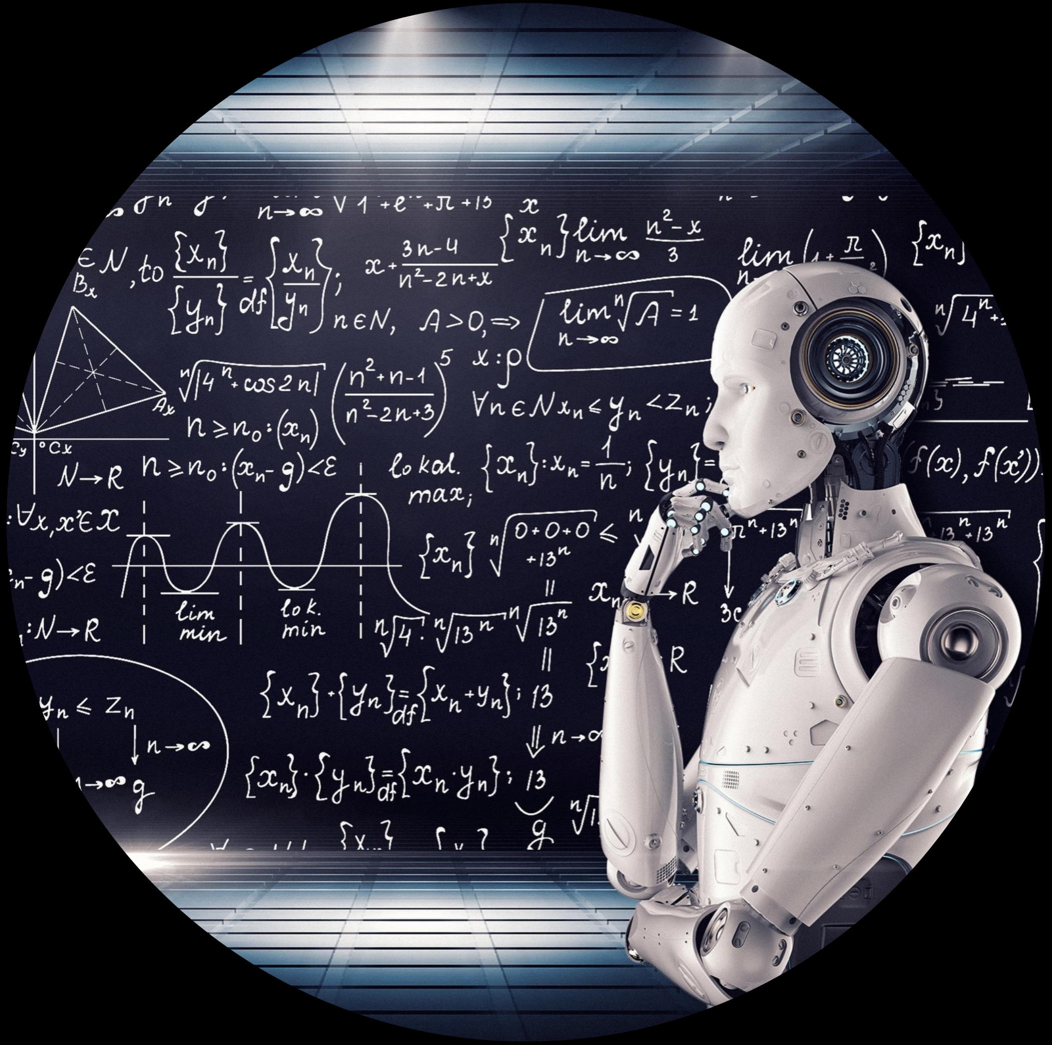


“Success in creating effective AI, could be the
biggest event in the history of our civilization. Or
the worst. We just don't know. So, we cannot kn
if we will be infinitely helped by AI, or ignored by
and side-lined, or conceivably destroyed by it”

