Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Artificial Intelligence (AI) for Cyber Security

Prof. Dr. (TU NN)
Norbert Pohlmann

Institute for Internet Security - if(is)
University of Applied Sciences Gelsenkirchen
http://www.internet-sicherheit.de

if(is) internet security.

AI for Cyber Security
→ Content

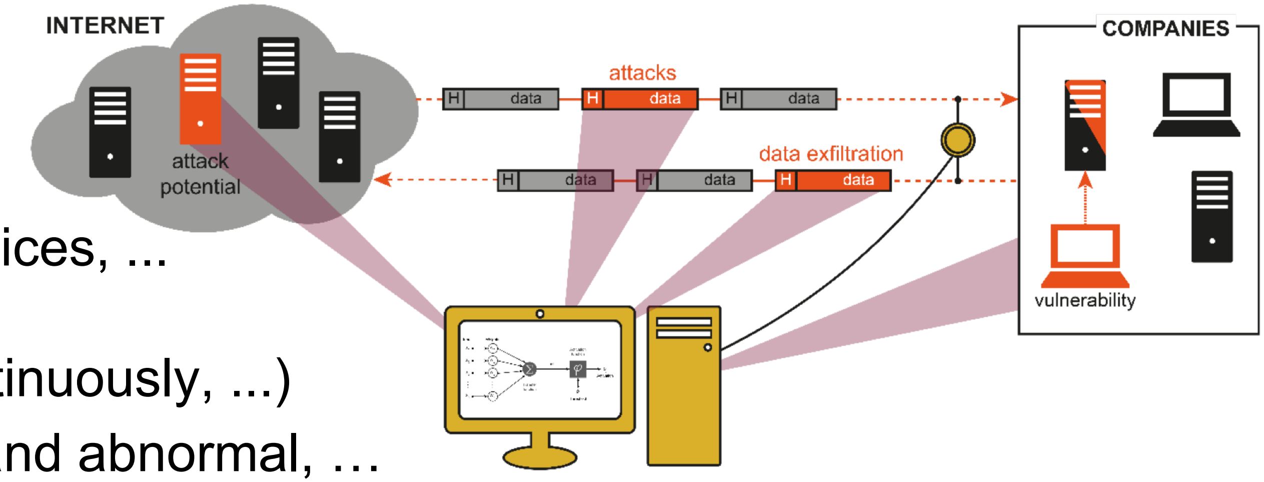
- **Classification**
  (Idea, data science, AI, ML, workflow, success factors, …)
- **Machine learning**
  (supervised/unsupervised, SVM, k-Means, h-clustering, …)
- **Artificial Neural Networks**
  (Idea, ANN, deep learning, …)
- **Application examples AI for Cyber Security**
  (Alert system for online banking, passive authentication, …)
- **Attacks on machine learning**
  (Idea, training data, traffic signs, …)
- **Further challenges**
  (Dual-Use, challenges, opportunities and risks, …)
- **Result and outlook**

internet security.

- **Classification**
  (Idea, data science, AI, ML, workflow, success factors, …)
- **Machine learning**
  (supervised/unsupervised, SVM, k-Means, h-clustering, …)
- **Artificial Neural Networks**
  (Idea, ANN, deep learning, …)
- **Applications examples AI for Cyber Security**
  (Alert system for online banking, passive authentication, …)
- **Attacks on machine learning**
  (Idea, training data, traffic signs, …)
- **Further challenges**
  (Dual-Use, challenges, opportunities and risks, …)
- **Result and outlook**

Artificial intelligence
→ for cyber security

- Increasing the **detection rate** of attacks
  - Network, IT end devices, ...
  - adaptive models (independently, continuously, ...)
  - Difference: normal and abnormal, …

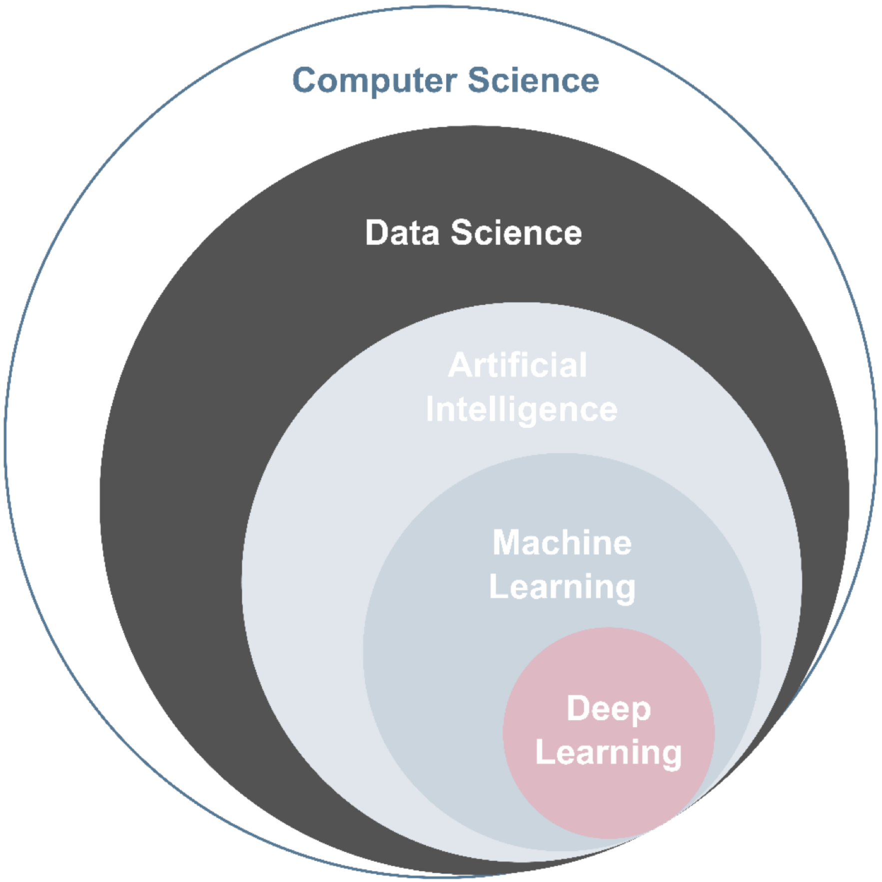


innovative detection of malicious network traffic

- **Support / Relief from cyber security experts** (of whom we do not have enough)
  - Finding **important** security-relevant events (prioritization)
  - **(Partial) autonomy** in response, …resilience, ...

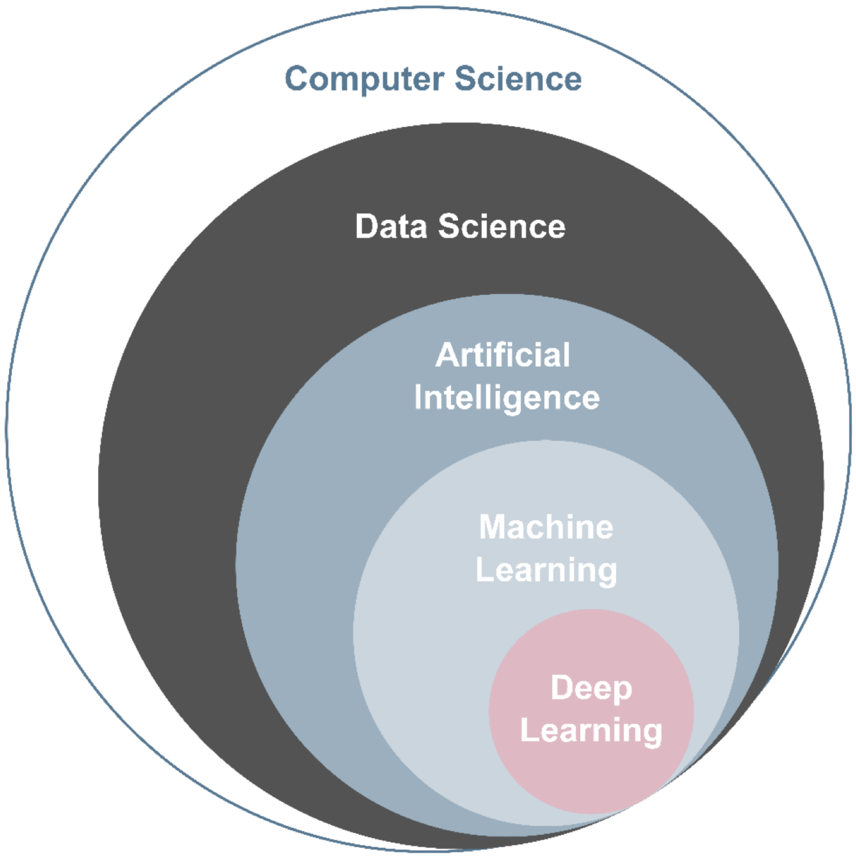
- **Improvements** to existing **cyber security solutions**
  - AI contributes to increased impact and robustness
  - For example: risk-based and adaptive authentication

Classification
→ Data Science



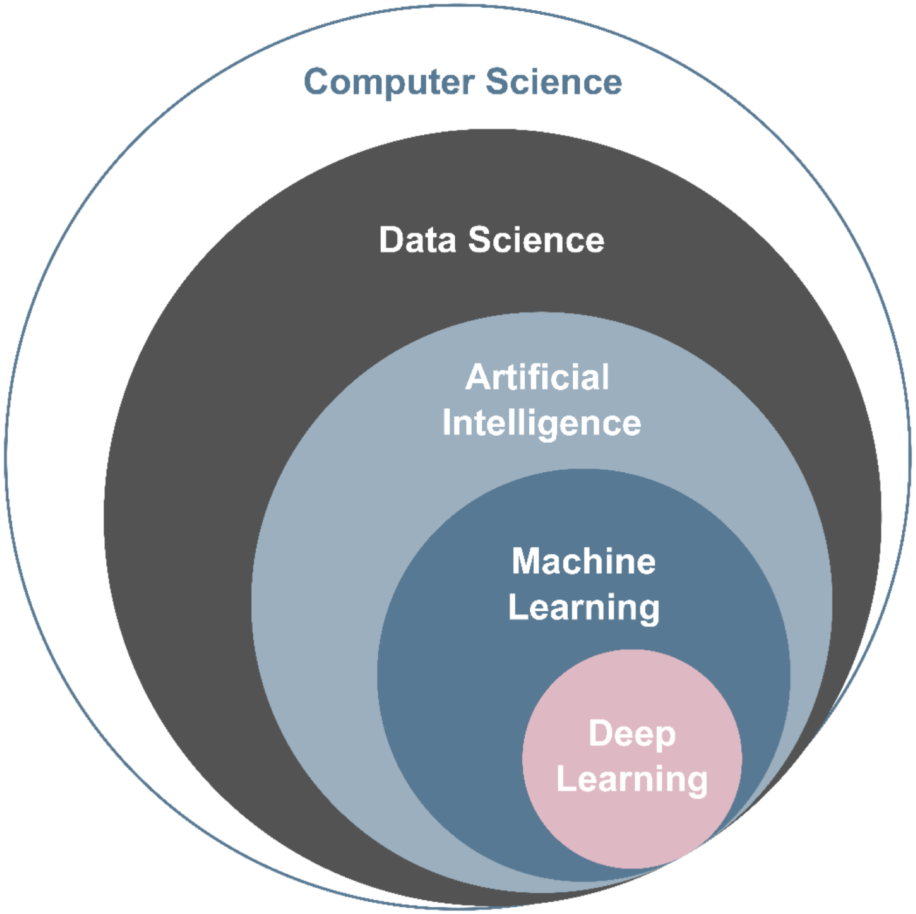
- **Data science generally refers to the extraction of knowledge from data.**
- **As there is** more and more **data,** more and more **knowledge can be derived from it.**
  (Important: data must contain information)
- Differentiation to Artificial Intelligence:
  - statistics
  - Key figures
  - data collection

Classification
→ Artificial intelligence



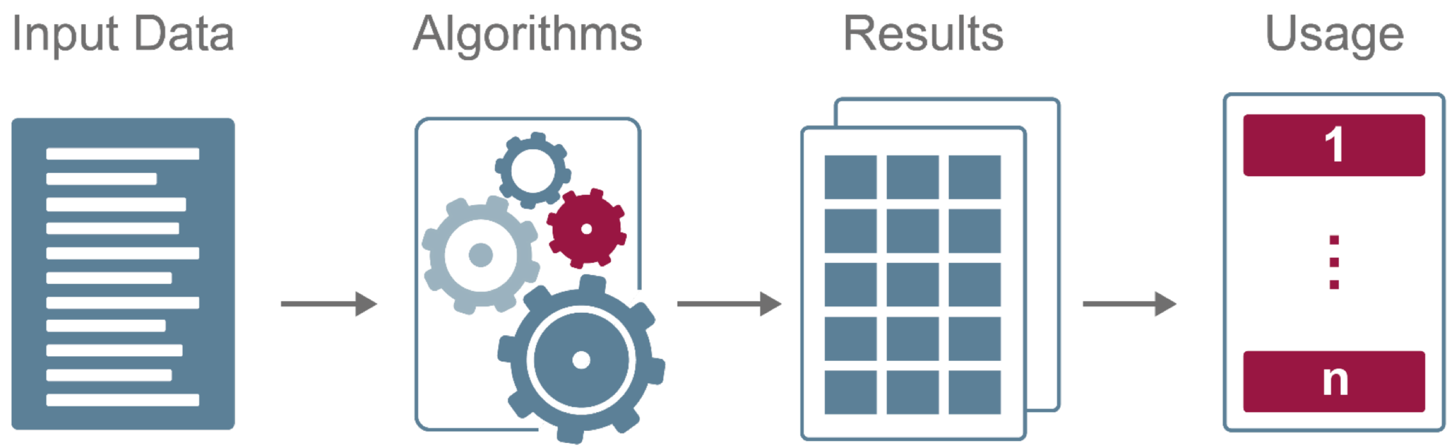
- **Artificial intelligence** is a field of computer science
- translates intelligent behavior into algorithms
- **(Aim)**
  - **automatically replicate „human-like intelligence".**
  - **Strong "Artificial Intelligence"** (Future)
    - Superintelligence
    - **Singularity** ("Machine" **improves itself**, is **more intelligent than humans**)

Classification
→ Machine learning



- **Machine learning** is a term for the "artificial" **generation of knowledge from experience** (in data) by computer.
- In **learning phases**, corresponding ML algorithms learn patterns and principles from examples (old data).
- The **resulting generalizations** can be applied to **new data**.
- **Weak "artificial intelligence"** (successfully implemented today)

Machine learning
→ Workflow



Input Data

Quality: Content, Completeness, Representativeness, … Processing

Algorithms (ML)

Support Vector Machine (SVM), k-Nearest Neighbor (kNN), ... Deep Learning

Results

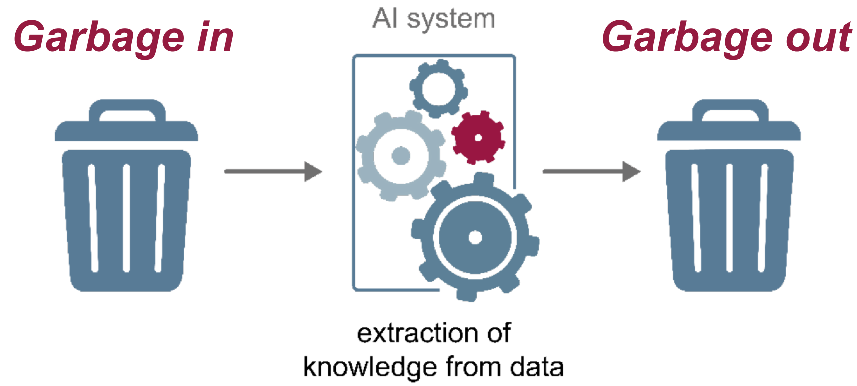
Results from the processing (algorithm) of the input data …

Usage

The application decides how to use results (trust).

