Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Impulsvortrag

Staat und Wirtschaft gemeinsam für mehr IT-Sicherheit

→ **Cyber-Sicherheit** braucht **Künstliche Intelligenz**

→ keine **Künstliche Intelligenz** ohne **Cyber-Sicherheit**

Prof. Dr. (TU NN)

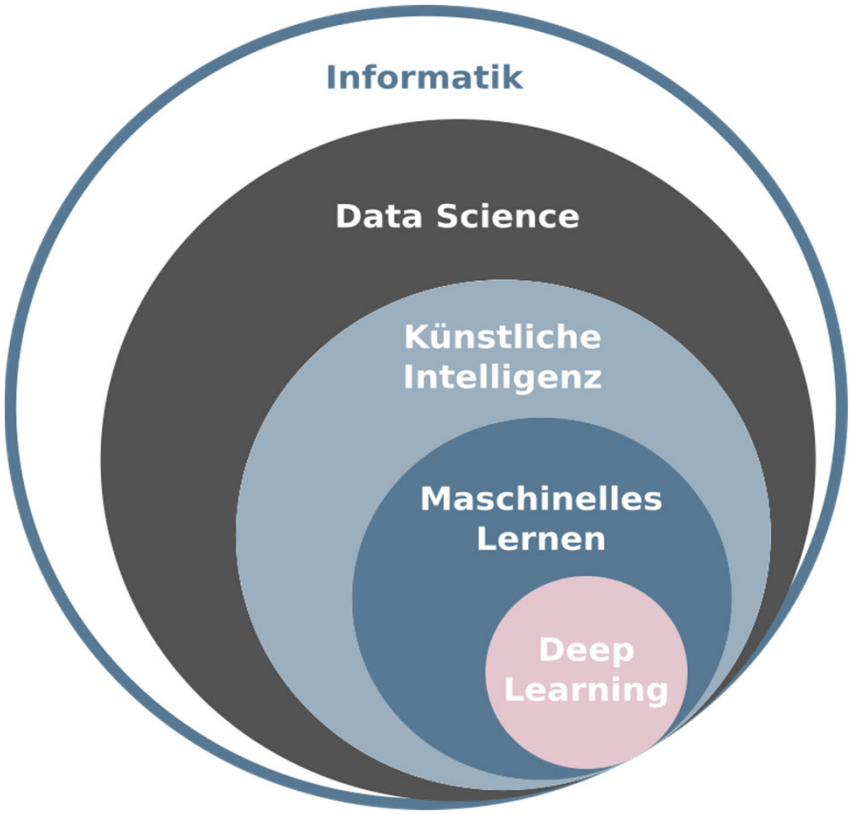
Norbert Pohlmann

Professor** für **Informationssicherheit
Leiter** des **Instituts für Internet-Sicherheit - if(is)
Vorstandsmitglied** des **Verbands der Internetwirtschaft - eco
Vorstandsvorsitzender** des **Bundesverbands IT-Sicherheit - TeleTrusT

if(is) internet-sicherheit.

Einordnung

→ (Künstliche Intelligenz) **Maschinelles Lernen**



- **Data Science** bezeichnet generell die **Extraktion von Wissen aus Daten**.

- **Maschinelles Lernen** ist ein Begriff für die „künstliche“ **Generierung von Wissen aus Erfahrung** (in Daten) durch Computer.

Herausforderungen für die Cyber-Sicherheit

- **(sicherheitsrelevante) Informationen in Daten**
  - Inhaltshöhe
  - Menge an (verschiedenen) SI-Informationen
  - …
- passende ML-Algorithmen
- leistungsfähige KI-Systeme

…

Erfolgsfaktoren

→ (Künstliche Intelligenz) **Maschinelles Lernen**

Leistungsfähigkeit der IT-Systeme

- enorme Steigerung (CPU, RAM, …) der IT-Systeme sehr viele CPU Kerne, …
- Spezial-Hardware: GPUs, FPGA, TensorFlow PU (TPU), …
- Frameworks, Cloud-Lösungen, …

Algorithmen

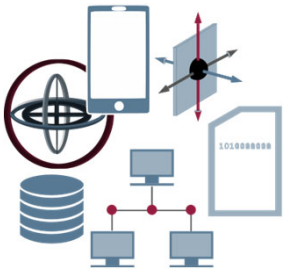
- Immer **bessere Algorithmen** (viel als OpenSource)
- Immer **mehr Erfahrungen** mit dem Umgang
- Immer **einfacherer Zugang** zu den Technologien und Diensten