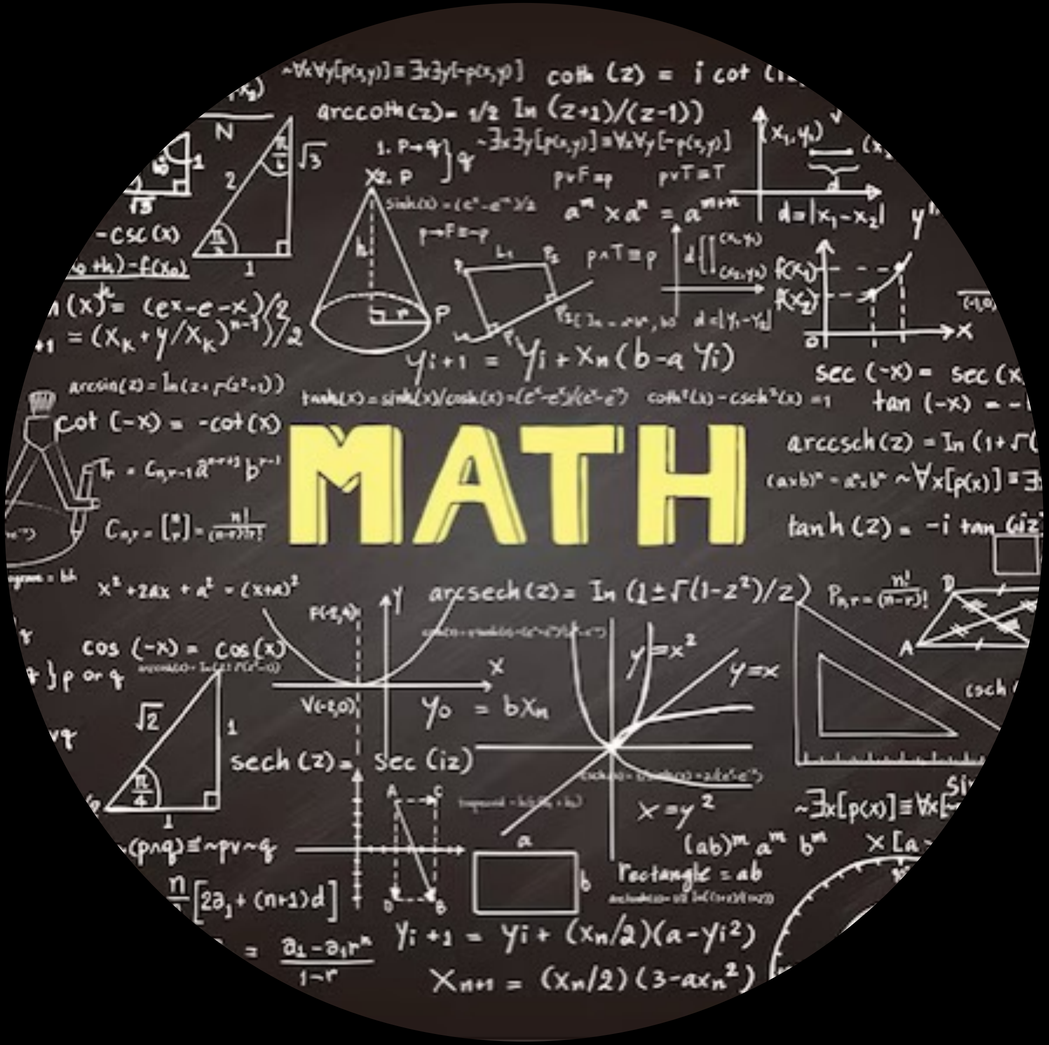
Stephen Hawking

AI Singularity?

Not so fast!