Trustworthiness
→ Quality of the data

Paradigm



Standards for data quality:

→ Content of the data and correctness

→ Traceability of data (including data sources)

→ Completeness and representativeness

→ Availability and timeliness

Motivate high quality and secure **sensors**

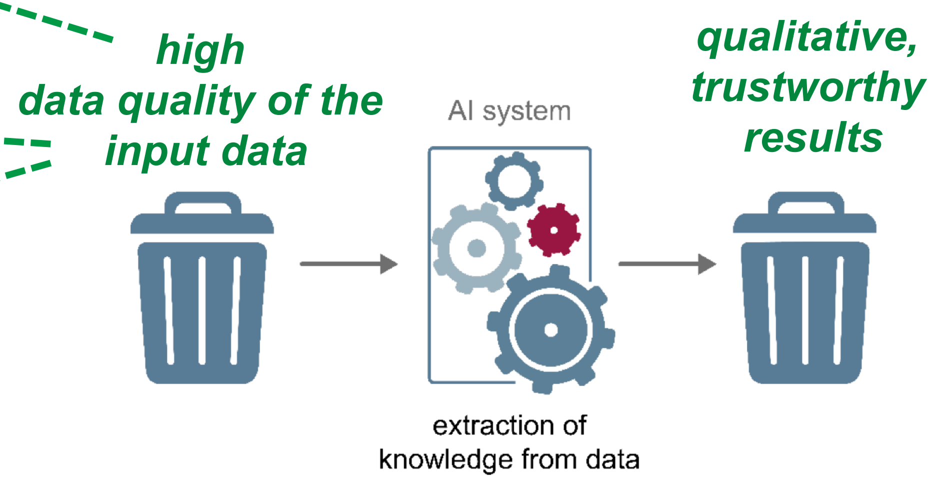
Other aspects to increase the quality:

→ Establish data pools

→ Promote exchange of data

→ Create interoperability

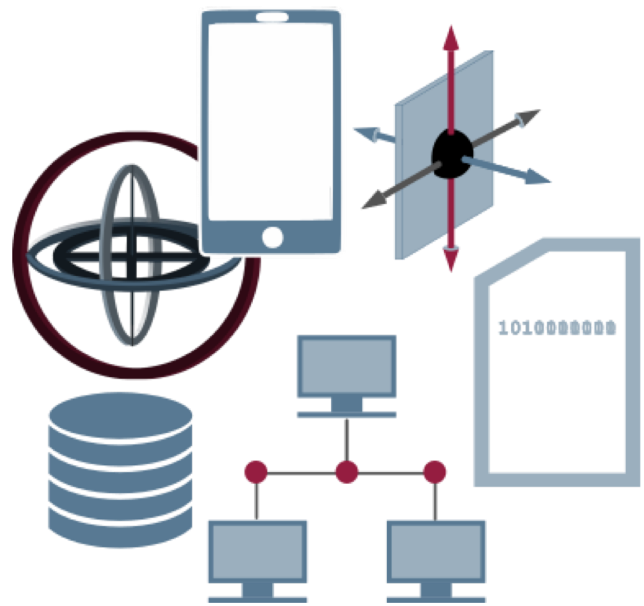
→ Push open data strategy



Success Factors – AI / ML
→ Input Data

Success factor: more and more existing data

- ***Smartphone, Smartwatch*** (close-to-body, person-oriented)
  - Position and acceleration sensors, user input, user behavior
- ***Computer***
  - User input, user behavior, log data
- ***Networks, network components (routers, firewalls, ...)***
  - log data, …
- **Web services**
  - User behavior, ...
- ***IoT (Internet of Things)***
  - Sensors and actuators
- ***Automobile, …***



Success Factors – AI / ML
→ Powerful IT and algorithms

Success factor: performance of IT systems

- **huge increase** (CPU, RAM, …) 20 CPU cores, 64 GB RAM, 1 TB SSD, etc. special hardware: GPUs, FPGA, TensorFlow PU (TPU),…

  … Parallelization, communication speeds, special software frameworks, …

- **powerful cloud solutions**, such as Amazon Web Services, Microsoft Azure, Google Cloud Platform, and the IBM Cloud.

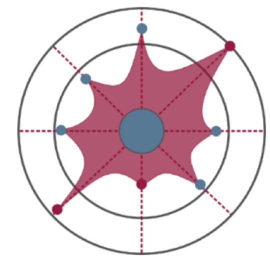
Success factor: algorithms

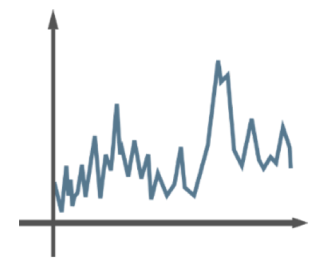
- Always **better algorithms** (much as open source)
- More and more **experience with dealing**
- Ever **easier access** to the technologies and services
- Examples: Support Vector Machine (SVM), k-Nearest Neighbor (kNN), k-Means Algorithm, Hierarchical Clustering, Convolutional Neural Network

Artificial intelligence
→ Results and usage

Results are **models** of the learned input data

- **Use of the models** leads to concrete application, for example:
  - **Classification of input data**, for detection of attacks
  - **Numerical values**, such as probabilities of normal behavior
  - **Binary values**, such as a successful biometric authentication



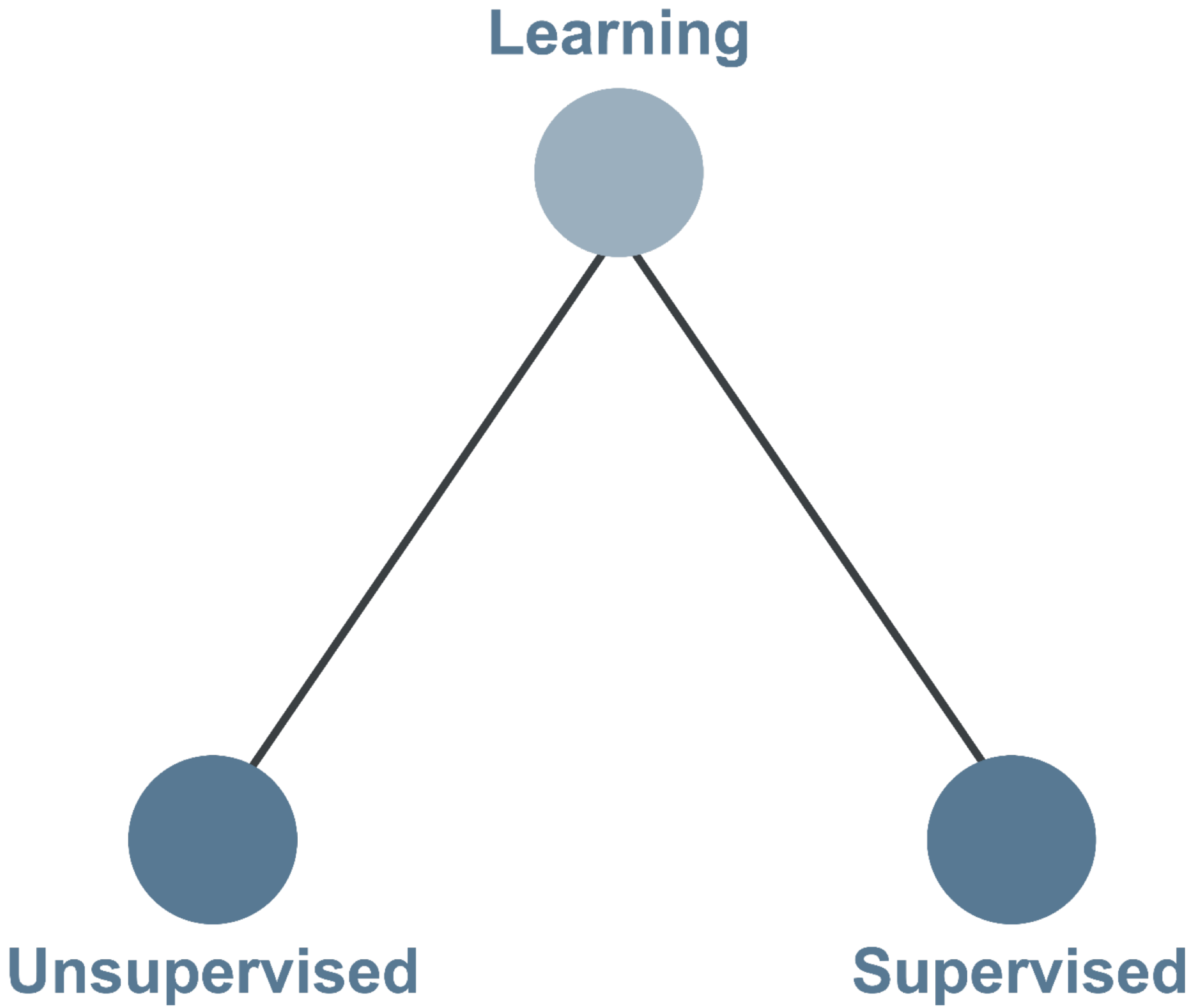


Usage: Policy on how to use the results.

AI for Cyber Security
→ Content

- **Classification**
  (Idea, data science, AI, ML, workflow, success factors, …)
- **Machine learning**
  (supervised/unsupervised, SVM, k-Means, h-clustering, …)
- **Artificial Neural Networks**
  (Idea, ANN, deep learning, …)
- **Applications examples AI for Cyber Security**
  (Alert system for online banking, passive authentication, …)
- **Attacks on machine learning**
  (Idea, training data, traffic signs, …)
- **Further challenges**
  (Dual-Use, challenges, opportunities and risks, …)
- **Result and outlook**

Machine Learning
→ Categories of Learning



ML algorithm
→ Supervised learning

- Goals of supervised learning
  - **Regression:** predicting numerical values
  - **Classification:** Classification of data in classes

- Example: detection of spam e-mails
- Input data contain **expected results**

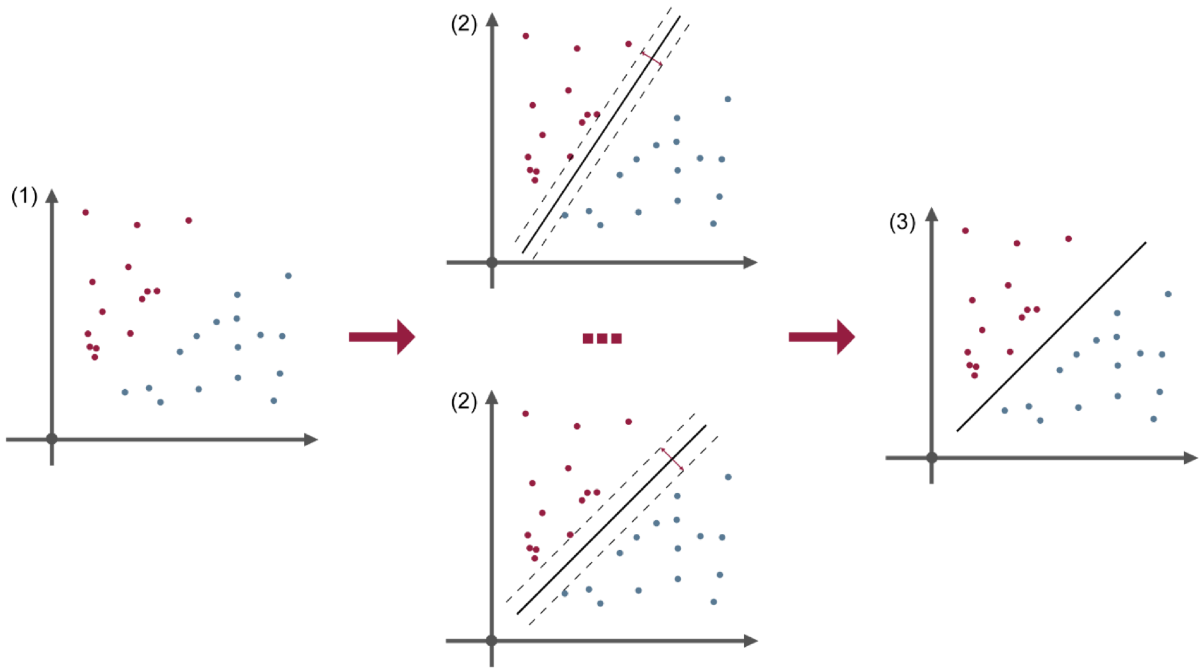
- Classification of data in **training data** and **data to be classified** (continuous learning)

