

setzung und Wahrung demokratischer Rechte in Software, Diensten und Infrastrukturen ein. Neben diesen Persönlichkeitsrechten erfordert die neue Situation bezüglich geheimdienstlicher und militärischer Akteure nun jedoch die Stärkung weiterer gefährdeter Werte, wie etwa des internationalen Friedens und der Sicherheit sowie der Unversehrtheit globaler IT-Infrastrukturen. Gleichzeitig müssen Maßnahmen wie die friedliche Nutzung und Weiterentwicklung der Domäne Cyberspace in den zugrunde liegenden technischen Systeme etabliert werden. So stellt sich beispielsweise die Frage, wie das Zerstörungspotenzial von *Cyber-Waffen* begrenzt oder geheimdienstliche und militärische Aktivitäten im Cyberspace transparent und kontrollierbar gestaltet werden können. Während Anonymität für Zivilist:innen im Cyberspace notwendig ist und geschützt werden muss, könnten militärische Netzwerke – also Teilsysteme, die in der Regel durch politische Regeln unterliegen und deren Zweck stark reguliert sind – modifiziert werden, um fremde Netzwerke nachvollziehbar zu machen.

erschienen in der *Fiff-Kommunikation*,
herausgegeben von *Fiff e.V.* - ISSN 0938-3476
www.fiff.de

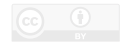
der Nichtverwendung solcher Technologien aussehen, welche die Prinzipien etablierter Regeln und Normen für staatliches Verhalten in dieser Domäne abbilden? Welche messbaren Parameter und Eigenschaften gibt es für Software und Hardware, die für eine Dual-Use-Differenzierung herangezogen werden können? Lassen sich Kriterien finden, um potentiell eher unkritische, defensive Maßnahmen der Cyberverteidigung von solchen Maßnahmen oder Werkzeugen, die auch offensiv gegen Gegner eingesetzt werden, abzugrenzen? Und zu guter Letzt: Wie können Verifikationsmaßnahmen von militärischen Cyber-Fähigkeiten als Grundlage für Vereinbarungen und Verträge aussehen?

Vielleicht gibt es auf viele dieser Herausforderungen keine zufriedenstellenden Antworten. Aber es ist dringend geboten, diese Fragen in den Worten von J. F. Kennedy zu stellen: „Wer, wenn nicht wir?“

Diese Gedankenspiele führen zu einer sehr wichtigen Schlussfolgerung: Wenn es die Informatiker:innen sind, die den Cyberspace gestalten und seine zukünftige Entwicklung entscheidend mitbestimmen, dann sind auch sie es, denen in Anbetracht der oben beschriebenen Herausforderungen die Aufgabe der Entwicklung technischer Lösungsansätze zufällt. Der Schwerpunkt sollte darauf liegen, wie IT gestaltet werden muss, um eine friedliche und sichere Entwicklung des Cyberspace zu ermöglichen. Davon ausgehend ergibt sich eine Vielzahl von Fragen und Herausforderungen, die es zu lösen gilt: Wie können Rüstungskontrolle und Nichtverbreitungskontrolle von Cyberwaffen in der Praxis funktionieren? Wie könnten neue Ansätze zur Sicherung und Kontrolle der Entwicklung, des militärischen Einsatzes und