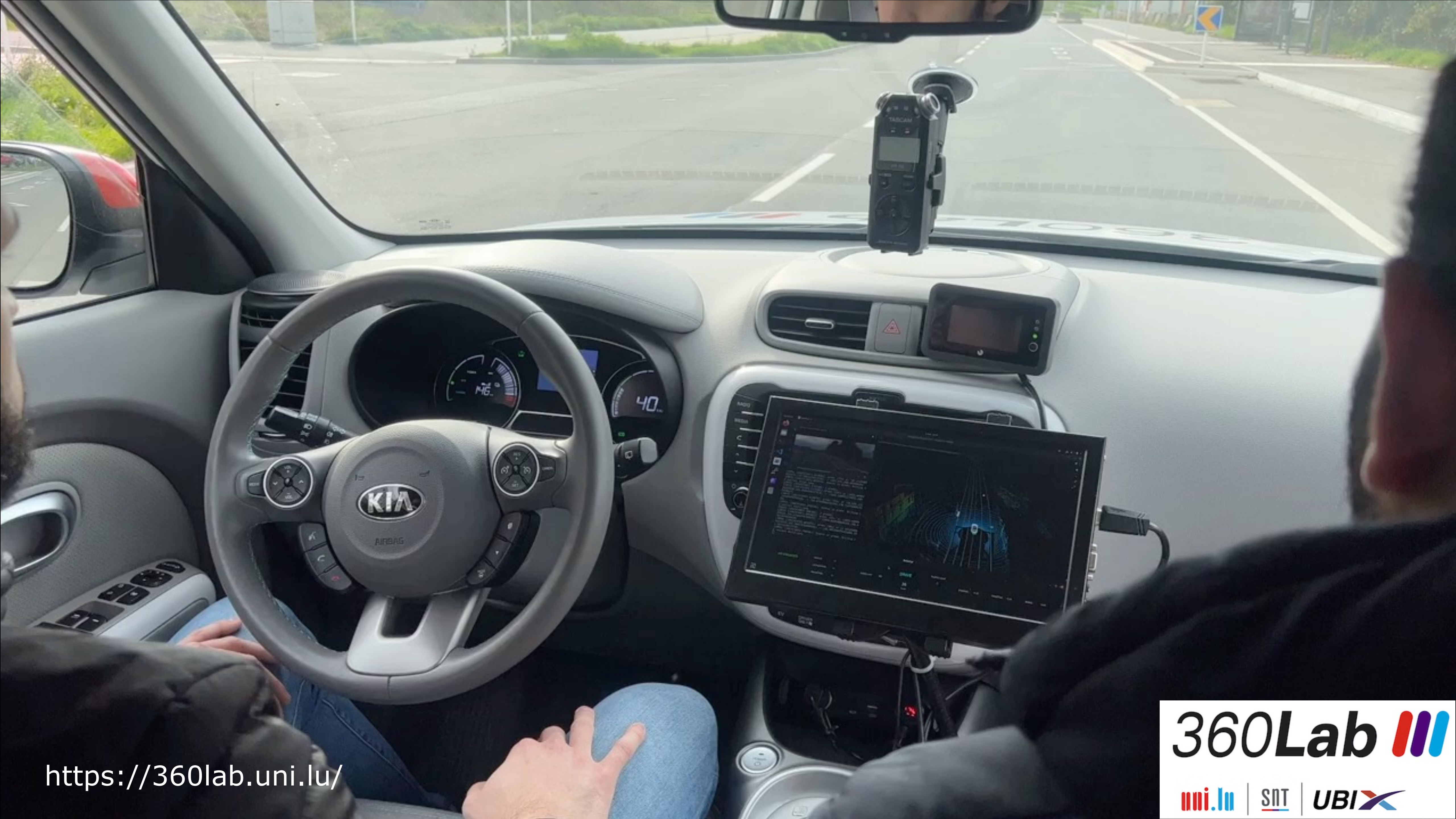


=


MATH

AI is not smart

- Learns and improves by rule sets and finetuning
- Only as good as its data set and programmer!
    - This makes it powerful at well-defined and delimited problem solving
        - Reading x-rays? Yes.
        - Cancer cells detection by image analysis? Yes.
        - Playing chess? AI usually wins (95%?)
    - Defined rule sets