- Goal: to generate results independently

- **ML algorithm, for example:**
  - Support-Vector-Machine (SVM)
  - k-Nearest-Neighbor (kNN)

ML algorithm
→ Support-Vector-Machine(SVM)/Training

2-Dimensional

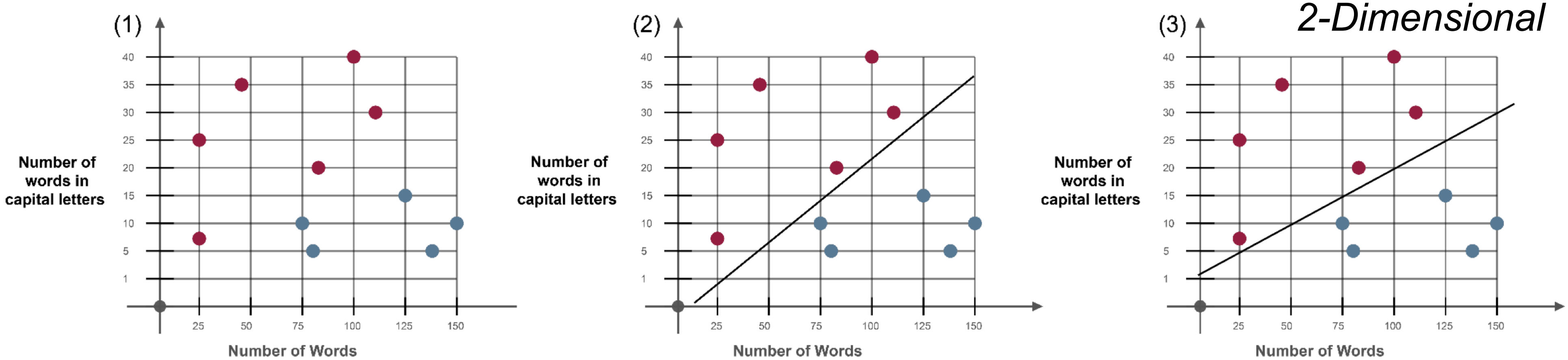


- **Input data (1):**
  - Already classified **data**
  - **Distance**
- **ML algorithm (2):**
  - **Calculate** straight line to separate the data
  - **Evaluate** results by distance to the points
  - **Select** of straight lines with maximum distance to both classes
- **Output (3):**
  - Straight line as a **model** for classification

ML algorithm
→ SVM - Example Training (Spam)E-Mail

internet security.

2-Dimensional



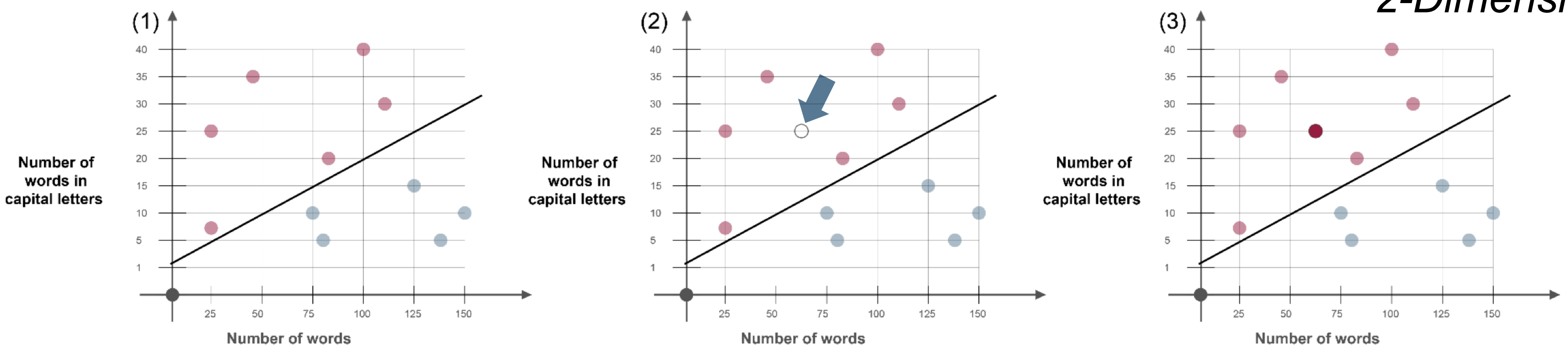
„Knowledge from experience“

Number of words	25	25	47	75	79	82	100	110	125	140	150
Number of words in capital letters	7	25	35	10	5	20	40	30	15	5	10
Spam e-mail	yes	yes	yes	no	no	yes	yes	yes	no	no	no

- **Input data (1):**
  - E-mails with corresponding classification **Spam** / **no Spam (Ham)**
- **ML algorithm (2):**
  - **Calculate** straight line to separate the data (Spam / Ham)
  - **Select** the best straight line between **Spam** and **Ham**
- **Output (3):**
  - Straight line as a model for classifying e-mails as **Spam** / **Ham**

ML algorithm
→ SVM – Example Spam - detection

2-Dimensional



„apply on new data“

Number of words	25	25	47	75	79	82	100	110	125	140	150	**63**
Number of words in capital letters	7	25	35	10	5	20	40	30	15	5	10	**25**
Spam e-mail	yes	yes	yes	no	no	yes	yes	yes	no	no	no	**?**

- **Input Data (1):**
  - **Model** for detecting possible spam mails
  - to be classified **e-mail** (e.g.: 63/25)
- **ML algorithm (2):**
  - Calculation of the situation of the data to be classified **e-mail (63/25)**
- **Output (3):**
  - Location of the **points** to the model classifies the e-mail as **Spam mail**

ML algorithm
→ Unsupervised learning

- **Strength in searching for patterns in unclassified data**

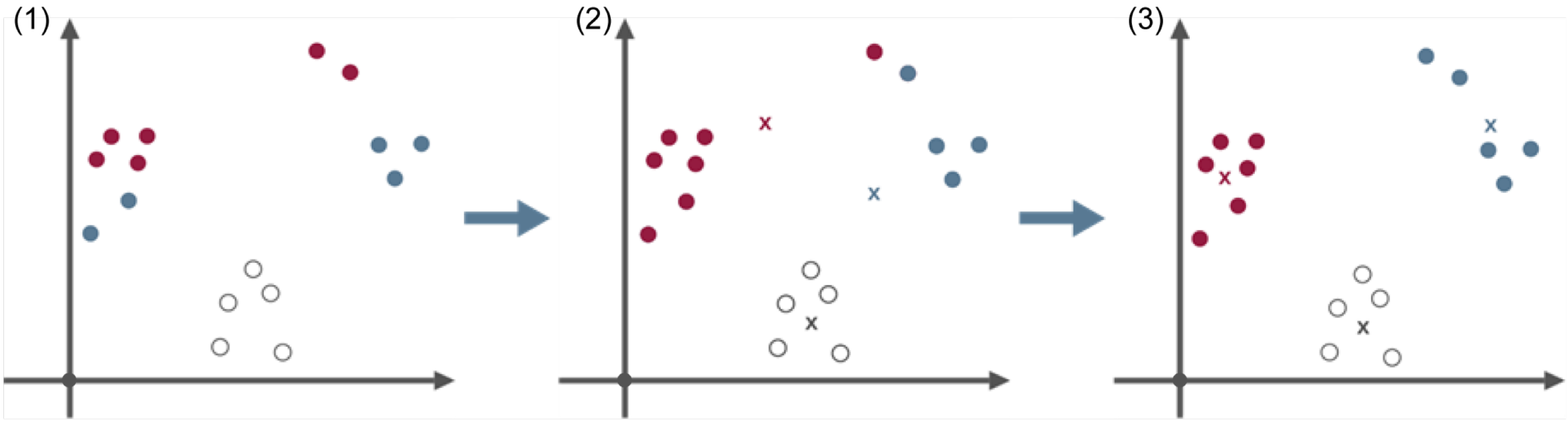
- ***Expectation of this approach:***
  - Recognize patterns that are too complex for humans (complexity)

- ML algorithm learns on its own
- Classic mistakes are not produced in this sense

- **ML algorithm**
  - **Clustering** connects similar data groups, for example:
    - k-means clustering
    - Hierarchical clustering procedures

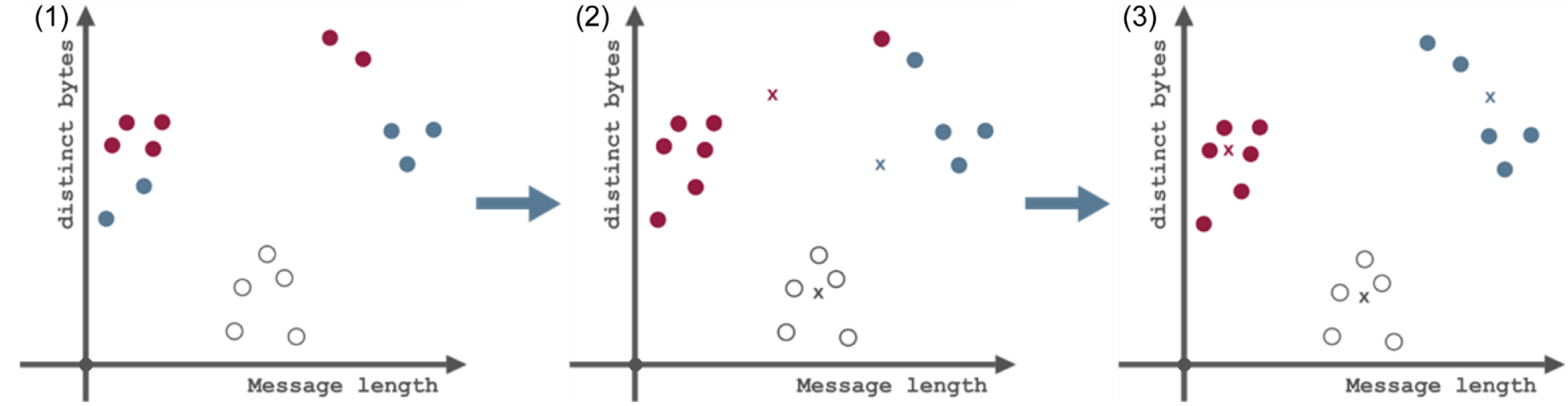
- **Problem:** Does the ML algorithm learn in the desired direction?

ML algorithm
→ k-Means-Algorithm



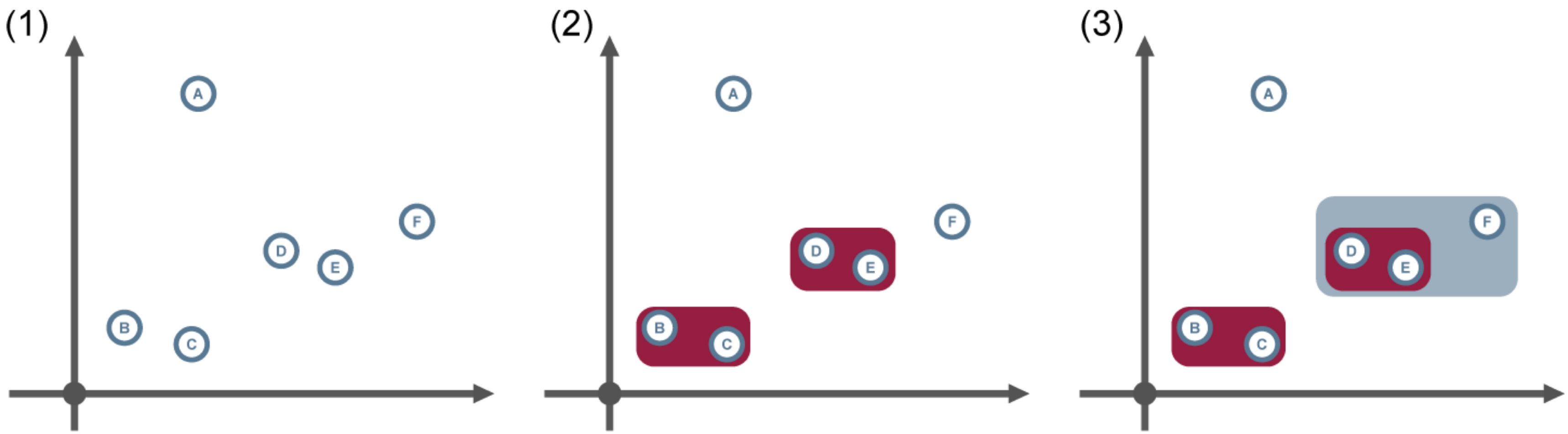
- **Input data:**
  - Any data
  - Distance
  - Number k cluster
  - Initial assignment of elements to clusters (random)
- **ML algorithm:**
  - Calculation of the centroids
  - Assignment of elements to clusters with the next centroid
  - Recalculation of the centroids and reassignment
- **Output:**
  - Classification of objects in k clusters

