Hans-Jörg Kreowski

Unbemannte Waffensysteme – nicht ohne Informatik

Die deutsche Verteidigungsministerin Ursula von der Leyen hat laut Medienberichten vor kurzem angekündigt, dass die Bundeswehr bewaffnungsfähige Drohnen anschaffen und Deutschland zusammen mit Frankreich und Italien eine eigene Kampfdrohne entwickeln will. Als kurzfristige Lösung ist wohl an die amerikanische Drohne Reaper *gedacht. Diese Nachricht sollte nicht nur alle friedliebenden Menschen in Deutschland alarmieren, sondern insbesondere auch alle Informatikerinnen und Informatiker. Ohne den Beitrag der Informatik wären unbemannte Waffensysteme nach Art der Kampfdrohnen völlig undenkbar.*

Ein Blick über den großen Teich

Die Entwicklung unbemannter Waffensysteme ist in den USA am weitesten fortgeschritten und durch diverse Quellen öffentlich zugänglich dokumentiert. Das US-amerikanische Verteidigungsministerium plant nach dem 160-seitigen Konvolut *Unmanned Systems Integrated Roadmap FY 2013-2038* einen erheblichen Teil der Bewaffnung der US-Streitkräfte in der Luft, am Boden sowie auf dem und unter Wasser auf unbemannte Systeme umzustellen. Ein Teil dieser Entwicklung ist bereits seit einiger Zeit im Gange, wie der 1000-fache Einsatz von Kampfdrohnen in Afghanistan, Pakistan und dem Jemen zeigt.

Was macht unbemannte Systeme für das Militär interessant?

In der Roadmap werden drei Attribute als Antwort genannt: *dull, dirty, dangerous.* Ein unbemanntes System mit Kamera und anderen Sensoren kann eine Szene stunden- und tagelang beobachten, ohne zu ermüden, abgelenkt zu werden oder auf dumme Gedanken zu kommen, auch wenn die meiste Zeit nichts passiert und die Aufgabe total langweilig ist. Ein unbemanntes System kann sich „unbeschadet" und mit vergleichsweise geringem Risiko in einem biologisch, chemisch oder nuklear verseuchten Gebiet aufhalten und agieren. Ein unbemanntes System kann viel unbedenklicher einer gefährlichen Situation ausgesetzt werden als ein Soldat oder eine Soldatin. Es kann einsturzgefährdete Gebäude inspizieren, es kann durch Gegenden fahren, die von Heckenschützen bedroht sind, es kann in Kampfhandlungen einbezogen werden, ohne dass direkt eigene Gefallene zu beklagen sind, sondern höchstens „Blechschaden". Für den Gegner bleibt das gefährlich, und genau genommen wird die Gefahr lediglich verlagert, denn während an der einen Stelle unbemannte Systeme schießen, jagen sich an anderer Stelle Selbstmordattentäter in die Luft.

In der Roadmap wird noch ein weiterer wichtiger Grund genannt, der sich durch das ganze Dokument zieht: das Geld. Unbemannte Systeme sind kleiner, leichter, weniger gepanzert als entsprechende bemannte Systeme und deshalb billiger. Sie werden angesichts nicht mehr allzu stark wachsender oder sogar sinkender Rüstungsetats als eine Option betrachtet, militärische Stärke und Überlegenheit zu wahren trotz knapper Kassen.

Und noch ein Argument spielt bei der Entwicklung unbemannter Waffensysteme eine wichtige Rolle: die Entwicklung unbemannter Waffensysteme. Einmal in die Welt gesetzt, folgen viele andere Länder der Welt dem US-amerikanischen Beispiel. Ein gigantisches Wettrüsten ist entbrannt. Die USA wollen gemäß ihrer spätestens seit dem Ende des Zweiten Weltkriegs herrschenden Allmachts- und Weltbeherrschungsphantasie auf allen technologischen Gebieten mit Priorität für die Kriegstechnik überlegen sein. Die Führungsposition ist aber nur dann zu halten, wenn man massiv weiter aufrüstet.

