Hans-Jörg Kreowski und Dietrich Meyer-Ebrecht

Der Missbrauch der Informationstechnik für die ‚Revolution' des Kriegsgeschäfts

*Informatik und Informationstechnik haben die Rüstungstechnik und in der Folge die militärischen Strategien und verteidigungspolitischen Doktrinen so grundlegend verändert, dass bereits in den 1990er Jahren, als die neuen technischen Optionen eher noch Visionen waren, der Begriff ‚*Revolution in Military Affairs*' geprägt wurde. Die mit dem Akronym* RMA *umrissenen Konzepte und Visionen beherrschen seither die sicherheits- und verteidigungspolitische Debatte. Korrespondierend zur informationstechnischen Durchdringung der öffentlichen und privaten Lebenssphären, zur stetigen Verlagerung realen Geschehens in virtuelle Räume scheint die Digitalisierung des Kriegsgeschäfts auch den Krieg zu einem virtuellen Szenarium werden zu lassen. Nur der Tod im Krieg, eingeplant oder kollateral in Kauf genommen, bleibt analog und mithin grausam wie je, versteckt jedoch hinter der Fassade des ‚sauberen' Neuen Kriegs …*

Die dunkle Seite der Informationstechnologie

Edward Snowden hat uns darauf gestoßen, was wir eigentlich alle hätten lange wissen müssen: Die Technologien, mit denen während des letzten Vierteljahrhunderts eine weltumspannende, immer dichter werdende informationstechnische Vernetzung aufgebaut wurde, bieten einzigartige Optionen für eine Überwachung, die gleichermaßen Unternehmen, Behörden, Institutionen wie Privatpersonen erfasst. Zu Protesten mobilisieren die öffentlich wahrgenommenen Missstände wie Wirtschaftsspionage, Eindringen in Regierungsgeschäfte, Ausspähung der Privatsphäre. Weniger bewusst ist sich die Gesellschaft, dass die mit gigantischem Aufwand und staatlich sanktioniertem kriminellen Vorgehen – nicht nur von der NSA – betriebene Agglomeration und Ausforschung vertraulicher Daten weltweit Teil einer neuen Kriegsführung ist: Je früher und umfassender ich weiß, was der Feind (oder Freund!) plant, desto wirkungsvoller kann ich eingreifen!

Nicht immer geheim zu halten ist eine Ausspähung dieses Ausmaßes, die alle bisherige Spionagetätigkeit quantitativ wie qualitativ weit hinter sich lässt. Allein, sie ist nur der sichtbarste Teil der neuen Kriegsführung. Strikter geheim gehalten werden Entwicklung und Anwendung von Software-Werkzeugen, mit denen funktional in fremde Datenverarbeitungssysteme und -strukturen eingegriffen werden kann, von Informationsmanipulation zur Desorientierung des Gegners bis zu Sabotageakten mit kinetischer Wirkung – *Cyber warfare.* All diese vom Grunde her militärischen Operationen schwimmen weitgehend unbemerkt mit in den Datenströmen der digitalen Kommunikationssysteme, die mit ihren Glasfaserkabeln und Funknetzen, terrestrisch und satellitengestützt, jeden Ort unserer Erde erreichen. Und dies sind just dieselben Systeme, die einst mit dem Versprechen einherkamen, ob ihrer Völker verbindenden, Grenzen überwindenden Wirkung den Frieden zu fördern. Mehr noch, sie werden gleichzeitig zum Nervensystem der Streitkräfte zu Lande, zu Wasser und in der Luft.

Network centered warfare – das war das *buzz word* der *„Joint Vision 2010"*, ein Positionspapier des US-Generalstabs, vorgestellt 1996, vier Jahre später aktualisiert in der *„Joint Vision 2020"*[1]. Als Kernbotschaft forderte es eine gründliche Restrukturierung der US-Streitkräfte mit dem Ziel einer umfassenden Nutzung moderner Kommunikations- und Informationstechnologie in Waffen, in Waffensystemen und in den zu ihren Einsatz notwendigen Infrastrukturen. Die *Joint Vision 2010* warb bereits für den Einsatz global vernetzter Gefechtseinheiten, für die Einbettung aller Arten von Kampffahrzeugen – vor allem auch unbemannter – bis hin zum einzelnen Soldaten im Schlachtfeld in eine einheitliche *Communication Command Control Intelligence*, C3I. Der Kreis schließt sich, wenn diese Systeme zunehmend dazu dienen, völkerrechtswidrige Drohneneinsätze gegen *high value targets* durchzuführen. ‚Hochwertziele', das sind Menschen, die vor allem durch Ausspähung ihrer Kommunikation als (potentielle) Terroristen identifiziert wurden, vielleicht auch nur auf Grund von verdächtig machenden Verhaltensmustern (*signature strike*), die schließlich über ihre Mobiltelefone als Abschussziel geortet werden.

