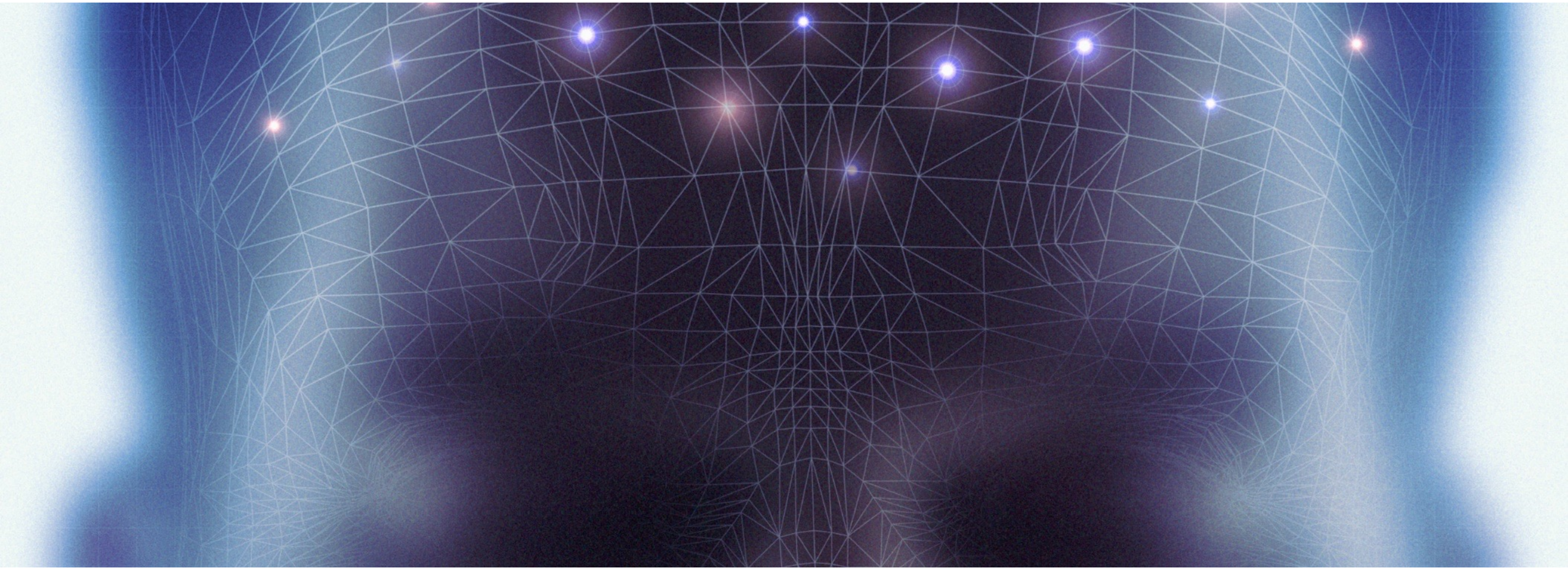
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Defence,
Civil Protection and Sport
armasuisse



The Role of Artificial Intelligence in Cyberdefence

Dr. Vincent Lenders, Director Cyber-Defence Campus

CYBER
DEFENCE
CAMPUS

When AI beats Human Intelligence

Chess

IBM Deep Blue

1997

2011

Go

Google Alpha Go

2016

2019

?

