Die weitgehend verborgene Entwicklung autonomer Waffen

Zusammenfassung des Vortrags von Hans-Jörg Kreowski

In den Waffenschmieden und Denkfabriken der NATO und sicher auch darüber hinaus findet seit einigen Jahren eine weitgehend vor der Öffentlichkeit verborgene Entwicklung autonomer Waffen statt. Sie sollen so programmiert werden, dass sie in der Luft, auf dem Boden, auf und unter Wasser eigenständig Ziele finden und zerstören können. Insbesondere sollen sie selbständig über Leben und Tod entscheiden können. In dem Vortrag geht der Autor auf den Stand der Technik, auf die technischen Herausforderungen autonomer Systeme und auf die Perversität des autonomen Tötens ein.

Der Vortrag befasste sich mit zwei Publikationen, die sich aus militärischer Sicht mit autonomen Waffen beschäftigen. Waffensysteme wie *Reaper*, *Predator*, *Swordfish*, *Talon SWORD* und *Protector* sind heute genutzte, unbemannte, aber nicht autonome Waffensysteme. Das Ziel ist es, vergleichbare Waffensysteme zu entwickeln, die autonom operieren.

Unmanned Systems Integrated Roadmap

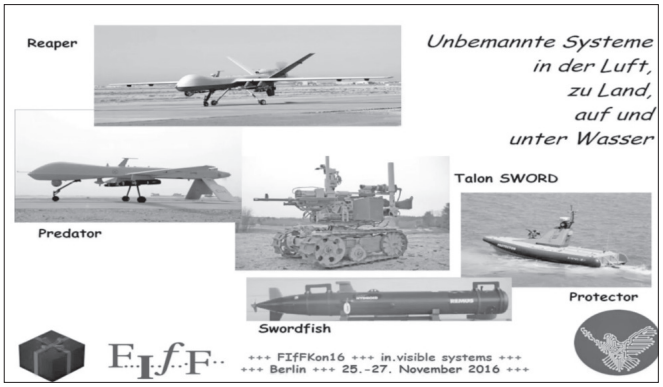
Das erste der behandelten Bücher ist der 160 Seiten starke Band *Unmanned Systems Integrated Roadmap*. Er erschien 2013 und schreibt die Entwicklung und Planung unbemannter und autonomer Waffen für 25 Jahre, bis 2038, fort. Die USA planen, einen erheblichen Teil ihrer Bewaffnung auf autonome Waffen umzustellen, und sehen dafür Ausgaben von 3–5 Mrd. US$ pro Jahr vor.

Was macht unbemannte Systeme für Politik und Militär interessant? Die Stichworte dafür sind „*dull – dirty – dangerous*“:

- *Dull:* Unbemannte Waffensysteme sind im Gegensatz zum Menschen in der Lage, über einen großen Zeitraum zu beobachten, ohne zu ermüden, abgelenkt zu werden, auf dumme Gedanken zu kommen oder sich zu langweilen.

- *Dirty:* Sie sollen weitgehend unbeschadet in einem biologisch, chemisch oder nuklear verseuchten Gebiet agieren können (wobei zweifelhaft ist, ob das auch für atomar verstrahlte Gebiete gilt).

- *Dangerous:* Sie können ohne Bedenken einer gefährlichen Situation ausgesetzt werden – im Verlustfall entsteht höchstens „Blechschaden“.



Für den Gegner bleibt es aber lebensgefährlich. Militärische Gefahren werden dadurch auch verlagert, z. B. wenn sich der Gegner durch Selbstmordattentate in anderen Gebieten zur Wehr setzt.

