

# Freezing Week 2025

## Changing AI Security Paradigm

19.02.2024

Prof Dr Matthias Mehrtens

Head of Cyber Security Management programme, Niederrhein University of Applied Sciences  
Cyber Campus NRW

# Cyber Campus NRW

[www.ccnrw.de](http://www.ccnrw.de)



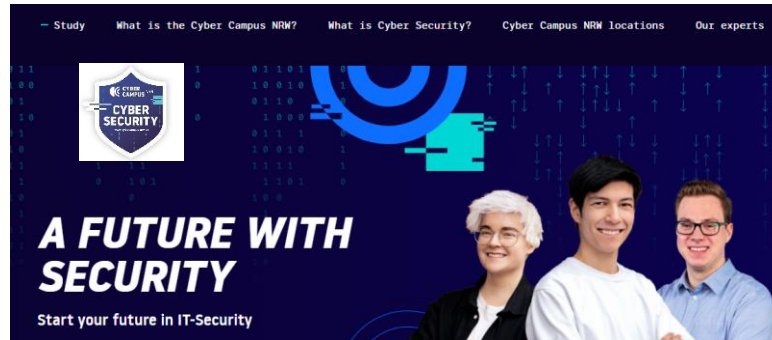
Cyber Campus NRW



**Cyber Security Campus**  
Hochschule Bonn-Rhein-Sieg  
Campus Sankt Augustin

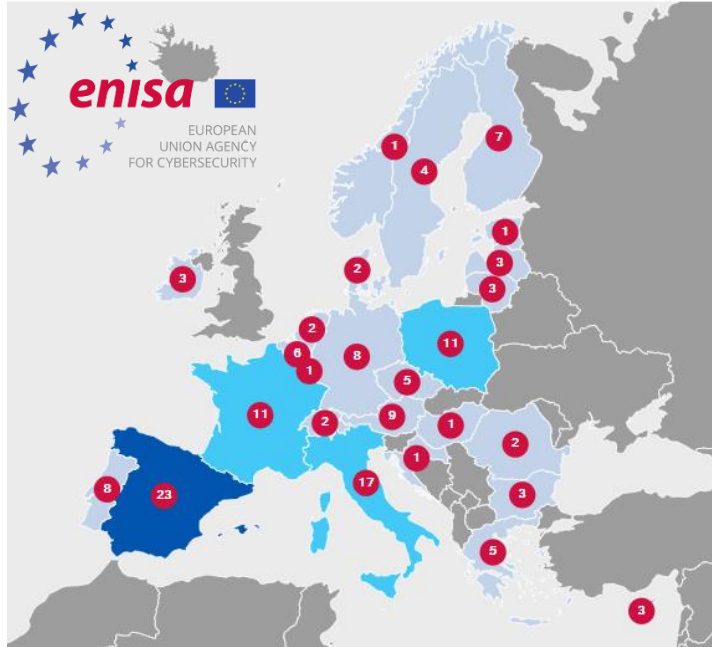


**Cyber Management Campus**  
Hochschule Niederrhein –  
Campus Mönchengladbach



# CYBERHEAD - Cybersecurity Higher Education Database

## 143 programmes in 26 countries



[CYBERHEAD - Cybersecurity Higher Education Database - ENISA \(europa.eu\)](https://europa.eu/cyberhead)



### Cyber Security Management

Hochschule Niederrhein  
Mönchengladbach, Germany

Master Degree

German Classroom Charges Apply



### Cyber Security Management

Hochschule Niederrhein  
Mönchengladbach, Germany

Bachelor Degree

German Classroom Charges Apply

Since 2023

*Digital Forensics (B.Sc.)*  
University of Applied Sciences  
Niederrhein  
Mönchengladbach, Germany

# Survey: Almost three-quarters of students use AI for homework

A large proportion of students have already used artificial intelligence to help with their homework. According to a study, many would like the topic to be on the curriculum.