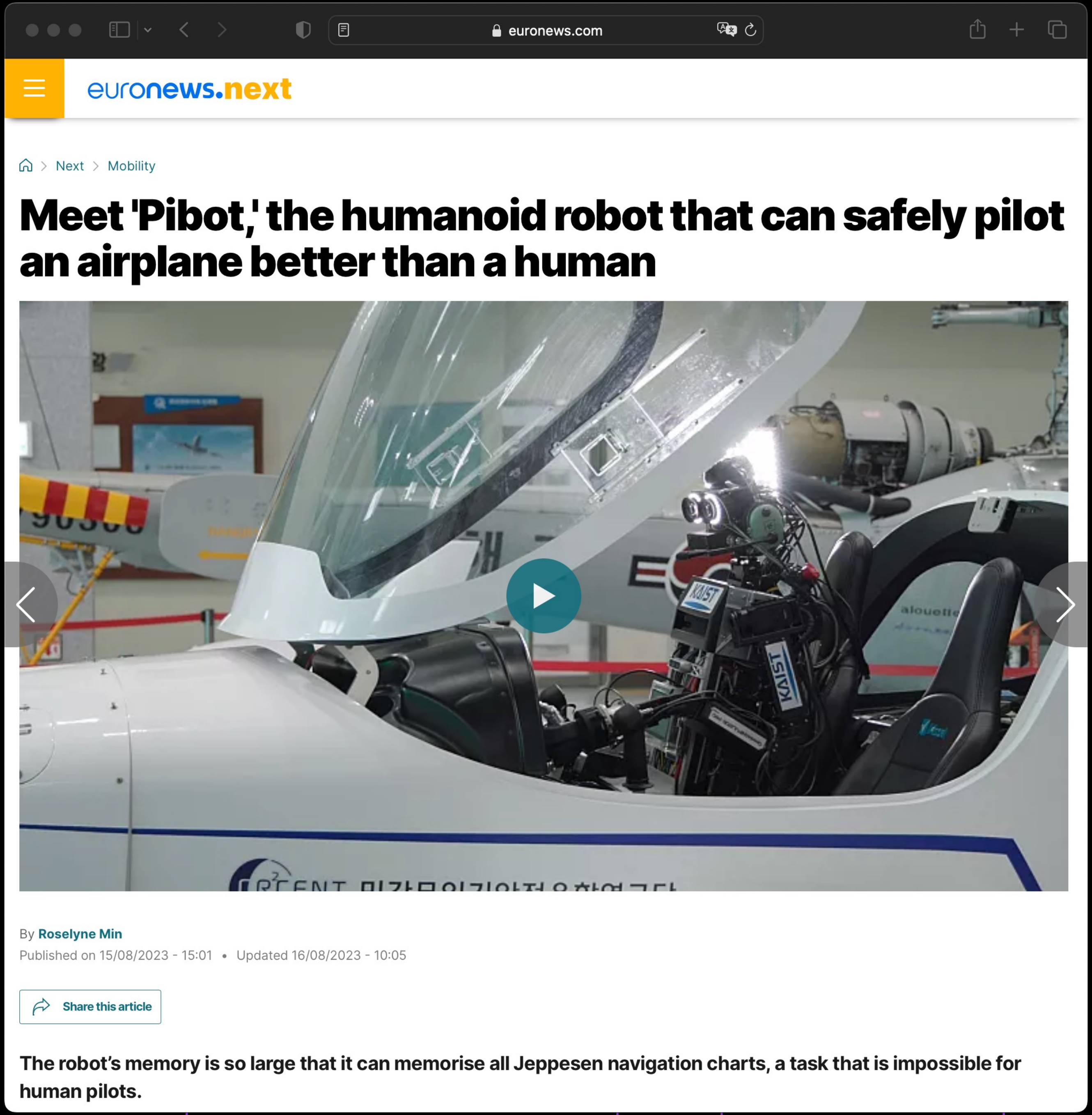
https://360lab.uni.lu/

360Lab

uni.lu | SnT | UBIX

Society of Automotive Engineers

Level 0: no automation
Level 1: hands on / shared control
Level 2: hands off
Level 3: eyes off
Level 4: mind off
Level 5: full driving automation



Next > Mobility

Meet 'Pibot,' the humanoid robot that can safely pilot an airplane better than a human

By Roselyne Min

Published on 15/08/2023 - 15:01 • Updated 16/08/2023 - 10:05

The robot's memory is so large that it can memorise all Jeppesen navigation charts, a task that is impossible for human pilots.