ML algorithm
→ k-Means-Algorithm - Example



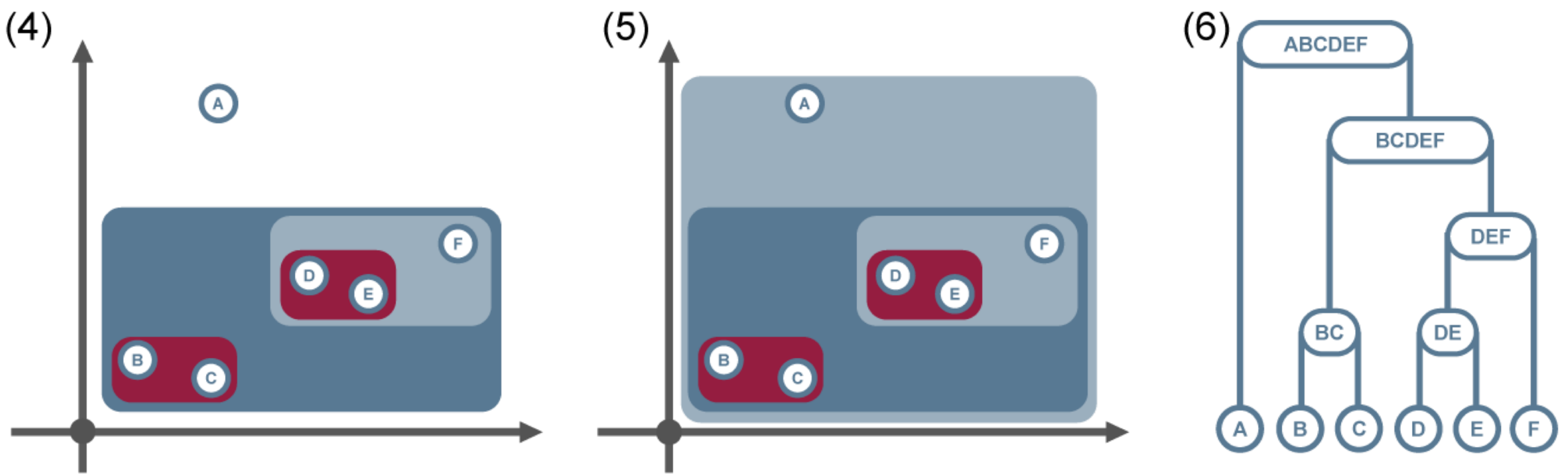
- **Input data (1):**
  - Data from malware *(Palevo, Virut, Mariposa)*
  - Distance
  - k = 3
  - Initial assignment after message length, distinct bytes
- **ML algorithm (2):**
  - Calculation of averages
  - Assign the elements to the malware with the next centroid
  - Recalculation of the centroids and reassignment
- **Output (3):**
  - Classification of the malware in the three types of malware
    - Red = Virut
    - White = Palevo
    - Blue = Mariposa

ML algorithm
→ Hierarchical clustering procedures (1/2)



- **Input data (1):**
  - any data
  - similarity
- **ML algorithm (2 to 5):**
  - each data point is a separate cluster
  - similar clusters are merged first
  - resulting clusters are reused as input data
  - iterative clustering induces a hierarchical structure

ML algorithm
→ Hierarchical clustering procedures (2/2)

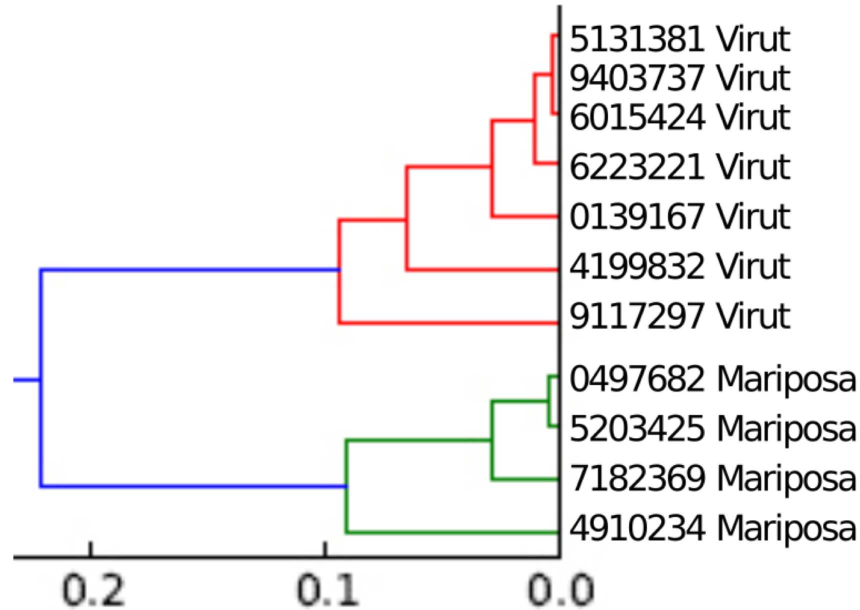


- **Output (6):**
  - Hierarchical relationships to each other in the form of a binary tree (dendrogram)

ML algorithm

→ Hierarchical clustering procedures - Example

- Clustering of data from botnet analysis
- Application of a complex distance function (value range [0, 1])
- Separation of family clusters at a distance of about 0.1
- Classification of data in two malware families Virut and Mariposa

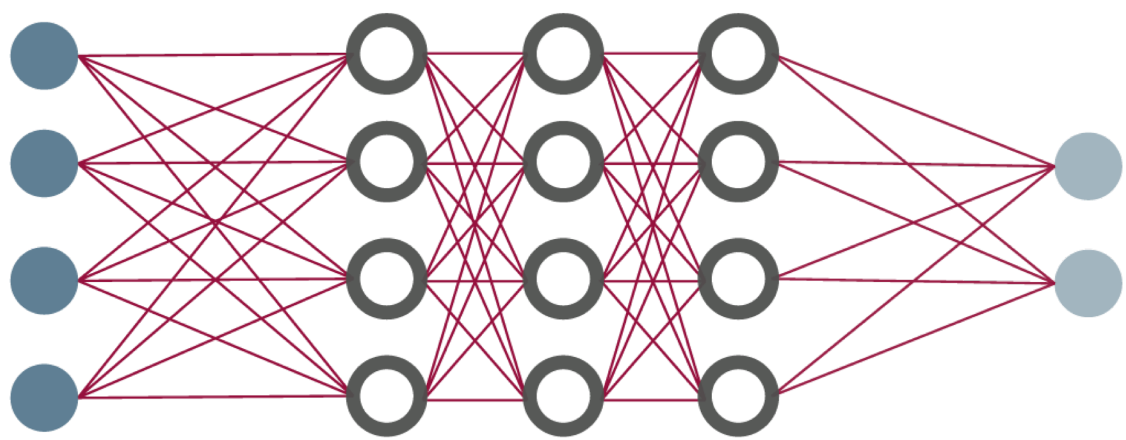


AI for Cyber Security
→ Content

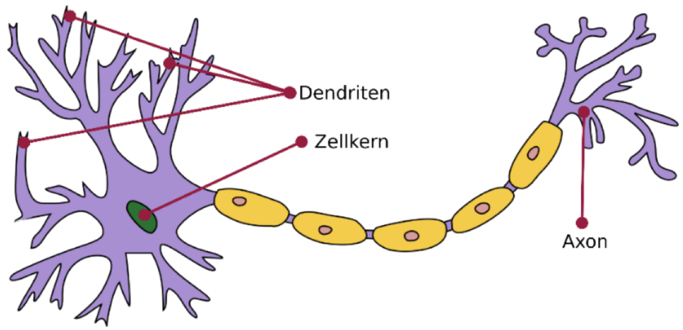
- **Classification**
  (Idea, data science, AI, ML, workflow, success factors, …)
- **Machine learning**
  (supervised/unsupervised, SVM, k-Means, h-clustering, …)
- **Artificial Neural Networks**
  (Idea, ANN, deep learning, …)
- **Applications examples AI for Cyber Security**
  (Alert system for online banking, passive authentication, …)
- **Attacks on machine learning**
  (Idea, training data, traffic signs, …)
- **Further challenges**
  (Dual-Use, challenges, opportunities and risks, …)
- **Result and outlook**

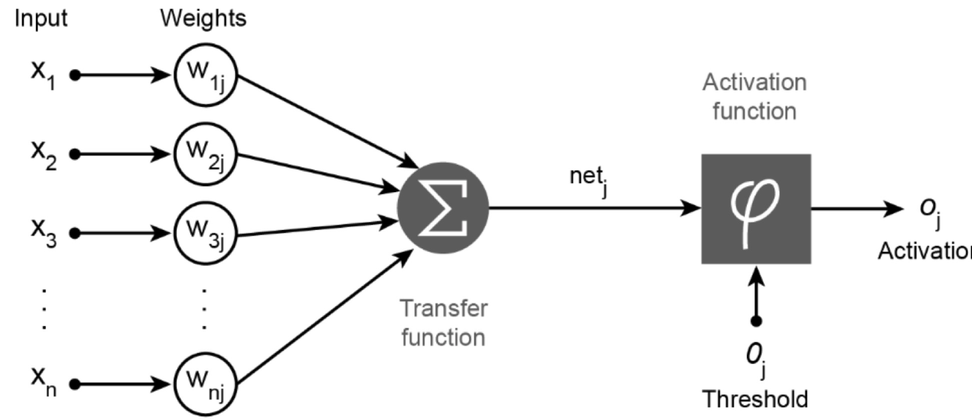
Artificial Neural Networks (ANN) → Networks of Artificial Neurons (1/2)

- Model is the biological structure of the brain / neuron
- Use weights and mathematical functions (for information processing)
- Information processing across multiple interconnected layers of artificial neurons



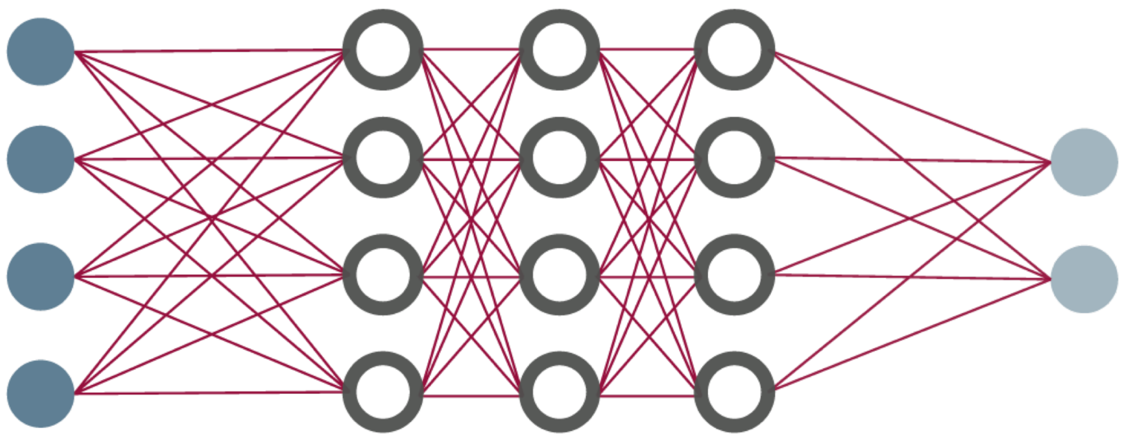
Artificial Neural Networks (ANN) → Networks of Artificial Neurons (2/2)





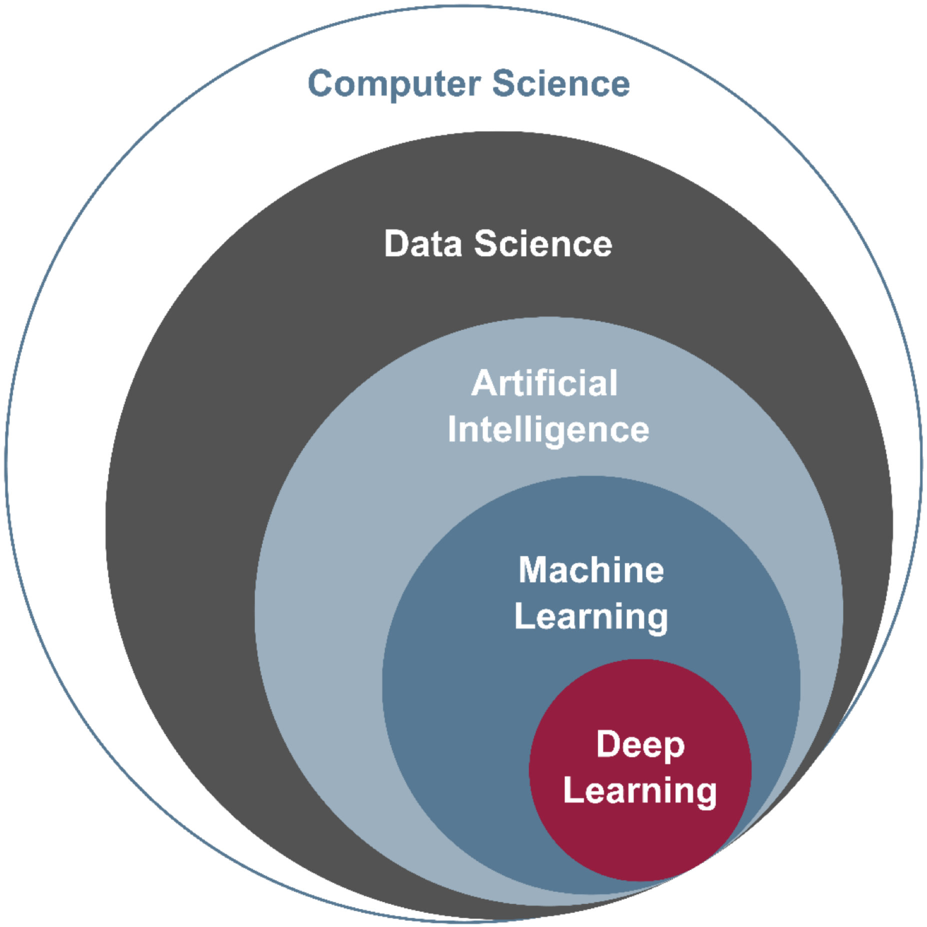
- **Biological Neuron:**
  - Dendrites:
    - Stimulus reception (signal input)
  - Axon:
    - Forward the information (signal output)
  - Nucleus:
    - Stimulus processing (signal processing)
- **Artificial Neuron:**
  - ***Transfer function:***
    - Calculated from the sum of the weights, the inputs, the network input
  - ***Activation function*** / output function:
    - Output of the information
  - ***Threshold:***
    - Value of a stimulus in which the neuron is activated