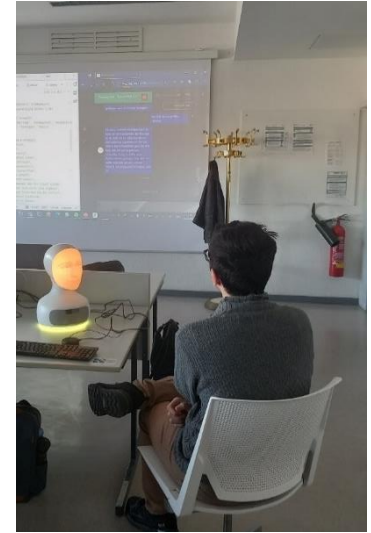
Technological developments also stimulate students' interest in school work. (Bild: Syda Productions/Shutterstock.com)

August 12, 2024, 6:19 p.m. Reading time: 4 minutes

From [Anika Reckeweg](#)

# Public understanding of AI through transdisciplinary teaching

- BMBF-funded project as part of the federal and state funding initiative "Artificial Intelligence in higher education"
- Computer science students develop and implement a dialogue dialogue in a Furhat robot (with the help of ChatGPT)
- Micro-learning units on AI basics for students
- Duration: Dec. 2022 - Nov. 2025
- **Project objective:** To prepare students in the best possible way for the AI-influenced professional world and society of tomorrow



GEFÖRDEBT VOM



Bundesministerium  
für Bildung  
und Forschung

# Nearly 4 Million Cybersecurity Jobs Are Vacant: Here's Why You Should Consider Breaking Into This Sector

**Jack Kelly** Senior Contributor 

*Jack Kelly covers career growth, job market and workplace trends.*

Follow



0

Aug 16, 2024, 06:00am EDT

<https://www.forbes.com/sites/jackkelly/2024/08/16/nearly-4-million-cybersecurity-jobs-are-vacant-heres-why-you-should-consider-breaking-into-this-sector/>

# Cyber cops are our answer to the shift of crime into the digital space



## Most Wanted

Ten Most Wanted Fugitives | Fugitives | Terrorism | Kidnappings/Missing Persons | Parental Kidnappings | Seeking Info | ECAP | [More](#)  
[Crimes Against Children](#) | [Murder](#) | [Additional Violent Crimes](#) | [Cyber](#) | [White Collar Crimes](#) | [Counterintelligence](#) | [CEI](#) | [Human Trafficking](#)

## Cyber Crimes

Select the images of suspects to display more information.

Filter by:  Filter by:

Sort by:

Results: 149 Items



DPRK IT WORKERS



JONG SONG HWA



RI KYONG SIK



KIM RYU SONG



RIM UN CHOL



KIM MU RIM



CHO CHUNG POM



HYON CHOL SONG



SON UN CHOL



SOK KWANG HYOK



# The end of updates through AI

*Rapid misuse of  
Weak points*

*AI speed makes updates  
too slow*

*Humans are too slow for  
action*

*Alternatives*

# Rapid abuse of vulnerabilities



# Speed of AI

**CURSOR** Pricing Features Forum Docs Careers Blog Sign In Download

## The AI Code Editor

Built to make you extraordinarily productive,  
Cursor is the best way to code with AI.

Download for Free Watch Demo 1 Minute

```
mod.rs M pingora-core/src/listeners/mod.rs {} impl TransportStack
impl TransportStackBuilder {
  pub fn build(&mut self, upgrade_listeners: ListenFds) -> TransportStack {
    upgrade_listeners,
  }
}
```

CHAT REVIEW

Normal Chat

Can you make it easier to switch certificates in the transport listeners

<https://www.cursor.com/>

# Effects of ISMS through AI

*Risks develop rapidly -  
frequent risk analyses  
required*

*Advanced threats more  
expensive measures*

*Different expertise is  
required*

*The type of attack can  
change quickly*

# The type of attack can change quickly

## Cyber Crime as a Service

<b>DDoS</b>	<u>From 9€/Hr up</u>
<b>Botnetz</b>	Starting at 75€/month
<b>Phishing Campaign</b>	<u>Starting at 499€/month</u>
<b>Keylogging Campaign</b>	Starting at 180€/month
<b>Ransomware &amp; RAT</b>	Starting at 1.000€/month
<b>Malware attack</b>	Starting at 40€
<b>Social Media Account</b>	Starting at 9€
<b>Netflix Account</b>	Starting at 0,90€
<u>Credit Card Cloning</u>	<u>Starting at 7€</u>
<b>E-Mail w/ Password</b>	<u>Starting at 0,60€</u>
<b>Admin Account</b>	500-140.000€



<https://www.linkedin.com/pulse/cybercrime-service-what-every-business-needs-know-5ixjf/>

# The risks are developing rapidly

80-90%

of all successful ransomware compromises originate through unmanaged devices.