Sind unbemannte Waffensysteme kriegstauglich?

Wenn der Einsatz von Kampfdrohnen in den letzten zehn Jahren in Afghanistan, Pakistan, Jemen und Somalia typisch ist dafür, wie auch zukünftig unbemannte Waffensysteme verwendet werden, lässt sich Folgendes festhalten:

1. Sie dienen gezielten Tötungen *(targeted killings)*, bei denen bestimmte Personen anhand von Todeslisten aufgespürt, angegriffen und „ausgeschaltet" werden.

2. Sie dienen sogenannten *signature strikes*, bei denen Personen einzeln oder in Gruppen ins Visier genommen und getötet werden, weil sie nach einer Checkliste verdächtig aussehen oder sich verdächtig verhalten.

3. Sie bringen viele zivile Tote mit sich, weil die Zielpersonen nach den Punkten 1 und 2 selten allein angetroffen werden, sondern sich in normalen Wohnräumen, auf öffentlichen Plätzen, im Kreis ihrer Familie oder bei Freunden aufhalten, und weil die Zielpersonen nach Punkt 2 tatsächlich selbst oft Zivilpersonen sind.

Tötungen von Menschen nach den Punkten 1 bis 3 sind nach dem humanitären Völkerrecht Kriegsverbrechen und deshalb ethisch völlig unvertretbar.

Hans-Jörg Kreowski

Prof. Dr. **Hans-Jörg Kreowski** ist Leiter der Forschungsgruppe *Theoretische Informatik* an der Universität Bremen. Von 2003 bis 2009 war er Vorsitzender des FIfF.

Gladiator Tactical Unmanned Ground Vehicle at Redstone Arsenal, Gladiator des United States Marine Corps

Von diesem Umstand ist, was wohl nicht wirklich überrascht, in der Roadmap nicht die Rede. Dort wird davon ausgegangen, dass unbemannte Systeme die Möglichkeiten der Kriegführung wesentlich erweitern. Wenig bis gar nichts findet sich zu den Einsatzgrenzen dieser Waffen. Beispielsweise wird kaum darauf eingegangen, dass heute verfügbare Drohnen von Luftabwehrsystemen leicht abgeschossen werden können, sodass Einsatzgebiete nur dort liegen, wo Luftabwehr fehlt.

Nicht ohne Wissenschaft und Technik, nicht ohne Informatik

Um unbemannte Waffensysteme bauen zu können, werden die Erkenntnisse und Hervorbringungen vieler wissenschaftlicher und technischer Bereiche benötigt: Materialforschung, Optik, Sensorik, Nachrichtentechnik, Ballistik, Maschinenbau und andere mehr. Ohne die Beiträge der Informatik käme man allerdings nicht sehr weit. Jedes System benötigt einen eingebetteten Computer, auf dem die eingehenden Daten aller Sensoren gesammelt, zusammengeführt, aufbereitet, interpretiert, ausgewertet und zu Kommandostationen übertragen werden. Durch den Bordcomputer werden alle Geräte einschließlich der Waffen gesteuert. Die Kommandostation verfügt notwendigerweise auch über ein Computersystem, mit dem die vom unbemannten System eingehenden Daten aufbereitet und ausgewertet werden, soweit das nicht bereits auf dem unbemannten System selbst erfolgt ist. Auf der Basis der enthaltenen Daten entscheidet der Kommandeur dann über den nächsten Waffeneinsatz.

In der Roadmap sind in Kapitel 4 – *Technologies for Unmanned Systems*, das mit über 50 Seiten längste – bestehende technologische Lücken und offene Forschungsfragen ausführlich dargelegt. Es werden sechs Problembereiche beschrieben:

- Interoperability and Modularity,
- Communication Systems, Spectrum and Resilience,
- Security: Research and Intelligence/Technology Protection (RITP),
- Persistent Resilience,
- Autonomy and Cognitive Behavior,
- Weaponry.