Anmerkungen

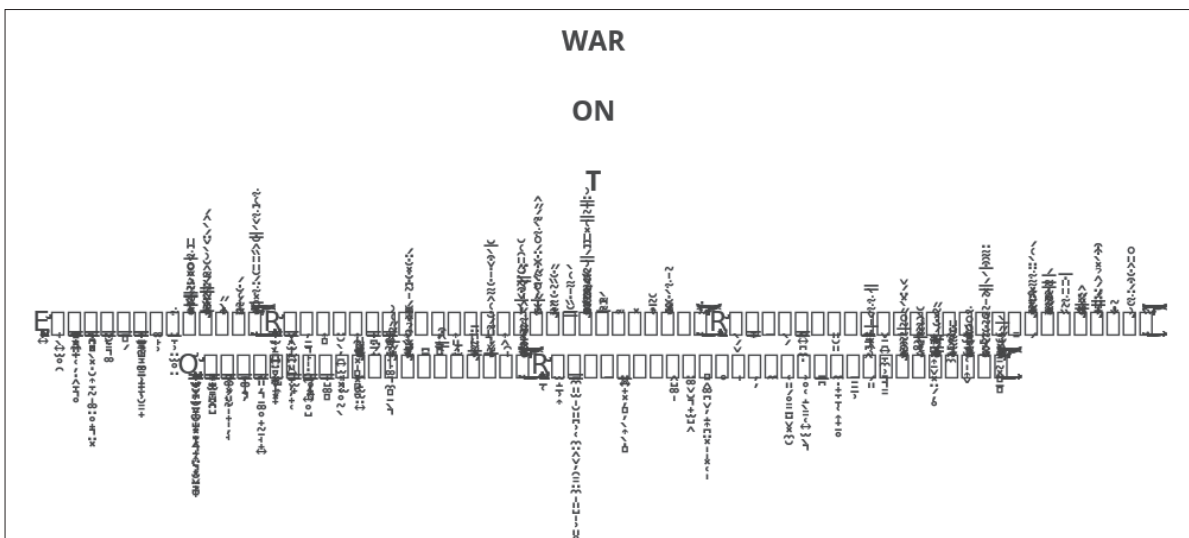
- 1 *Der Cyber-Index – Internationale Sicherheitstrends und Realitäten* <http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf>
- 2 <https://www.bmvg.de/de/themen/cybersicherheit/cyber-verteidigung/entwicklung-des-org-bereich-bei-der-bw>
- 3 *Charta der Vereinten Nationen* – <http://www.unric.org/de/charta>
- 4 *Informationen zur EternalBlue-Sicherheitslücke und zur WannaCry-Schadsoftware-Kampagne* <https://cyber-peace.org/cyberpeace-cyberwar/relevante-cybervorfalle/wannacry-eternalblue/>
- 5 *Informationen zur NotPetya-Schadsoftware-Kampagne* https://cyber-peace.org/cyberpeace-cyberwar/relevante-cybervorfalle/petya_notpetya/



Christian Heck

War on Error

Am 15. August 2021 hatten die militant-islamistischen Taliban praktisch kampflos die afghanische Hauptstadt Kabul eingenommen. Niemand hat damit gerechnet, so Heiko Maas, Bundesminister des Auswärtigen, „das war offensichtlich eine Fehleinschätzung, die die komplette internationale Gemeinschaft, auch ich und die Bundesregierung hatten.“ In der Nacht zum 31. August 2021 verließ die letzte US-Militärmaschine das Land.



Viel zu lange richteten die Geheimdienste der NATO-Verbündeten ihre Blicke auf Zahlen, auf Graphendarstellungen, Heatmaps und Texte statt auf Menschen. Auf Listen und Datenbanken und statistische Auswertungen statt auf den Alltag und die Bedürfnisse gesellschaftlicher Subjekte. Viel zu lange richteten sie ihre Blicke auf Zahlen von Streitkräften, die sie ausbildeten, den Ausbildungsstand, den Ausrüstungsstand anstatt auf Gesellschaft und Kultur derer, die sie im Kampf gegen die Taliban auszubilden versuchten. Viel zu lange richteten sie ihre Blicke auf symbolische Repräsentationen von Menschen. Auf technische Bilder, Mobilfunktelefonnummern, GPS-Daten, auf softbiometrische Datensätze, Lebensmuster und Bewegungsprofile. Auf Daten und Technologien, die nun in nicht zu verachtenden Teilen in den Händen der Taliban liegen¹.

Gleich dem französischen Philosophen Grégoire Chamayou für sein Buch *Ferngesteuerte Gewalt – Eine Theorie der Drohne*² nehmen wir heute eine Reflexion der anarchistischen Philosophin Simone Weil in den 1930er Jahren als Leitfaden:

„Es wäre das denkbar unzulänglichste Vorgehen, sich dem Krieg und den Phänomenen der Gewalt von den Zielen her, die verfolgt werden, zu nähern, als vielmehr auf die durch die Art der eingesetzten Mittel notwendig implizierten Folgen zu untersuchen.“

Die folgenden zehn Beispiele zeigen den Horror und die Perfidie von War on Error.



So sehen wir uns die Waffen etwas genauer an. Ihre spezifischen Eigenschaften. Die Mittel und Wege, die Handlungen bestimmen, durch die man sieht und durch die man tut und die einen beim Denken helfen. Waffen, die letzten Endes auch die Wirkkraft der jeweiligen Handlungen mitbestimmen. Also die Übertragungen von Handlungswissen und Handlungsmacht in diese technischen Objekte hinein und von dort in uns zurück.

