Jürgen Altmann

Bomben, Chips und Algorithmen – Informationstechnik zwischen Krieg und Frieden

Informationstechnik war seit ihrem Beginn durch Kriegsbedürfnisse geprägt. Das letzte Jahrhundert liefert wichtige Beispiele. Im 2. Weltkrieg gelang es Großbritannien, die mit der Enigma-Maschine verschlüsselten deutschen Funksprüche zu entschlüsseln, was entscheidend für die Schlacht im Atlantik und den Nachschub der Alliierten war. Nach 1945 wurden die ersten Großrechner für ballistische Rechnungen und die Modellierung der Prozesse in Kernwaffen entwickelt. Wie es im Computer-Archiv des US-Army Research Laboratory heißt: „The Purpose of This Archive: To help the public remember that it was the U. S. Army which initiated the computer revolution ... all modern computers are descended from ENIAC, EDVAC, ORDVAC, and BRLESC — all of which were conceived of and built to address pressing Army needs." (ftp.arl.mil/~mike/comphist/)

1. Informationstechnik und Militär/Krieg: Stichworte zur Geschichte

Über Jahrzehnte war dann das Militär der Hauptfinanzier der Entwicklung von Computern, Software, Netzwerken usw. Die jeweils stärksten Supercomputer (in den USA ab 1948 UNIVAC, 1964 CDC 6600, 1977 Cray–1 usw.) wurden für Entwicklung neuer Atomwaffen eingesetzt, für Aerodynamik, Raketen und vieles andere mehr [1]. Kleinere Rechner wurden für die Echtzeitsteuerung von Waffensystemen entwickelt. In den USA wurde Robotikforschung an Universitäten seit etwa 1960 vom Militär finanziert. Das ARPAnet wurde für die sichere Datenübertragung unter Atomkriegsbedingungen entwickelt und wurde dann zum Vorläufer des heutigen Internet. Integrierte Schaltkreise und Mikrocomputer wurden zwar im zivilen Bereich entwickelt, aber auf der Basis von vorangegangener intensiver militärischer Halbleiterforschung. Damit wurde der PC möglich, und ein Massenmarkt für Computer und Informationstechnik entwickelte sich, in dem dann mehr Geld in Forschung und Entwicklung floss, so dass sich nun im zivilen Bereich der technische Fortschritt schneller vollzog als im militärischen.

2. Aktuelle Entwicklungen und Trends

Auch wenn bei den Massenprodukten die technische Dynamik inzwischen vom zivilen Bereich ausgeht (und die Streitkräfte immer mehr zivile IT-Produkte einsetzen müssen), lässt das Militär weiterhin in sehr großem Umfang Forschung und Entwicklung für Aufnahme, Verarbeitung und Übertragung von Informationen betreiben – gegenwärtig heißt eines der zentralen Ziele Informationsdominanz. Da die USA am aktivsten sind, kommen die folgenden Beispiele von dort, aber andere Länder folgen in der Regel zügig nach.

Ein Bereich ist die stetige Erhöhung der *Zielgenauigkeit*. War es mit Hilfe der Trägheitsnavigation gelungen, die mittlere Zielabweichung bei Interkontinentalraketen bei 10.000 km Reichweite auf unter 100 m zu verringern, wurde zur Driftkorrektur bei Marschflugkörpern zunächst der Geländehöhen- und dann der Szenenvergleich entwickelt. Dann kamen die hochgenauen Satellitennavigationssysteme (GPS der USA, GLONASS der Sowjetunion/Russlands). Heute wird an automatischer Zielerkennung gearbeitet. Bei allen diesen Verfahren spielen digitale Daten und mathematische oder Mustererkennungs-Algorithmen eine zentrale Rolle.

Das aktuelle Leitbild moderner Streitkräfte heißt *Netzwerk-zentrierte Kriegführung*. Die eigene Truppe soll so vernetzt werden, dass aufgenommene Informationen breit verteilt werden bzw. abgerufen werden können. Dadurch soll sich ein gemeinsames Lagebewusstsein herausbilden, das durch Selbst-Synchronisierung erheblich stärkere Wirksamkeit im Kampf ergeben soll. Als zentrales System soll das Global Information Grid aufgebaut werden, das Netz, das alle Waffenplattformen, Sensoren und Führungszentren vereinigt, in gewisser Weise wie das öffentliche Internet. Allerdings ergeben sich hier erhebliche Probleme: Wie kann die notwendige Übertragungsbandbreite – etwa für Echtzeit-Videodaten von Aufklärungsdrohnen – zur Verfügung gestellt werden? Wie lässt sich eine sichere Übertragung gewährleisten, die auch noch gegen feindliches Mitlesen oder Stören geschützt ist? Wie lässt sich vermeiden, dass die beteiligten Menschen und Systeme nicht durch zu viel Information überlastet werden?

