Thomas Gruber

Die Informatik in der modernen Kriegsführung

Die Berührungspunkte der Informatik mit militärischen Interessen sind zahlreich. Nicht wenige Forschungsgebiete der Informatik werden – meist durch Drittmittelprojekte oder Honorarprofessuren – erheblich von der Rüstungsindustrie oder den nationalen Verteidigungsministerien kofinanziert. In den Universitäten entwickelt sich immer wieder punktueller Widerstand, aus dem ein grundlegender Diskurs über die Militarisierung der Wissenschaften hervorgegangen ist.

Wenn Forschung relevant für militärische Zwecke wird, betrifft dies nicht allein die Forschungseinrichtungen und die ihr angehörenden Forschungsgruppen, es wirkt auch auf die Gesellschaft im Ganzen. Forschung mit militärischen Zielen oder militärisch verwendbaren Ergebnissen arbeitet den aktuellen und den zukünftigen Kriegen zu, und diese führen unabdingbar zu einschneidenden Folgen für die Gesellschaft. Hier steht zunächst einmal die Verantwortlichkeit von Wissenschaftler.innen für die Folgen ihrer Forschungsergebnisse auf dem Prüfstand. Aufgrund der Auswirkungen dieser Ergebnisse auf gesellschaftliche Prozesse außerhalb der Universitäten scheint es deshalb notwendig, den Diskurs auf eine gesamtgesellschaftliche Ebene zu heben.

Trotz einiger medialer Aufmerksamkeit, die vom Pentagon in deutschen Forschungseinrichtungen geförderte militärrelevante Drittmittelprojekte im Jahr 2013 erhielten,[1] bleibt eine gesellschaftliche Diskussion über die universitäre Militärforschung weitgehend aus. Der Blick von außen in den Elfenbeinturm der Wissenschaften scheint ebenso schwer wie der Blick von ihm herab auf die Gesellschaft. Das Ziel dieses Artikels ist es, die Einbettung des Diskurses über Forschung für militärische Zwecke an zivilen Forschungseinrichtungen und über die diesbezügliche Verantwortlichkeit von Forscher.innen in einen gesamtgesellschaftlichen Kontext zu motivieren. Der Fokus soll daher im Folgenden auf zwei zentralen Aspekten dieser Einbettung liegen:

1. Ist die Anwendung einer Erkenntnis, einer Methode oder eines Verfahrens der Informatik in der Technologie oder der Methodik der modernen Kriegsführung ohne Weiteres erkennbar? Und weiter: Wo sind diese Technologie und Methodik ohne Forschungsergebnisse aus der Informatik undenkbar?

2. Welche Fragen und Anforderungen ergeben sich aus dieser Verflechtung bezüglich der Verantwortlichkeit von Forscher.innen? Welche Sonderstellung nehmen die gesellschaftlichen Grundwerte des Friedens und der Wissenschaftsfreiheit in diesem Diskurs ein?

Die erste Fragestellung kann aufgrund der Vielfalt militärrelevanter Forschungsergebnisse aus der Informatik nur exemplarisch behandelt werden. Dabei sollen im Folgenden drei prominente Beispiele aus verschiedenen Bereichen der modernen Kriegsführung auf ihre Abhängigkeit von Forschungsergebnissen aus der Informatik überprüft und einige weitere Beispiele dieser Verflechtung gegeben werden.

Die Informatik im Krieg

Als vergleichsweise junges Forschungsfeld arbeitet kriegsrelevante Forschung in der Informatik vorwiegend einer Kriegstechnologie und -methodik zu, die seit dem Zweiten Weltkrieg entstanden ist. Mit dem Begriff ‚moderne Kriegsführung' werden die aktuellen strategischen Entwicklungen von den historischen Mechanismen des Krieges abgegrenzt. In einer Analyse der historisch einschneidenden Änderungen in der Schlachttaktik und der Modernisierung von Kriegsgerät seit dem Zweiten Weltkrieg[2] lassen sich drei Parallelen in den Anforderungen an die Forschung und Entwicklung für eine moderne Kriegsführung erkennen: die Neu- und Weiterentwicklung von Kriegstechnologie, Methoden für eine kriegsrelevante Informationsakquise sowie Prädiktoren und Analysemodelle zur Unterstützung der Schlachttaktik[3]. In jeder dieser Anforderungen finden sich erhebliche Schnittpunkte zu Forschungsfeldern der Informatik. Gerade in der Steuerung computergestützter Kriegstechnologie sowie der militärischen Informations- und Datenverarbeitung sind diese Überschneidungen am deutlichsten sichtbar – ein Umstand, dem auch in den nachfolgenden Beispielen Rechnung getragen werden soll.