Wir fragen uns heute:

Wie wird der Mensch durch diese Technologien verdinglicht? Zu einer materiellen Sache, die benutzt, schlimmstenfalls zerstört werden kann? Zu einem Zeichen?

How to make human machine readable?

Wann wird Töten zu einer technisch-administrativen Maßnahme, wird Mensch zu einer Variablen, die durch eine weitere ersetzt, zu einer Konstanten, die ohne weiteres gelöscht werden kann?

Ab welchem Punkt tastet die Maschinenlesbarmachung gesellschaftlicher Subjekte die Würde des Menschen nicht nur ab, sondern an?

„Gorgon Stare Test uncovers Major Glitches The US Air Force's much-touted new Intelligence, Surveillance and Reconnaissance (ISR) System for use with remotely piloted Aircraft which is developed to be used in Afghanistan has significant operational glitches and is not ready to be fielded, Air Force Field Testers conclude.“³

Bildquelle: „Gorgon Stares operational glitches“, by Christian Heck

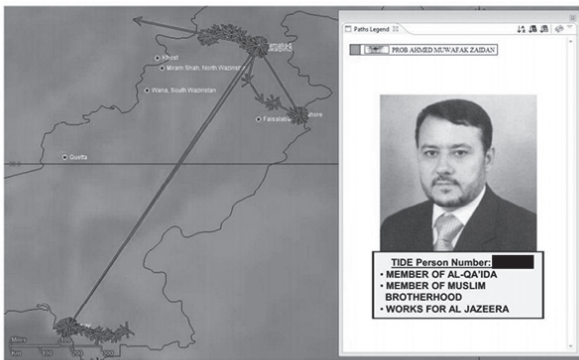
Dynamic Target Storyboard RC(SW) – TFH J3 Tgts – Op STEN TAKAY Obj DOODY – Mullah Niaz Muhammed – IS3673			
Unit: TFH J3 Tgts	Objective: DOODY	ISAF: UGLY 50 conducted a 429 strike on JPEL, UGLY 50 engaged target above and on foot in the open with 100 x 30mm, 1 x WIA.	Engagement Summary: 071017D*FEB11 – UGLY 50, 41R PQ 1768 9260, 1 x AGM-114, 071017D*FEB11 – UGLY 50, 41R PQ 1768 9260, 100 x 30mm.
FOC:	Date of Engagement: 7 Feb 11 (7D)	ISAF No.: IS3673	Missions Employed: 071017D*FEB11 – 1 x AGM-114, 071017D*FEB11 – 100 x 30mm.
Engagement Asset: UK AH-64 CFS UGLY 50	Location: 41R PQ 1768 9260	Description: JPEL, Tgt	Further Details of Tgt Struck: All Targets: LOCAL (D*)
Qualified Observer: WIDOW 87	Function: Mid-level commander and facilitator	Significance: JPEL (D) 3 Tgt	0741 – RELINT strikes Obj DOODY at 41R PQ 1768 9260 in NDACS AD
	Follow-on Plans: Ground CS arrived at engagement site at 1334D* local BDA 1 x EWIA (Obj DOODY), 1 x WIA (local male), 1 x KIA (male child), immediate first aid given to 1 x EWIA and 1 x WIA, with subsequent Casualty at 1344D* 1 x KIA taken to compound by UN for immediate burial.	NET Summary: Obj DOODY is a mid-level commander who operates from NDACS and M3H. He maintains links to CR, KOLAK, from whom he receives direction and Obj STRIKER with whom he is assessed to discuss command matters, particularly TB dispute resolution by verbal means. Obj DOODY is active in planning attacks on CF and NSA OCC. He also directs subordinates to conduct attacks and facilitates the supply of heavy weapons and ammunition. Obj DOODY is a new commander who has been given the responsibility for Subarea by Obj KOLAK.	0560 – Obj DOODY conducts Shura with 5 x adult males at 41R PQ 1768 9260.
Expectation: The removal of Obj DOODY will deny the INS within NDACS and M3H of a competent commander linked into the INS Military Commission. The networks within this area are suffering as a result of recent targeting and IED operations. Carrying the link the commander will further impact on the INS ability to conduct attacks against CF and ANSF and the resupply of weapons.			