Die militärische Nutzung der Informatik und Informationstechnik hat eine kaum beachtete Rückwirkung auf die Zivilgesellschaft. Mit einem kurzen Rückblick auf die Geschichte ihrer militärischen Entwicklung, einem Überblick über den derzeitigen Entwicklungsstand hoch technologisierter Waffen und einem Einblick in die zunehmende Verwischung zwischen ziviler und militärischer Forschung und Entwicklung möchten wir auf die daraus resultierenden Gefahren aufmerksam machen – und an die Verantwortung unseres Berufsstandes erinnern.

Die Militärischen Wurzeln der Computertechnik und der Informatik

Die Entwicklung von Computertechnik und Informatik ist in ihren Anfängen stark vom Geld und von den Wünschen des Militärs beeinflusst[2]. Konrad Zuse baute seit 1936 an einer Serie von Computern. Was in einem privaten Rahmen begann, ist bald mit erheblichen nationalsozialistischen Geldmitteln im kriegerischen Kontext vorangetrieben worden und hat unter anderem zu einem Spezialrechner für die Flügelvermessung einer ferngesteuerten Gleitbombe geführt. Unter der Leitung von Alan Turing wurde an der *Government and Cypher School* im englischen Bleachley Park die „*bombe*" entwickelt, die computergestützt die deutsche Verschlüsselungsmaschine *ENIGMA* geknackt hat und so einen wesentliche Einfluss auf den U-Boot-Krieg im Atlantik hatte. In den USA wurde spätestens ab 1943 die Computerentwicklung massiv betrieben. Unter anderem entstanden die *ENIAC* zur Berechnung ballistischer Tabellen, der *STRETCH*-Computer, der bei der Entwicklung der Wasserstroffbombe zum Einsatz kam, sowie die *WHIRLWIND*-Serie, die in den 1950er Jahren zu den *SAGE*-Computern führte als Teil eines Luftabwehrsystems. Wie bei *SAGE* verlässt sich der militärische Komplex der USA in den 1950er und 1960er Jahren mehr und mehr auf große, teure und unzuverlässige Computerprogramme u.a. *beim North American Defence System*, beim *Ballistic Missile Early Warning System* und beim *Anti Ballistic Missile System*.

Wegen der immensen Kosten und großen Fehleranfälligkeit der Systeme wurde die ‚Softwarekrise' proklamiert. Die Antwort des US-amerikanischen Department of Defence und der NATO war die Etablierung des Fachgebiets Softwaretechnik durch eine Konferenzserie ab 1969, die Entwicklung der Programmiersprache *ADA* als NATO-Standard in den 1970er Jahren, die Entwicklung von *Very High Speed Integrated Circuits* ab 1980 und die Ausschreibung zweier umfangreicher Forschungsförderungsprorammen im Jahre 1983: *Software Technology for Adaptable Reliable Software* (*STARS*) und *Strategic Computing Initiative* (*SCI*). Beide hatten eine prägende Wirkung auf Softwaretechnik und Künstliche Intelligenz als Schlüsselgebiete der Informatik. Ebenfalls im Jahre 1983 wurde die *Strategic Defence Initiative* (*SDI*) aufgelegt, die noch gigantischer konzipiert war, aber neben der Informatik vor allem auch andere Technogiebereiche einbezog. Mit diesem gewaltigen Schub durch militärische Finanzmittel und kriegerische Absichten in den 1970er und 1980er Jahren aber kam auch die kommerzielle und zivile Informations- und Kommunikationstechnik stark auf, so dass sich die Informatik ein Stück weit von ihren militärischen Wurzeln emanzipieren konnte.

