XINHUA/IMAGO

Der Tod von oben ist immer häufiger »KI«-gestützt: Graffiti gegen die Killerdrohnen am Himmel über Jemen (Sanaa, 6.11.2013)

Neue Technologien für neue Kriege

Auf dem Schlachtfeld der Zukunft ist Hightech ein entscheidender Faktor. **Von Christian Heck**

Mit der »Industrie 4.0«, dem »Web 4.0« und »Krieg 4.0« haben sich in den letzten Jahren Cyber-, Kriegs- und Sicherheitslogiken mit unserem zivilen Lebensalltag verwoben. Kommerzielle Sprachtechnologien à la Chat-GPT verschmelzen mit digitalen Führungssystemen des Militärs; Bildtechnologien wie Gesichtserkennungssoftware mit Assistenzsystemen für Kampfpiloten; Cloud-Dienste mit Zielerkennungs-, bzw. Identifikationssoftware und Big-Data-Logiken gestalten algorithmische Entscheidungsunterstützungssysteme zur »gezielten Tötung«.

Es entstand eine lukrative Zusammenarbeit von unterschiedlichsten Akteuren. Bei einem Forschungsprojekt der Bundeswehr namens »Ghostplay« z. B. arbeitet das Startup 21 Strategies mit dem Rüstungsunternehmen Hensoldt, dem Beratungsunternehmen Borchert und dem Defence AI Observatory (DAIO) der Helmut-Schmidt-Universität zusammen an einem Simulationssystem zur »»KI«-basierten Entscheidungsfindung in Maschinengeschwindigkeit«. »Ghostplay« soll Daten schneller auswerten und aufarbeiten können, so dass Soldaten mehr Zeit bekommen, »ethische und informierte Entscheidungen zu treffen« – so die militärische Vision von Gary Schaal, dem Leiter des Forschungsprojekts.

Aus eben jener technisch-militärischen Notwendigkeit, in »Maschinengeschwindigkeit« handeln zu müssen, ist der Trend zur Forschung an immer ausgefeilteren Technologien zur Mensch-Maschine-Interaktion rasant gestiegen. Im selben Moment ist die Hemmschwelle, sich bei multidomänen Operationen (MDO), also mehrere Bereiche übergreifenden Operationen, auf diese Systeme zu verlassen, aber auch drastisch gesunken.

MDO erreicht derzeit im Zuge der für 2026 vorgesehenen Stationierung von US-Mittelstreckenraketen in Deutschland die breite Öffentlichkeit. Während SPD-Verteidigungsminister Boris Pistorius von »Abschreckungsfähigkeit« und einem Nachholen militärischer Fähigkeiten spricht, sieht die US-Regierung darin ein »organisatorisches Herzstück« für die »nationale Sicherheit der USA«. Unter anderem in Wiesbaden soll ein entsprechender Verband stationiert werden: die »Multi-Domain Task Force« (MDTF). Auch die am 4. April vorgestellte Strukturreform der Bundeswehr baut auf dem MDO-Konzept auf und setzt auf »komplexe militärische Operationen zu Land, zu Wasser, in der Luft, im Weltraum und im Cyberraum«, d. h. dem Internet, auch dem der Dinge.

Letztere waren noch nie vom Militär trennbar. Der Begriff »Internet of Military Things« (IoMT), also das »Internet der Militärdinge«, fasst die Verschmelzung präzise und hält begrifflich fest, wie sich Drohnen, Satellitensysteme, Clouds, intelligente Waffen, autonome Systeme und »KI«-gestützte digitale Führungssysteme (Battle Management Systeme (BMS)) als Ableger aus militärischer und ziviler Forschung entwickelt haben.