Mullah Niaz Muhammed bekam den Namen Doody, die ISAF No. IS3673 und er lebte in 41R PQ 1768 9260, bis zu seiner Ermordung in 41R PR 17897 92491 am 071017D*Feb11 durch eine UGLY 50 .AGM-114, bei welchem versehentlich auch ein KIA (ein kleiner Junge) getötet + 1 WIA (sein Vater) schwer verwundet wurde.

Bildquelle: „Ob DOODY – Mullah Niaz Muhammed – IS3673“⁴

Man nutze **Telefonnummern oder E-Mail-Adressen als Selektoren**, um die Kommunikation von Zielpersonen aus großen Datenströmen herauszufischen; **mit Hilfe der dadurch gewonnenen Informationen sei es dann möglich, diese Personen zu finden, anzuvisieren und umzubringen**. „Man muss schon sehr viel Vertrauen in die dabei eingesetzte Technologie haben“, gab die Quelle, die *The Intercept*, die Leaks zu spielte, zu bedenken. „Ich kenne unzählige Beispiele, bei denen die so gesammelten Informationen fehlerhaft waren.“ Das sei der Hauptgrund für die Tötung unbeteiligter Zivilisten. „Oft entdecken die mit überwachenden Geheimdienstler erst nach Monaten oder sogar Jahren, dass sie die ganze Zeit das Telefon der Mutter der Zielperson überwacht haben.“¹³

TOP SECRET//COMINT//REL TO USA, FVEY
The highest scoring selector that traveled to Peshawar and Lahore is PROB AHMED ZAIDAN



Bildquelle: „SKYNET: Courier Detection via Machine Learning“¹⁴

Ahmad Muaffaq Zaidan wuchs in Syrien auf. Er spricht fließend Arabisch und traf im Zuge einer Reportage Osama bin Laden im November 2000 in Kabul. Einige Monate später wurde er zur Hochzeit von bin Ladens Sohn in Kandahar eingeladen, über die er auch für das Fernsehen berichtete. Nach dem Einmarsch der USA in Afghanistan 2001 wurde Zaidan einer der wenigen Empfänger von Al-Qaida-Videobändern, die in den darauffolgenden zehn Jahren veröffentlicht wurden.

Nach der Logik des Random Forest (der SKYNET-Lern-Algorithmus) ist die Erkennung von Zaidan keineswegs irrtümlich gewesen, im Gegenteil, der Algorithmus hat so funktioniert wie er konzipiert wurde, er erzeugte einen rationalen Selektor auf Basis der Bewegungsmuster der couriers. Er lernte, Teile von Welt durch die Einwirkung von Zufälligkeit zu differenzieren, bzw. zu klassifizieren.

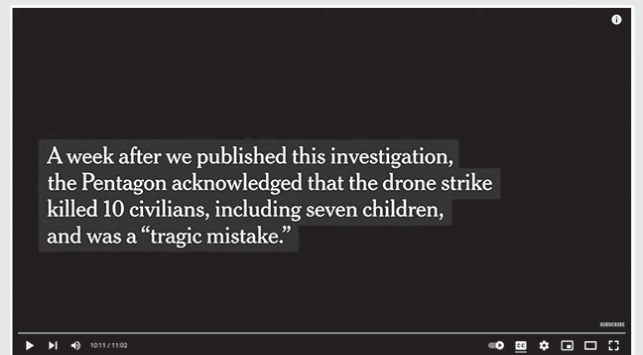


Christian Heck

Christian Heck (Medienkünstler und Graswurzelaktivist) arbeitet als Künstlerisch-wissenschaftlicher Mitarbeiter für *Ästhetik und neue Technologien* an der Kunsthochschule für Medien Köln (KHM). Er unterrichtet dort im Fachbereich *Experimentelle Informatik* und ist Teil der Forschungsgruppe *ground zero – Aesthetics of technics and cognition*. Heck studierte *Künstlerische Arbeit im Kontext der medialen und wissenschaftlichen Bildproduktion* und *Medienkunst* in München, Berlin und den Niederlanden. Seine Masterarbeit beschäftigte sich mit fehlerbehafteten symbolischen Repräsentationen gesellschaftlicher Subjekte durch tradierte und disruptive Bildtechnologien. Er promoviert derzeit bei Georg Trogemann an der KHM über subversive Strategien, die sich an der Schnittstelle zu Politischer Lyrik und Adversarial Attacks (Das Hacken Künstlicher Neuronaler Netze) befinden.