Die Triebfeder der IT-Evolution

Die Genesis der Computer war militärisch motiviert und angetrieben, und immer noch und sogar zunehmend sind sie essentielle Teile von Waffen und Waffensystemen. Erstaunlich, dass wir Computer dennoch nicht als genuin militärische Technologie identifizieren. Das hat zwei Gründe. Zum Einen werden Computer in Waffen kaum wahrgenommen. Betrachten wir beispielsweise eine Drohne – offensichtlich eine besondere Art von Flugkörper – weit weniger offensichtlich, dass ihr Rumpf mit Informationstechnologie vollgestopft ist und eine noch umfassendere informationstechnische Infrastruktur ihre Operationen unterstützt. Zum Anderen verkörpern Computer *das* klassische Beispiel einer Dual-Use-Technologie.[3] Denn kaum hatten Computer ihre Funktionsfähigkeit und Nützlichkeit in militärischen Anwendungen bewiesen, setzte eine nicht mehr zu bremsende Entwicklung ziviler Anwendungen ein. Mittlerweile ist Informationstechnologie in allen zivilen Lebensbereichen zu einer solchen Selbstverständlichkeit geworden, dass ihre Nutzung (auch) in Waffensystemen nicht mehr als eine Besonderheit wahrgenommen wird. Die Alltäglichkeit der Computer ist es, die ihre fundamentale Rolle in militärischen Anwendungen relativiert und sogar verschleiert. Ihre Dual-Use-Natur macht selbst Fachleute blind für ihr zerstörerisches Potential.

Andererseits werden Computer mittlerweile nicht nur als eine zivile Technologie wahrgenommen, sie sind sogar zu einer 'zivilen' Technologie geworden – mindestens, wenn wir von der Triebkraft ausgehen, mit der die Flut ziviler Anwendungen ihre Weiterentwicklung und Reifung vorangetrieben hat. Die Subtilität der Produktionsprozesse, die Komplexität ihrer Funktionalität, beides konnte sich in der heute erreichten Perfektion, Zuverlässigkeit und Wirtschaftlichkeit nur in einem Jahrzehnte währenden Evolutionsprozess entwickeln. Mutation und Selektion in vielen kleinen Schritten, ein Prozess, der sich auf myriadenfache (zivile) Anwendung stützt – und auf unseren Konsum von IT-Produkten, mit dem wir die dahinterstehenden Investitionen für eine hoch gezüchtete Produktionstechnologie finanziert haben. Den Nutzen hat *auch* die Rüstungstechnik! Weitgehend nutzt sie dieselbe Technologie, dieselben Komponenten, dieselben informatischen Methoden. Denn selbst wenn eine eigenständige militärische Informationstechnologie wünschenswert wäre, sie könnte nicht in kurzer Zeit aus dem Boden gestampft werden,

auch nicht mit immensen Mitteln, denn ihr fehlte der Evolutionsprozess, der sich auf die ungeheure Vielfalt und Vielzahl von Anwendungen stützt.

Wir können es auch so sehen: Uneingeschränkt nutzen militärische Anwendungen die ausgereiften Produktionstechnologien für zivile IT-Produkte. Forschung und Entwicklung, mögen sie auch primär auf zivile Nutzungen ausgerichtet sein, kommen letztlich ebenfalls auch der militärischen Anwendung zugute. Die Folge ist eine sich ausdehnende Grauzone zwischen zivilen und militärischen Zielsetzungen. Ein prominentes Beispiel ist die Robotertechnologie.

Der Alptraum autonomer Killerroboter

Im Rahmen der *Strategic Computing Initiative* wurden der Künstlichen Intelligenz drei Aufgaben gestellt: eine Pilotenassistenz, ein Schlachtenlenksystem und ein Militärfahrzeug, das sich autonom in fremdem Gelände zurechtfindet, Hindernissen ausweichen und sich bei Bedarf auch verstecken kann. In den letzten 30 Jahren sind mit Milliarden an Forschungsförderungsmitteln weltweit die wissenschaftlichen Grundlagen vorangetrieben worden, die solche und verwandte Anwendungen möglich machen. Vieles davon fand im zivilen Bereich und zivilen Anwendungszielen statt, was insbesondere auch für die Entwicklung autonomer Systeme in der Robotik gilt. Parallel dazu aber gibt es umfangreiche Programme, Roboter kriegstauglich zu machen. Die USA planen in den nächsten Jahrzehnten ein Drittel ihrer Waffensysteme durch unbemannte Kampfvehikel in der Luft, an Land sowie auf und unter Wasser zu ersetzen[4]. Der Prozess ist bereits in vollem Gange, wie die Killerdrohnen *Predator* mit zwei *Hellfire*-Raketen und *Reaper* mit acht *Hellfire*-Raketen und deren tausendfache Einsätze in Afghanistan, Pakistan und Jemen belegen.