Mit der wachsenden Bedeutung von Rechnernetzen steigt das Interesse an *Cyber-Kriegführung*. Man möchte in gegnerischen Netzen spionieren, sie ggf. blockieren und infiltrieren. Dabei lässt sich – anders als bei den meisten Angriffen in der realen Welt – die Herkunft verschleiern, so dass der Verursacher seine Beteiligung abstreiten kann. Das eröffnet viele Möglichkeiten für Manipulation, wenn eine Macht z.B. zwei andere gegeneinander aufhetzen möchte. Weil militärische IT-Systeme erheblich besser gegen Fremdeinwirkung geschützt sind, ist abzusehen, dass Cyber-Kriegführung sich zum großen Teil gegen zivile Netze wenden wird.

Ein ganz anderer Bereich ist *biologisch inspirierte Informationstechnik*. Projekte in den USA widmen sich z.B. dem Nachbilden biologischer Sensoren, der Verarbeitung von Sinnesdaten ähnlich wie in den Nervensystemen von Lebewesen oder dem Lernen aus Erfahrungen

Ein Haupttrend der nächsten Jahrzehnte ist der zu *besatzungslosen* bzw. *robotischen Kampfsystemen*. Schon 2001 hat der US-Kongress beschlossen, die Streitkräfte sollen die Fernsteuerungstechnik so entwickeln, das 2010 ein Drittel der Angriffsflugzeuge und 2015 ein Drittel der Land-Kampffahrzeuge ohne Besatzung fliegen bzw. fahren. Aufbauend auf Jahrzehnte militärischer Roboterforschung und -entwicklung sowie Tausende von Einsätzen von Aufklärungsdrohnen bemüht sich das US-Verteidigungsministerium nun um die Teilstreitkräfte übergreifende Vereinheitlichung; auch für besatzungslose Land-, Über-

Titelseite der UMS Roadmap (US DoD)
Bildquelle: US-Regierung

wasser- und Unterwasserfahrzeuge wird intensiv gearbeitet. Der Fahrplan sieht breite Nutzung vor, mit vielen Stufen wachsender Fähigkeiten [2]. Die kompliziertesten Aufgaben – das verbundene Gefecht auf Land, die U-Boot-Bekämpfung auf und unter Wasser sowie der Luftkampf – sollen ab etwa 2020 möglich werden. Auch kleine Roboter werden erforscht; während sie schon heute zum Entschärfen von Sprengkörpern eingesetzt werden (aus einigen 10 m Abstand ferngesteuert), gibt es auch Ideen, sie große Entfernungen zurücklegen zu lassen, etwa beim US-Scorpion-Projekt, das beim deutschen Fraunhofer-Institut für Autonome Intelligente Systeme bearbeitet wurde. Kleinstflugzeuge sollen unbemerkt aufklären oder Zielpersonen bekämpfen – hier zeigen sich aber auch Grenzen bei der Höchstgeschwindigkeit (einige 10 km/h) und der Betriebsdauer (bisher einige 10 Minuten). Ein Spezialgebiet der Forschung ist die Schwarm-Intelligenz.