Find out more on page 18



A return on mitigation (ROM) framework is helpful for prioritization and may highlight actions requiring low effort or resources but that have a high impact.

Find out more on page 41



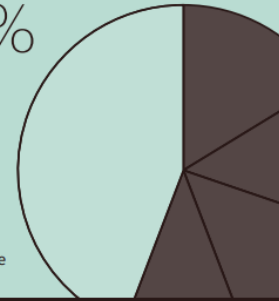
70%

of organizations encountering human-operated ransomware had fewer than 500 employees.

Find out more on page 18

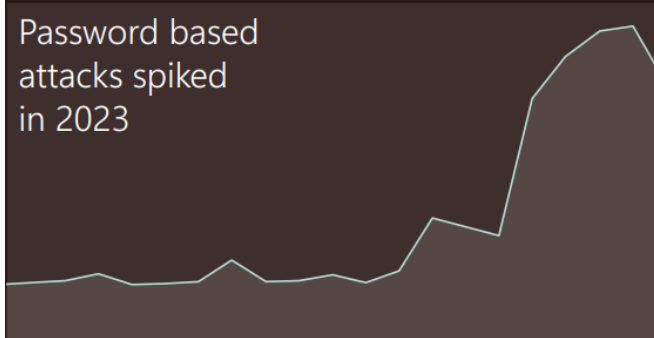


Human-operated ransomware attacks are up more than 200%



Find out more on page 17

Password based attacks spiked in 2023



Last year marked a significant shift in cybercriminal tactics

with threat actors exploiting cloud computing resources such as virtual machines to launch DDoS attacks. When hundreds of millions of requests per second originating from tens of thousands of devices constitute an attack, the cloud is our best defense, due to the scale needed to mitigate the largest attacks.



<https://www.microsoft.com/de-de/security/security-insider/microsoft-digital-defense-report-2023>

# People are susceptible

*Personalised phishing mails*

*Real appearing  
Voicemails from  
colleagues*

*Established awareness tools  
become useless*

*Loss of control*

*It's easier to hack a  
person than a  
system*

# Real appearing messages (deepfake)



<https://www.mark-thorben-hofmann.de/6-deepfake-gefahren/>



# Real appearing messages (deepfake)



<https://www.thedorbrothers.com/>

# Personalised phishing mails

[specials](#) > [definitions](#) > What is WormGPT?

Definition WormGPT

## What is WormGPT?

May 2, 2024 · By [Dipl.-Ing. \(FH\) Stefan Luber](#) · 3 min reading time · 

WormGPT is an AI chatbot. It is based on the open source GPT-J language model published by EleutherAI in 2021. It was trained for WormGPT for cybercriminal purposes. The chatbot is offered on the darknet and in criminal forums. Its use is subject to a fee and must be paid for in cryptocurrency. Compared to publicly available or commercially offered chatbots, WormGPT does not have any security restrictions or minimum ethical standards.

<https://www.security-insider.de/was-ist-wormgpt-a-5796962f97df6867e00e100c889e73bc/>

## Cybercriminals train AI chatbots for phishing, malware attacks

By Bill Toulas

August 1, 2023 10:08 AM 0



In the wake of [WormGPT](#), a ChatGPT clone trained on malware-focused data, a new generative artificial intelligence hacking tool called FraudGPT has emerged, and at least another one is under development that is allegedly based on Google's AI experiment, Bard.

<https://www.bleepingcomputer.com/news/security/cybercriminals-train-ai-chatbots-for-phishing-malware-attacks/>

## DarkBERT is trained with data from the darknet – ChatGPT's dark brother?

Researchers have developed an AI model that is trained with data from the darknet – DarkBERT's sources are hackers, cyber criminals, and politically persecuted people.

