**Cybersecurity & Vertrauen wir der KI zu viel**

* ALLES Belegen mit Literatur oder Fragebogen, keine eigenen Behauptungen Gliederung/Inhaltsverzeichnis
* Literatur organisieren: benutz von Anfang zitiere Plattform -> Citavi (Sammelband wichtig)
* Erste 2-3 Wochen nur lesen
* ~~(parallel Fragebogen laufen lassen ab spätestens 2. Woche)~~
* Einleitung & Fazit am Ende schreiben
* Lofi YTube oder andere zsm. lernen Webseiten -> Motivation (so 7 stunden pro tag/3wochen)
* Scribbr = Rechtschreibprüfung
* zum Ende Korrekturlesen lassen von Mama
* Plagiatsprüfung

**Künstliche Intelligenz in der Cybersicherheit**

*„*Unterstützung im Kampf gegen Hacker oder eine neue Bedrohung*.”*

Saskia Jürgens

Matrikelnr.: 6143565

Betreuer: Tim Laue & Dr. ...

​​

​

​

​

​

​

​

​

​

​

​

​

​

​

​​

Table of Contents

[Einleitung 4](#_Toc190790835)

[Hauptteil 4](#_Toc190790836)

[Grundlagen und Definitionen 4](#_Toc190790837)

[KI und ihre rasante Entwicklung 4](#_Toc190790838)

[Cybersicherheit im Kontext von KI 4](#_Toc190790839)

[KI als Schutz vor Cyberbedrohungen 5](#_Toc190790840)

[Fazit 6](#_Toc190790841)

[Quellenverzeichnis 7](#_Toc190790842)

# Einleitung

* Kurze Einführung in das Thema
* Relevanz von Cybersicherheit und KI in der heutigen Zeit
* Problemstellung und Relevanz des Themas
* Zielsetzung der Arbeit
* Forschungsfrage
* Aufbau der Arbeit

Die rasante Entwicklung der künstlichen Intelligenz (KI) ist oft nützliche, aber auch herausfordernden für die Cybersicherheit. Industrie 4.0 führt in der produzierenden Wirtschaft zu mehr Computertechnologie und mehr Vernetzung – intern und extern. Dabei treffen zwei Welten aufeinander, die Automatisierung (Operational Technology – OT) und Informationstechnologie (IT).

AM ENDE SCHREIBEN!!!

# Hauptteil

## Grundlagen und Definitionen

* **Künstliche Intelligenz (KI)**
* Was ist KI? Grundbegriffe, Typen von KI (schwache vs. starke KI, maschinelles Lernen, etc.)
* **Cybersicherheit**
* Was versteht man unter Cybersicherheit? Schutzziele, Bedrohungen, Risiken
* **Hacking und Scam**
* Erklärung von Hacking-Techniken, Phishing, Social Engineering, Malware

## KI und ihre rasante Entwicklung

* Fortschritte in der KI-Technologie
* Ausblick auf zukünftige Entwicklungen in der KI

## Cybersicherheit im Kontext von KI

Warum ist Cybersicherheit für KI so wichtig?

* Sicherheitsaspekte bei der Entwicklung von KI-Systemen
* Schutz vor Manipulation und Missbrauch von KI
* [Der Einsatz von KI & Robotik in der Medizin - Nomos eLibrary](https://www.nomos-elibrary.de/10.5771/9783748939726/der-einsatz-von-ki-robotik-in-der-medizin?page=1)
* [Künstliche Intelligenz: Wird 2025 das Jahr der KI-Agenten? - ZDFheute](https://www.zdf.de/nachrichten/wissen/kuenstliche-intelligenz-ki-2025-trends-100.html#at_medium=Social%20Media&at_campaign=ZDFheuteApp&at_specific=ZDFheute&at_content=Android)
* [KI-basiertes Virtuelles Testen von Sicherheitskritischen Fahrfunktionen in Kombination mit Realtests | SpringerLink](https://link.springer.com/chapter/10.1007/978-3-658-36430-4_39)
* [Sicherheit trotz KI | Datenschutz und Datensicherheit - DuD](https://link.springer.com/article/10.1007/s11623-023-1799-4)
* [Thieme E-Journals - Gesundheitsökonomie & Qualitätsmanagement / Abstract](https://www.thieme-connect.de/products/ejournals/abstract/10.1055/a-2031-6957)