Artificial Neural Networks (ANN)
→ Layers in an ANN



- **Input layer:**
  - Input neurons (e.g., ears, retina, or skin)
  - Input data is translated into appropriate representation
- **Hidden layers:**
  - Depending on the complexity of the task 1-N linked neurons
  - Detection of simple patterns and structures
  - With each layer, more and more complex features are filtered out
- **Output layer:**
  - Output of all possible representations of the results

Classification
→ Deep Learning



- Machine learning becomes even more effective by:
  - **Deep Learning**
- Deep learning is a specialization of machine learning
- Mainly uses of neural networks
  - **Allows incomplete data**
  - **Allows noise and interference**
- Coming next to the "human brain"

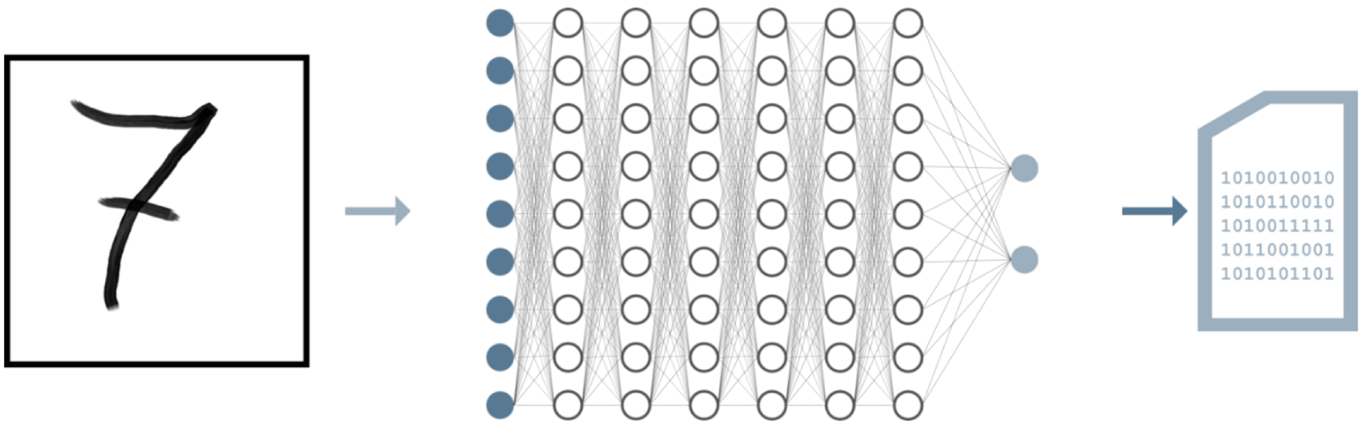
Deep Learning
→ Architectures (1/2)

- Research by more powerful hardware and increasing data availability has increased significantly in recent years
- In addition to classic feed-forward networks Recurrent Neural Networks are also manageable
  - Edges can also be attributed to previous layers
- **High number of layers**, which can be summarized by function
- Different architectures have proven to be particularly effective for different problems
- **Better scalability**

Deep Learning
→ Architectures (2/2)

- **Convolutional Neural Networks (CNN):**
  - Two-dimensional "window" is "pushed" over data
  - Influence by neighboring fields is considered
  - Particularly successful with Computer Vision (e.g., handwriting recognition)
- **Long Short-Term Memory Networks (LSTM):**
  - Special form of a Recurrent Neural Network
  - Neurons can store states for a longer period of time
  - Particularly successful with spoken language (Alexa, Siri, etc.)

Deep Learning
→ Handwriting recognition - Example



Digit	0	1	2	3	4	5	6	**7**	8	9
Accordance	0 %	7 %	1%	0 %	4 %	0 %	0 %	**85 %**	0 %	3 %

- **Input data (1):**
  - Image file with a number (7) to be classified
- **ML algorithm (2):**
  - Input data is processed in the artificial neurons in the layers
  - For example, using a Convolutional Neural Network (CNN)
- **Output (3):**
  - Table with a distribution of the **probabilities** for a match with a **digit**

AI for Cyber Security
→ Content

- **Classification**
  (Idea, data science, AI, ML, workflow, success factors, …)
- **Machine learning**
  (supervised/unsupervised, SVM, k-Means, h-clustering, …)
- **Artificial Neural Networks**
  (Idea, ANN, deep learning, …)
- **Applications examples AI for Cyber Security**
  (Alert system for online banking, passive authentication, …)
- **Attacks on machine learning**
  (Idea, training data, traffic signs, …)
- **Further challenges**
  (Dual-Use, challenges, opportunities and risks, …)
- **Result and outlook**

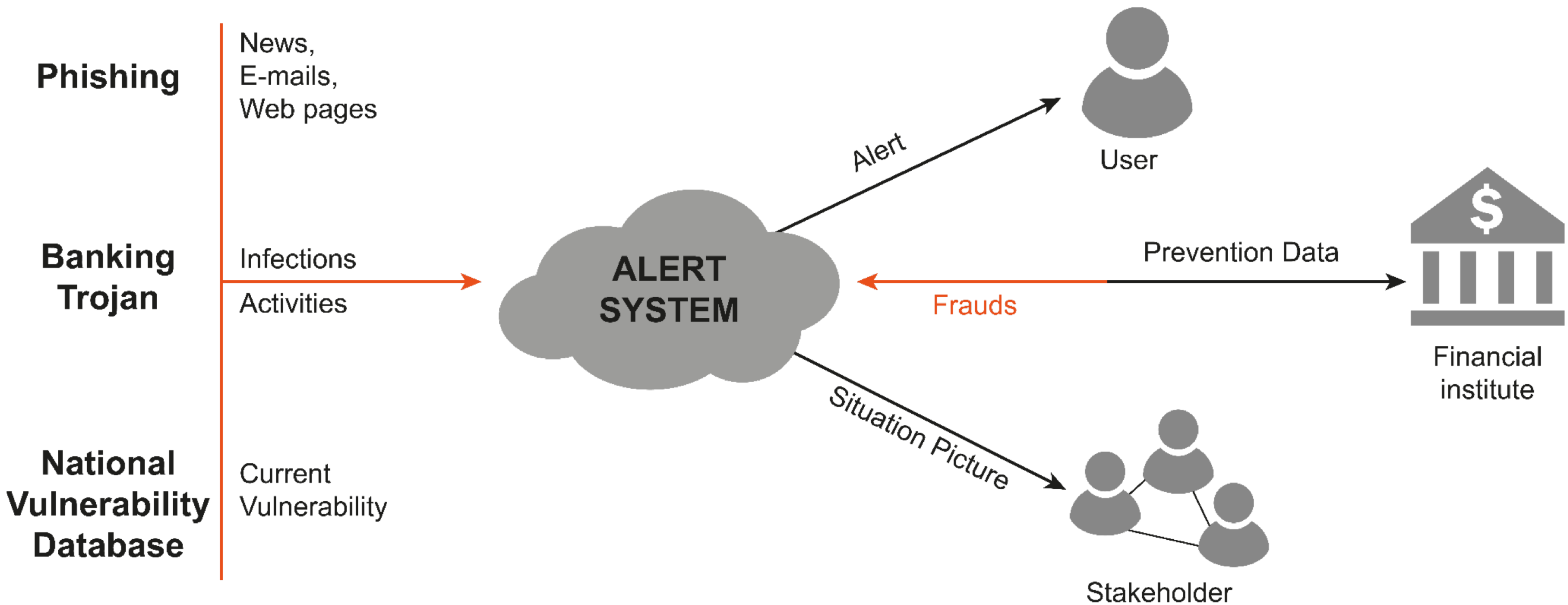
Applications examples (1/2)
→ Alert-System for online banking

- How could a solution look like?
  - Daily warnings in the event of an increased risk situation (online banking)
    → enable the bank customer and the bank to react
  - Instruct the users when there are dangers
    → so that the bank customer can behave "correctly"

- **Approach of the alert system**
  - Identify **security metrics** for fraud
  - Determine **danger situation** with AI
  - **Warn** users and banks

© Daniel Nimmervoll - Fotolia.com

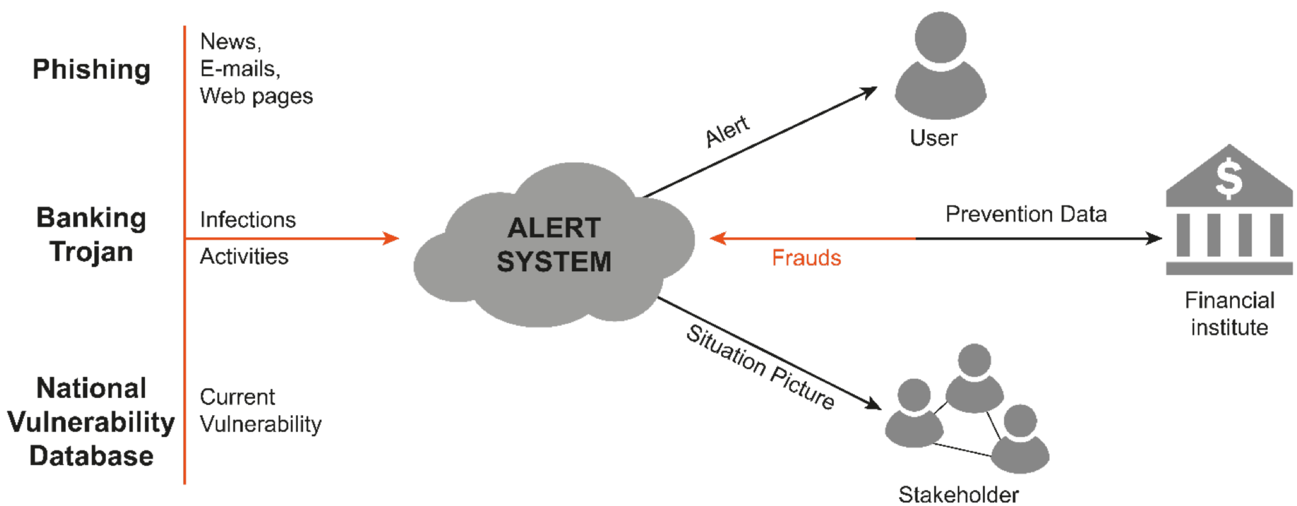
Alert-System for online banking
→ Concept



Alert-System for online banking

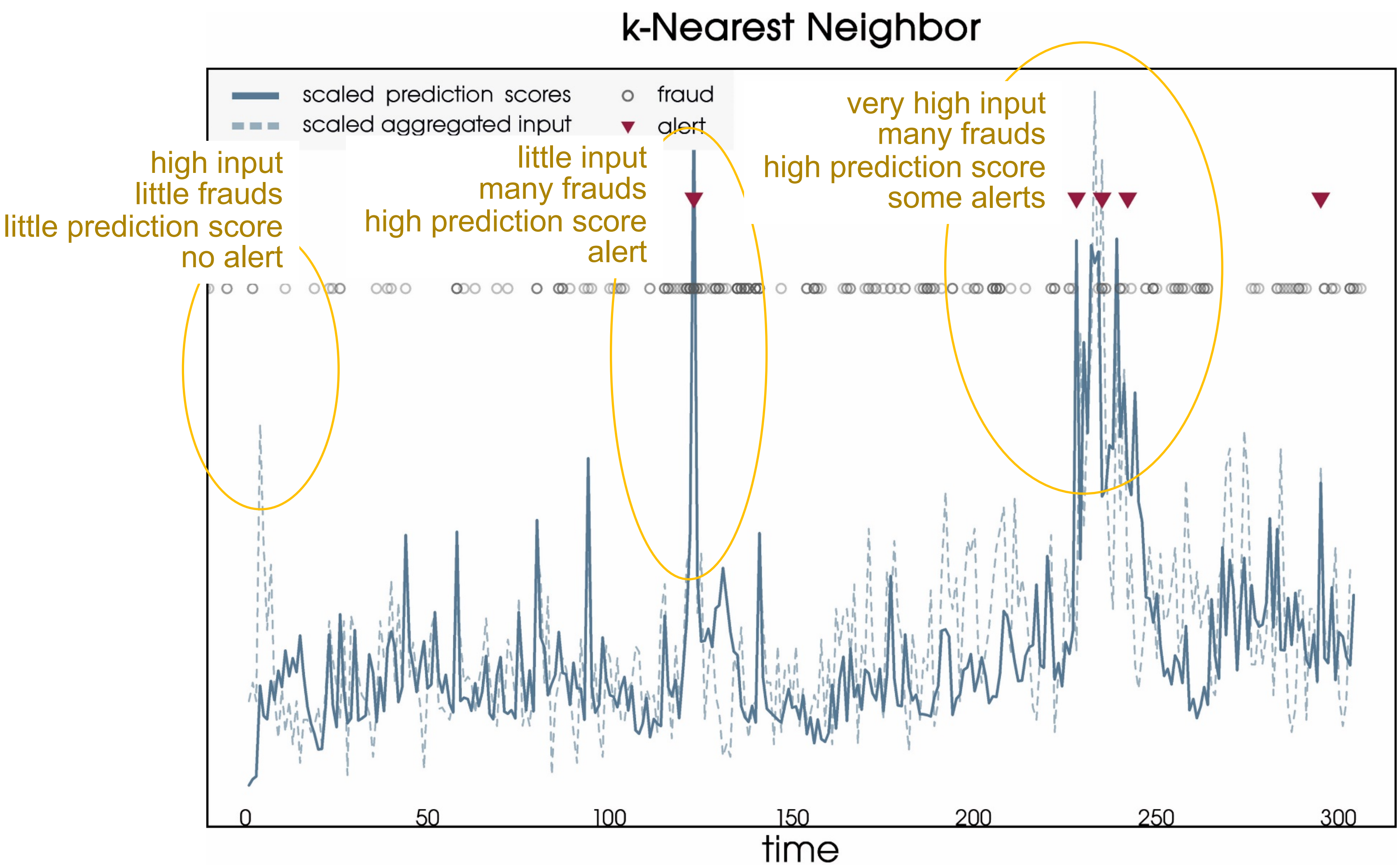
→ Numbers for the test period of 456 days