🔒 🔊 🖨️ 💬 56



<https://www.heise.de/news/DarkBERT-ist-mit-Daten-aus-dem-Darknet-trainiert-ChatGPTs-dunkler-Bruder-9060809.html>

## GPT4All: Your own ChatGPT without an internet connection

<https://www.heise.de/news/GPT4All-ausprobiert-Das-eigene-ChatGPT-ohne-Internetverbindung-9163132.html>

# AI is becoming more powerful

*AI runs on standard  
laptops*

*How do you  
supervise AI?*

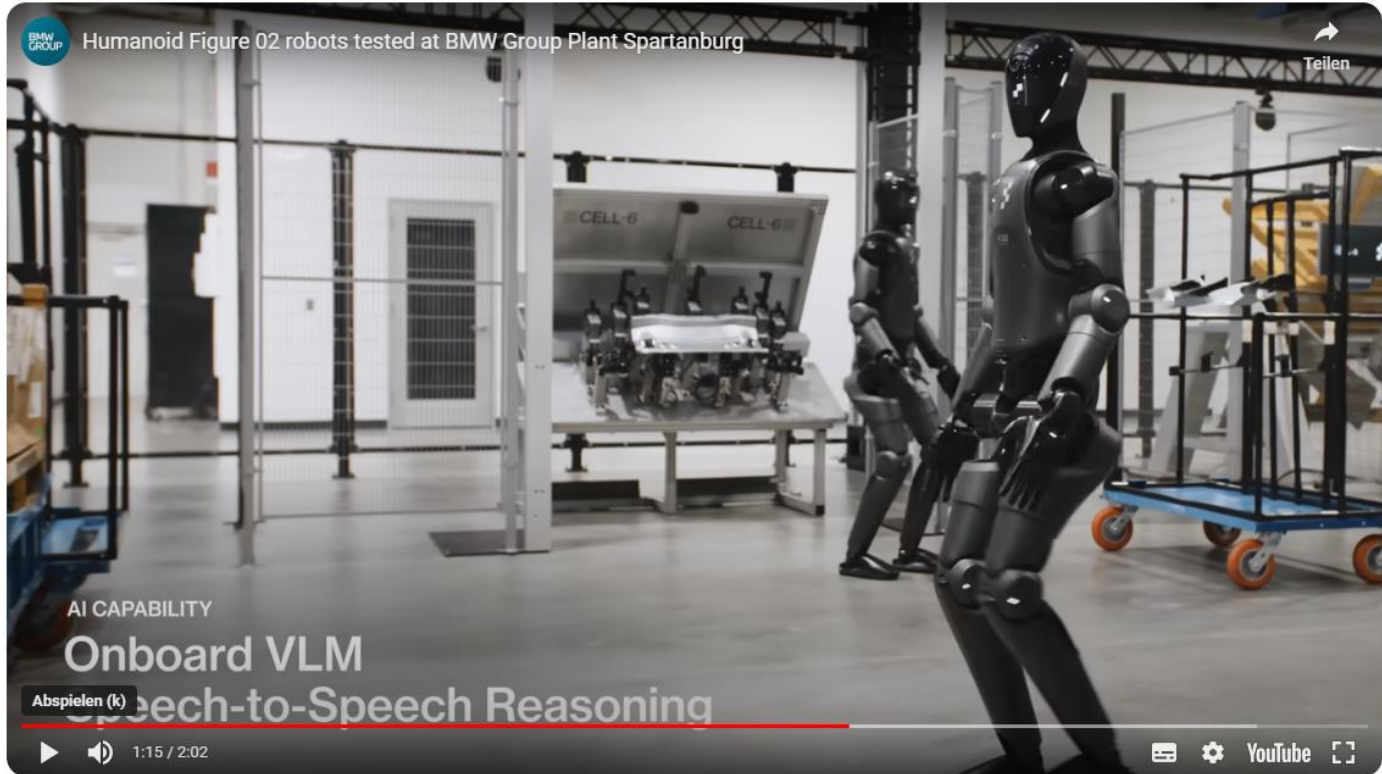
*Hardware is getting  
faster and faster*

*Legal rules*

# Humanoid Figure 02 robots tested at BMW Group Plant ...

YouTube · BMW Group · 06.08.2024

YouTube 



<https://www.youtube.com/watch?v=xLVm-QKEZSI>

# Digital sovereignty

*Unknown ethics or ethics from  
the USA, China, India*

*Data and control outside the  
EU*

*Control of world  
affairs?*

*Access for  
governments*

# Maritime crime - drug smuggling

- The vast majority of illegal drugs entering the EU are smuggled by sea. 70% of drug seizures take place in EU harbours.
- Ports account for 75% of the EU's external trade volume and 31% of the EU's internal trade volume. Ports are therefore particularly vulnerable to drug smuggling and exploitation by high-risk criminal networks.
- Criminals use the ports to organise the transit of containers with illegal goods to the EU.