Was macht unbemannte Systeme für Politik und Militär interessant? Ein wesentlicher Aspekt ist Geld: Die USA wollen ihre militärische Überlegenheit trotz knapper Kassen wahren. Unbemannte Systeme sind kleiner, leichter, weniger gepanzert als entsprechende bemannte Systeme und deshalb billiger. Gleichzeitig folgen andere dem US-amerikanischen Beispiel der Entwicklung unbemannter Waffensysteme. Ein gigantisches Wettrüsten ist deswegen entbrannt. Dennoch herrschen in den USA weiterhin Allmachts- und Weltbeherrschungsphantasien; weitere Überlegenheit kann nur durch massive Aufrüstung erreicht werden. An den zugrundeliegenden Technologien ist die Informatik stark beteiligt. Kapitel 4 der Roadmap, *Technologies for Unmanned Systems*, das sich auf 50 Seiten mit bestehenden technologischen Lücken und offenen Forschungsfragen auseinandersetzt, identifiziert sechs Problembereiche:

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

Hier ist vor allem der fünfte Punkt der Aufzählung wichtig: *Autonomy and Cognitive Behavior*. 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.

Autonomous Systems – Issues for Defence Policymakers

Der zweite behandelte Band ist eine Veröffentlichung der NATO, ein 321-seitiger Sammelband, 2015 erschienen, mit Autorinnen und Autoren aus Militär, Wirtschaft und Wissenschaft. Er gliedert sich in vier Abschnitte und ein Nachwort:

Part 1: Introduction (60 Seiten)

Die Herausgeber beschreiben in der Einleitung Herausforderungen und Möglichkeiten autonomer Waffen einschließlich der Charakterisierung autonomer Systeme. Sie definieren autonome Systeme als Systeme, die auf der Basis integrierter Sensorik, Analytik, Kommunikationsmöglichkeit, Planung und Entscheidung agieren, um vorgegebene Ziele zu erreichen. Spezielles Charakteristikum autonomer Systeme ist, dass sie das in sich ändernder Umgebung mit potenziellem Nichtdeterminismus tun. In jeder gegebenen Situation kann es mehrere Handlungsoptionen geben, aus denen ausgewählt werden muss.

Part 2: Ethical, Legal, and Policy Perspectives (85 Seiten)

Die Anwendung und Einhaltung des Kriegsvölkerrechts muss beim Einsatz autonomer Waffen sichergestellt werden, sonst wären die Operationen Kriegsverbrechen. Militärische Entwicklungen haben eine Beziehung zu zivilen Entwicklungen, aus der zivilen Entwicklung autonomer Systeme wird für die militärische Entwicklung gelernt.

Part 3: Autonomous Systems and Operational Risk (80 Seiten)

Wichtig ist die Sicherstellung menschlicher Kontrolle. Das Autonomie-Level muss so gewählt werden, dass Menschen trotz autonomem Operieren letztendlich die Kontrolle behalten. Diese Systeme dürfen nicht außer Kontrolle geraten, damit ist immer ein möglichst niedriges Level an Autonomie sicherzustellen. Das erfordert prüffähige Strategien (die Forderung dabei ist: Überwachung muss möglich sein).

Part 4: Perspectives on Implementing Autonomy in Systems (90 Seiten)

Im Gefecht müssen (menschliche) Soldaten und autonome Waffen miteinander interagieren. Bei dieser Interaktion treten Schwierigkeiten auf, die zu berücksichtigen sind. Agenten-basierte Simulation wird vorgeschlagen, um autonome Waffensysteme zu testen – es ist aber fraglich, ob dies für die Beurteilung der korrekten Funktion ausreicht.

Für die Navigation in unbekannten Umgebungen sind vor allem optische Sensoren wichtig, die die Umgebung erfassen können. Doch bereits 1983, in der *Strategic Computing Initiative* der USA, finanziert mit 500 Mio. US$, war die Entwicklung autonomer Fahrzeuge eine der zentralen Forderungen. Die zugrundeliegende Problematik ist heute, nach über 30 Jahren, immer noch nicht gelöst.

Afterword (4 Seiten)

Das nur vier Seiten lange Nachwort enthält eine Forschungsagenda für die NATO, die vom *NATO Chief Scientist* Major-General Husniaux geschrieben wurde und besonders interessant ist.