- 1.904 News (phishing attack) – “Stackoverflow Network”
- 5.589 **E-mail** (phishing attack) – „Spam Archive“
- 2.776 Phishing **websites** – „PhishTank“
- 23.184 **infections** of banking Trojans (malware) - Anti-malware companies
- 875 relevant **vulnerabilities** (NVD)
- 459 successful **fraud cases** in online banking - banking group



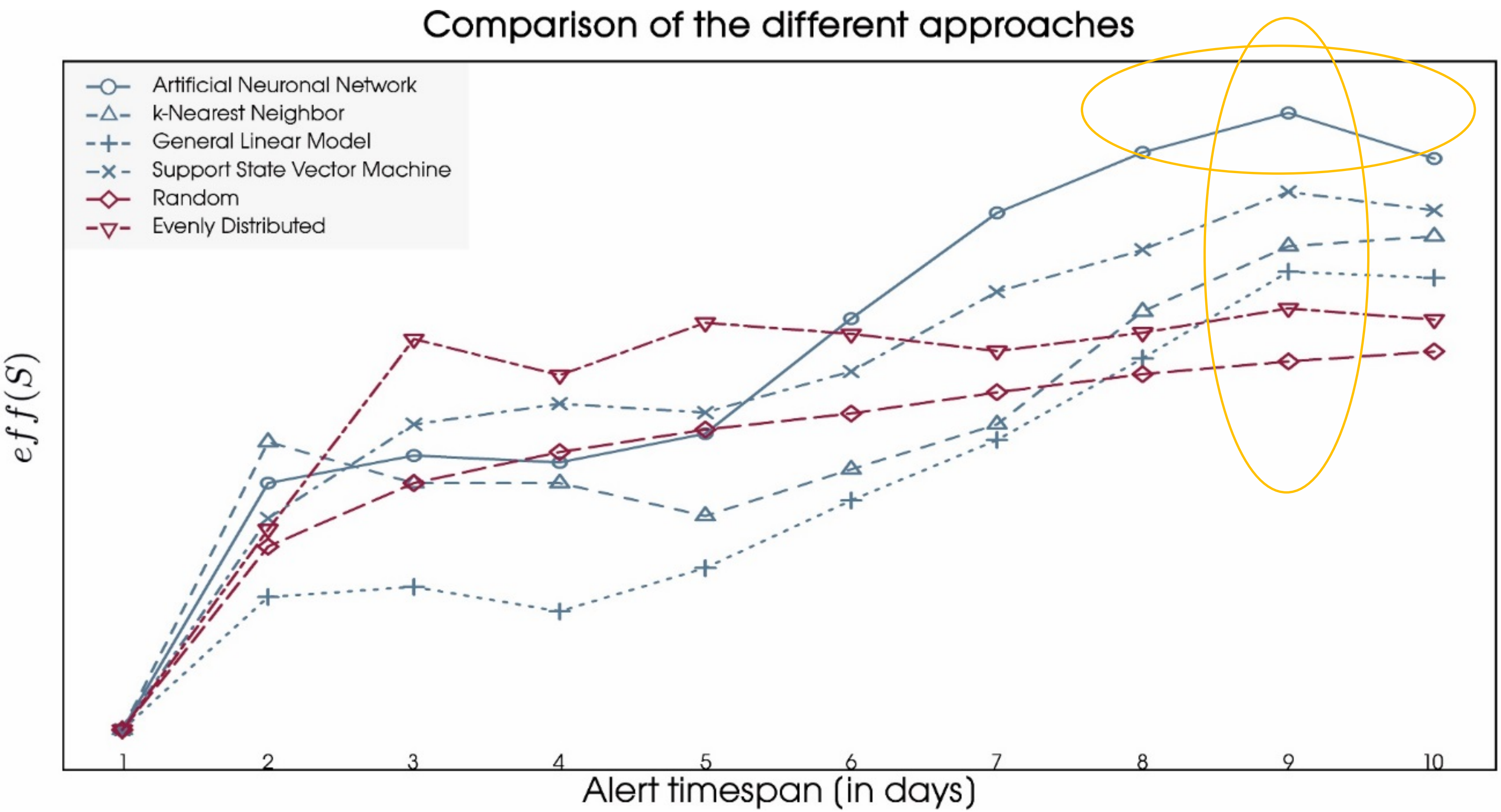
1/3 for the training period (152 days) 2/3 for evaluation period (304 days)

Assess the result
→ k-Nearest Neighbor

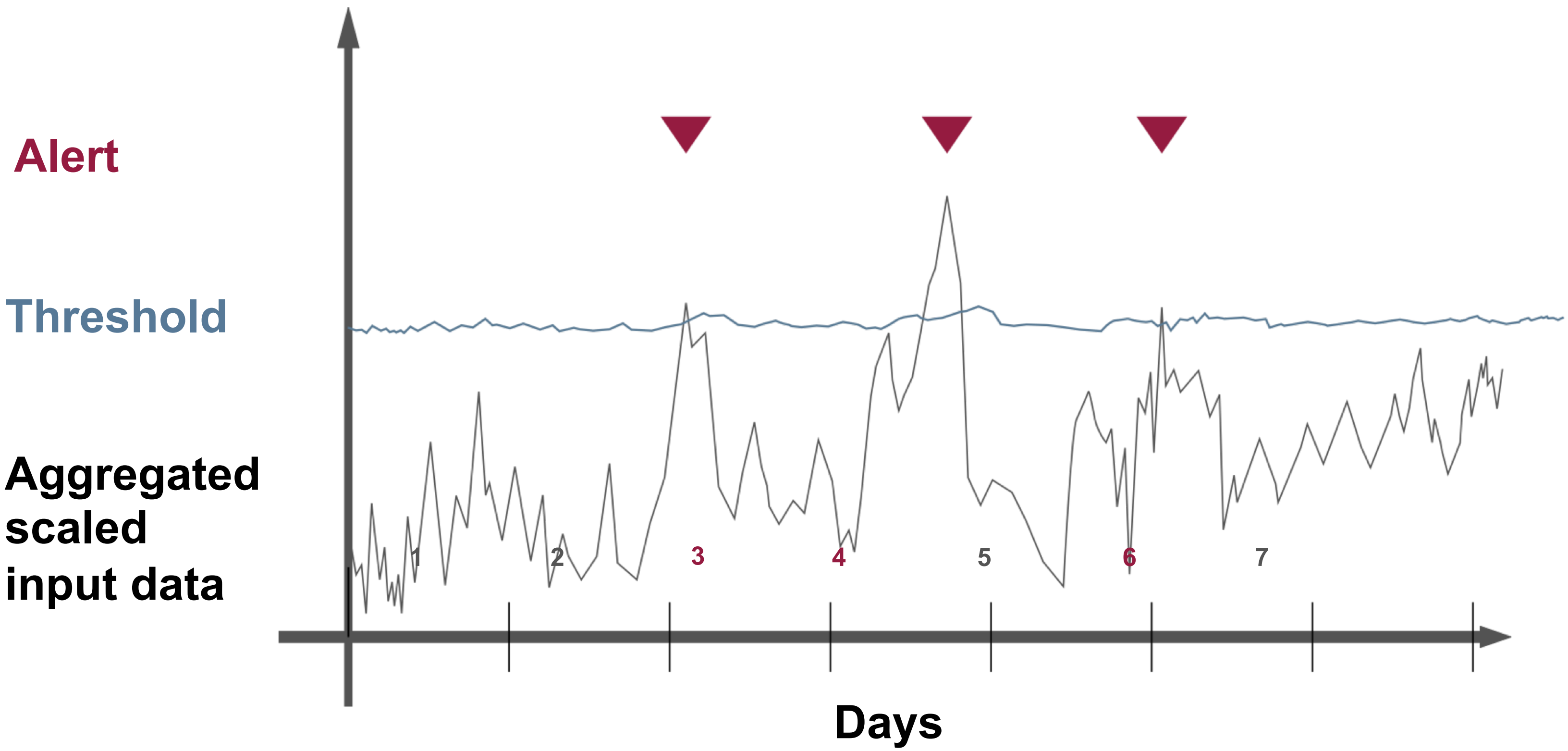


Results
→ Comparison of the different methods

„But, three times as much time for training Artificial Neural Networks“



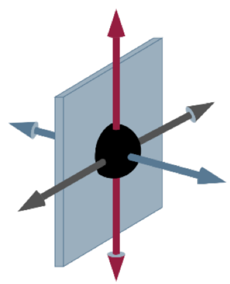
Alert-System for online banking
→ Result



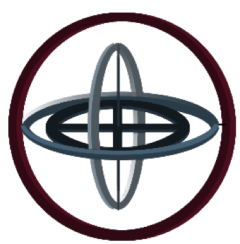
- **Output:**
  - Predicted threat values on days 3, 4, and 6 exceed the threshold set for this alert system
  - because the threshold has been exceeded, an alert is triggered

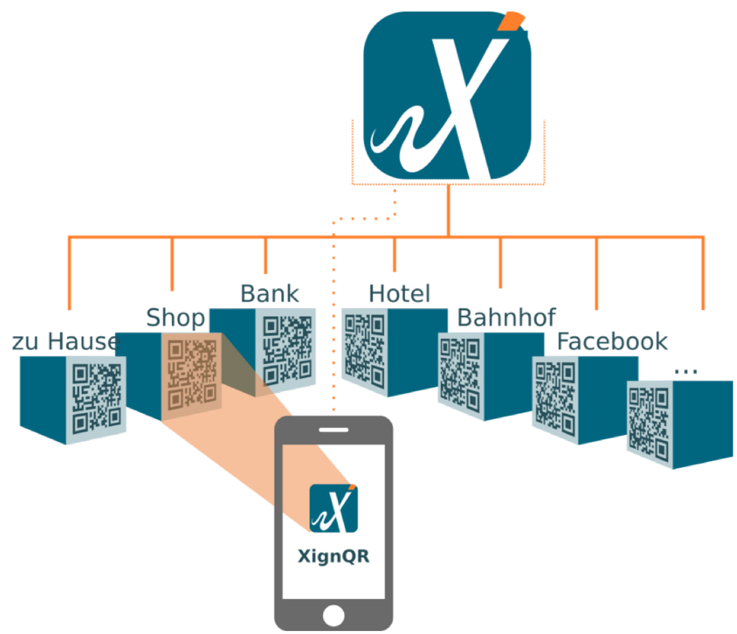
Applications examples (2/2)
→ Passive Authentication - XignQR

- A user is automatically detected by the way of scanning the QR code.
- Throughout the process, passive biometric movement data is measured.
- Data collection by
  - **Accelerometer**