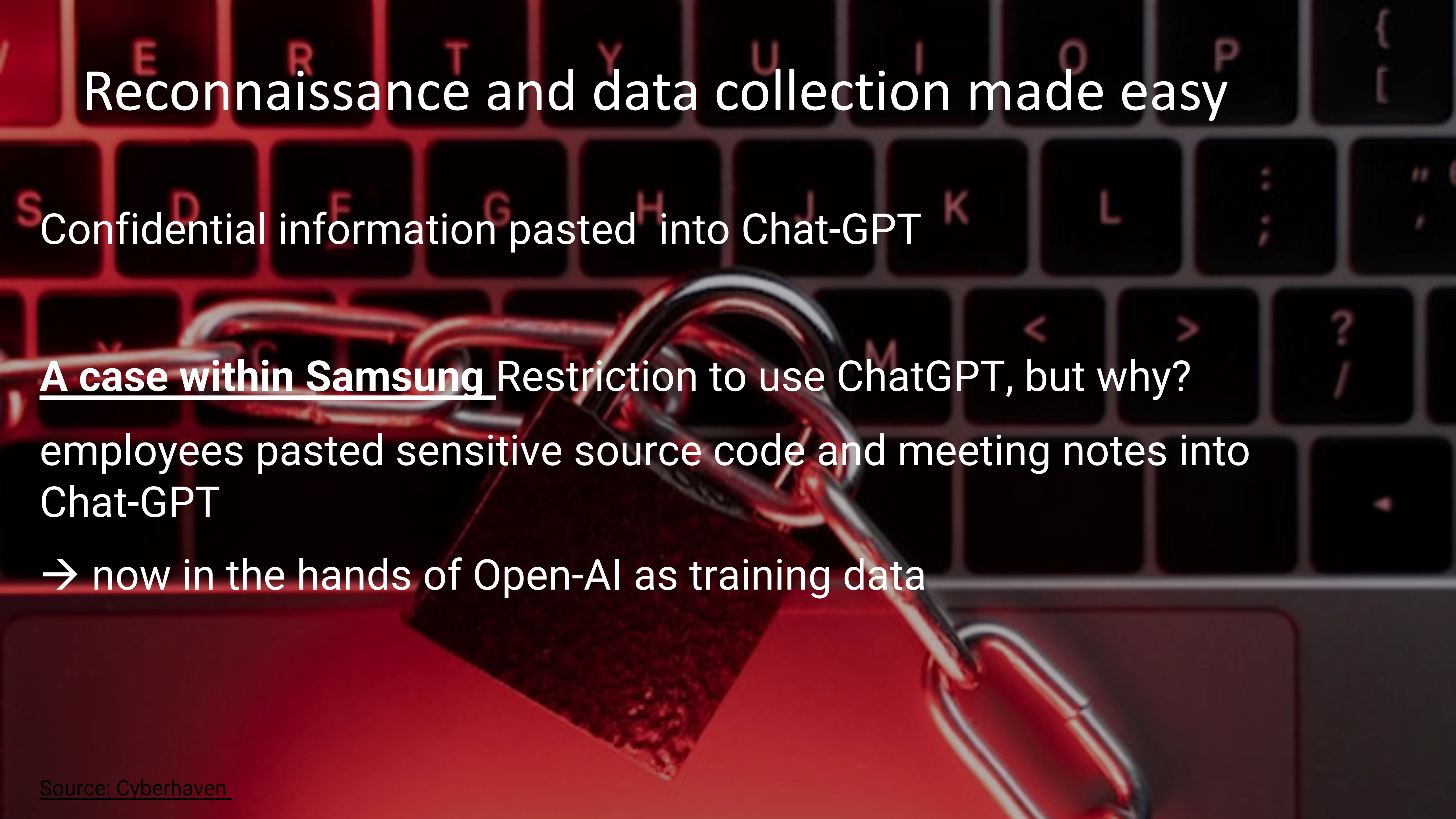
AI and Hackers?

FraudGPT, a new malicious generative AI tool emerges

FraudGPT, another new cybercrime generative artificial intelligence (AI) tool has been advertised on various dark web marketplaces and Telegram channels.

WormGPT

ChatGPT's Malicious Cousin



Reconnaissance and data collection made easy

Confidential information pasted into Chat-GPT

A case within Samsung Restriction to use ChatGPT, but why?