„We see how the war on terror in Afghanistan started and how it is ending now: It's with drones and civilian casualties“, sagt der afghanische Journalist Emran Feroz in einem Interview mit *Democracy Now!* Bereits der allererste Angriff am 7. Oktober 2001 traf nicht Taliban-Chef Mullah Omar, sondern namenlose Afghanen, so Feroz weiter. „Dieses Szenario hat sich stets wiederholt. Bis heute.“¹⁵



Bildquellen: Frames von „How a U.S. Drone Strike Killed the Wrong Person“¹⁶

Dienten die letzten Jahre in Afghanistan als Trial-and-Error-Zone zur Erforschung disruptiver Kriegstechnologien? Zahlreiche technische Fehler und militärische Fehlentscheidungen in dieser neuen Art des High Tech-Krieges legen diesen Verdacht nahe.

Fehler, die dem Design *disruptiver Technologien* immanent sind. Disruptive Technologien werden nicht mehr im Labor erprobt. Sie werden unausgereift in Gesellschaften hineingeworfen. Das ist es, was wir im Moment miterleben. Mitten unter uns findet ihr Trial-and-Error statt – im zivilen Raum, in Kriegsgebieten und in *Combat Zones*. *Dabei ist eine Combat Zone ein Gebiet, das vom US-Präsidenten per Executive Order als ein Gebiet bezeichnet wird, in dem US-Streitkräfte an Kampfhandlungen teilnehmen*

men oder teilgenommen haben. Afghanistan (und der darüber liegende Luftraum) wurde durch Executive Order No. 13239 ab dem 19. September 2001 als Combat Zone ausgewiesen.¹⁷

Etablierte sowie alt eingesessene Firmen setzen zur Leistungssteigerung ihrer bestehenden Produkte (im Sinne eines Fortschritts) auf (in der Gesellschaft) bereits erprobte Technologien, die *sustaining technologies*, so der US-amerikanische Wirtschaftswissenschaftler Clayton Christensen in seinem Buch *The Innovator's Dilemma* (1997). Disruptive Technologien bieten dem Markt ein anderes Wertversprechen. Start-Up-Unternehmen, die *Big* bzw. *New Tech Industries*, insbesondere die Eliten der Künstliche-Intelligenz-Forschung stellen im Vergleich zu nachhaltigen Technologien zwar schlechtere und unausgereifte Produkte her (im Sinne eines Rückschritts also), sie schaffen jedoch gänzlich andere Zielgruppen im Blickfeld und fördern gezielt traditionelle und Mainstream-Kunden im Umgang mit ihren Produkten.

