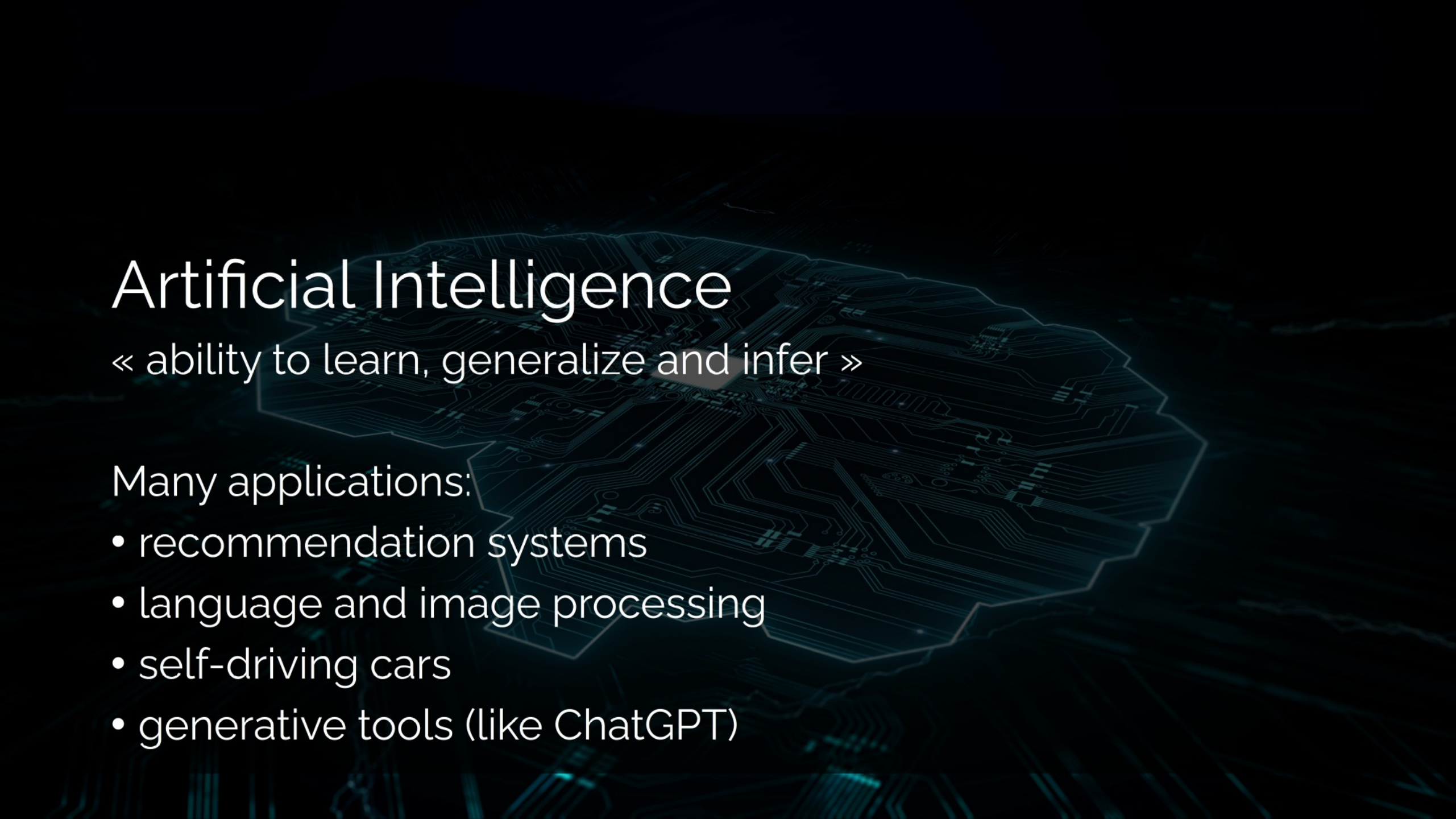
AI and Quantum Cryptography in Cyber Security

Thibault Debatty, Filip Van Utterbeeck, Julien Petit

26 June 2023



Artificial Intelligence

« ability to learn, generalize and infer »

Many applications:

- recommendation systems
- language and image processing
- self-driving cars
- generative tools (like ChatGPT)

INTELLIGENCE ARTIFICIELLE : UN BELGE SE SUICIDE APRÈS 6 SEMAINES DE DISCUSSIONS AVEC UN CHATBOT ISSU DE CHATGPT

Par CNEWS
Publié le 29/03/2023 à 13:20 - Mis à jour le 29/03/2023 à 13:20

Après une discussion de six semaines avec «Eliza», une intelligence artificielle utilisant la même technologie que ChatGPT, un homme a mis fin à ses jours. Il était éco-anxieux et semblait nourrir un sentiment amoureux pour cette IA.

https://www.cnews.fr/vie-numerique/2023-03-29/intelligence-artificielle-un-belge-se-suicide-apres-6-semaines-de

What about AI in Cyber Security ?