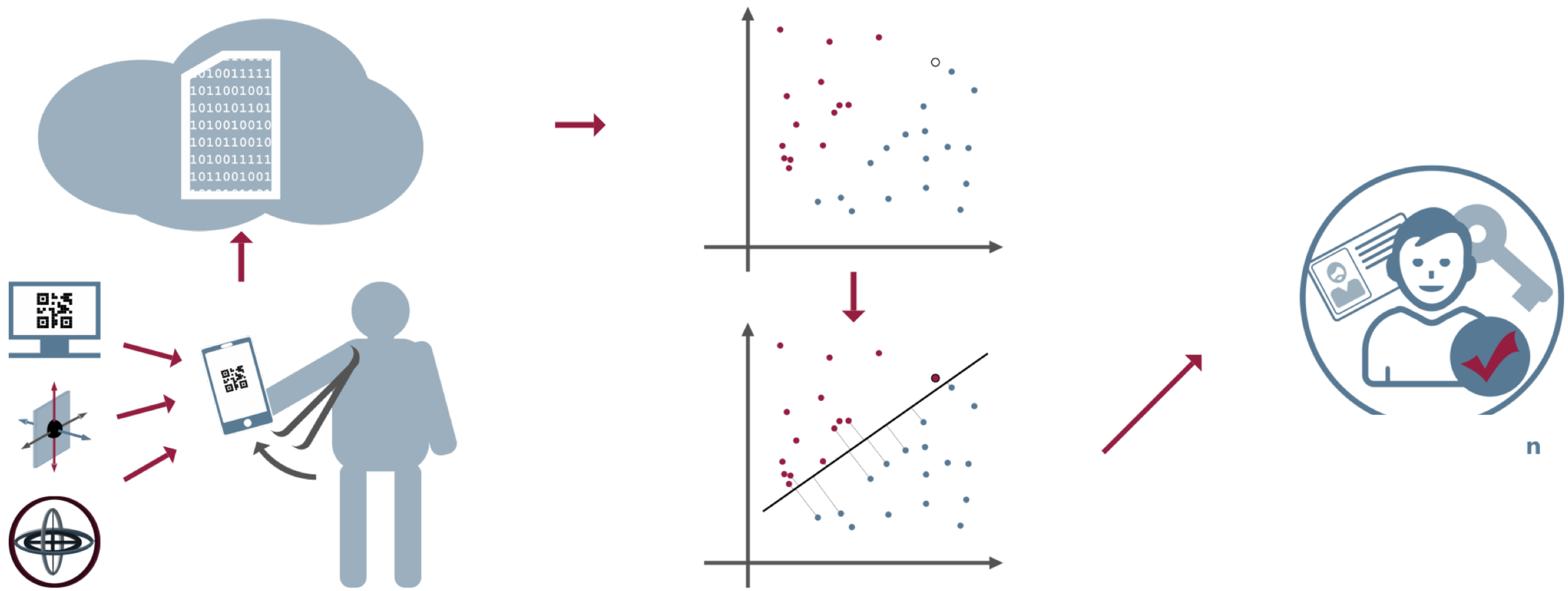


  - **Position sensor**



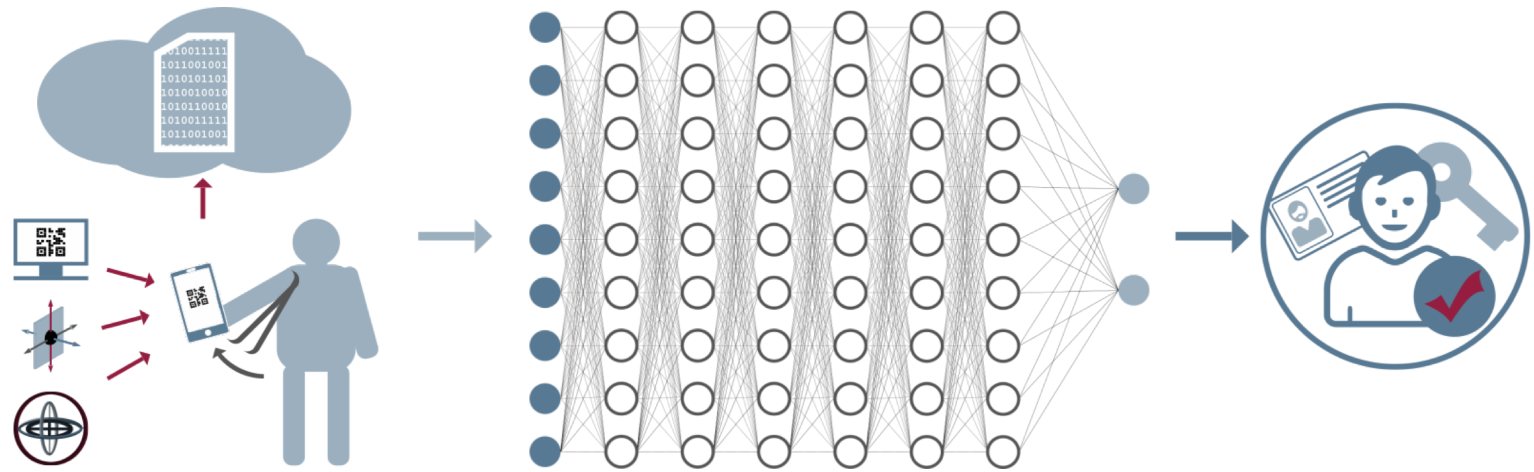


Passive Authentication - XignQR
→ Support-Vector-Machine (SVM)



- **Input data:**
  - User takes the smartphone from pocket
  - Measure **location** and **acceleration** of the smartphone
- **ML algorithm:**
  - Data is classified by a model
  - red match is **positive** classification
  - blue a **negative** classification (e.g. of other users)
- **Output:**
  - Authentication is either successful or fails (**95 %**)

Passive Authentication - XignQR
→ Artificial Neural Networks



- **Input data:**
  - Location and acceleration data of the user are generated

```
time, type, x, y, z
271, Accelerometer, -0.07606506, 9.173798, 3.6333618
277, Accelerometer, 1.0681152E-4, 9.146423, 3.5619507
279, Gyroscope, 0.027664185, 0.06774902, 0.02182006
...
```

- **ML algorithm:**
  - Input data is processed in the artificial neurons in the layers

- **Output:**

User	Accordance
0	0,059 %
1	99,85 %
2	0,087 %

```
[[5.9110398e-04 9.9853361e-01 8.7528664e-04]]
Predicted Class [1]
Predicted Person: Sandra Kreis
```

AI for Cyber Security
→ Further examples

- Log analysis
- Malware detection
- Security Information and Event Management (SIEM)
- Threat Intelligence
- Voice recognition
- Image recognition (ID card, video, ...)
- Authentication method
- Fake News
- IT Forensics
- Secure software development
- ...

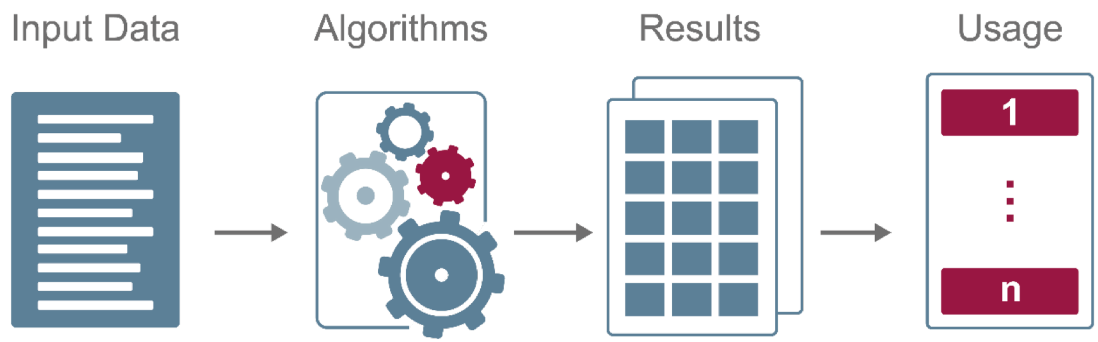
AI for Cyber Security
→ Content

- **Classification**
  (Idea, data science, AI, ML, workflow, success factors, …)
- **Machine learning**
  (supervised/unsupervised, SVM, k-Means, h-clustering, …)
- **Artificial Neural Networks**
  (Idea, ANN, deep learning, …)
- **Applications examples AI for Cyber Security**
  (Alert system for online banking, passive authentication, …)
- **Attacks on machine learning**
  (Idea, training data, traffic signs, …)
- **Further challenges**
  (Dual-Use, challenges, opportunities and risks, …)
- **Result and outlook**

Attacks
→ on machine learning (AI)

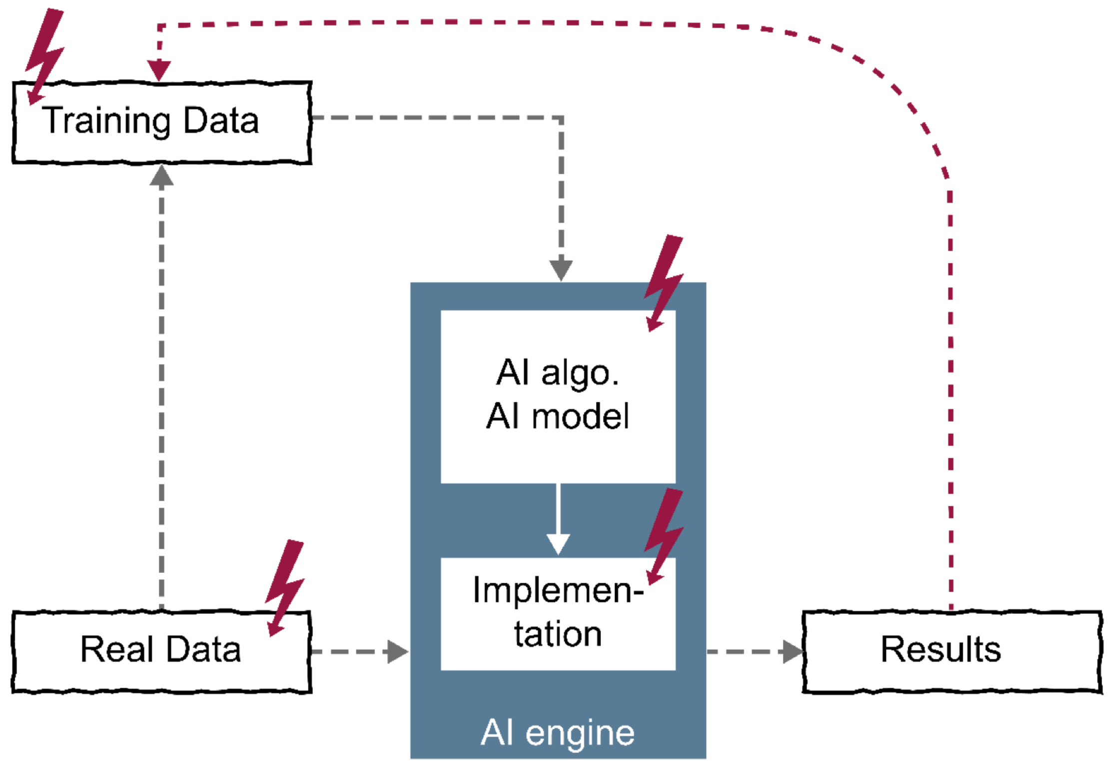
Hackers attack and manipulate the workflow (“result”)

- Input data (input)
  - Manipulation
  - Privacy
- Algorithms
- Results (output)
- Usage



Trustworthiness
→ Quality of implementation

State of the art
IT security measures
for protection
→ *the **data** (training, real, result),*
→ *the **AI engine** and*
→ *the **application***



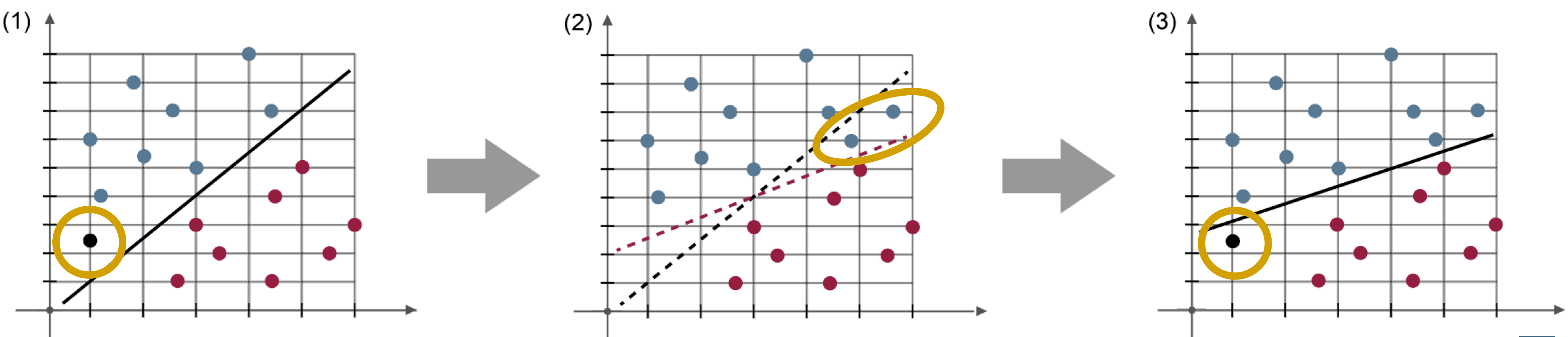
Use of a
high quality
AI technology

Security goals:
→ ***Integrity***
(detection of data manipulation)
→ ***Confidentiality***
(protection of business secrets)
→ ***Data protection***
(protection of personal data)
→ ***Availability***
(of the application and results)

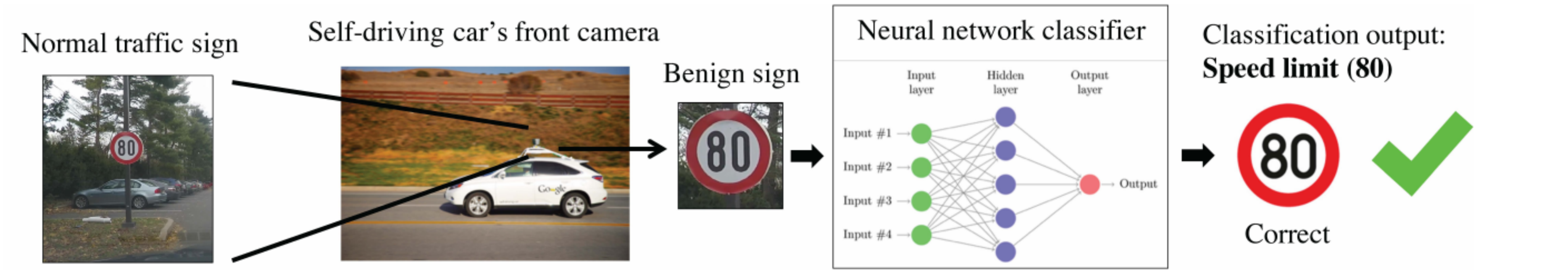
Cooperation of experienced
AI and application experts

Attacks on machine learning
→ Manipulation of training data

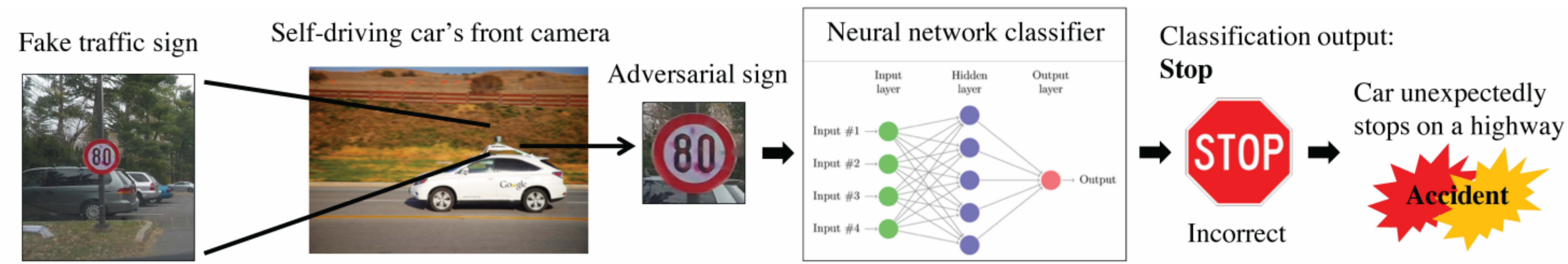
- (1) **Normal classification** of a new input.
  (new black dot belongs to the blue class)
- **(2) Example: manipulation of training data**
  - Incorrectly classified data will be injected into the training process as an attack (two more blue dots).
  - This manipulates the straight line of the model for classification (straight line becomes flatter).
- (3) This can be used by an attacker to create **wrong classifications**.
  (now the new black dot belongs to the red class)



Attacks on machine learning
→ Manipulation of traffic signs



(a) Operation of the computer vision subsystem of an AV under *benign conditions*



(b) Operation of the computer vision subsystem of an AV under *adversarial conditions*

Fig. 1. **Difference in operation of autonomous cars under benign and adversarial conditions**. Figure 1b shows the classification result for a drive-by test for a physically robust adversarial example generated using our Adversarial Traffic Sign attack.