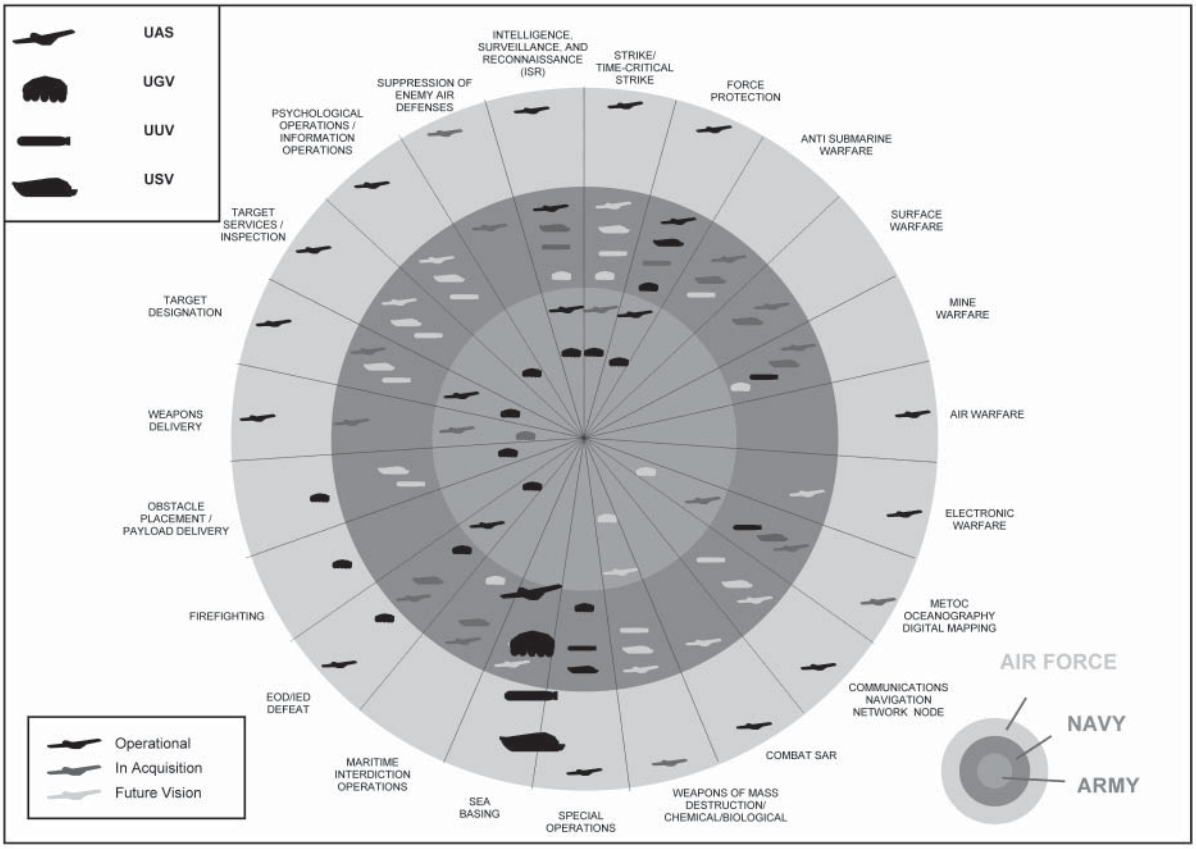
Die USA haben ihr besatzungsloses Aufklärungsflugzeug Predator (Länge 8 m) nachträglich mit Hellfire-Flugkörpern ausgestattet und im sog. Krieg gegen den Terrorismus seit 2002 eingesetzt. Inzwischen gibt es mit dem Reaper (Länge 11 m) ein besonders für den Kampf konstruiertes Flugzeug mit 1100 kg Waffennutzlast. Diese Typen werden von einer Basisstation in den USA aus gesteuert. Insbesondere über den Waffeneinsatz muss immer noch ein menschlicher Bediener entscheiden. Angedacht wird aber auch die *autonome Entscheidung* durch die Computer an Bord; insbesondere wenn es zukünftig auch gegnerische besatzungslose Fahr- und Flugzeuge geben wird, wird es einen Druck geben, schneller zu entscheiden, als die Satellitenverbindung und menschliche Reaktionszeit am anderen Ende der Übertragungsstrecke es erlauben. Es gibt in der Robotik Forschungsprojekte zum Töten durch autonome Systeme – ein Forscher argumentiert, man könne robotischen Systemen die Regeln des Kriegsvölkerrechts (z.B. Unterscheidung zwischen Kombattanten und Zivilisten) einprogrammieren, und sie würden sie sogar genauer einhalten, da Überreaktionen wie bei menschlichen Soldaten vermieden würden. Ein Konzept für ein „künstliches Gewissen" sieht sogar die Möglichkeit der Befehlsverweigerung vor, wenn ein dem Völkerrecht widersprechender Auftrag gegeben wird [3]. Ob autonome Kampfsysteme tatsächlich mit dieser Fähigkeit ausgestattet würden, kann man bezweifeln. Wichtiger ist die Frage, ob die absehbare „Intelligenz" von KI-Systemen ausreicht, um eine Situationsbeurteilung und Aktionsentscheidung mindestens auf der Höhe menschlicher Fähigkeiten zu gewährleisten [4].