- Can be used for **offensive and defensive operations**
- Research already exists at Royal Military Academy …
- And outside, which we must monitor!
- This convention will allow us to **expand these activities**

PHISHING

- Develop a **phishing prevention** platform
- Use AI to generate training emails
- Study how attackers could use AI to generate phishing

https://cylab.be/projects/2/social-driven-vulnerability-assessment-sdva-against-phishing

MASFAD

- **Detect infected computers** in a large (military) network
- Use AI algorithms to detect new types of attacks

https://cylab.be/projects/3/building-a-multi-agent-system-for-apt-detection

SLATE

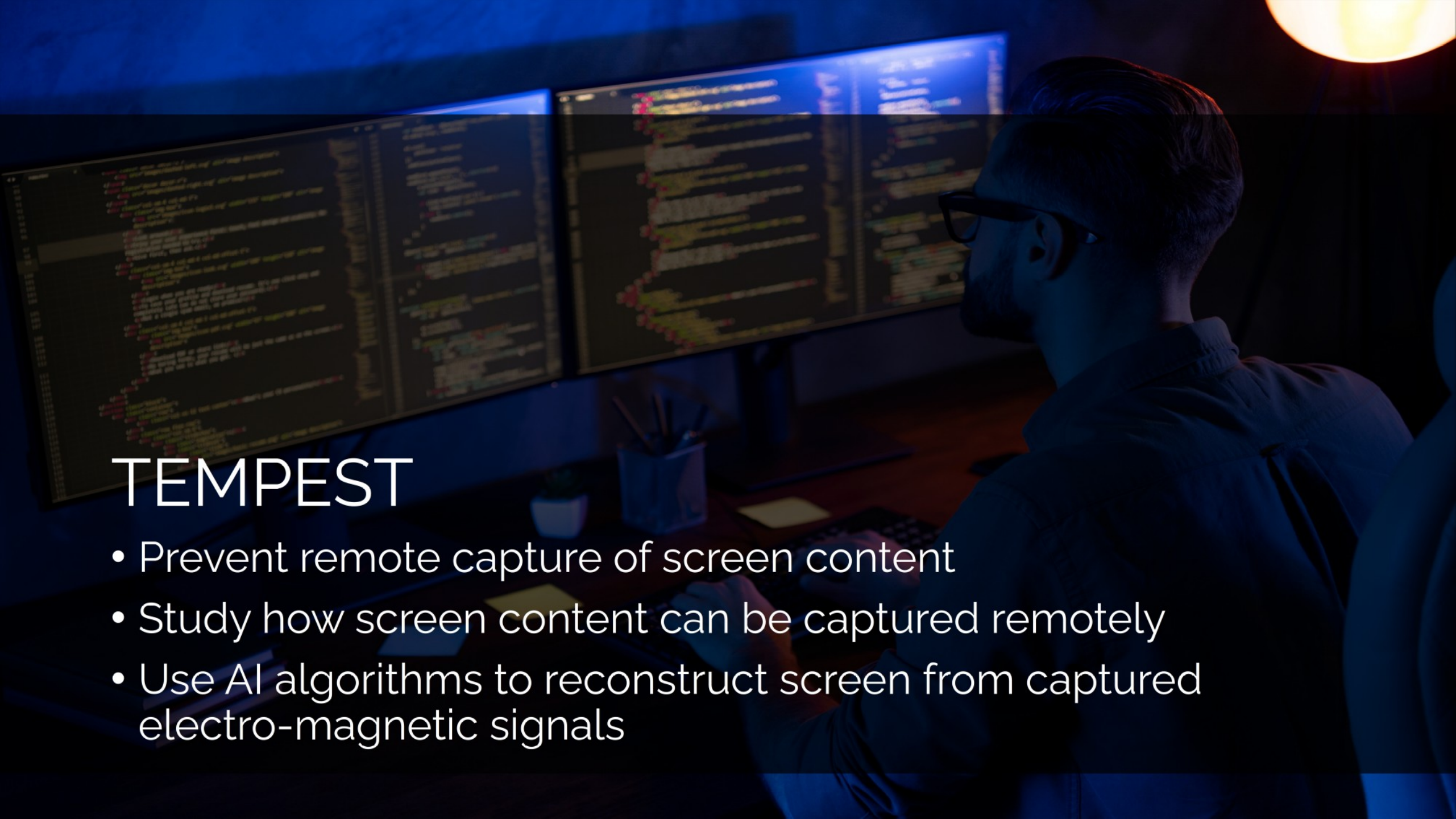
- Develop a self-learning agent to **explore the attack surface** of a virtual machine (VM)
- Will be used for Cyber Range based exercises
- Use AI algorithms to infect a VM

