

# KI: Forscher fordern Schutz vor Missbrauch

[Originalartikel](#)

[Backup](#)

<html> <p class=„printversionback-to-article printversion-hide“><a href=„<https://www.heise.de/newsticker/meldung/Kuenstliche-Intelligenz-Forscher-fordern-Schutz-vor-Missbrauch-3975122.html>“>zur&#252;ck zum Artikel</a></p><figure class=„printversionlogo“><img src=„<https://1.f.ix.de/icons/svg/logos/svg/heiseonline.svg>“ alt=„heise online“ width=„180“ height=„40“/></figure><figure class=„aufmacherbild“><img src=„[https://heise.cloudimg.io/width/700/q75.png-lossy-75.webp-lossy-75.foil1/\\_www-heise-de\\_/imgs/18/2/3/7/5/3/7/2/KuenstlicheIntelligenz-5d0165c2d420df20.jpeg](https://heise.cloudimg.io/width/700/q75.png-lossy-75.webp-lossy-75.foil1/_www-heise-de_/imgs/18/2/3/7/5/3/7/2/KuenstlicheIntelligenz-5d0165c2d420df20.jpeg)“ alt=„K&#252;nstliche Intelligenz, Informationsfreiheit“/><figcaption class=„akwa-caption“><p class=„source akwa-captionsource“>(Bild:&#160;iX)</p></figcaption></figure><p><strong>Die KI-Technik sei so weit entwickelt, dass sie eine ernste Bedrohung darstellt, sollten Schurkenstaaten, Kriminelle oder Terroristen sie einsetzen, meinen Experten. Sie &#228;u&#223;ern sich in einer Studie zu m&#246;glichen Gegenma&#223;nahmen und Kontrolle.</strong></p> <p>Internationale Forscher beleuchten in einer Studie den aktuellen Stand von k&#252;nstlicher Intelligenz (KI) und maschinellem Lernen (ML) und gehen der Frage nach, wie diese Technik zum Risiko werden kann, wenn Kriminelle, Terroristen oder Schurkenstaaten sie benutzen. Dabei richtet sich die Sorge der Autoren vor allem auf fortgeschrittene ML-Techniken, die bereits jetzt &#8211; nicht erst in ferner Zukunft &#8211; ohne menschliches Zutun agierten, <strong>berichtet BBC[1]</strong>.</p> <h3 class=„subheading“ id=„nav\_nutzen\_von\_ki1“>Nutzen von KI unbestritten, aber Gefahren ignoriert</h3> <p>Aktuelle KI-Technik sei so ausgereift, dass sie eine Bedrohung darstelle, sollte sie in feindlicher Absicht benutzt werden, legen die Autoren dar. Und die Gefahr eines Missbrauchs sei real, wie j&#252;ngste Beispiele etwa von gezielten Angriffen oder Desinformation zeigten. KI habe unbestritten viele positive Wirkungen, jedoch w&#252;rden die Gefahren bislang kaum thematisiert. Eine Feststellung, die auch j&#252;ngst <strong>auf der M&#252;ncher Sicherheitskonferenz ge&#228;u&#223;ert[2]</strong> wurde.</p> <p>Deshalb fordern die Autoren der Studie Politiker und KI-Spezialisten auf, sich &#252;ber die Eind&#228;mmung der Gefahren durch KI zu verst&#228;ndigen, ohne die Forschung allzu sehr zu beeintr&#228;chtigen. In den falschen H&#228;nden k&#246;nne KI die digitale, physische und politische Sicherheit bedrohen, beispielsweise <strong>durch Cyberattacken[3]</strong>, Dronen und Manipulation. Insbesondere Entwickler m&#252;ssten bereits beim Design von KI-Systemen auf m&#246;glichen Missbrauch achten.</p> <h3 class=„subheading“ id=„nav\_verantwortungsvo2“>Verantwortungsvolle Offenlegung von Schwachstellen</h3> <p>Als konkrete Gegenma&#223;nahmen schlagen die Autoren unter anderem vor, Verfahrensweisen aus der IT-Sicherheit zu &#252;bernehmen wie Schwachstellen verantwortungsvoll offenzulegen (Ver&#246;ffentlichung erst bei Verf&#252;gbarkeit eines Patches). Bei Forschung, Lizenzierung und Freigabe von KI-Technik sollten &#228;hnliche Regelungen wie bei Dual-Use-G&#252;tern erwogen werden.</p> <p>Die 100 Seiten lange <strong>Studie „The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation“[4]</strong> ist als <strong>PDF-Datei[5]</strong> frei verf&#252;gbar. An ihr waren 26 Wissenschaftler sowie Mitglieder wissenschaftlicher und zivilgesellschaftlicher Einrichtungen beteiligt, darunter die Electronic Frontier Foundation, das Future of Humanity Institute, das Centre for the Study of Existential Risks, das Projekt OpenAI, mehrere Universit&#228;ten und der regierungsnahe US-Think-Tank Center for New American Security.</p> <p>Die Studie beruht auf der Forschungsarbeit der Autoren sowie auf Diskussionen des <strong>Workshops „Bad Actor Risks in Artificial Intelligence“[6]</strong> (deutsch etwa: Risiken von KI in Schurkenh&#228;nden), der vom 19. bis 20. Februar 2017 in Oxford stattfand. Die Themen des Workshops waren automatisiertes Hacken,

gezielte Propaganda mit KI-Hilfe und (teil-)autonome Waffensysteme sowie der Umgang von Regierungen mit Besitz und Nutzungsbeschränkung von KI-Technik.

(**tiw[7]**)  

---

**URL dieses Artikels:**  
**Links in diesem**

**Artikel:**  
**[1]** <http://www.bbc.com/news/technology-43127533>  
**[2]** <https://www.heise.de/meldung/Muenchener-Sicherheitskonferenz-Ruf-nach-Debatte-ueber-Risiken-der-KI-3972708.html>  
**[3]** [https://www.heise.de/meldung/Zerstoererischste-Cyber-Attacke-USA-und-Grossbritannien-beschuldigen-Russland-fuer-](https://www.heise.de/meldung/Zerstoererischste-Cyber-Attacke-USA-und-Grossbritannien-beschuldigen-Russland-fuer-NotPetya-3971466.html)

[NotPetya-3971466.html](https://maliciousaireport.com/)  
**[4]** <https://maliciousaireport.com/>  
**[5]** [https://img1.wsimg.com/blobby/go/3d82daa4-97fe-4096-9c6b-376b92c619de/downloads/1c6q2kc4v\\_50335.pdf](https://img1.wsimg.com/blobby/go/3d82daa4-97fe-4096-9c6b-376b92c619de/downloads/1c6q2kc4v_50335.pdf)  
**[6]** <https://www.fhi.ox.ac.uk/bad-actors-and-artificial-intelligence-workshop/>

**[7]** <mailto:tiw@ix.de>  

Copyright © 2019, 2018 Heise Medien

From:  
<https://schnipsl.qgelm.de/> - Qgelm

Permanent link:  
[https://schnipsl.qgelm.de/doku.php?id=wallabag:ki\\_forscher-fordern-schutz-vor-missbrauch](https://schnipsl.qgelm.de/doku.php?id=wallabag:ki_forscher-fordern-schutz-vor-missbrauch)

Last update: 2021/12/06 15:24