employees pasted sensitive source code and meeting notes into Chat-GPT

→ now in the hands of Open-AI as training data

Source: Cyberhaven

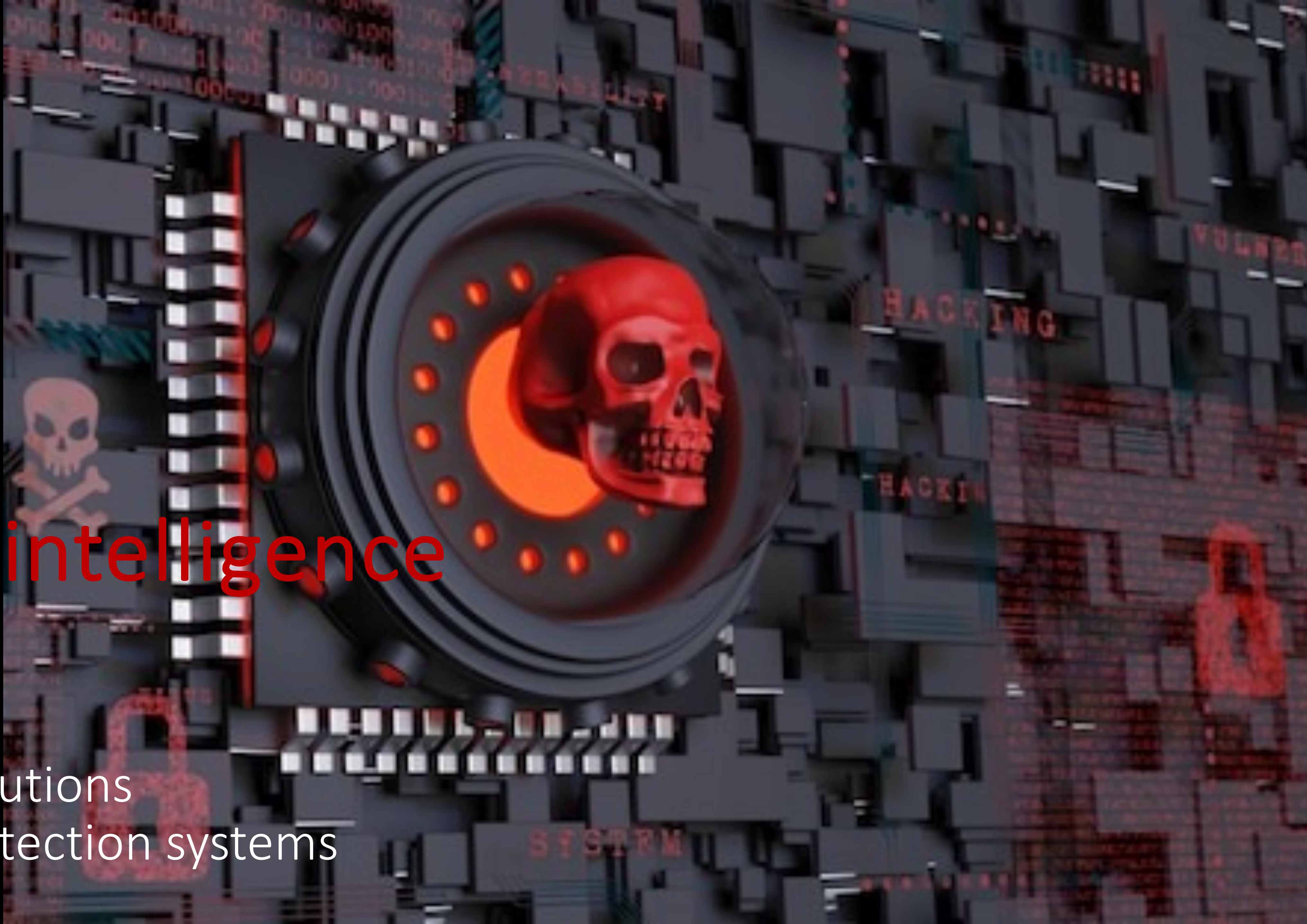
AI and Cybersecurity?

Yes - Maybe - No

YES!

Threat intelligence

Example:
Antivirus solutions
Intrusion Detection systems



YES!

- AI automates repetitive tasks
  - In alerting for triage tasks and data enrichment for analysts
  - L1 Help desk assistance with ChatGPT
- Better threat intelligence baseline
  - higher performance with machine learning for visualizing and processing potential actions
- Increased performance and accuracy by combining AI and Human