Herausforderungen der Cybersicherheit im Zeitalter der KI

* Komplexität der KI-Systeme und neue Angriffsvektoren
* KI als Angriffsmittel und als Schutzmittel in Cybersicherheit
* [Manipulierbare KI – Ein unüberwindbares Hindernis für die Sicherheit autonomer Fahrzeuge? | SpringerLink](https://link.springer.com/chapter/10.1007/978-3-658-32266-3_27)
* [Wie KI die Gesetze der Cybersicherheit verschiebt | Das Magazin für Health Professionals – ÖKZ](https://link.springer.com/article/10.1007/s43830-024-0465-y)
* [Künstliche Intelligenz in der Cybersicherheit – zwischen Hype und Notwendigkeit | Wirtschaftsinformatik & Management](https://link.springer.com/article/10.1365/s35764-020-00244-4)
* [Künstliche Intelligenz für die Cybersicherheit - Research Collection](https://www.research-collection.ethz.ch/handle/20.500.11850/417506)
* [Künstliche Intelligenz und Cyber-Sicherheit | SpringerLink](https://link.springer.com/chapter/10.1007/978-3-658-36243-0_15)

## KI als Schutz vor Cyberbedrohungen

* **Wie KI hilft, Scam im Internet zu verhindern**
* Maschinelles Lernen zur Erkennung von Betrug und Phishing
* KI-basierte Sicherheitslösungen zur Überwachung und Früherkennung
* **KI als Werkzeug zur Abwehr von Hackerangriffen**
* Automatisierte Bedrohungserkennung und -analyse
* KI-basierte Firewalls und Intrusion Detection Systeme
* [Microsoft PowerPoint - Cybersicherheit braucht Ku nstliche Intelligenz - IHK - Prof. Norbert Pohlmann - 19\_11\_23](https://norbert-pohlmann.com/wp-content/uploads/2023/12/428-Cyber-Sicherheit-braucht-Kuenstliche-Intelligenz-Prof-Norbert-Pohlmann.pdf)
* Oma-Daisy-KI:
* [Eine KI-Oma gegen Betrug: Wie Künstliche Intelligenz Kriminalität verhindern kann](https://www.rnd.de/wirtschaft/eine-ki-oma-gegen-betrug-wie-kuenstliche-intelligenz-kriminalitaet-verhindern-kann-NDWFQWUHWFDM3P7VTVIM2JGVVY.html)
* [Virtuelle KI-Seniorin bekämpft lästige Scam-Anrufe - Nachrichten - WDR](https://www1.wdr.de/nachrichten/Scam-anrufer-aergern-ki-daisy-telefoniert-100.html)

1. Die dunkle Seite der KI: KI als Angriffsvektor

5.1. KI als Mittel zum Hacken

* Einsatz von KI zur Automatisierung von Angriffen (z.B. Phishing-Angriffe, Password Cracking)
* Exploits und Schwachstellen in KI-Systemen

5.2. Deepfake-Technologie und ihre Bedrohung für Cybersicherheit

* Erstellung und Erkennung von Deepfakes
* Missbrauchsmöglichkeiten von Deepfakes für Betrug und Rufschädigung
* [Neueste Betrugsmasche: Telefonbetrug mittels KI-Deepfake - ZDFheute](https://www.zdf.de/nachrichten/ratgeber/betrugsmasche-telefonbetrug-ki-deepfake-100.html)
* [Wie KI für Kinderpornografie missbraucht wird | tagesschau.de](https://www.tagesschau.de/investigativ/report-mainz/internet-ki-pornografie-kinder-100.html)

5.3. ChatGPT und andere KI-Tools im Cyberbereich

* Möglichkeiten und Risiken bei der Nutzung von KI-basierten Chatbots
* Wie diese Tools sowohl für legitime Sicherheitszwecke als auch für Angriffe missbraucht werden könnten
* [„ChatGPT, generiere mir einen Hackerangriff": Wie Künstliche Intelligenz Cybersicherheit neu definiert. | EBSCOhost](https://openurl.ebsco.com/EPDB%3Agcd%3A11%3A26325915/detailv2?sid=ebsco%3Aplink%3Ascholar&id=ebsco%3Agcd%3A170958464&crl=c&link_origin=scholar.google.com)

1. Zukunftsperspektiven und Handlungsempfehlungen

* Die Balance zwischen Sicherheit und Datenschutz
* Die Rolle der KI in der Zukunft der Cybersicherheit

5.1 Langfristige Herausforderungen in der Cybersicherheit durch KI

5.2 Strategien zur Minimierung von Risiken und Förderung der Resilienz

5.3 Die Rolle von Ethik und Gesetzen im Umgang mit KI

# Fazit

* Zusammenfassung der wichtigsten Erkenntnisse
* Ausblick auf die zukünftige Entwicklung von KI und Cybersicherheit

AM ENDE SCHREIBEN!!!