Immer **mehr** vorhandene (sicherheitsrelevante) **Daten** für die

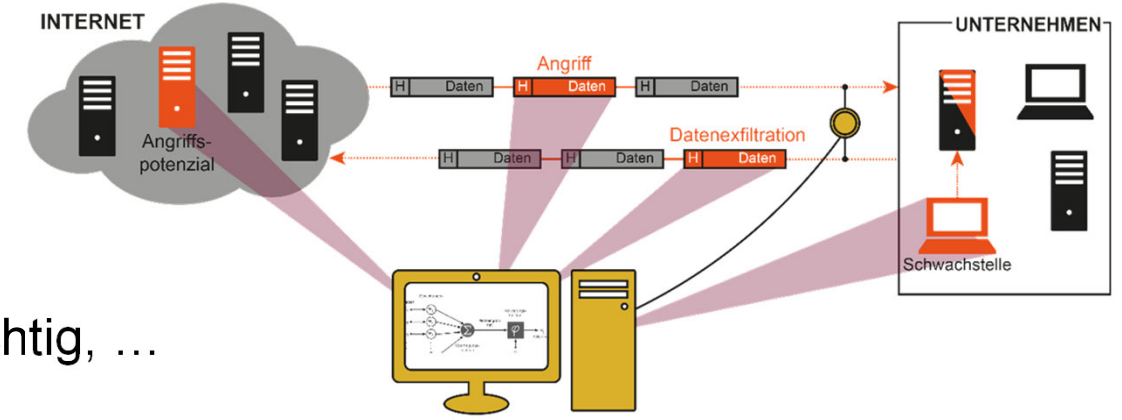
- **Verteidiger**

aber auch für die

- **Angreifer**



Cyber-Sicherheit braucht
→ Künstliche Intelligenz



- Erhöhung der **Erkennungsrate** von **Angriffen**
  - Netzwerk, IT-Endgeräte, …
  - adaptive Modelle
  - Unterschied: normal und verdächtig, …

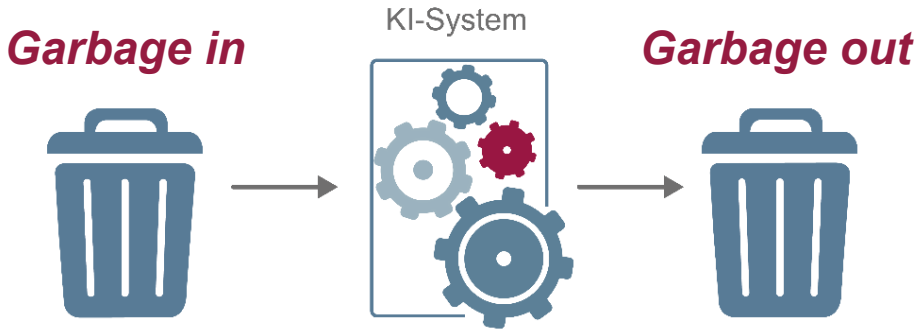
- **Unterstützung / Entlastung** von **Cyber-Sicherheitsexperten**
  - Erkennen von **wichtigen** sicherheitsrelevanten Ereignissen *(Priorisierung)*
  - **(Teil-)Autonomie** bei Reaktionen, … Erhöhung der Resilienz, …

- **Verbesserungen** von bestehenden **Cyber-Sicherheitslösungen**
  - KI leistet einen Beitrag zu einer erhöhten Wirkung und Robustheit
    - Z.B.: Risiko-basierte und adaptive Authentifizierung
  - um **Schäden** zu **vermeiden** und **Risiken** zu **minimieren**!

Weitere Bereiche: Erkennung von Malware, Spam, Fake-News, Deep-Fake, usw.
sichere Softwareentwicklung, IT-Forensik, Threat Intelligence, …