Er benennt die Wissenschafts- und Technologieprioritäten der NATO, um Autonomie zu erreichen:

- advanced human performance
- cultural, social & organisational behaviours
- data collection & processing
- information analysis & decision support
- communications & networks
- power & energy
- advanced system concepts

Einer der wichtigsten Punkte dabei: die Systeme brauchen Energie, die heute übliche Energiespeichertechnik reicht für den Bedarf nicht aus. Doch auch *soft factors* spielen eine Rolle: Soldaten brauchen eine neue Einstellung, die Performanz muss verbessert werden. Kulturelle, organisatorische und soziale Aspekte müssen im militärischen Bereich neu gedacht werden.

Der Abschnitt schließt mit einem Zitat von *Theodore von Kármán*:

> *„Scientific results cannot be used efficiently by soldiers who have no understanding for them, and scientists cannot produce results useful for warfare without an understanding of the operations."*

Kritik

Die Kritik beginnt mit der Frage: Was ist Autonomie?

In der Wissenschaft wird immer auf die Autonomie von Menschen verwiesen, es geht um Entscheidungen für unser menschliches Handeln. Doch heute ist in der Biologie bekannt: Auch Tiere sind in der Lage, autonom zu handeln, Pflanzen können es in bestimmtem Umfang auch; die Mechanismen der Autonomie in der Natur sind uns aber weitgehend unbekannt.

In der Technik agieren Roboter, Systeme, Prozesse autonom; die Mechanismen sind vom Menschen gemacht – vorgedacht und programmiert –, im Rahmen des algorithmisch Möglichen.

Hans-Jörg Kreowski

Hans-Jörg Kreowski ist Professor (i.R.) für Theoretische Informatik an der Universität Bremen und Vorstandsmitglied des *Forums InformatikerInnen für Frieden und gesellschaftliche Verantwortung*. Neben seinen fachlichen Schwerpunkten hat er seit vielen Jahren auch immer wieder zur unheilvollen Verflechtung von Informatik und Rüstung in Wort und Schrift Stellung genommen.

Mit autonomen unbemannten Waffensystemen überlässt man die Entscheidung über Leben und Tod autonomen Maschinen. Daraus ergeben sich Fragen:

- Ist es verantwortbar?
- Darf das sein?
- Ist das ethisch vertretbar?
- Können Maschinen das Kriegsvölkerrecht beachten?

Beide Bücher sagen zur letzten Frage: Ja, das können sie. Maschinen können das Kriegsvölkerrecht beachten.

Die Antwort Hans-Jörg Kreowskis dagegen ist: Nein.

Ein autonomes Waffensystem führt programmierte Planungs- und Entscheidungsalgorithmen aus. Programmsysteme sind fast immer fehlerhaft, bei Entscheidung und Planung sind Fehler nahezu zwangsläufig. Planungs- und Entscheidungsprobleme sind meist NP-schwer, d. h. es sind keine effizienten Lösungen bekannt, sondern nur näherungsweise und heuristische. Können wir *näherungsweises* und *heuristisches* Töten akzeptieren? *Fehlerhaftes* Töten würde damit in Kauf genommen.

Testen, Validieren, Simulieren und Verifizieren der Systeme ist nötig, man braucht aber immer ein Vergleichsmodell. Das Wissen über die Modellierung von Autonomie ist unterentwickelt; es ist noch nicht einmal vollständig klar, was Autonomie überhaupt ist. Letztlich werden auch „autonome" Entscheidungen von Menschen gemacht, der Eingriff der Menschen ist nur zeitlich vorverlegt (und damit noch viel weniger beherrschbar).