Wie schwierig die Umsetzung von Konzepten für netzwerkzentrierte Kriegführung mit besatzungslosen Fahrzeugen sein kann, zeigt das *Future Combat System* (FCS) der US Army. Seit 2000 wurde das Konzept entwickelt, 2002 wurden die Firmen Boeing und Sciende Applications International als führende Systemintegratoren verpflichtet, seit 2003 läuft die Systementwicklung. Neben Bodensensoren, einem Flugkörperstartsystem und „intelligenter Munition" sollte das FCS vier Klassen besatzungsloser Flugzeuge und drei Typen besatzungsloser Bodenfahrzeuge umfassen, neben fünf Arten mit Personen besetzter Fahrzeuge. Die 18 verschiedenen Systeme sollten mit einem Netzwerk verbunden werden. 2005 hat der Rechnungshof des US-Kongresses erhebliche Verzögerungen festgestellt, die Kosten waren von 80 auf 108 Milliarden $ gestiegen. Daraufhin verlangt der Kongress seit 2006 jährlich einen Bericht. Im Jahr 2007 wurden drei besatzungslose Systeme gestrichen, dadurch konnten die Kosten auf 161 Milliarden $ begrenzt werden. In seinen Berichten von 2008 stellte der Rechnungshof fest [5]:

- Nach fast fünf Jahren Entwicklung sei unklar, ob das Informationsnetzwerk, der Kern des FCS, entwickelt, gebaut und demonstriert werden kann.

- Die in Entwicklung befindliche Software für Netzwerk und Plattformen umfasse 95 Millionen Kodezeilen, fast dreimal

Predator mit Hellfire-Flugkörpern (US Air Force)
Bildquelle: US-Regierung



UMS Roadmap: besatzungslose Fahrzeuge für alle Medien vorgesehen (US DoD)
Bildquelle: US-Regierung

so viele wie 2003 vorgesehen und viermal so viele wie die nächsten beiden Software-intensiven Militärprogramme.

- Es sein unklar, wann oder wie demonstriert werden könne, dass die FCS-Software funktioniert.
- Die Army werde den Entscheidungsträgern 2013 wahrscheinlich ein teilweise entwickeltes und weitgehend nicht demonstriertes System zur Produktion präsentieren.
- Der Meilenstein 2009 sei entscheidend, er könne die letzte Gelegenheit zur Kursänderung bieten.

Auch das breite Feld von *Nanotechnik* und *konvergenten Techniken* soll intensiv militärisch genutzt werden [6]. Bei Nanotechnik geht es um die Untersuchung und Gestaltung von Systemen auf der Ebene von Nanometern (10^{-9} m), mit Strukturgrößen etwa zwischen 0,1 nm (Atom) and einigen 100 nm (großes Molekül). Auf dieser Ebene verschwimmen die Grenzen zwischen den Disziplinen – Nanotechnik, Biotechnik, Informationstechnik, Kognitionswissenschaft und andere Felder konvergieren. Diese Techniken sollen die nächste industrielle Revolution bringen, mit weit reichenden Konsequenzen in allen Lebensbereichen. In den USA wird von einer „neuen Renaissance" gesprochen, die „Weltfrieden, universellen Wohlstand, ... einen höheren Grad von Mitgefühl und Erfüllung" bringen werde. Im Bereich „nationale Sicherheit" wird jedoch betont, dass „militärische Überlegenheit" der USA unerlässlich sei [7].

Nanotechnik soll dafür sorgen, dass das „Mooresche Gesetz" der exponentiell wachsenden Rechnerleistung auch dann noch weiter gilt, wenn die Lithographie auf Halbleiteroberflächen ihre Grenzen erreicht hat, etwa mittels Kohlenstoff-Nanoröhren oder Molekülen als Speicher- und Schaltelemente. Mutige KI-Forscher extrapolieren, dass 1000-Dollar-Computer in 15 Jahren die rohe Rechenleistung des menschlichen Gehirns erreichen werden. Kleine und kleinste Rechner würden in alle militärischen Systeme integriert. Durch fähigere Steuerungen, festere Materialien usw. wird Nanotechnik neue kleine Waffen ermöglichen, etwa Flugkörper zur Flugabwehr, die vielleicht 30 cm lang sind und 3 kg Masse haben, somit viel leichtere Möglichkeiten für Terrorangriffe bieten als die bisherigen Schulter getragenen Flugabwehrsysteme (MANPADS) mit 1,5 m und 30 kg. Auch kleinste Satelliten zum Andocken und Manipulieren anderer werden möglich werden.