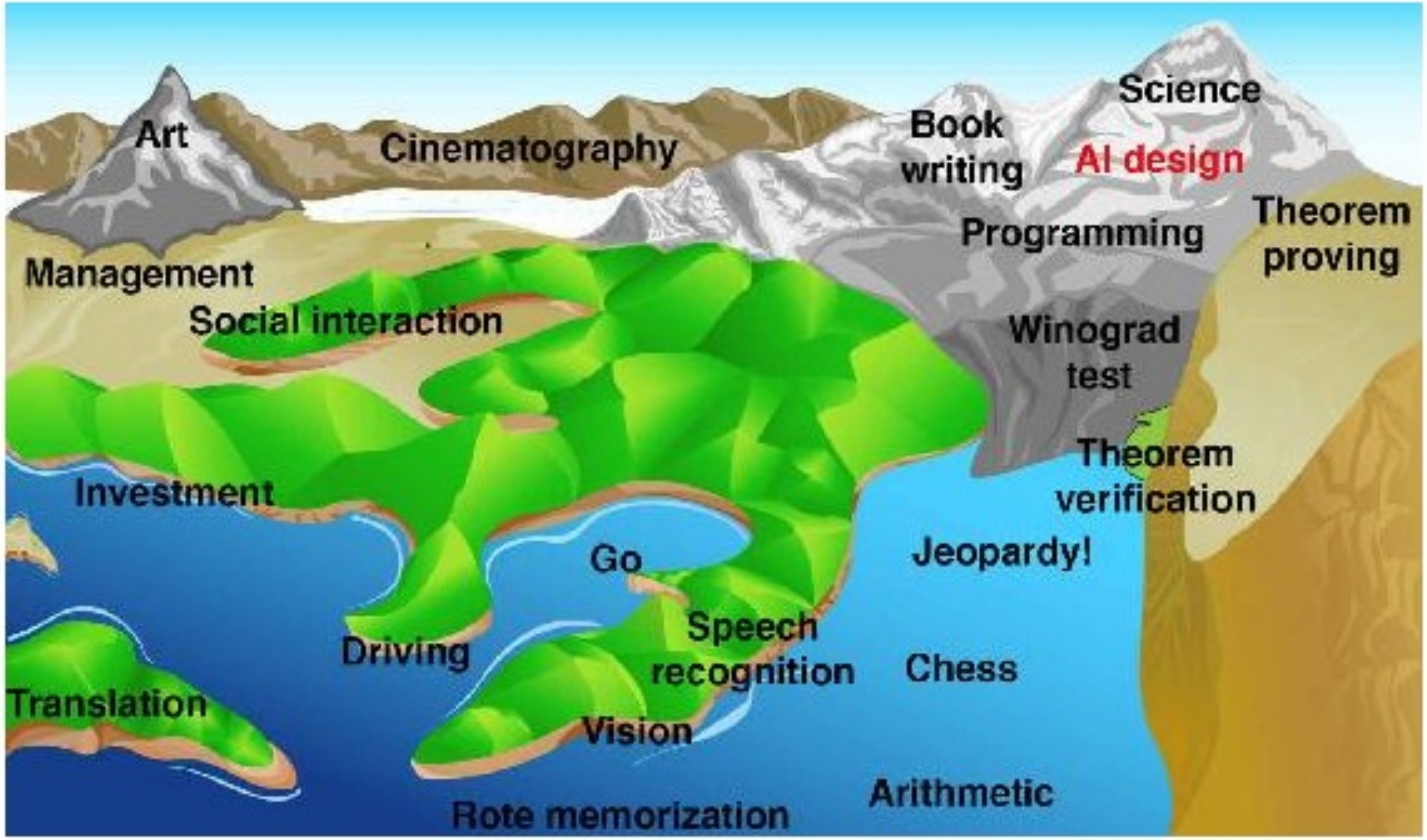
Jeopardy!