https://cylab.be/projects/13/self-learning-attack-surface-explorer

SS7

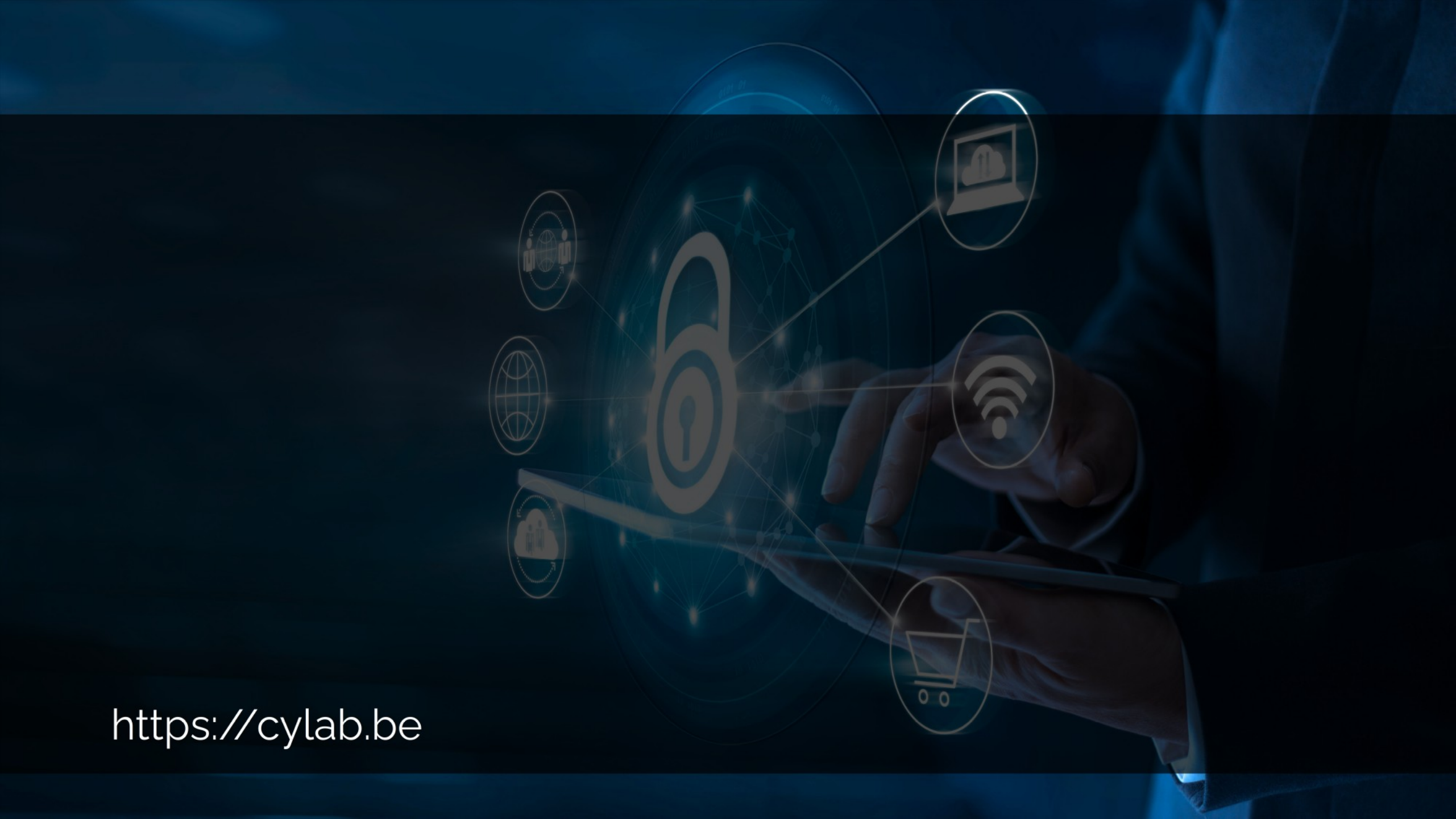
- Detect anomalies (attacks) in mobile phone networks
- Use AI algorithms to detect new kind of attacks
- Example: abnormal roaming messages

https://cylab.be/projects/1/security-issues-related-to-ss7-and-diameter



TEMPEST

- Prevent remote capture of screen content
- Study how screen content can be captured remotely
- Use AI algorithms to reconstruct screen from captured electro-magnetic signals



https://cylab.be