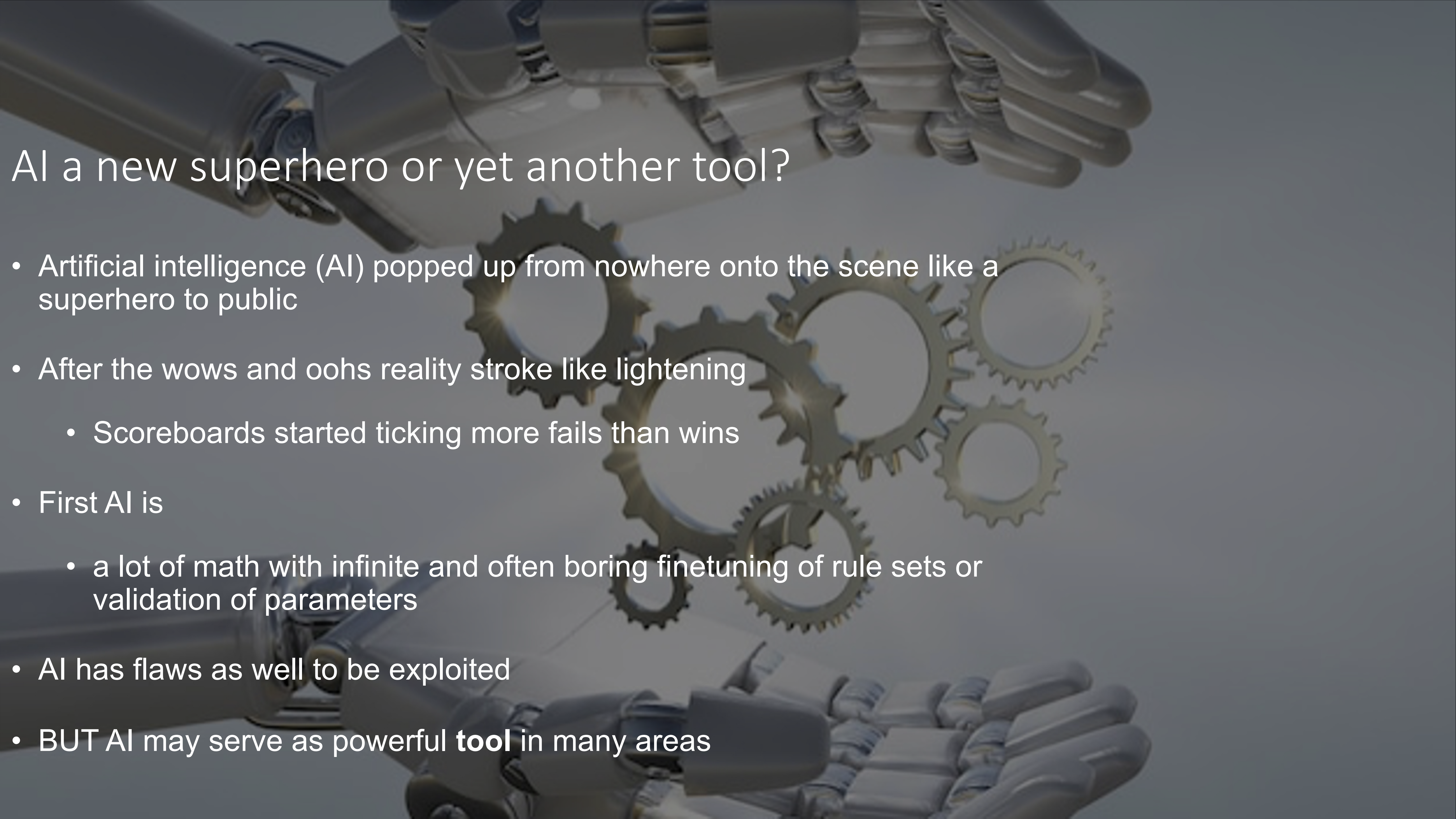
Maybe

- No 2 IT environments are identical
- Add the users
- Attackers do not follow rules
- Limitation for AI
  - Human input needed

- Tool that suggests code for completion
- Trained on code from publicly available sources
- **What if the training set includes insecure code?**
- In 2022 added a vulnerability filtering

BUT

- An Attack vector? Yes, add insecure code in repositories
- What about intellectual property?



AI a new superhero or yet another tool?

- Artificial intelligence (AI) popped up from nowhere onto the scene like a superhero to public
- After the wows and oohs reality stroke like lightening
  - Scoreboards started ticking more fails than wins
- First AI is
  - a lot of math with infinite and often boring finetuning of rule sets or validation of parameters
- AI has flaws as well to be exploited
- BUT AI may serve as powerful **tool** in many areas

- Human is key in innovation
  - intuition
  - Out of the box thinking

- AI is a tool to be demystified

  - By Knowledge
  - By Skills
  - By Education

Resistance is futile?

Maybe not!

Picture of Jean-Luc Picard as Locutus after Borg assimilationn from Star Trek DS9 "Emissary””Picture of Jean-Luc Picard in “Picard” –Paramount+

MERCI

Digital Learning Hub_

serge.linckels@dlh.lu

restena
network · security · .lu

cynthia.wagner@restena.lu