In der medizinischen Nanobiotechnik wird intensiv an Kapseln für den sicheren Einschluss und die verzögerte Abgabe von Agentien gearbeitet, mittels aktiver Gruppen sollen sie sich an spezifische Ziele in Organen und Zellen binden. Erforscht werden Mechanismen zum leichteren Eintritt in Körper oder Zellen, insbesondere durch die Blut-Hirn-Schranke, Mechanismen zur selektiven Reaktion mit speziellen Genmustern oder Eiweißen sowie zur Überwindung der Immunreaktion des Zielorganismus. Alles dies könnte auch für feindliche Zwecke verwendet werden, wobei man das Risiko durch Begrenzung der Haltbarkeit, programmierte Selbstzerstörung, Aktivierung oder Deakti-

vierung durch zweites Agens oder zuverlässige Impfung für die eigene Seite verringern könnte. Somit kann es möglich werden, die Wirkung auf besondere Gruppen oder gar ein einzelnes Individuum einzugrenzen. Nanotechnik wird aber auch schnellere, billigere, empfindlichere und selektivere Sensoren für chemische oder biologische Kampfstoffe erlauben, bessere Filtermaterialien und effektivere Dekontamination.

Damit Nanotechnik schneller in die Armee eingeführt werden kann, finanziert die US Army das Institute for Soldier Nanotechnologies, das 2002 am Massachusetts Institute of Technology gegründet wurde. Hier arbeiten über 170 Personen in fünf multidisziplinären Forschungsfeldern an einem schützenden Kampfanzug, Sensoren für den Körperzustand und medizinischen Techniken. Nach Bedarf sollen Wirkstoffe verabreicht und Wundkompressen gebildet werden.

Im Bereich *Hirn-Maschine-Schnittstelle* gelang es, mit Multielektroden auf der motorischen Hirnrinde eines Affen die Signale für Armbewegungen zu erkennen, so dass schließlich der Affe einen Roboterarm wie seinen eigenen steuern konnte. Andersherum konnte eine Ratte mittels implantierter Hirnelektroden über beliebige Kurse gesteuert werden.

In den USA ist die Defense Advanced Research Projects Agency (DARPA) für weit in die Zukunft reichende Forschung zuständig [8]. Sie hat fünf fachliche Abteilungen; Informationstechnik-Fragen werden vor allem im Information Processing Techniques Office bearbeitet. Dort gibt es sechs Schwerpunktbereiche; Tabelle 1 gibt einen Eindruck von den darin bearbeiteten Programmen.

Die DARPA hat, wie erwähnt, auch das Future Combat System mitkonzipiert, vielleicht wegen des Herangehens: „And please, please tell us that something simply cannot be done – it's science fiction. That is the challenge we cannot resist." [9]

Zwei kurze Schlaglichter auf die EU und Deutschland sollen folgen. Die Europäische Verteidigungsagentur (EDA) der *Europäischen Union* hat ein Defence R&T Joint Investment Programme on Innovative Concepts and Emerging Technologies. Dort spielen Informationstechnik und Nanotechnik eine herausragende Rolle; Tabelle 2 zeigt die Themenbereiche der ersten beiden Ausschreibungen.

Für *Deutschland* wird zunächst auf das European Land-Robot Trial (ELROB) verwiesen, einen Wettbewerb für besatzungslose Landfahrzeuge, den die Bundeswehr – nach dem Muster der DARPA Grand Challenges – seit 2006 jährlich durchführt, im Wechsel militärisch und zivil. Von den 14 deutschen Teams, die am militärischen ELROB 2008 teilnahmen, kamen 4 aus Informatik-/Robotik-Gruppen deutscher ziviler Universitäten [10].

Das zweite Beispiel betrifft die Entwicklung besatzungsloser Kampfflugzeuge (unmanned combat air vehicle, UCAV). EADS entwickelt das Barracuda mit 8 m Länge, über 7 m Spannweite und etwa 3 t Startmasse. Es flog im April 2006 zum ersten Mal, stürzte dann aber weniger Monate später ins Meer.

Das Deutsche Zentrum für Luft- und Raumfahrt untersucht Technologien für die Entwicklung von besatzungslosen Kampfflugzeugen, für die ab 2020 ein möglicher Bedarf zur Bekämpfung mobiler Ziele zu Lande, in der Luft gesehen wird.

3. Probleme und Auswege

Beim Nachdenken über Frieden und internationale Sicherheit muss ein Grundproblem berücksichtigt werden. Im gegenwärtigen internationalen System gibt es – anders als im Inneren von Staaten – keine übergeordnete Autorität mit einem Monopol legitimer Gewalt, die die Einhaltung von Regeln durchsetzen und vor allem Staaten vor Angriffen schützen kann. Jeder Staat versucht, die eigene Sicherheit durch die Drohung mit seinen Streitkräften zu gewährleisten. Dabei erhöht er aber gerade auch die Bedrohung für andere, so dass sich in der Summe die Sicherheit aller verringert.