Vertrauenswürdigkeit
→ Qualität der Daten

Paradigma



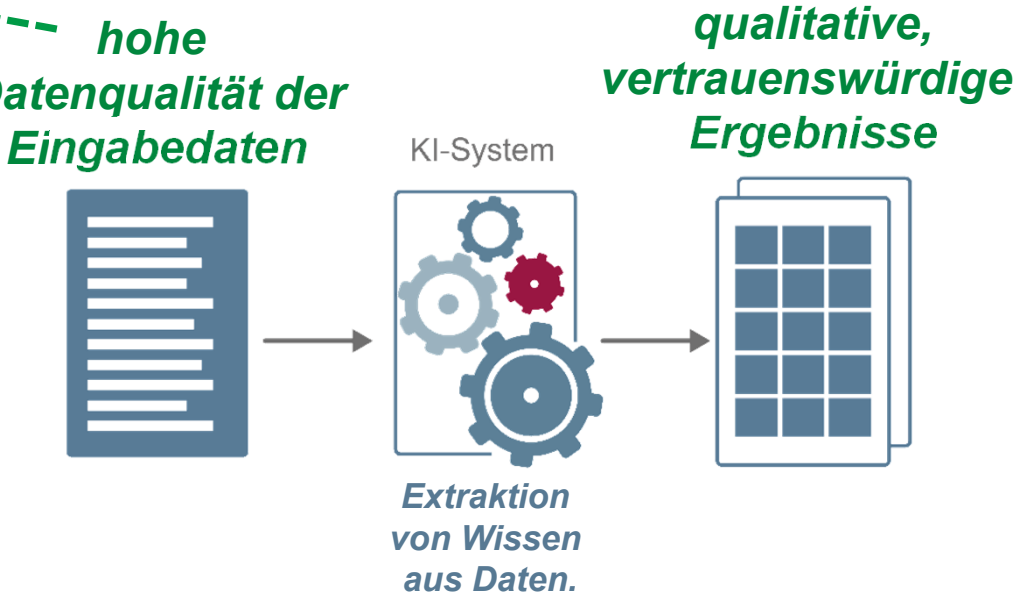
Standards für die Datenqualität:

→ Inhalthöhe der Daten und Korrektheit
→ Nachvollziehbarkeit (Datenquellen)
→ Vollständigkeit und Repräsentativität
→ Verfügbarkeit und Aktualität

Qualitativ hochwertige und sichere **Sensoren** motivieren

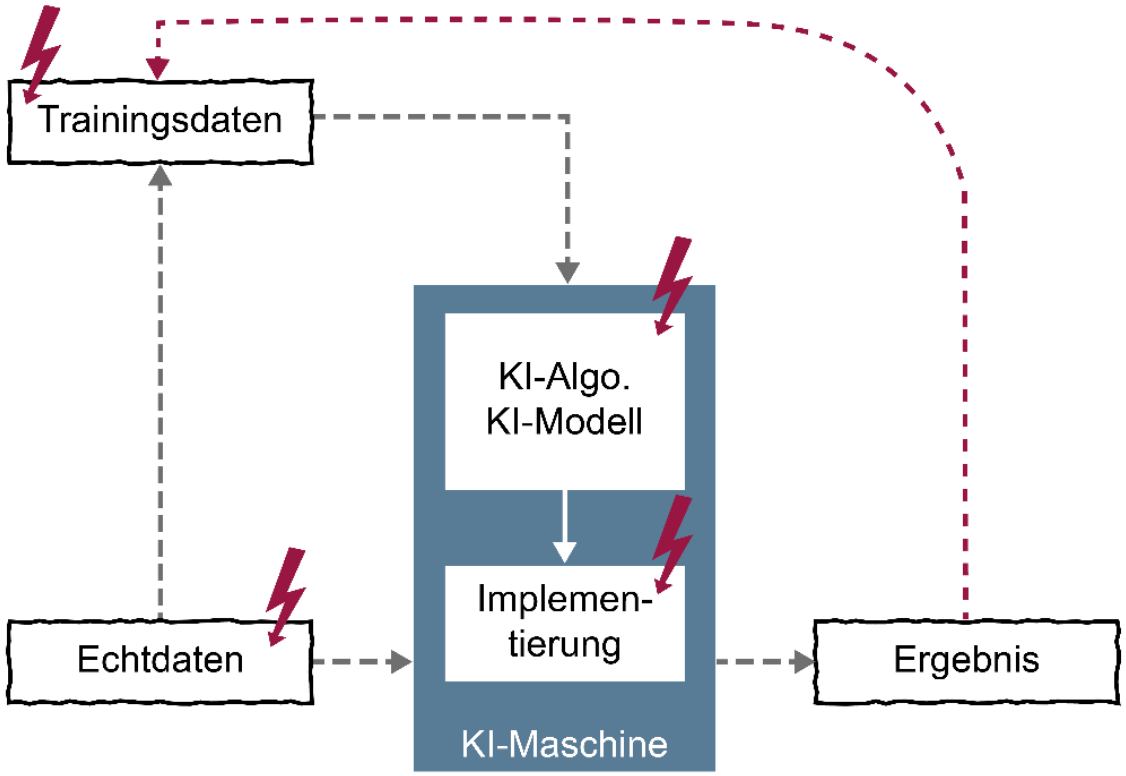
Weitere Aspekte zur Erhöhung der Qualität:

