Christian Heck und Hans-Jörg Kreowski

Krieg mit Künstlicher Intelligenz

Bericht über das Online-Hearing am 10. März 2022

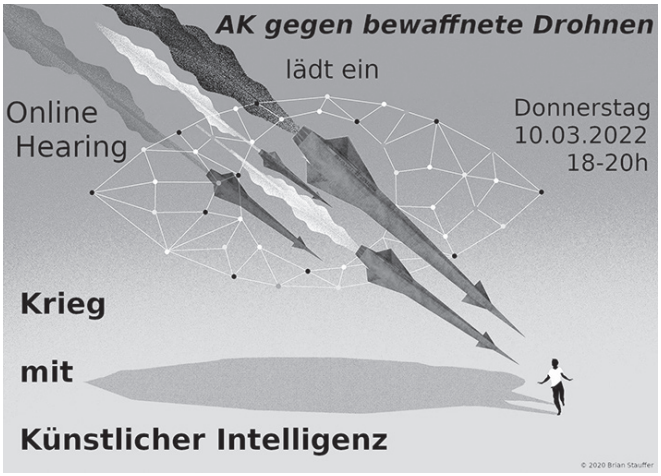
Das bisher letzte in einer Serie von Online-Hearings des Arbeitskreises Gegen bewaffnete Drohnen (http://drohnen.frieden-und-zukunft.de/) hat am 10. März 2022 zum Thema Krieg mit Künstlicher Intelligenz stattgefunden. Im Arbeitskreis arbeiten elf Organisationen der Friedensbewegung zusammen. Bewaffnete Drohnen, die schon seit Jahrzehnten tausendfach eingesetzt werden, sind ein Musterbeispiel für Waffensysteme, die ohne die Nutzung von Künstlicher Intelligenz (KI) undenkbar wären. Aber die Verflechtung von KI und Rüstung reicht weit darüber hinaus.

Viele Regierungen in aller Welt haben in den letzten Jahren nationale Strategien für Künstliche Intelligenz entwickelt, in denen KI zur Schlüsseltechnologie zukünftiger Wertschöpfung erklärt und mit immensen Finanzmitteln gefördert wird. In der Regel ist dabei der Einsatz im militärischen Bereich verschämt ausgeklammert. Tatsächlich aber werden seit Jahrzehnten KI-Methoden für Waffensysteme wie Killerdrohnen und für militärische Plattformen wie Battle-Management-Systeme entwickelt und eingesetzt – mit aktuell wachsender Tendenz. Nach den Plänen der Weltmächte und ihrer Militärs soll Krieg künstlich intelligent werden. Es gibt weltweit erhebliche Anstrengungen, um autonome Waffen und KI-gestützte militärische Planungs- und Entscheidungssysteme zum Einsatz bringen zu können. Es ist zu befürchten, dass die KI-Rüstung mit KI-Waffen (in Verbindung zu staatlicher bzw. universitärer Forschung und Start-Up-Unternehmen) die Gefahr von Kriegen noch einmal erheblich vergrößern wird. Denn durch neuartige *KI-basierte Waffen- und Kriegsführungssysteme wird die Rüstungsspirale weitergedreht, die Rüstungskontrolle erschwert und die Einsatzschwelle auf Grund vermeintlicher Überlegenheit gesenkt.*

Aus diesen Gründen hat ein breites Bündnis der Zivilgesellschaft gegen bewaffnete Drohnen zu einer öffentlichen Online-Debatte eingeladen. Das zweistündige Programm bestand aus acht Kurzvorträgen von je sieben Minuten, so dass etwa gleich viel Zeit für Fragen und Diskussion blieb. Die Vorträge waren in zwei Blöcke aufgeteilt: der erste zu der technologischen und der zweite zu der gesellschaftlichen Dimension des KI-Kriegs.

In den ersten vier Vorträgen wurde ein weiter Bogen vom Stand der Technik in die Zukunftsplanung des KI-Kriegs gespannt. Jakob Foerster (AIScientists4Peace) sprach zu *Der kurze Schritt von bewaffneten Drohnen zu autonomen tödlichen Waffen*, Christoph Marischka (IMI – Informationsstelle Militarisierung) zu *Das gläserne Gefechtsfeld*, Marius Pletsch (DFG-VK) zu *Menschen und Maschinen als Team im KI-Krieg* und Aaron Lye (FIfF – Forum InformatikerInnen f**ü**r Frieden und gesellschaftliche Verantwortung) zu *Künstliche Intelligenz für den Luftkampf der Zukunft*.