Die Genfer Konvention und vergleichbare Bestimmungen sind Gesetzestexte, die keine eindeutigen Interpretationen besitzen, auch nicht vollständig und widerspruchsfrei sind. Ethik ist nicht berechen- und programmierbar. (Was allerdings Politik, Wissenschaft und Wirtschaft nicht aufhalten wird, es zu versuchen, wenn wir es nicht schaffen, dies zu verhindern.) Maschinen mit Entscheidungsverfahren über Tod und Leben auszustatten, ist abgründig und pervers, weil sie weder technisch einwandfrei funktionieren noch ethische Anforderungen erfüllen können. Fazit: Es ist weder ethisch noch technisch möglich, solche Waffensysteme zu bauen, die nach den Regeln des Kriegsvölkerrechts operieren.

Gegenentwurf

Es gibt verschiedene Initiativen gegen unbemannte und autonome Waffen:

- Weltweiter Aufruf zum Bann autonomer Waffen: *Autonomous Weapons: an Open Letter from AI & Robotics Researchers*. Bisher wurden 20806 Unterschriften gesammelt, davon rund 3000 von AI- und Robotik-Fachleuten (Stand November 2016).

- International Committee for Robot Arms Control (ICRAC).

- Kampagne Stopp Ramstein: Kein Drohnenkrieg!

Hans-Jörg Kreowski

- Cyberpeace-Kampagne des FIfF, unter anderem mit den Ausgaben der FIfF-Kommunikation *1/2014 – Schwerpunkt Cyberpeace* und *3/2015 – Schwerpunkt Rüstung und Informatik*.

Der Vortrag schloss mit einem Zitat von Albert Einstein:

„Das Denken der Zukunft muss Kriege unmöglich machen."

Diskussion

Bei der anschließenden Diskussion wurden folgende Aspekte angesprochen:

- Wichtig ist zusätzlich der Aspekt der Verantwortung: Wer hat die Entscheidung getroffen, durch die die Ereigniskette in Gang gesetzt wurde?

- Ist die Problematik vollkommen neu? Beispiel Landminen: Keiner kann letztlich beeinflussen, ob ein Soldat oder ein Kind davon getroffen wird; damit ist auch keiner für diese *Entscheidung* verantwortlich. Minen sind aber passive Waffen; autonome Waffen suchen sich ihre Ziele selbständig, deswegen haben sie eine andere Qualität. Landminen sind bereits verboten, es gibt politische Initiativen, auch autonome Waffensysteme zu verbieten.

- Es gibt das Problem der Asymmetrie: der Angegriffene hat keine Möglichkeit, gegen den Angreifer anzugehen, nur die Maschine kann zerstört werden. Eine „asymmetrische" Antwort auf Angriffe mit unbemannten Waffen sind z. B. Selbstmordattentate.

- Es mangelt an Vertrauen in die „guten" Intentionen der Hersteller autonomer Waffensysteme. Vergleichbar mit dem Abgasskandal kann ein „Genfer-Konventions-Modul" abgeschaltet werden, es kann am ernsthaften Bemühen fehlen, Ethik in die Systeme zu integrieren.

- Es stellt sich die Frage, wie kontrolliert werden kann, ob andere Staaten ebenfalls solche Waffen bauen – diese Kontrolle ist evtl. nicht möglich. Die USA machen Pläne öffent-

lich (zumindest teilweise), viele andere tun das nicht. Die Waffen sind vergleichsweise billig und leicht zu bauen; das führt zu einer Rüstungsspirale. Durch internationale Verträge wird heute auf biologische und chemische Waffen verzichtet; dieser Versuch sollte auch bei autonomen Waffen gemacht werden.

- Das Problem am autonomen Waffensystem ist, dass es ein Waffensystem ist, nicht dass es autonom ist. Dennoch ist es für Informatiker.innen wichtig, sich klar zu machen, was sie in ihrer Arbeit tun. Die Informatik darf als Disziplin nicht missbraucht werden.