Anmerkungen

- 1 <https://theintercept.com/2021/08/17/afghanistan-taliban-military-biometrics/>
- 2 <https://www.passagen.at/gesamtverzeichnis/thema-3/ferngesteuerte-gewalt/>
- 3 Welsch, William. *Gorgon Stare test uncovers major glitches*. 24.01.2011. URL: <https://defensesystems.com/articles/2011/01/24/gorgon-stare-test-shows-serious-glitches.aspx> (letzter Zugriff 27.10.2021).
- 4 <http://www.spiegel.de/international/world/secret-docs-reveal-dubious-details-of-targeted-killings-in-afghanistan-a-1010358.html>
- 5 Bauman, Zygmunt. *Daten, Drohnen, Disziplin*. Berlin: Suhrkamp. 2013
- 6 Jung, Wolfgang. *Ein Glossar mit Bildern, Dekodierung der Sprache des verdeckt geführten US-Drohnen-Krieges*. 28.10.2015. URL: https://www.luftpost-kl.de/luftpost-archiv/LP_13/LP20015_281015.pdf. Übersetzung des Artikels »A Visual Glossary« von Josh Begley, *The Intercept*, 15.10.2015. URL: <https://theintercept.com/drone-papers/a-visual-glossary/> (letzter Zugriff 27.10.2021)
- 7 <https://theintercept.com/document/2015/10/14/operation-haymaker/>
- 8 Jung, Wolfgang. *Ein Glossar mit Bildern, Dekodierung der Sprache des verdeckt geführten US-Drohnen-Krieges*. 28.10.2015. URL: https://www.luftpost-kl.de/luftpost-archiv/LP_13/LP20015_281015.pdf. Übersetzung des Artikels »A Visual Glossary« von Josh Begley, *The Intercept*, 15.10.2015. URL: <https://theintercept.com/drone-papers/a-visual-glossary/> (letzter Zugriff 27.10.2021)
- 9 <https://theintercept.com/document/2015/10/14/geolocation-watchlist/10> Jung, Wolfgang. *Feuern auf Verdacht, Fehler der Geheimdienste und die Grenzen der Drohnen-Technologie*. 06.11.2015. URL: https://www.luftpost-kl.de/luftpost-archiv/LP_13/LP20015_281015.pdf. Übersetzung des Artikels »Firing Blind« von Cora Currier und Peter Maass, *The Intercept*, 15.10.2015. URL: <https://theintercept.com/drone-papers/firing-blind/> (letzter Zugriff 27.10.2021)
- 11 http://www.luftpost-kl.de/luftpost-archiv/LP_13/LP01613_030213.pdf
- 12 Jung, Wolfgang. *Die Befehlskette für die gezielten Tötungen, Die tödliche Bürokratie hinter Obamas Drohnen-Krieg*. 30.10.2015. URL: https://www.luftpost-kl.de/luftpost-archiv/LP_13/LP20115_301015.pdf. Übersetzung des Artikels »The Kill Chain« von Cora Currier, *The Intercept*, 15.10.2015. URL: <https://theintercept.com/drone-papers/the-kill-chain/> (letzter Zugriff 27.10.2021)
- 13 Jung, Wolfgang. *Der Mordkomplex. Aus geheimen Militärdokumenten geht hervor, wie Obamas Drohnen-Krieg abläuft*. 26.10.2015. URL: https://www.luftpost-kl.de/luftpost-archiv/LP_13/LP19915_261015.pdf. Übersetzung des Artikels »The Assassination Complex« von Jeremy Scahill, *The Intercept*, 15.10.2015. URL: <https://theintercept.com/drone-papers/the-assassination-complex/> (letzter Zugriff 27.10.2021)
- 14 <https://theintercept.com/document/2015/05/08/skynet-courier/>
- 15 Amy Goodman. *U.S. Winds Down Afghanistan Occupation Like It Began, with Drone Strikes & Civilian Casualties*. 30.08.2021. URL: https://www.democracynow.org/2021/8/30/emran_feroz_afghanistan_us_withdrawal
- 16 *The New York Times*, 10.09.2021. URL: <https://www.nytimes.com/2021/09/10/world/asia/us-air-strike-drone-kabul-afghanistan-isis.html>
- 17 <https://www.irs.gov/newsroom/combat-zones>



Der folgende öffentliche Appell gegen die Bewaffnung von Drohnen und für die Ächtung autonomer tödlicher Waffen ist am 1. November 2021 verschickt und veröffentlicht worden. Die Initiative dazu ging insbesondere von Wissenschaftler:innen der University of Oxford aus und mehrere FfF-Mitglieder konnten als Erstunterzeichner:innen gewonnen werden. Der Brief steht jetzt auch auf der Webseite: <https://aiscientists4peace.org/> und kann dort von allen, die wollen, unterschrieben werden. Hoffentlich nutzt das auch etwas.

Die Bewaffnung von Drohnen für die Bundeswehr stoppen – autonome Waffensysteme ächten!

Öffentlicher Appell von Forscher:innen der Künstlichen Intelligenz und Informatik

Sehr geehrte Vorsitzende der Parteien SPD, Bündnis 90/Die Grünen und FDP,
sehr geehrte Verhandlungsführende der Koalitionsverhandlungen,
sehr geehrte Mitbürger:innen der Bundesrepublik,

wir wenden uns als Forscher:innen der Künstlichen Intelligenz und Informatik und als Bürger:innen an die Politik und die Öffentlichkeit, damit die Bewaffnung von Drohnen für die Bundeswehr aus humanitären wie aus sicherheitspolitischen Gründen gestoppt wird.

Als Forscher:innen der Künstlichen Intelligenz (KI) und Informatik sprechen wir uns entschieden gegen autonome Waffensysteme aus, so wie viele Tausend unserer internationalen Kolleg:innen.¹ Eine Maschine „sieht“ einen Menschen nur als eine lange Liste aus Zahlen, und „versteh“ den Wert eines Menschenlebens nicht. Sie