Es sind wirklich nur ein paar kurze Schritte, wie es im Titel des ersten Vortrags heißt, von der Forschung an Drohnentechnologie, ihrer Beschaffung und ihrer Ausstattung mit Feuerwaffen hin zu letalen autonomen Waffensystemen (oft abgekürzt durch LAWS für *Lethal Autonomous Weapon Systems*), bei denen die letzte Entscheidung über Leben und Tod einem Computerprogramm übertragen ist. Bei den militärischen Zukunftsplanungen geht es jedoch nicht nur um die KI-gestützte Weiterentwicklung von Waffensystemen sondern auch von entsprechenden



Führungssystemen sowie der Personal- und Materialwirtschaft. Die Integration dieser Elemente führt zu „gläsernen Gefechtsfeldern“ mit der Implementierung ganz konkreter Kriegshandlungen. Eine der besonderen Schwierigkeiten bei dieser neuen Form der Kriegsführung besteht im Zusammenwirken der weitgehend eigenständig agierenden Militär- und Waffentechnik mit den beteiligten Soldat:innen. Die sogenannte Teambildung von Mensch und Maschine ist schon heute ein vieldiskutiertes Problem im Militär. Verschärft wird es zutage treten bei der Entwicklung des neuen deutsch-französisch-spanischen Kampfflugzeugs *(Future Combat Air System, kurz FCAS)*, das bis 2040 fertiggestellt sein soll und einschließlich Beschaffung Hunderte Milliarden Euro verschlingen wird. Bei FCAS soll ein KI-System dafür sorgen, dass ein Netz aus Kampfflugzeugen der sechsten Generation, Drohnenschwärmen, Satellitenanlagen und Cloud-Services reibungslos ineinandergreift. Vieles, was in diesem Bereich passiert und geplant ist, bleibt bisher für Außenstehende unsichtbar, eine öffentliche Debatte darüber ist aber dringend geboten.

Im zweiten Block trug Elke Schwarz (Queen Mary University of London) vor zu *Silicon Valley macht Krieg*, Jacqueline Andres (IMI – Informationsstelle Militarisierung) zu *No Cyber Valley und die Ökonomie der Angst*, Thomas Reinhold (PEASEC – Wissenschaft und Technik für Frieden und Sicherheit) zu *Die Militarisierung von KI und die Probleme für die Rüstungskontrolle* sowie Edwick Madzimure (WILPF – *Women's International League for Peace and Freedom Zimbabwe*) zu *Warum sich Frauen im globalen Süden gegen autonome Waffen engagieren*.

Ziel des zweiten Blocks war, einige tiefgreifende gesellschaftliche Dimensionen vorzustellen und zu versuchen, sie so zu konkretisieren, dass sie öffentlich debattiert und diskutiert werden

können. Dazu gehört, die Rolle der aktuellen KI-Forschung und des Militarismus für den Klimawandel und ihren Einfluss auf die Wirksamkeit von Grassroots-Bewegungen und den Lebensalltag für die Bevölkerung im globalen Süden zu untersuchen. Dazu gehört auch, in deutschen Städten die Folgen dieser Forschung auf die Straße zu bringen, wie es unter anderem das Bündnis gegen das *Cyber Valley* in Tübingen seit ein paar Jahren tut. Es geht um gesellschaftliche Konsequenzen, die durch den Bau von Komplexen wie dem Cyber Valley im Neckartal eintreten. Solche von öffentlichen Geldern geförderte Forschungscluster, die der Verschmelzung von freier Grundlagenforschung mit der Industrie und insbesondere mit Start-Up- sowie Rüstungsunternehmen dienen, entstehen seit einigen Jahren in weiten Teilen Europas, und sie stehen nicht nur in der Wahl ihrer Namensgebung dem Silicon Valley sehr nahe. Es geht konkret darum, differenziert zu zeigen, wie einzelne Instanzen des Silicon Valleys zu Kriegen unseres Jahrtausends beitragen, andere sich dem auch verweigern.

Das Hearing fand auf der datenschutzfreundlichen BigBlueButton-Instanz *senfcall.de* statt. Die Videokonferenzplattform ist eine Initiative von Studierenden vor allem aus Karlsruhe und Darmstadt, die eine datensparsame und sichere Alternative zu bekannten Konferenzsystemen bietet. Der Service ist DSGVO-konform und datensparsam, d. h. senfcall.de erhebt nur die Daten, die auch für den Service nötig sind. Alle Daten werden auf Servern in Deutschland verarbeitet. Das System hat mit den 90 Teilnehmerinnen und Teilnehmern einwandfrei funktioniert, so dass es für derartige Veranstaltungen sehr empfehlenswert ist.