Ein Ausweg aus diesem so genannten Sicherheitsdilemma ist die freiwillige wechselseitige Begrenzung der Streitkräfte, also *Rüstungskontrolle* oder gar Abrüstung (allerdings gibt es Widersprüche mit dem Ziel des Sieges, sollte dennoch Krieg ausbrechen). Rüstungsbegrenzung ist nur verlässlich, wenn die Staaten überprüfen können, ob die Vertragspartner die Vereinbarungen auch einhalten. Diese *Verifikation* braucht eine ausgewogene Mischung zwischen Offenheit und Geheimhaltung und wird umso schwieriger, je kleiner, billiger oder häufiger die nachzuweisende Objekte werden.

Für neue militärische Technologien ist präventive Rüstungskontrolle relevant – also ein Verbot oder eine Beschränkung einer militärisch nutzbaren Technologie oder von Waffensystemen, die wirken, bevor die neuen Systeme beschafft werden. Für solche vorbeugenden Beschränkungen gibt es eine Reihe von Präze-

Schwerpunktbereich	Anzahl Programme	Beispielprogramm
Cognitive Systems	15	Learning Applied to Ground Robots
Command & Control	8	Urban Leader Tactical Response, Awareness & Visualization
High Productivity Computing	3	Disruptive Manufacturing Technology, Software Producibility
Language Processing	3	Spoken Language Communication and Translation System for Tactical Use
Sensors & Processing	14	Camouflaged Long Endurance Nano Sensors
Emerging Technologies	3	Information Theory for Mobile Ad-Hoc Networks

Tabelle 1
Schwerpunktbereiche des Information Processing Techniques Office der US-DARPA mit je einem willkürlich ausgewählten Programm (Quelle: www.darpa.mil/ipto/thrust_areas/thrust_areas.asp)

denzfällen. Die Teststoppverträge (partiell 1963, vollständig 1996) verbieten nukleare Testexplosionen. Der Raketenabwehrvertrag (1972-2002) verbot Abwehrsysteme, die luft-, see- und beweglich landgestützt sind. Sowohl das Biologische-Waffen-Übereinkommen (1972) als auch das Chemiewaffen-Übereinkommen (1993) verbieten nicht nur die Herstellung, sondern schon Entwicklung und Erprobung solcher Waffen.

First Call	Second Call
Non Linear Control Design	Remote Detection of Hidden Items
Integrated Navigation Architecture	Nanostructures – Electro-Optical and Other
Nanotechnologies	Radar Technologies – Processing
Structural Health Monitoring	Radar Technologies – Components

Tabelle 2
Themenbereiche der ersten zwei Projektausschreibungen der Europäischen Verteidigungsagentur für innovative Konzepte und aufkommende Technologien (Quelle: www.eda.europa.eu/genericitem.aspx?id=368)

Präventive Rüstungskontrolle braucht die folgenden Schritte: Zunächst müssen die technischen Eigenschaften und die mögliche militärische Nutzung vorausschauend analysiert werden. Die Ergebnisse müssen dann unter Kriterien bewertet werden. Schließlich sind dann mögliche Beschränkungen und Verifikationsmethoden zu entwerfen. Die Kriterien lassen sich in drei Gruppen einteilen. Bei der ersten geht es um die Einhaltung und Weiterentwicklung von Rüstungskontrolle, Abrüstung und Völkerrecht. Die zweite betrachtet die militärische Stabilität einschließlich der Weiterverbreitung. Die dritte Gruppe hat den Schutz von Mensch, Umwelt und Gesellschaft zum Inhalt.

Am Beispiel der Nanotechnik hat sich gezeigt, dass von 21 möglichen militärischen Anwendungen 8 besonders gefährlich sind und präventiv verboten werden sollten, darunter metallfreie Schusswaffen, kleine Flugkörper und kleine Roboter. U.a. damit die Verifikation nicht zu aufdringlich wird, sollten die Verbote nicht an der Verwendung von Nanotechnik festgemacht werden, sondern an militärischen Systemen oder Aufgaben, unabhängig von der im Innern verwendeten Technik. Die Regelungen sollten in die allgemeine Rüstungsbegrenzung und Abrüstung integriert werden, z.B. sollten kleine Satelliten als Antisatellitenwaffe im Rahmen eines allgemeinen Verbots von Weltraumwaffen erfasst werden. Neue biologisch-chemische Waffen sind schon verboten, aber das Biologische-Waffen-Übereinkommen sollte durch ein System für Einhaltung und Verifikation ergänzt werden, wie es beim Chemiewaffen-Übereinkommen schon existiert.