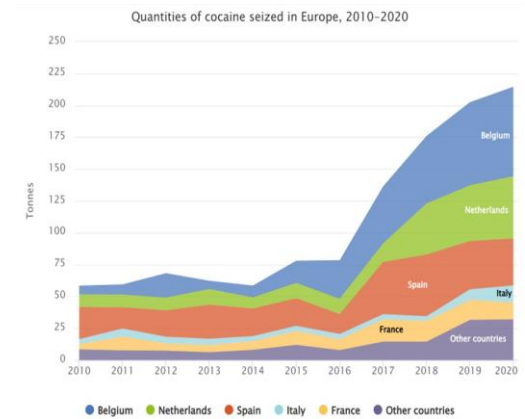


Source: *Insight into crime.*

Ref.: [https://ec.europa.eu/commission/presscorner/detail/de/ip\\_24\\_344](https://ec.europa.eu/commission/presscorner/detail/de/ip_24_344)

# Maritime crime - drug smuggling

- After cannabis, cocaine is the second most commonly consumed illicit drug in Europe.
- The increasing availability and consumption of cocaine in Europe is causing higher costs, both in terms of both in terms of the impact on public health and the crime and violence the crime and violence associated with the cocaine market.
- The trade in illegal drugs is extremely dynamic and adapts quickly to geopolitical developments, regional conflicts and changes in trade routes.
- In addition to the use of commercially available containers, a number of other methods are used today, often in combination, to evade detection.

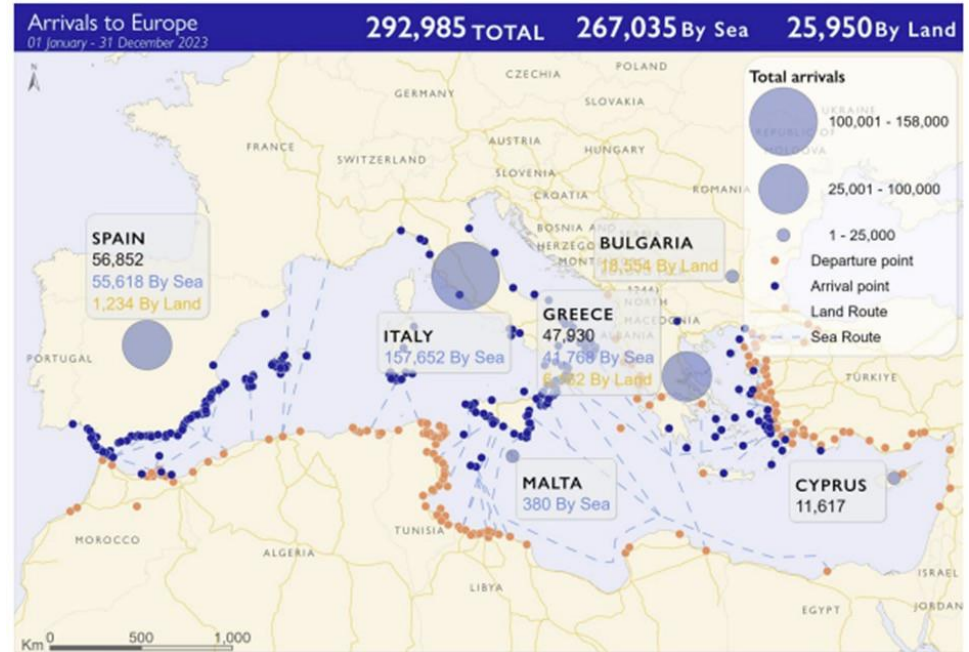


Reference: EMCDDA, 2023 European medicines report 2023 (as of 16 June)