Die Vorträge wurden von Ting Chun Liu mit der Open Source Software OBS-Studio aufgezeichnet und geschnitten. Die Video-Mitschnitte sind zu finden unter *https://media.ccc.de/c/kriegundki* und *https://vimeo.com/690465548*.

Die Begrüßung haben Christian Heck und Hans-Jörg Kreowski (FIfF – Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung) übernommen, moderiert haben Angelika Wilmen und Susanne Grabenhorst (IPPNW – Internationale Ärzt:innen für die Verhütung des Atomkrieges), Reiner Braun (International Peace Bureau) hatte das Schlusswort.

Dank des breiten Spektrums an interessanten Vorträgen ist die Veranstaltung gut angekommen. Die Diskussion hat gezeigt, dass der Informationsbedarf zum Thema Künstliche Intelligenz und Krieg groß ist und alle friedlich gesonnenen Menschen noch lange beschäftigen wird. Teilweise im direkten Zusammenhang mit den Vorträgen, aber insgesamt mit engem thematischen Bezug sind Ende 2021 von Hans-Jörg Kreowski und Aaron Lye zwei Publikationen unter dem Titel *Künstliche Intelligenz zieht in den Krieg* herausgegeben worden, erschienen als Dossier 93 der Zeitschrift Wissenschaft und Frieden und als Schwerpunkt der *FIfF-Kommunikation* 4/2021.

Das Hearing sollte dazu beitragen, ein Stück weit Einblicke in die gesellschaftlichen und in die technologischen Dimensionen von zukünftigen, aber auch von ganz aktuellen High-Tech-Elementen konventioneller Kriege zu gewinnen. High-Tech in Form von Killerdrohnen, Präzisionslenkwaffen, netzwerkzentrierten Kriegsführungstaktiken, Cyberattacken und Informationskrieg ist auch derzeit im Ukraine-Krieg wirksam, wenn auch für die Öffentlichkeit eher im Verborgenen. Einblicke in Kriegstechnologien zu gewinnen ist eine wichtige Basis der Friedensarbeit in Zeiten des Krieges – Kriege, in denen immer Menschen sterben: Soldat:innen und Zivilist:innen, Eltern und Kinder. Um Einblicke in die Rolle der „neuen" Technologien und in ihre Funktion im Kontext der Grausamkeiten des Krieges zu erlangen, ist es wichtig, sich ein bisschen tiefer in diese kognitiven Systeme hineinzudenken und ein Stück weit sehen zu lernen, in welchem Maße diese technischen Objekte und künstlich intelligenten Systeme unterstützend wirken beim Treffen von menschlichen Entscheidungen.

Aaron Lye

Quantenschlüsselverteilung: Von Glasfaser zu Satelliten

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

Seit einigen Jahren wird wieder vermehrt über Quantencomputer berichtet. Die Entwicklung dieser Computertechnik wird aktuell weltweit massiv vorangetrieben und Milliardengelder fließen in die Erforschung und Entwicklung dieser Technologie – auch in Deutschland. Die Bundesregierung hat 2021 Fördergelder in Höhe von insgesamt zwei Milliarden Euro für die Entwicklung von Quantencomputern freigege[illegible] argumentiert wird das mit der industriellen Nutzung dieser Te[illegible]tion, dem Lösen von schweren kombinatorischen Problemen (z[illegible]gen dieser Technologie auf die Kryptographie (Verschlüsselung) [illegible]yptographie und die Raumfahrt untrennbar mit Geheimdiensten, Militär und Rüstungsindustrie verbunden. Die im Folgenden dargestellten Entwicklungen im Bereich der Quantenverschlüsselung haben daher immer auch geheimdienstliche und militärische Relevanz.

Quantencomputer nutzen quantenmechanische Eigenschaften und arbeiten deshalb anders als klassische Computer. Dies ist bemerkenswert, da mit diesen Rechnern bestimmte Probleme schneller berechnet werden können. Zu diesen Problemen gehören jene, auf die wir aktuell bei Verschlüsselung vertrauen. Das ist seit 1994 in Fachkreisen bekannt (und führte zu einem Schub dieser Technologie). Wenn es gelingt, entsprechende Quantencomputer zu bauen, dann sind wesentliche, weltweit täglich und viel genutzte Verschlüsselungsverfahren unsicher. Und da Kommunikation abgehört und gespeichert werden kann, kann sie auch nachträglich entschlüsselt werden. Aus diesem Grund wird nach neuen Verschlüsselungsverfahren gesucht, die von Quantencomputern nicht effizient berechnet werden können. Ein Ansatz ist, quantenmechanische Eigenschaften ebenfalls für Verschlüsselung zu verwenden. Photonen (Lichtteilchen) haben diese Eigenschaften und lassen sich einfach kontrolliert