Bei der *Interoperabilität* und der *Modularität* geht es darum, dass der Datenaustausch zwischen den verschiedenen Komponenten (insbesondere Sensoren und Bewaffnung) innerhalb eines unbemannten Systems sowie zwischen unbemannten und bemannten Systemen reibungslos funktioniert, trotz unterschiedlicher Datenformate und ständiger Fortentwicklung der Sensor- und Waffentechnologie sowie der algorithmischen Prozesse.

Die heutigen unbemannten Systeme sind extrem abhängig von *Kommunikationssystemen*, wobei die Funktionsfähigkeit der Kommunikationslinks, ihre Bandbreite, ihr Frequenzspektrum und ihre Härtung gegen jede Art von Interferenz signifikant sind.

Unbemannte Systeme sind in der Regel mit kritischen Programmen und klassifizierten (d. h. geheim zu haltenden schutzwürdigen) Daten ausgestattet, um ihre Aufgaben erledigen zu können. Deshalb spielen *Sicherheitsmaßnahmen* eine wesentliche Rolle, um unautorisierten Zugriff zu vermeiden, unabsichtliche Offenlegung der Daten zu verhindern und die technologische Überlegenheit zu wahren.

Persistenz verweist auf die Verkleinerung, Gewichtsreduktion, Energieersparnis und verbesserte Kühlung bei gleichzeitiger Erhaltung von Zuverlässigkeit, Wartbarkeit und Lebensdauer. Unbemannte Systeme besitzen ein erhebliches Potenzial in dieser Hinsicht.

Praktisch alle im Einsatz befindlichen unbemannten Systeme bedürfen der aktiven Kontrolle durch geeignetes Personal bei der Analyse gesammelter Daten und der Planung und Durchführung von Steuerung und Waffengebrauch. Da vor allem Personalkosten das Budget des *U.S. Department of Defense* belasten, hat die Entwicklung *autonomer Waffensysteme* höchste Priorität. Autonomie bedeutet dabei, dass die Systeme selbst die Signifikanz der gesammelten Informationen erkennen und eigenständig über weitere Aktionen entscheiden, ohne dass Menschen direkt eingreifen. Die Entscheidung über Leben und Tod wird also auf die Maschine verlagert, wobei aber Autonomie technisch zu verstehen ist. Das autonome Waffensystem wird programmierte Entscheidungsalgorithmen ausführen. In dieser Phase greift der Mensch nicht ein, aber die Algorithmen stammen immer noch von menschlichen Akteuren.

An Unmanned Surface Vehicle demonstration at Hampton, Virginia, January 2009, U.S. Navy photo by Mass Communication Specialist Seaman Apprentice Joshua Adam Nuzzo

Bei der *Bewaffnung* geht es darum, Waffen und unbemannte Plattformen aufeinander abzustimmen, spezifische Waffen und neue Munition für unbemannte Systeme zu entwickeln und perspektivisch auch Waffen auf der Basis der Nanotechnologie zur Verfügung zu stellen. Es wird davon ausgegangen, dass die Weiterentwicklung der Bewaffnung davon abhängt, ob die vorgenannten Technologien zum Durchbruch gebracht werden.

Auch wenn die Analyse der militärischen Wünsche an Wissenschaft und Technik viel vertiefter und detaillierter durchgeführt werden müsste, um verlässliche Schlussfolgerungen zu treffen, zeichnet sich auch schon bei einer ersten flüchtigen Sichtung ab, dass insbesondere von der Informatik viel erwartet wird. Als Forschungsgebiete der Informatik sind vor allem Datenfusion, Big Data, cyberphysikalische Systeme, sichere Systeme, Robotik, Künstliche Intelligenz und Autonome Systeme gefordert. Sind das nicht auch genau die Gebiete, die in der zivilen Informatik gerade mit immensen Finanzmitteln besonders gefördert werden? Ein Schelm, der Böses dabei denkt. Aber wenn dem so ist, wäre interessant zu untersuchen, ob immer noch wie in den 1950er- bis 1980er-Jahren der militärische Komplex die Entwicklung der Informatik maßgeblich bestimmt, oder ob das Militär sich einfach die aktuellen Hervorbringungen der zivil emanzipierten Informatik zunutze und zu eigen macht.