4. Informationswissenschaft und -technik für Abrüstung und Frieden

Informationswissenschaft und –technik kann auf verschiedene Weise direkt für Abrüstung und Frieden eingesetzt werden. Eine Art ist die kritische Begleitung militärischer Forschung und Entwicklung. Können große militärische Softwaresysteme funktionieren, oder sind sie zu komplex, nicht durchschaubar, nicht verifizierbar und nicht validierbar? Zum Beispiel ist der Softwaretechnik-Pionier David Parnas 1985 aus dem Panel on Computing in Support of Battle Management des US-Raketenabwehrprogramms "Strategic Defense Initiative" ausgetreten, weil die Aufgaben der Gefechtsmanagement-Software nicht erfüllbar waren: Sie sollte feindliche Raketen erkennen ohne Wissen über deren genaue Eigenschaften. Sie werde – als auf viele Satelliten und andere Knoten verteiltes System – unzuverlässig arbeiten und könne die Echtzeitanforderungen nicht erfüllen (D. Parnas erhielt dafür 2001 den FIfF-Preis).

Für die in Entwicklung befindlichen ferngesteuerten Waffensysteme sind folgende Fragen zu bearbeiten: Kann eine sichere Datenverbindung – auch unter Feindeinwirkung – gewährleistet werden? Ist die per Videokamera verfügbare Information ausreichend, um kriegsrechtskonforme Entscheidungen zu treffen, ob ein bestimmtes Ziel angegriffen werden darf? Ist die Bedienerschnittstelle für die tödliche Entscheidung angemessen gestaltet? Gibt es bei Fernsteuerung eine größere Enthemmung durch die extreme Trennung vom Ort des Kampfes, die Ähnlichkeit mit einem Videospiel?

Weitere wichtige Forschungsfragen sind [11]:

- Kann künstliche Intelligenz gewährleisten, dass autonome Kampfsysteme das Kriegsvölkerrecht einhalten?
- Wenn Krieg immer mehr automatische Entscheidungen umfasst – welche Folgen wird das für den Frieden oder für die militärische Stabilität zwischen potentiellen Gegnern haben?
- Welche Wechselwirkungen können sich ergeben zwischen Cyber-Angriffen durch Hacker und militärischen Aktionen und Reaktionen?
- Kann man einen Schutz für kritische Informationsinfrastruktur im Kriegsvölkerrecht verankern?
- Ist es möglich, Vorbereitungen auf den Cyber-Krieg durch Rüstungskontrolle zu beschränken?
- Kann man die Informationstechnik, die für legitime UN-Einsätze gebraucht wird, von der für einen großen Krieg trennen?

Im Bereich Verifikation ist Forschung nötig für die automatisierte Verarbeitung von Satelliten- oder Luftbildern sowie von Daten von Vor-Ort-Sensoren.

Ein wenig problematisch und ambivalent ist die Frage, ob man mittels *data mining* Indikatoren für heimliche bzw. illegale Aktivitäten finden kann, etwa in Bezug auf die Weiterverbreitung beschränkter Technologien.

5. Verantwortung für Frieden in der Informationstechnik

Es gibt verschiedene Arten, wie man die Verantwortung, die man für die friedliche Nutzung der eigenen Wissenschaft/Technik hat, wahrnehmen kann. Einige wenige können die eigene Forschung oder Entwicklung direkt der Abrüstung widmen. Die vielen anderen, die „normale" zivile Forschungs- oder Softwareprojekte bearbeiten, können wachsam sein und militärische Forschung und Entwicklung im eigenen Feld verfolgen. Insbesondere in den USA, wo die Militärförderung von Universitäten eine starke Tradition hat, können die Computerwissenschaftler/innen überlegen, ob sie solche Finanzierung annehmen wollen.

Ein Beispiel für die bewusste Ablehnung gibt Benjamin Kuipers von der University of Texas, Austin [12]. Problematische militärische Anwendungen können in der Fachgemeinschaft zur Diskussion und in Frage gestellt werden, wie es Noel Sharkey macht [13].

Ich denke, dass zur Wahrnehmung der Verantwortung für den Frieden auch Grundkenntnisse in Abrüstung gehören, einschließlich der entsprechenden Verträge sowie der Methoden, wie die Einhaltung überprüft wird. Auch elementares Wissen über das Völkerrecht sollte vorhanden sein.