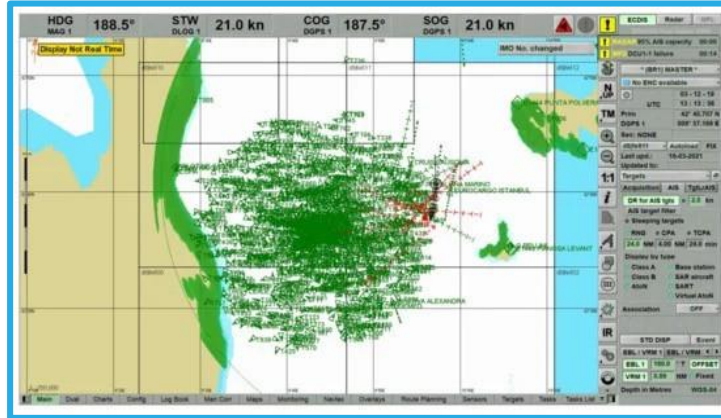
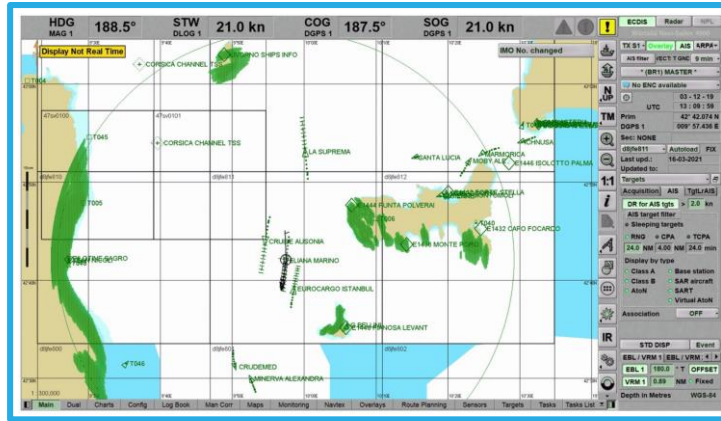
# Maritime crime - people smuggling

- People smuggling is the movement of people across international borders for financial gain.
- The migrant smuggling business could be worth USD 10 billion or more per year, considering that the routes from West, East and North Africa to Europe and from South America to North America are worth around USD 6.75 billion annually.



Source: International Organisation for Migration, 2024. global migration data portal. Smuggling of migrants.

# Jamming & spoofing



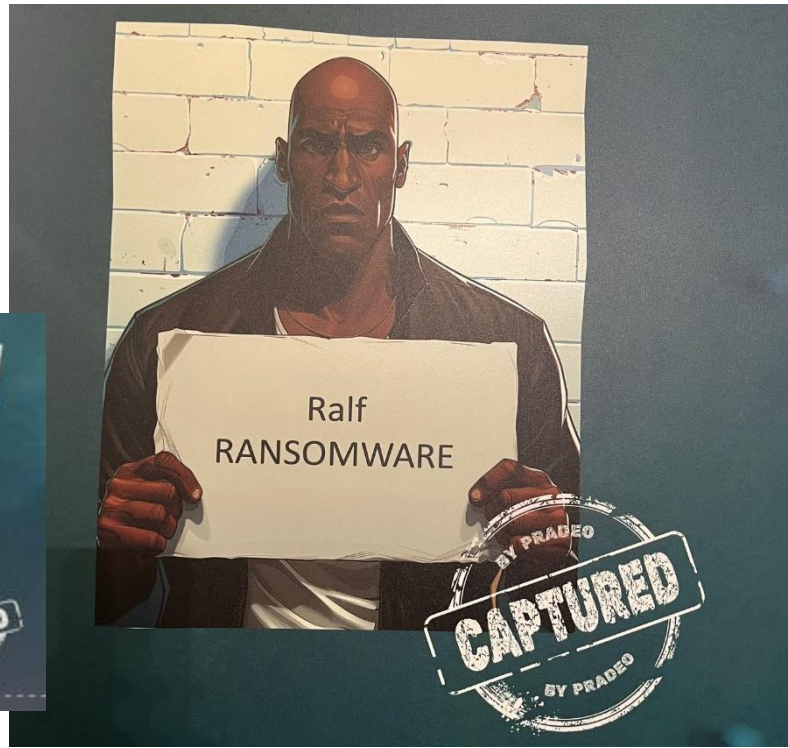
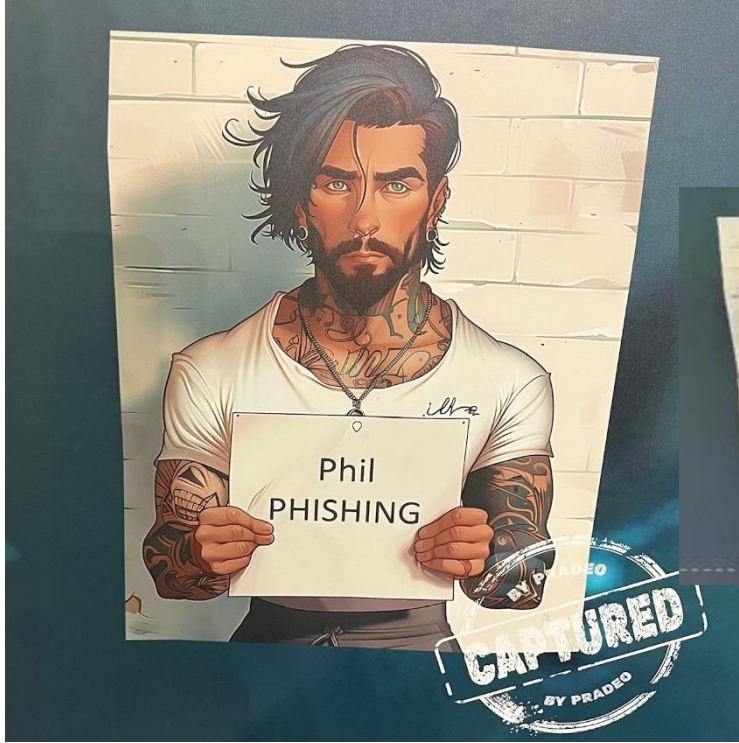
AIS = Automatic Identification System