Ursprünge dieses »organisatorischen Herzstücks« sind in der letzten sogenannten Revolution in Military Affairs, dem »Network Centric Warfare« (auf Deutsch in etwa »netzwerkzentrierte Kriegführung«) der späten 90er Jahre, zu finden. Diese trieb die Forschung an technologischen Innovationen zur Vernetzung von Informations- und Aufklärungssystemen voran. Der zweite Golfkrieg war das erste Testfeld für den neuen Ansatz. Zur selben Zeit wurden diese Logiken als netzwerkanalytische bzw. soziometrische Verfahren beispielsweise durch Algorithmen auch im Netz erforscht. Im Jahr 1998 versuchte Google potentielle Nutzer auszumachen, ihr zukünftiges Verhalten vorherzusagen und seiner Marktlogik entsprechend zu manipulieren.

Dank Edward Snowden und weiteren Whistleblowern wissen wir heute, wie eng und effektiv Militär, Geheimdienste und IT-Unternehmen zusammenarbeiten. Auch die Bezeichnung für diese ganz spezielle Art, Daten für den jeweiligen Zweck zu deuten, wurde im Zuge der globalen Überwachungsaffäre einem breiteren Publikum bekannt: Metadaten. Dabei handelt es sich quasi um Muster, die unter anderem im »Krieg gegen den Terror« errechnet wurden, um algorithmisch »unknown knowns« (Donald Rumsfeld) aufzuspüren, sprich »unbekannte Terroristen«, deren möglicherweise bevorstehender Anschlag bestenfalls vorbeugend verhindert werden solle. Eine Praxis, die im militärischen Jargon als »Targeted Killing«, also »gezieltes Töten« bezeichnet wird. Sie steht repräsentativ für den Drohnenkrieg: Gezieltes Töten, das als sicherheitspolitische Farce den Glauben schürte, immer ausgefeiltere Waffensysteme, wie präzisionsgelenkte Munition, könnten Zivilisten schützen.

Das Gegenteil ist der Fall. In 20 Jahren Afghanistan-Krieg fielen Tausende Zivilisten dem Drohnenkrieg zum Opfer. Auch in Gaza wird der Welt vor Augen geführt, was »Präzision« bedeutet, wenn Schulen, Krankenhäuser, Hilfskonvois und Wohnhäuser teils flächendeckend bombardiert werden, um einzelne Hamas-Kämpfer zu töten. Dies geschieht unter anderem mittels »KI«-gestützter Systeme wie »Lavender«. Dieses wurde nach dem 7. Oktober vom israelischen Militär eingesetzt, um Kämpfer der Hamas und des Islamischen Dschihads auf Basis von Metadaten zu identifizieren und Todeslisten zu erstellen, um daraufhin in kürzester Zeit zu entscheiden, ob ihre Wohnhäuser mit Drohnen bombardiert werden sollen oder nicht. »Lavender« setzte auf Basis von Metadaten bis zu 37.000 Palästinenser auf die algorithmisch erstellte Liste, so ein von *+972 Magazine* interviewter Soldat der israelischen Armee.

Wie genau die Listen erstellt wurden, steht unter Geheimhaltung. Doch auch wenn wir freien Zugang zu diesem System hätten, könnten wir die Frage nicht beantworten. Selbst in formalen Sprachen ist es derzeit nicht möglich, die inneren Verhaltensweisen von Systemen »künstlicher Intelligenz« nachzuvollziehen, geschweige denn, sie in Alltagssprache verständlich zu erklären. Weder Verhältnismäßigkeit noch Nachvollziehbarkeit von militärischen Operationen, die auf Grundlage »KI«-gestützter Systeme durchgeführt wurden, können in Hightechkriegen gewährleistet werden. Aus friedenspolitischer Perspektive sollte man prüfen, inwieweit solche »KI«-gestützten Praxen der »gezielten Tötung« als Kriegsverbrechen betrachtet werden müssen, wie es Experten im Bereich der Informatik und unbemannten Waffensystemen unlängst gefordert haben.

Christian Heck lehrt und forscht seit 2017 an der Kunsthochschule für Medien Köln (KHM)