An der Einsatzfähigkeit solcher Waffen ist die Informatik erheblich beteiligt, weil Erkenntnisse über eingebettete Systeme, digitale Kontrolle, Sensortechnik, Bildverarbeitung, Kommunikationsnetze, Big Data und anderes mehr in militärische Roboter Eingang finden. Allerdings sind solche Systeme heute noch nicht vollautomatisch im Einsatz. Die Killerdrohnen Predator und Reaper zum Beispiel schießen Raketen erst ab, wenn dazu der Befehl eines Soldaten aus Nevada (oder teils wohl auch aus Rammstein) kommt. Erklärtes Ziel ist jedoch die Entwicklung völlig autonomer bewaffneter Roboter, die insbesondere auch selbst entscheiden, wann sie töten.

Wenn Maschinen entscheiden, ob sie ihre Waffen gegen Menschen richten oder nicht, dann ist das nach dem Kriegsvölkerrecht nur im Krieg zulässig, wenn die entsprechenden Regeln in der Haager Landkriegsordnung und der Genfer Konvention eingehalten werden. Autonom tötende Roboter müssen also kämpfende Soldaten von anderen Personen – insbesondere Zivilpersonen – unterscheiden können sowie kulturelle Güter schonen. Sie müssen in diesem Sinne ethisch korrekt handeln können. Einige Fachleute wie beispielsweise Ron Arkin vom Georgia Institute of Technology sind überzeugt, dass Maschinen gebaut werden können, die dazu in der Lage sind[5]. Sie seien sogar besser als menschliche Kämpfer, weil sie nicht in Panik geraten und unethische Befehle verweigern ohne Rücksicht auf die Folgen für sie selbst.

An dieser Position seien erhebliche Zweifel erlaubt. Eine künstliche Ethik ist wohl kaum einfacher zu entwickeln und zu programmieren, wenn es überhaupt möglich ist, als künstliche Intelligenz. Daran arbeiten Tausende von Wissenschaftlerinnen und Wissenschaftlern schon seit über 50 Jahren, aber trotz aller beachtlicher Einzelerfolge kann bisher nicht wirklich von *Intelligenz* die Rede sein.

Das Problem ist, dass nur programmiert werden kann, wofür es ein formales berechenbares Modell gibt. Das könnte bei ethischen Fragen bereits scheitern. Aber selbst wenn es prinzipiell ein solches Modell gäbe, könnte es zuviel Zeit benötigen oder fehlerhaft sein. Für die meisten Entscheidungsprobleme sind keine effizienten Lösungen bekannt. Warum sollten ethische Entscheidungen da eine Ausnahme machen? Die meisten Programmsysteme sind nicht fehlerfrei und es ist schon gar nicht bewiesen, dass keine Fehler auftreten. Warum sollte bei Programmen, die ethisch korrekt arbeiten sollen, das anders sein? [6]

Autonome Killerroboter werden unserer Meinung nach gar nicht oder jedenfalls nicht in absehbarer Zeit nach dem Kriegsvölkerrecht agieren können. Sie werden deshalb die schon heute virulenten Probleme von Kampfrobotern verschärfen wie der Einsatz in unerklärten Kriegen, viele zivile Opfer, gezielte Tötungen, Ausdehnung der Asymmetrie der kriegführenden Parteien und damit Provokation terroristischer Anschläge. Da sich diese Probleme

und Gefahren nicht technisch beherrschen lassen, müssen autonome Waffensysteme wie biologische und chemische Waffen verboten werden.

Die gesellschaftliche Brisanz einer zivil-militärischen Verflechtung

Roboter sind ein alarmierendes Beispiel einer gefährlichen Verschmelzung ziviler und militärischer Technologie. gerade im Bereich der Informatik. Denn mehr als irgendeine andere Waffe beruhen autonome Waffenträger auf avancierten Methoden der Informatik, speziell auf dem Gebiet der Künstlichen Intelligenz. Wir müssen daher im Rückschluss argwöhnen, dass militärische Ziele zur treibenden Kraft hinter manch einem zivil deklarierten Forschungsprojekt werden. Besonders auffällig ist die Verflechtung der Interessen bei – offen oder verdeckt gesponserten – Roboterwettbewerben wie *Robocup* für Fußball spielende Roboter oder *DARPA Grand Challenge* für autonome Fahrzeuge in den USA.