# Quellenverzeichnis

Universität Bremen Online Bibliothek

* [Wie KI die Gesetze der Cybersicherheit verschiebt | Das Magazin für Health Professionals – ÖKZ](https://link.springer.com/article/10.1007/s43830-024-0465-y)
* [Angriffssicherheit und Manipulationssicherheit bei KI-Systemen | SpringerLink](https://link.springer.com/chapter/10.1007/978-3-658-41935-6_9)
* [Thieme E-Journals - Gesundheitsökonomie & Qualitätsmanagement / Abstract](https://www.thieme-connect.de/products/ejournals/abstract/10.1055/a-2031-6957)
* [Sicherheit trotz KI | Datenschutz und Datensicherheit - DuD](https://link.springer.com/article/10.1007/s11623-023-1799-4)
* [Manipulierbare KI – Ein unüberwindbares Hindernis für die Sicherheit autonomer Fahrzeuge? | SpringerLink](https://link.springer.com/chapter/10.1007/978-3-658-32266-3_27)
* [KI-basiertes Virtuelles Testen von Sicherheitskritischen Fahrfunktionen in Kombination mit Realtests | SpringerLink](https://link.springer.com/chapter/10.1007/978-3-658-36430-4_39)
* [Individualisiertes und adaptives Lernen durch KI in der Arbeitssicherheit](https://sisdigital.de/ce/individualisiertes-und-adaptives-lernen-durch-ki-in-der-arbeitssicherheit/detail.html)
* [Der Einsatz von KI & Robotik in der Medizin - Nomos eLibrary](https://www.nomos-elibrary.de/10.5771/9783748939726/der-einsatz-von-ki-robotik-in-der-medizin?page=1)
* [wiso - Digitaler Stress: Schattenseite der neuen Arbeitswelt](https://www.wiso-net.de/document/HAUF,AHAU,VHAU__9783648177129239)

(Zeitungs-)Artikel:

* [Künstliche Intelligenz: Wird 2025 das Jahr der KI-Agenten? - ZDFheute](https://www.zdf.de/nachrichten/wissen/kuenstliche-intelligenz-ki-2025-trends-100.html#at_medium=Social%20Media&at_campaign=ZDFheuteApp&at_specific=ZDFheute&at_content=Android)
* [Wie KI für Kinderpornografie missbraucht wird | tagesschau.de](https://www.tagesschau.de/investigativ/report-mainz/internet-ki-pornografie-kinder-100.html)
* [ChatGPT und KI: Siegeszug und Sorgen vor Manipulation - ZDFheute](https://www.zdf.de/nachrichten/politik/chatgpt-ki-studie-arbeitswelt-manipulation-100.html#at_medium=Social%20Media&at_campaign=ZDFheuteApp&at_specific=ZDFheute&at_content=Android) [passt nicht mehr zum theama cybersecurity]
* Oma-Daisy-KI:
* [Eine KI-Oma gegen Betrug: Wie Künstliche Intelligenz Kriminalität verhindern kann](https://www.rnd.de/wirtschaft/eine-ki-oma-gegen-betrug-wie-kuenstliche-intelligenz-kriminalitaet-verhindern-kann-NDWFQWUHWFDM3P7VTVIM2JGVVY.html)
* [Virtuelle KI-Seniorin bekämpft lästige Scam-Anrufe - Nachrichten - WDR](https://www1.wdr.de/nachrichten/Scam-anrufer-aergern-ki-daisy-telefoniert-100.html)
* [https://www.zdf.de/nachrichten/ratgeber/betrugsmasche-telefonbetrug-ki-deepfake-100.html](https://deref-web.de/mail/client/M3OQr4QySXc/dereferrer/?redirectUrl=https%3A%2F%2Fwww.zdf.de%2Fnachrichten%2Fratgeber%2Fbetrugsmasche-telefonbetrug-ki-deepfake-100.html)

Google-Scholar

* [Microsoft PowerPoint - Cybersicherheit braucht Ku nstliche Intelligenz - IHK - Prof. Norbert Pohlmann - 19\_11\_23](https://norbert-pohlmann.com/wp-content/uploads/2023/12/428-Cyber-Sicherheit-braucht-Kuenstliche-Intelligenz-Prof-Norbert-Pohlmann.pdf)
* [„ChatGPT, generiere mir einen Hackerangriff": Wie Künstliche Intelligenz Cybersicherheit neu definiert. | EBSCOhost](https://openurl.ebsco.com/EPDB%3Agcd%3A11%3A26325915/detailv2?sid=ebsco%3Aplink%3Ascholar&id=ebsco%3Agcd%3A170958464&crl=c&link_origin=scholar.google.com)

* [Künstliche Intelligenz in der Cybersicherheit – zwischen Hype und Notwendigkeit | Wirtschaftsinformatik & Management](https://link.springer.com/article/10.1365/s35764-020-00244-4)
* [Künstliche Intelligenz für die Cybersicherheit - Research Collection](https://www.research-collection.ethz.ch/handle/20.500.11850/417506)
* [Künstliche Intelligenz und Cyber-Sicherheit | SpringerLink](https://link.springer.com/chapter/10.1007/978-3-658-36243-0_15)