Quelle: https://arxiv.org/abs/1802.06430

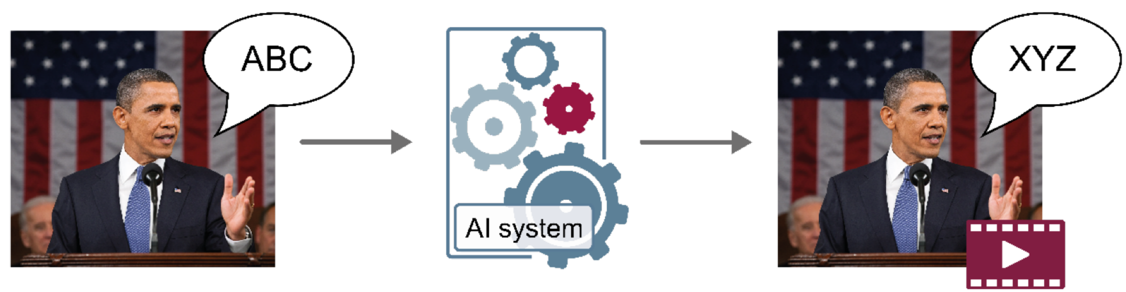
AI for Cyber Security
→ Content

- **Classification**
  (Idea, data science, AI, ML, workflow, success factors, …)
- **Machine learning**
  (supervised/unsupervised, SVM, k-Means, h-clustering, …)
- **Artificial Neural Networks**
  (Idea, ANN, deep learning, …)
- **Applications examples AI for Cyber Security**
  (Alert system for online banking, passive authentication, …)
- **Attacks on machine learning**
  (Idea, training data, traffic signs, …)
- **Further challenges**
  (Dual-Use, challenges, opportunities and risks, …)
- **Result and outlook**

Artificial intelligence
→ Attackers use AI

Hacker also use AI for their own purposes (dual-use)

- Vulnerability search (faster attack, new attack vectors, …)
- Social engineering (chat bots, ...)
- Password cracker
- New attack structures and procedures
- Video manipulation (deep fake)
  - "Fake Obama Video„
  - "Make Putin Smile Video"



Artificial intelligence
→ General challenges

- **Data protection**
  (personal data ... European General Data Protection Regulation)

- **Self-determination** ("human in the loop")

- **Discrimination** (balanced data ... problem: does not exist)
  → woman / man, origin, education, ...

- **Trustworthiness** of data and results
  → **AI seal**

- …

Artificial intelligence
→ Opportunities and risks

- **Individual knowledge** and **complexity of thinking humans** are superior to algorithms! **+**

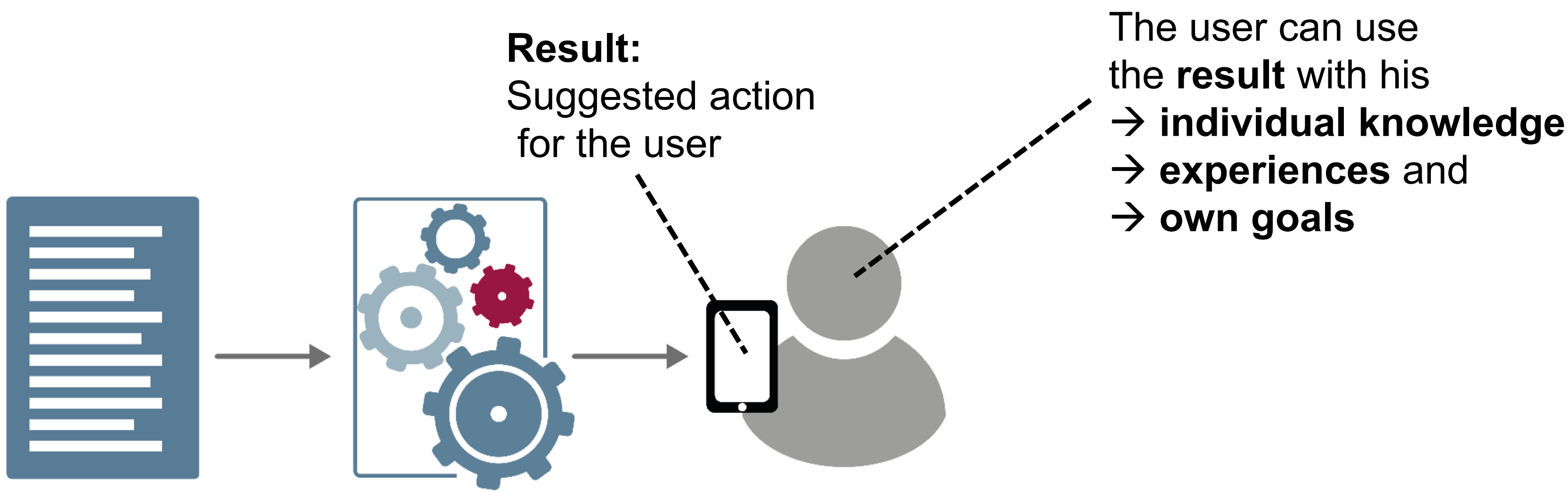
- **Algorithms can more quickly generate knowledge** from existing data! **+**

- Individual knowledge + algorithms knowledge = **+++**

- **Practical Problem Medicine / Watson**
  - Diagnostics (machine)
  - Liability (human)

Trustworthiness
→ Traceability of the results

- **„Keep the human in the loop“**
  - AI result must be understood as a **recommendation for the** user.
  - This promotes the **self-determination** of users and increases their trustworthiness.



- **Automated applications** (e.g., autonomous driving)
  - Simulation, test and **validation**
  - Responsibility, **liability** and insurance

AI for Cyber Security
→ Content

- **Classification**
  (Idea, data science, AI, ML, workflow, success factors, …)
- **Machine learning**
  (supervised/unsupervised, SVM, k-Means, h-clustering, …)
- **Artificial Neural Networks**
  (Idea, ANN, deep learning, …)
- **Applications examples AI for Cyber Security**
  (Alert system for online banking, passive authentication, …)
- **Attacks on machine learning**
  (Idea, training data, traffic signs, …)
- **Further challenges**
  (Dual-Use, challenges, opportunities and risks, …)
- **Result and outlook**

AI for Cyber Security
→ Result and outlook

- **AI / ML is an important technology for the future, including cyber security**
  - Detect threats, vulnerabilities, attacks, ...
  - Recognition of users (authentication)
  - Support of cyber security experts
  - ...
- **Very good data is especially important**
  - New, better sensors (data with very good content)
  - Collaboration and exchange of data
  - …
- **Technological and data sovereignty is becoming increasingly important**

Research questions
→ Security/trustworthiness of AI systems

- **Security and trustworthy of the data used** (training, real, …)
  - Security infrastructure for
    - Integrity (detection of data manipulation)
    - Confidentiality (protection of business secrets)
    - Data protection (protection of personal data)
    - Availability (of the application and results)

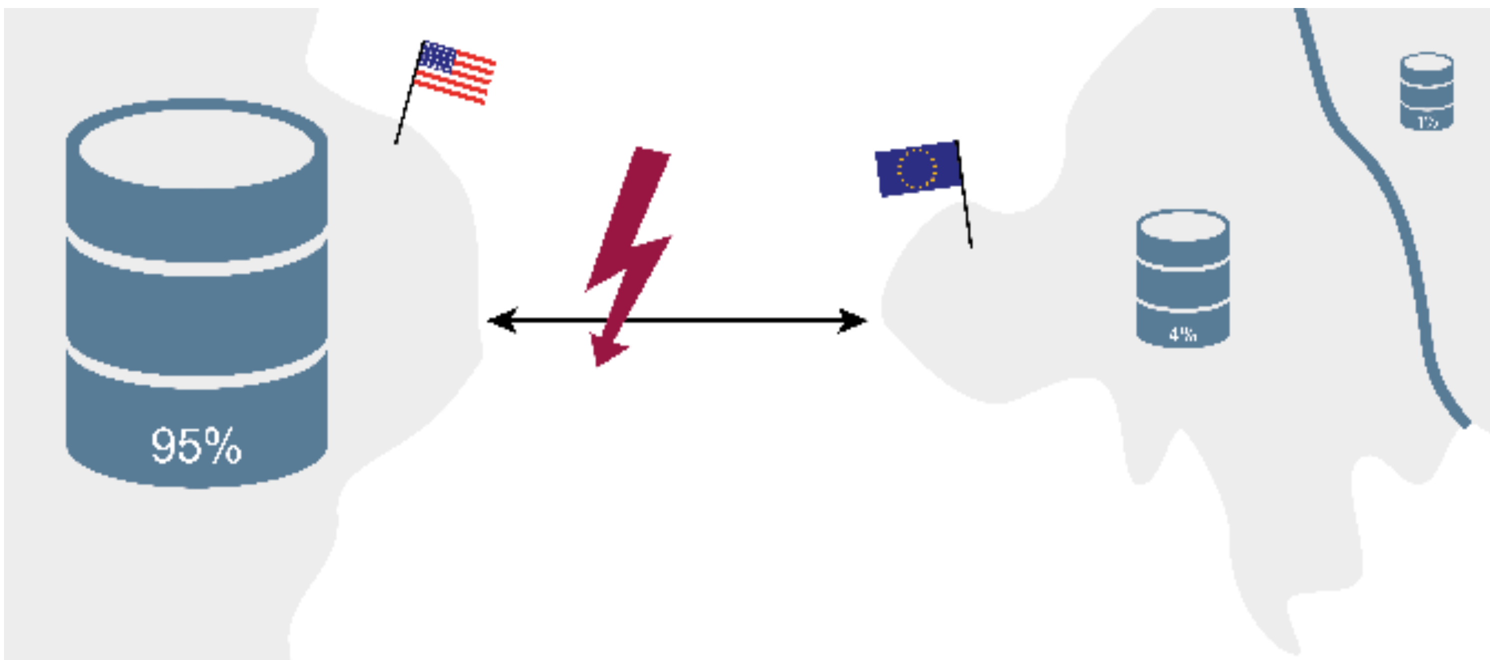
- **Secure and trustworthy implementation of AI systems**
  - IT security solutions for protection of
    - data,
    - AI engine and
    - application

- **Traceability of decisions**
  - Infrastructure for validating the responsible (Blockchain, PKI, …)

Research questions
→ Sovereignty

- We need a powerful AI infrastructure to maintain digital sovereignty.

- Availability of the data



Research questions
→ Exchange of security relevant data

internet security.

- Useful for better results!
- How can this point be motivated?
- What are the disadvantages?
- …

Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Artificial Intelligence (AI) for Cyber Security

With **Artificial Intelligence** into a more secure future!

Prof. Dr. (TU NN)
Norbert Pohlmann

Institute for Internet Security - if(is)
University of Applied Sciences Gelsenkirchen
http://www.internet-sicherheit.de

if(is) internet security.

Appendic / Credits

Wir empfehlen

- **Kostenlose App securityNews**

- **7. Sinn im Internet (Cyberschutzraum)**
  https://www.youtube.com/cyberschutzraum

- **Master Internet-Sicherheit**
  https://it-sicherheit.de/master-studieren/

Besuchen und abonnieren Sie uns :-)

WWW
https://www.internet-sicherheit.de

Facebook
https://www.facebook.com/Internet.Sicherheit.ifis

Twitter
https://twitter.com/_ifis

YouTube
https://www.youtube.com/user/InternetSicherheitDE/

Prof. Norbert Pohlmann
https://norbert-pohlmann.com/

Quellen Bildmaterial

Eingebettete Piktogramme:
- Institut für Internet-Sicherheit – if(is)

Der Marktplatz IT-Sicherheit

(IT-Sicherheits-) Anbieter, Lösungen, Jobs, Veranstaltungen und Hilfestellungen (Ratgeber, IT-Sicherheitstipps, Glossar, u.v.m.) leicht & einfach finden.
https://www.it-sicherheit.de/

Literature

N. Pohlmann, S. Schmidt: „Der Virtuelle IT-Sicherheitsberater – Künstliche Intelligenz (KI) ergänzt statische Anomalien-Erkennung und signaturbasierte Intrusion Detection“, IT-Sicherheit – Management und Praxis, DATAKONTEXT-Fachverlag, 05/2009

D. Petersen, N. Pohlmann: "Ideales Internet-Frühwarnsystem", DuD Datenschutz und Datensicherheit – Recht und Sicherheit in Informationsverarbeitung und Kommunikation, Vieweg Verlag, 02/2011

M. Fourné, D. Petersen, N. Pohlmann: “Attack-Test and Verification Systems, Steps Towards Verifiable Anomaly Detection“. In Proceedings der INFORMATIK 2013 - Informatik angepasst an Mensch, Organisation und Umwelt, Hrsg.: Matthias Horbach, GI, Bonn 2013

D. Petersen, N. Pohlmann: „Kommunikationslage im Blick - Gefahr erkannt, Gefahr gebannt“, IT-Sicherheit – Management und Praxis, DATAKONTEXT-Fachverlag, 4/2014

U. Coester, N. Pohlmann: „Verlieren wir schleichend die Kontrolle über unser Handeln? Autonomie hat oberste Priorität“, BI-SPEKTRUM Fachzeitschrift für Business Intelligence und Data Warehousing, 05-2015

U. Coester, N. Pohlmann: „Diskriminierung und weniger Selbstbestimmung? Die Schattenseiten der Algorithmen“, tec4u, 12/17

N. Pohlmann: „Künstliche Intelligenz und Cybersicherheit - Unausgegoren aber notwendig“, IT-Sicherheit – Fachmagazin für Informationssicherheit und Compliance, DATAKONTEXT-Fachverlag, 1/2019

N. Pohlmann: Lehrbuch „Cyber-Sicherheit“, Springer Vieweg Verlag, Wiesbaden 2019
ISBN 978-3-658-25397-4

See more articles: https://norbert-pohlmann.com/artikel/