Verantwortung beginnt in der Lehre: Dort sollten Abrüstungsthemen mit Bezug zu Informationstechnik und Informatik einbezogen werden, z.B. bei Lehrveranstaltungen zu "Informatik und Gesellschaft". Sehr hilfreich wäre die Entwicklung entsprechender Lehreinheiten, auch für die Schule. Zur Information der Öffentlichkeit kann man Vorträge halten oder Gespräche mit Medienvertretern führen.

Das Forum Informatiker/innen für Frieden und gesellschaftliche Verantwortung spielt für Initiativen in diese Richtung eine wichtige Rolle, daher sollte es gestärkt werden.

Quellen und Anmerkungen

1 *S. z.B. Computer History Museum, www.computerhistory.org*

2 *UMS Roadmap 2007-2032, Washington DC: US Department of Defense, 2007.*

3 *Arkin, R. C., Governing Lethal Behavior: Embedding Ethics in a Hybrid Deliberative/Reactive Robot Architecture, Technical Report GIT-GVU-07-11, College of Computing, Georgia Institute of Technology, 2007, www.cc.gatech.edu/ai/robot-lab/online-publications/formalizationv35.pdf*

4 *Siehe dazu den Artikel von Noel Sharkey in diesem Heft.*

5 *Government Accountability Office, 2009 Is a Critical Juncture for the Army's Future Combat System, GAO-08-408, Washington DC: U.S. Government Printing Office, 2008, www.gao.gov/new.items/d08408.pdf; 2008: Defense Acquisitions – Significant Challenges Ahead in Developing and Demonstrating Future Combat System's Network and Software, GAO-08-409, 2008, www.gao.gov/new.items/d08409.pdf*

6 *J. Altmann, Military Nanotechnology: Potential Applications and Preventive Arms Control, Abingdon/New York: Routledge, 2006; s. auch www.bundesstiftung-friedensforschung.de/pdf-docs/berichtaltmann.pdf.*

7 *M. C. Roco, W. S. Bainbridge, (eds.), Converging Technologies for Improving Human Performance – Nanotechnology, Biotechnology, Information Technology and Cognitive Science, Boston MA: Kluwer, 2003 (auch in: www.wtec.org/ConvergingTechnologies/1/NBIC_report.pdf); das europäische Konzept für konvergierende Techniken ist deutlich anders, High Level Expert Group Foresighting the New Technology Wave, Converging Technologies – Shaping the Future of European Societies, A. Nordmann (Rapporteur), Brussels: European Communities, 2004.*

8 *www.darpa.mil*

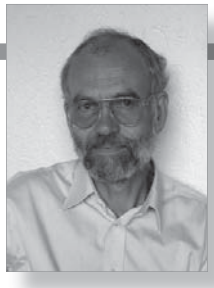
9 *B. Giroir, Ideas Begin Here, Teleprompter Script, presented at DARPATech, DARPA's 25th Systems and Technology Symposium, August 7, 2007, Anaheim CA, www.darpa.mil/DARPATech2007/proceedings/dt07-dso-giroir-ideas.pdf*

10 *Institute for Systems Engineering (ISE) Leibniz-Universität Hannover; FB 12, Universität Siegen; FB Informatik, Univ. Kaiserslautern; Jacobs University Bremen, www.elrob.org/Teams_Exhibitors.38.0.html*

11 *Wer interessiert ist, solche Forschung zu beginnen, kann sich gern an den Autor wenden.*

12 *B. Kuipers, Why don't I take military funding?, www.cs.utexas.edu/~kuipers/opinions/no-military-funding.html*

13 *Siehe den Artikel von Noel Sharkey in diesem Heft.*



Jürgen Altmann

PD Dr. Jürgen Altmann ist Physiker und Friedensforscher. Er hat Rechner betreut und Computer-Mustererkennung (an Bildern, an akustischen und seismischen Signalen) betrieben. Seit 1985 macht er Abrüstungs-orientierte Forschung. Schwerpunkte sind kooperative Verifikation von Abrüstungs- und Friedensabkommen mit akustischen, seismischen und magnetischen Sensoren sowie Militär-Technikfolgenabschätzung und präventive Rüstungskontrolle. Im letzteren Bereich hat er u.a. geforscht über „nicht tödliche" Waffen, Nanotechnik und besatzungslose militärische Systeme. Er ist Mitgründer des Forschungsverbundes Naturwissenschaft, Abrüstung und internationale Sicherheit FONAS und ein stellvertretender Sprecher des Arbeitskreises Physik und Abrüstung der Deutschen Physikalischen Gesellschaft DPG. *(altmann@e3.physik.tu-dortmund.de)*