- Es ist eine neue Qualität autonomer Systeme, dass sie sich verselbständigen und autonom weiterentwickeln können; evtl. können sie im Gegensatz zu normalen Waffen auch nicht mehr deaktiviert werden. Zumindest die Energie kann ihnen jedoch entzogen werden; es ist skeptisch zu beurteilen, ob solche Systeme wirklich im menschlichen Sinne intelligent werden können.

- Größte Gefahr ist, dass Entscheidungen irgendwann nicht mehr nachvollziehbar sind, dass nicht mehr klar ist, ob der Mensch den Krieg begonnen hat oder die Maschine.

- Programmierer sind verantwortlich für die von ihnen produzierten Systeme. Doch auch diejenigen tragen eine Verantwortung für die Folgen, die unbegründete Theorien von der Möglichkeit einer Maschinenethik in die Welt setzen.

FIfF-Konferenz 2016

Die neue Globalisierung – wenn das Inland zum Ausland wird

Zusammenfassung des Vortrags von Klaus Landefeld

Was hat die Klage gegen den BND wegen Überwachung am Internetknoten DE-CIX mit der BND-Reform nach dem Beschluss zur Ausland-Ausland-Fernmeldeaufklärung zu tun? Sehr, sehr viel – darum ging es im Beitrag von Klaus Landefeld.

Klaus Landefeld leitete seinen Vortrag mit einem Zitat des Bundesverfassungsgerichts ein, in dem es deutlich machte, dass Überwachung nicht in Einklang zu bringen ist mit der verfassungsrechtlichen Identität der Bundesrepublik Deutschland:

> *„Dass die Freiheitswahrnehmung der Bürger nicht total erfasst und registriert werden darf, gehört zur verfassungsrechtlichen Identität der Bundesrepublik Deutschland, für deren Wahrung sich die Bundesrepublik in europäischen und internati… einsetzen muss." (BVerfG, 20…*

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

Ähnlich sieht es der Europäische G…

> *„Aus der Gesamtheit dieser Daten können sehr genaue Schlüsse auf das Privatleben der Personen, deren Daten auf Vorrat gespeichert werden, gezogen werden, etwa auf Gewohnheiten des täglichen Lebens, ständige oder vorübergehende Aufenthaltsorte, tägliche oder in anderem Rhythmus erfolgende Ortsveränderungen, ausgeübte Tätigkeiten, soziale Beziehungen dieser Personen und das soziale Umfeld, in dem sie verkehren." (EuGH, 2014)*

Anders sieht es Bundesinnenminister Thomas de Maizière:

> *„Es ist nicht Aufgabe des Gerichts, ständig dem Gesetzgeber in Sachen Sicherheit in den Arm zu fallen." (Bundesinnenminister Thomas de Maizière, 2016)*

Landefeld unterschied zwischen zwei Kategorien der Fernmeldeüberwachung: Gezielte behördliche Maßnahmen, die unmittelbar auf einzelne Personen zielen, und ungezielte Maßnahmen, die die übergreifende strategische Überwachung zum Ziel haben. Zur ersten Kategorie zählt er anbietergestützte Maßnahmen nach § 110ff. TKG – Quellen-TKÜ, Vorratsdatenspeicherung, Funkzellenabfrage, Bestandsdatenauskunft und Online-Durchsuchung; Maßnahmen im Rahmen des G10-Gesetzes im Inland. Zu den strategischen Maßnahmen zählen die Maßnahmen nach G10-Gesetz mit Auslandsbezug (§ 5 G10-Gesetz): z.B. Ausland-Ausland-Fernmeldeüberwachung und Überwachung durch den Verfassungsschutz, um „Cyberbedrohungen" im Inland zu erkennen.

Klaus Landefeld

Seit den Enthüllungen durch Edward Snowden wurden die Überwachungsbefugnisse durch mehrere Gesetzesinitiativen systematisch ausgeweitet:

- Gesetz zur Verbesserung der Zusammenarbeit im Bereich des Verfassungsschutzes vom 20.11.2015