IBM Watson

Poker

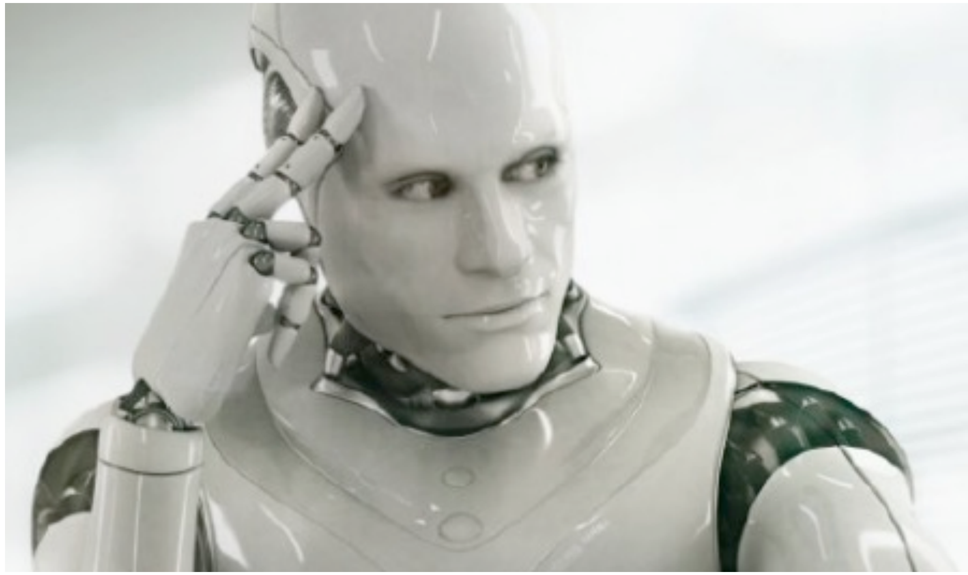
Facebook Pluribus

The Uphill Path of AI Challenges

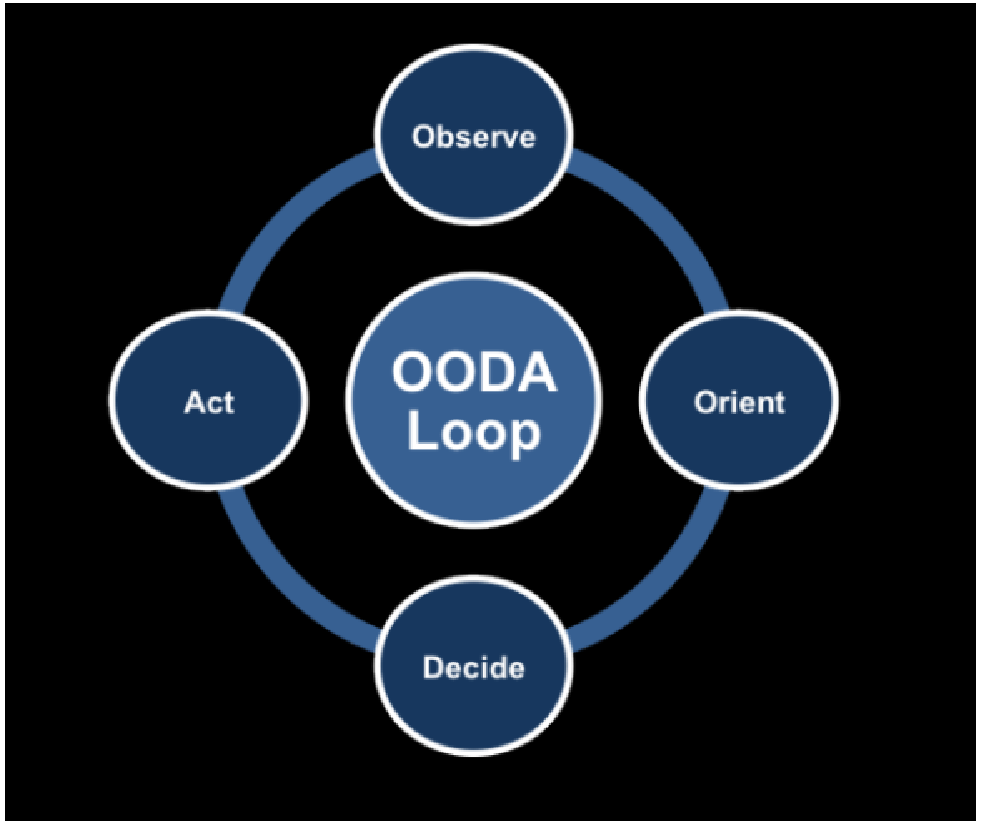


Source: Max Tegmark / Life 3.0

When could **AI** beat **human intelligence** in cyberdefence?