Source: Androjna, A. et al, 2021. AIS Data Vulnerability Indicated by a Spoofing Case-Study.

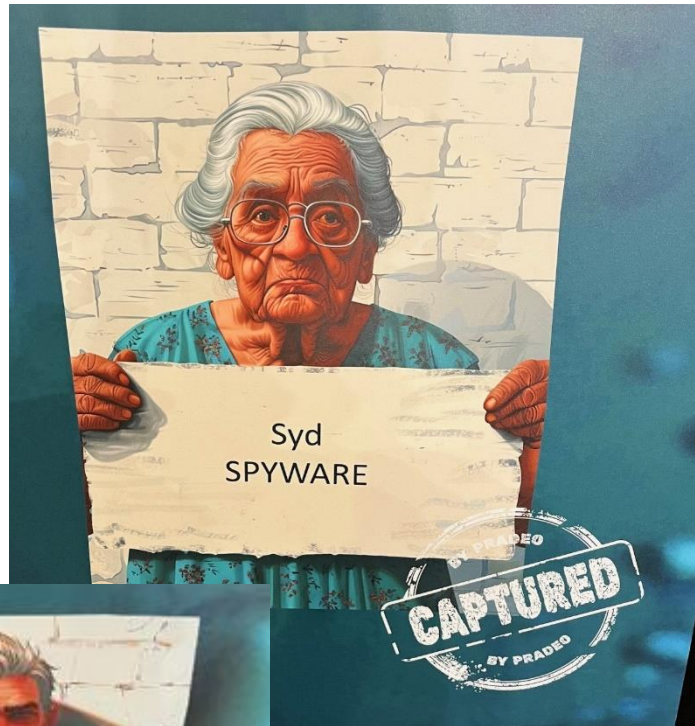
FACT SHEETS

# FACT SHEET: PRESIDENT DONALD J. TRUMP TAKES ACTION TO ENHANCE AMERICA'S AI LEADERSHIP

January 23, 2025



Source: Pradeo



Source: Pradeo

# Great interest at the Civil Protection Day




Source: BSI 2023



[https://www.bsi.bund.de/DE/Service-Navi/Presse/Alle-Meldungen-News/Meldungen/Bevoelkerungsschutztag\\_230626.html](https://www.bsi.bund.de/DE/Service-Navi/Presse/Alle-Meldungen-News/Meldungen/Bevoelkerungsschutztag_230626.html)

# Thank you for your attention!

Federal Administration > Department: DDPS > NCSC Homepage Report C

 Schweizerische Eidgenossenschaft  
Confédération suisse  
Confederazione Svizzera  
Confederaziun svizra

## National Cyber Security Centre NCSC

---

**News** Cyberthreats Information for Reporting obligation NCS Strategy Documentation About NCSC

Homepage NCSC > News > Hot topics > Week 49: Use of artificial intelligence in fraud attempts

< Hot topics

### Week 49: Use of artificial intelligence in fraud attempts

12.12.2023 - The NCSC is observing an increase in the use of so-called artificial intelligence (AI) in phishing and fraud attempts. Below, we look at three examples of how AI is already being used in this way.