→ Datenpools etablieren
→ **Austausch von Daten fördern**
→ Interoperabilität schaffen
→ Open Data-Strategie puschen



Keine Künstliche Intelligenz ohne → Cyber-Sicherheit

Stand der Technik *an*
Cyber-Sicherheitsmaßnahmen
zum ***Schutz***
→ *der* ***Daten*** *(Training, Echt, Ergebnis),*
→ *der* ***KI-Maschine*** *und*
→ *der* ***Anwendung***



Schutzziele:
→ ***Integrität***
(Erkennen von Manipulation der Daten)
→ ***Vertraulichkeit***
(Wahrung von Geschäftsgeheimissen)
→ ***Datenschutz***
(Schutz von personenbezogenen Daten)
→ ***Verfügbarkeit***
(der Anwendung und Ergebnisse)

Nutzung *einer* ***qualitativ hochwertigen KI-Technologie***
(Evaluierung / Zertifizierung / Souveränität / GAIA-X)

Zusammenarbeit *von* ***erfahrenen KI-*** *und* ***Cyber-Sicherheitsexperten***
(Aufbau / Sicherstellung vom Kompetenzen - Ergebnisse, Ethik, …)

Neue Strategien und Lösungen
→ Mehr Zusammenarbeit statt Separation

Ungleichgewicht bei Angreifern und Verteidigern

Zusammenarbeit hilft das Ungleichgewicht zu überwinden.

- **Echtzeitaustausch** von sicherheitsrelevanten Informationen (Daten) zwischen Wirtschaft, Staat, … **motivieren** *(Vertrauen aufbauen, Kosten und Risiken reduzieren, …)*
- **Erfahrungen** von Reaktionen (Daten) auf Angriffe **austauschen**
- **Gemeinsame Reaktionen** auf Angriffe **umsetzen,** um höhere Effekte zu erzielen und Schäden zu reduzieren …
- **Gemeinsame** Definition und Umsetzung von notwendigen **Cyber-Sicherheitsmechanismen fördern**
- Notwendigkeit einer **Ethik-Diskussion** bei der Nutzung von KI
- …

Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Impulsvortrag

Staat und Wirtschaft gemeinsam für mehr IT-Sicherheit

→ Cyber-Sicherheit braucht Künstliche Intelligenz

→ keine Künstliche Intelligenz ohne Cyber-Sicherheit

*Wir brauchen die Künstliche Intelligenz in der **Cyber-Sicherheit**.*
*Wir müssen die **Risiken** der **KI** aktiv **reduzieren**!*

Prof. Dr. (TU NN)

Norbert Pohlmann

Professor** für **Informationssicherheit
Leiter** des **Instituts für Internet-Sicherheit - if(is)
Vorstandsmitglied** des **Verbands der Internetwirtschaft - eco
Vorstandsvorsitzender** des **Bundesverbands IT-Sicherheit - TeleTrusT

if(is) internet-sicherheit.

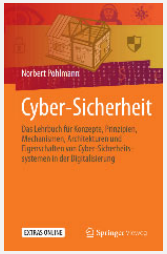
Anhang / Credits

Wir empfehlen

- **Kostenlose App securityNews**

securityNews

- **7. Sinn im Internet (Cyberschutzraum)**
  https://www.youtube.com/cyberschutzraum
- **Master Internet-Sicherheit**
  https://it-sicherheit.de/master-studieren/
- **Cyber-Sicherheit**
  Das **Lehrbuch** für Konzepte, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung“, Springer Vieweg Verlag, Wiesbaden 2019
- https://norbert-pohlmann.com/cyber-sicherheit/



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/

Literatur

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

U. Coester, N. Pohlmann: „Ethik und künstliche Intelligenz – Wer macht die Spielregeln für die KI?“, IT & Production – Zeitschrift für erfolgreiche Produktion, TeDo Verlag, 2019

N. Pohlmann: „Künstliche Intelligenz und Cybersicherheit – Diskussionsgrundlage für den Digitalgipfel 2018“ https://norbert-pohlmann.com/app/uploads/2018/12/Künstliche-Intelligenz-und-Cybersicherheit-Diskussionsgrundlage-für-den-Digitalgipfel-2018-Prof.-Norbert-Pohlmann.pdf

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 978-3-658-25397-4s

Weitere Artikel siehe: https://norbert-pohlmann.com/artikel/