Cyberdefence Process
The OODA Loop



Source: Lt. General Thomas Süssli, Chief of the Swiss Armed Forces

CYD Campus Conference on AI, 2019

Cyberdefence as a Game: Locked Shields

- Yearly live-fire cyberdefence exercise
- **Human teams** compete against each other

Teams	Role
~20 Blue Teams (BT)	Defenders
Red Team (RT)	Attacker
Green Team (GT)	Infrastructure operator
Yellow Team (YT)	Monitoring
User Simulation Team (UST)	Benign users
White Team (WT)	Organizer

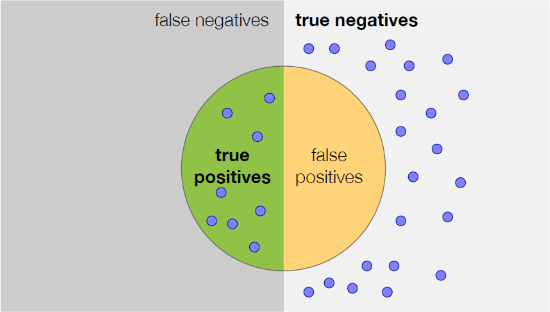
- Blue team with the **highest** score wins the game

Towards an AI-Powered Blue Team in Locked Shields

[R. Meier, A. Lavrenovs, K. Heinäaro, L. Gambazzi and V. Lenders, CyCon 21]

Machine Learning Use Cases

Detection of malicious network traffic



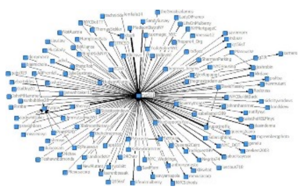
Continuous user authentication

Wireless signal classification

Detection of Malicious Network Traffic

Locked Shields Evaluation

Machine learning pipeline

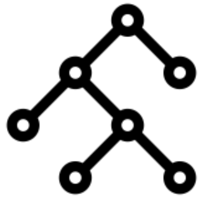


Network activity

→

Feature extraction
- Flow stats
- Packet headers
- Timing

→



Random forest classification

→

malicious
begnin

Workflow execution, 10 cores / 16Gb RAM

Dataset	Feature extraction	Classifier training	Inference time	
			dataset	flow
LS17	42 min	19 min	50 s	3 µs
LS18	85 min	47 min	30 s	

Classifier quality

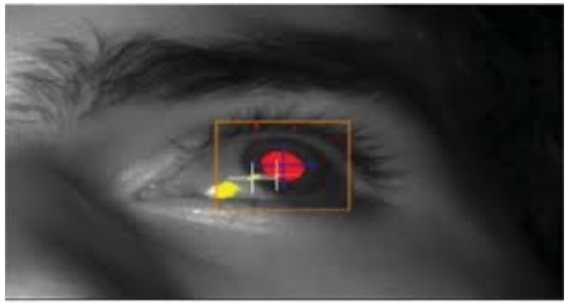
Model	Precision	Recall
LS17-tuned	99%	98%
LS18-tuned	99%	90%

[N. Känzig, R. Meier, L. Gambazzi, V. Lenders and L. Vanbever, CyCon 19]