Eine strikte Trennung ist sicherlich auch gar nicht im Interesse der Industrie, denn welches große ‚zivile' Unternehmen ist nicht auch mit Rüstungsaufträgen befasst? Unterstützt wird sie darin von nationaler und Europäischer Politik. Interessant ist, wie die Grenze zwischen ziviler und militärischer Forschung und Entwicklung absichtsvoll verwischt wird. 1. Akt: Euphemistische Sprachregelungen werden etabliert, mit denen die Abgrenzung verschleiert wird: *Sicherheitsforschung, Sicherheitsarchitektur, Sicherheitstechnologie* ... – unter dieser Decke lässt sich gerade bei informationstechnischen Applikationen, Komponenten und Systemen eine genuin militärische Bestimmung gut verbergen. 2. Akt: Organisatorische Strukturen werden ‚angepasst': Die Fraunhofer-Gesellschaft legt beispielsweise fünf ihrer Institute mit drei Instituten der vom Bundesverteidigungsministerium finanzierten *Forschungsgesellschaft für angewandte Naturwissenschaften* (FGAN) zum *Verein für Verteidigungs- und Sicherheitsforschung* (VVS) zusammen, wo nun zivile und militärische Forschung unter einem Dach stattfindet. Und schließlich der 3. Akt: Budgets werden geschaffen: Unter Bundesministerin Schavan wurde ‚Sicherheitsforschung' ein relevantes Segment ihrer sechs Milliarden Euro schweren ‚*Hightech-Strategie*'. Das korrespondierende ‚*Security Research Programme*' der Europäischen Kommission allein war mit 1,4 Milliarden Euro bestückt.[7]

Das Verschmelzen ziviler und militärischer Technologieentwicklung ist kein Alleinstellungsmerkmal der Informatik und Informationstechnik. Nur wird sie dort mit einem besonderen Nachdruck betrieben. Und ob der Alltäglichkeit und Allgegenwärtigkeit der Computer passiert sie unauffällig, selbstverständlich. Das scheint uns der Grund zu sein, warum die *Revolution in Military Affairs*, die von Informatik und Informationstechnik angetriebene Revolution des Kriegsgeschäfts mit so wenig öffentlichen Aufhebens voranschreitet. Dennoch, sie *ist* eine Revolution. Natürlich zuvorderst für militärische Strategen. In ihrer Folge aber verändert sie gesellschaftliche Einstellungen und politische Doktrinen, stört ausbalancierte Machtgefüge, beeinflusst Konfliktbereitschaft und Konfliktlösungsansätze. Gerade für Waffen, die in hohem Maße auf informatische Methoden und Informationstechnik aufbauen, gilt Jürgen Altmanns Aussage, „dass Krieg und Frieden zwar im Kern politische Fragen seien, dass jedoch neue Waffentechnologien […] massiven Einfluss auf gesellschaftliche Prozesse und Entwicklungen haben und den Frieden gefährden".[8]

Wird veröffentlicht in: Buchreihe Kritische Informatik Band 6 „30 Jahre FIfF", LIT-Verlag 2014

---

1 Volltexte zu finden unter http://www.dtic.mil/jv2010/jv2010.pdf und http://www.fs.fed.us/fire/doctrine/genesis_and_evolution/source_materials/joint_vision_2020.pdf

2 Siehe für eine ausführlichere Darstellung z.B. Joachim Bickenbach, Reinhard Keil-Slawik, Michael Löwe, Reinhard Wilhelm (Hrsg.): Militarisierte Informatik, Schriftenreihe Wissenschaft und Frieden Nr. 4, Berlin 1985 oder Hans-Jörg Kreowski: Informatik und Militär: Zusammen in den Abgrund, In: Umdenken in der Informatik [2. Jahrestagung des Forums Informatiker für Frieden und gesellschaftliche Verantwortung e.V., Oktober 1986, Berlin], S. 37-42

3 Dietrich Meyer-Ebrecht: Dual-use und die Zivilklausel: ‚Sicherheitsforschung' – oder wie Rüstungsforschung zivile Forschung vereinnahmt. FIfF Kommunikation 4/2012, S. 56–58

4 Siehe http://www.defense.gov/pubs/DOD-USRM-2013.pdf

5 Ronald C. Arkin: Lethal Behavior in Autonomous Robots, Chapman & Hall/CRC 2009

6 Für ausführlichere Überlegungen dazu siehe Hans-Jörg Kreowski: Gehören Killerroboter vor ein Kriegsgericht, FIfF-Kommunikation 4/2011, S. 27-30

7 Eric Töpfer: Zivil-militärische Sicherheitsforschung. Wissenschaft und Frieden 4/2012, S. 16–19

8 Jürgen Altmann: Grundfragen der Bewertung und Gestaltung von Naturwissenschaften und Technik. In: J. Altmann et al.: Naturwissenschaft – Rüstung – Frieden. Basiswissen für die Friedensforschung. Wiesbaden 2007, S. 451