Was will die Bundeswehr mit Kampfdrohnen?

Waffentragende Drohnen werden bisher und vor allem für gezielte Tötungen, *signature strikes* und unter Inkaufnahme vieler Ziviltoter eingesetzt, sodass mit ihnen in den meisten Einsatzfällen Kriegsverbrechen begangen werden. Will die Bundeswehr auch solche Kriegsverbrechen begehen können? Wenn JA, wo soll das zukünftig geschehen? Welche Feinde Deutschlands sollen so bekämpft werden? Was hätte das mit dem Verteidigungsauftrag der Bundeswehr zu tun? Wenn NEIN, was sonst? Aus politischen und militärischen Kreisen hört man dazu oft litaneiartig wiederholt: Die Kampfdrohnen sollen dem Schutz der Soldaten bzw. dem Schutz von Feldlagern dienen. An welche zukünftigen Feldlager in welchen Ländern der Welt ist dabei gedacht?

A BAE Raven during flight testing, Brigadier Lance Mans, Deputy Director, NATO Special Operations Coordination Centre

Auf welche Kriegseinsätze bereitet sich die Bundeswehr vor? Welche Angreifer werden nicht über eine Flugabwehr verfügen, sodass Drohnen überhaupt dort fliegen können?

Hoffnung

Trotz der vielen Gegenbeispiele habe ich die Hoffnung nicht aufgegeben, dass Menschen vernünftig denken und handeln können, und dass sich insbesondere in einer Demokratie die Vernunft bei politischen Entscheidungen durchsetzen kann. Bezogen auf die Entwicklung unbemannter Waffensysteme hoffe ich, dass sich Informatikerinnen und Informatiker wo und wie immer möglich diesem Irrsinn verweigern. Bezogen auf bewaffnungsfähige Drohnen hoffe ich, dass die deutsche Regierung auf ihre Beschaffung und Neuentwicklung verzichtet, weil die immensen notwendigen Finanzmittel besser verwendet werden können, weil diese Waffen keinen Verteidigungsbedarf decken, weil diese Waffensysteme mit oder ohne Autonomie unüberwindliche ethische Probleme aufwerfen.

Daniel Leisegang

Der cyber-militärische Komplex

Die dunkle Seite des Silicon Valley

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

Den Begriff „militärisch-industri… …ut 50 Jahren. Er beschrieb damit eine Entwicklung, in der die Rüs… …ten Krieges erheblich an Einfluss auf die politischen Entscheidunge… …sant fortgeschritten; es sind vollständig neue Technikfelder entst… …se-Potenzial. Im digitalen Bereich, im „Cyberraum", ist die Verknüpfung von Militär und Industrie besonders eng, wie der Autor hier an zahlreichen Beispielen aufzeigt.

Das Silicon Valley gilt als die postindustrielle Innovationsschmiede der USA. Die dort angesiedelten IT- und Hightech-Unternehmen sind überzeugt, dass ihre *smarten* Produkte selbst die kompliziertesten Probleme des Alltags lösen können. Und in der Tat: Apples iPhone hat die Kommunikation von Millionen Menschen geradezu revolutioniert. Facebook verbindet über 1,3 Milliarden Menschen miteinander, derweil Google nicht weniger als sämtliche Fragen der Menschheit beantworten will.

Doch das sonnige Tal südlich von San Francisco steht nicht nur im Dienst der guten Sache, sondern ist bereits seit Jahrzehnten auch Teil des militärisch-industriellen Komplexes der USA. Die