Machine Learning Use Cases

Detection of malicious network traffic

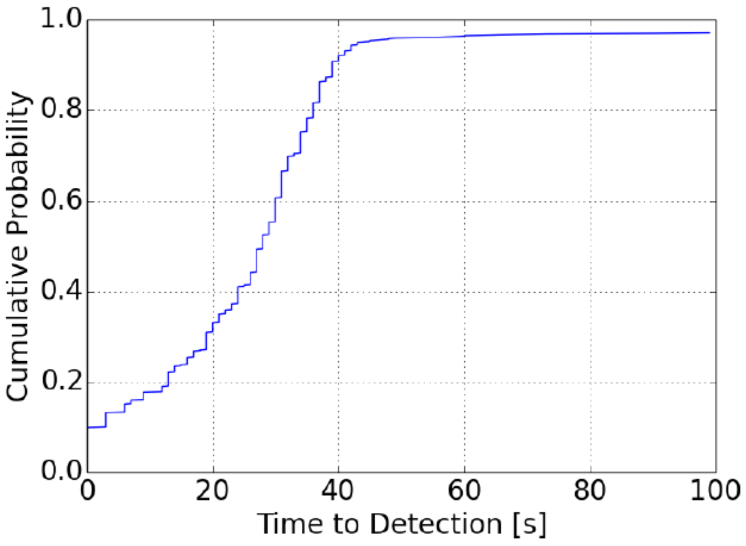
Continuous user authentication



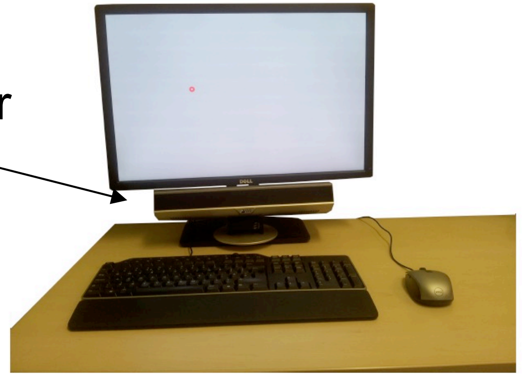
Wireless signal classification

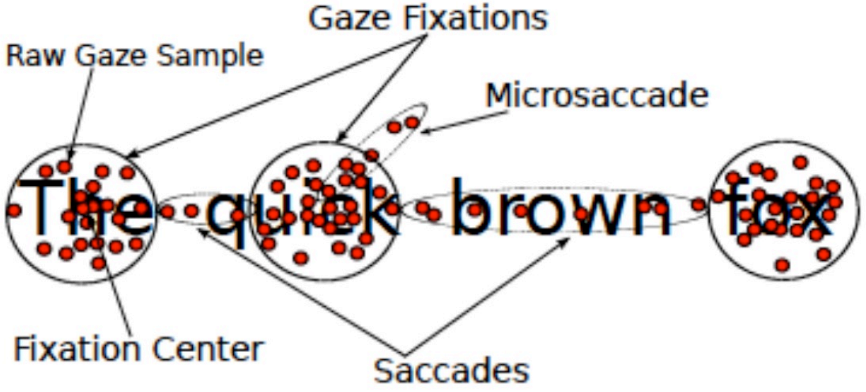
Continuous User Authentication

authentication accuracy



gaze tracker





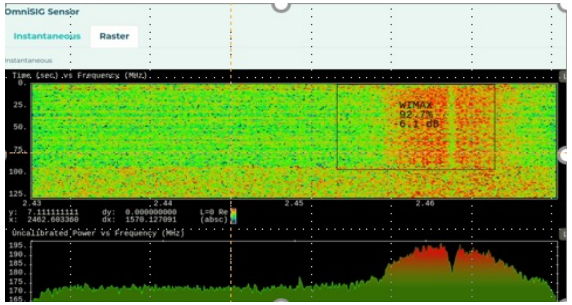
[S. Eberz, K. Rasmussen, V. Lenders and I. Martinovic, ACM TOPS 15]

Machine Learning Use Cases

Detection of malicious network traffic

Continuous user authentication

Wireless signal classification

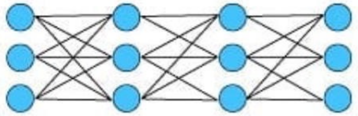


Wireless Signal Classification

Deep learning pipeline

→

Convolution network

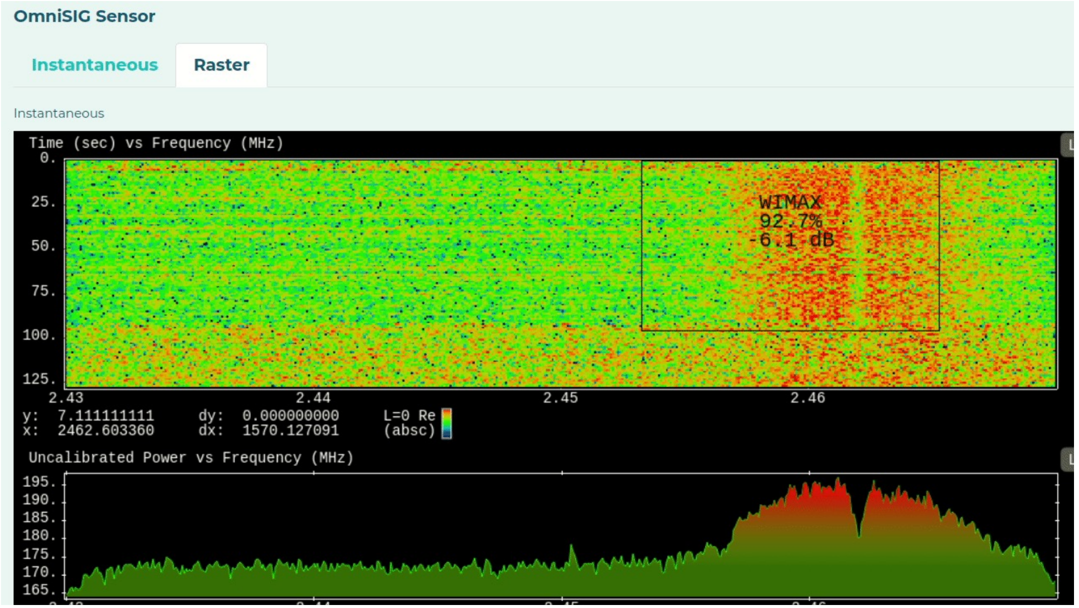


Feature extraction + classification

→

LTE
Bluetooth
WiFi

Real-time signal classification



[S Rajendran, W Meert, D Giustiniano, V Lenders, S Pollin, IEEE TCCN 18]

Further AI Use Cases investigated at CYD Campus

Supervised learning

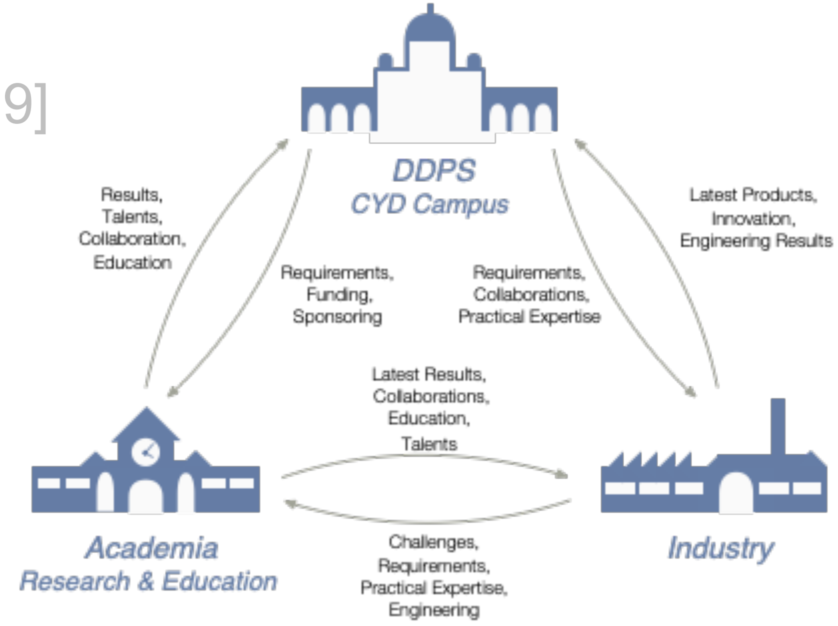
- Detection of malicious shell sessions [CyCon 19]
- Natural language understanding and machine translation [AAAI 21]
- Fake news detection
- Prediction of flight destination in aviation [OpenSky 21]

Unsupervised learning

- Wireless spectrum anomaly detection [TCCN 19]
- Mitigation of DDoS attacks
- Ranking of cyber threat feeds [CyCon 18]
- Detection of APT threats [DIMVA 17]
- Knowledge representation [arxiv 21]

Reinforcement learning

- Text generation [RanLP 21]
- Botnet detection [arxiv 21]



Conclusions

Pros of AI
- AI provides already today opportunities to improve cyberdefence
- Relatively easy to develop and apply new AI solutions

Cons of AI
- Hard to provide explainability
- Succeptible to attacks