Die Erschließung des Weltraums mittels militärisch genutzter Satelliten steht auf der Agenda beinahe jeder so genannten militärischen Großmacht. Die taktischen Vorteile eines eigenen, sicheren Kommunikations-, Aufklärungs- und Navigationssystems im Kriegsfall sind schwer von der Hand zu weisen. Satellitenbilder sind in der Durchführung eines vermeintlich präzisen militärischen Schlags oft eine Voraussetzung. Neben den dazu benötigten Methoden zur Informationsverarbeitung und -übertragung lässt sich an Militärsatelliten darstellen, wie unverzichtbar eine tiefgehende theoretische Forschung in den Bereichen Informatik, Mathematik und Elektrotechnik, hier speziell Regelungstech-

Thomas Gruber

Thomas Gruber ist Mathematiker und promoviert an der Universität Bremen zum Thema *Verquickung mathematischer und informationstechnologischer Forschung an deutschen Forschungseinrichtungen mit der modernen Kriegsführung*. Er ist Stipendiat der Rosa-Luxemburg-Stiftung und Mitglied der Informationsstelle Militarisierung (IMI) in Tübingen.

nik, ist. Ohne sie wäre beispielsweise eine ausreichend präzise Bahnsteuerung undenkbar. Ein mit genügender Geschwindigkeit in die Erdumlaufbahn geschossener Körper wird sich ohne weitere Steuerung durch die Triebwerke in eine elliptische Bahn um die Erde begeben, die durch viele Einflussfaktoren bestimmt ist. Für künstliche Satelliten, gerade auch die militärisch genutzten, muss eine vorbestimmte Bahn präzise erreicht werden. Kommunikationssatelliten sollen sich als fest ansteuerbare Punkte geostationär, das heißt über einem fixen Punkt der Erdoberfläche, bewegen. Überwachungssatelliten dagegen sollen sich geosynchron bewegen, um einen gewünschten Bereich der Erdoberfläche möglichst regelmäßig abzudecken. Einen Satelliten präzise auf eine vorbestimmte Bahn zu bringen, ist eine hochkomplexe Aufgabe. Zur Realisierung der gewünschten Flugeigenschaften werden Triebwerke benötigt, die zum genau richtigen Zeitpunkt und mit der richtigen Stärke feuern, und das ist ohne eine komplexe algorithmische Unterstützung undenkbar. Bei einer ungewünschten Neigung des Satelliten während des Fluges, sei es durch äußere Einflüsse oder durch eine Fehlzündung der eigenen Triebwerke, muss der Satellit dem Fehlverhalten gegensteuern, da sonst der künstlich erzeugte Orbit verlassen würde. Das dazu implementierte Programm im Steuerungssystem des Flugkörpers muss mathematische Grundlagen der Kontrolltheorie mit der ingenieurswissenschaftlichen Umsetzung in der Regelungstechnik verbinden. Eine zuverlässige, schnell reagierende und minutiös arbeitende Ausgleichssteurung für die Flugbahn des Satelliten ist ohne umfassende theoretische Forschung nicht realisierbar. Die Forschungsergebnisse aus der Informatik bezüglich der flugstabilisierenden und steuernden Algorithmen sind daher eine unverzichtbare Voraussetzung für die Nutzung eines militärischen Satelliten.

Eine Technologie, die neben der Nutzung durch zivile Sicherheitsinstitutionen vor allem in der asymmetrischen Kriegsführung wie in Guerilla- oder Bürgerkriegen Anwendung findet, ist die militärische Überwachung und Spionage. Überwachungs-Hardware des deutschen IT-Sicherheitskonzerns *Utimaco* wurde beispielsweise an das syrische Assad-Regime verkauft, das diese Ausrüstung zum Ausspionieren syrischer Demonstrant.innen nutzte.[4] Die von Utimaco so genannten *Lawful Interception Management Systems* (LIMS) sind vollständige funktionale Überwachungssysteme zum Abfangen privater Kommunikation u. a. über E-Mail, SMS und MMS. Verschlüsselte Kommunikation wird dabei mittels eines integrierten *LIMS-Decoders* gebrochen, und für ihre Weiterverarbeitung werden die gesammelten Kommunikationsdaten vom System wieder verschlüsselt[5] – ein erheblicher kryptographischer Aufwand also, der einer theoretischen Auseinandersetzung mit den verwendeten Kryptosystemen und mit einer algorithmischen Umsetzung der Decodier- und Codiervorgänge bedarf. Solche kryptoanalytischen und kryptographischen Anforderungen sind aktueller Forschungsstand in Mathematik und Informatik, und sie sind daher ohne Forschungsergebnisse aus diesen Disziplinen nicht umsetzbar.

Ein weiteres, viel diskutiertes Beispiel für die Modernisierung der Kriegsführung ist der militärische Einsatz von Drohnen. Überwachungs- oder Kampfdrohnen werden weltweit für Aufklärungs- oder Kriegseinsätze genutzt. Sie tragen zur Entstehung einer Asymmetrie zwischen den Parteien aktueller Konflikte bei. Dabei sind die verwendeten Drohnen nicht einfach ferngesteuerte Kampfflugzeuge, sondern sie sind umfangreich mit schlachtunterstützender Technologie ausgerüstet, die den Pilot.innen die durchzuführenden militärischen Schläge erheblich vereinfacht. Der US-amerikanische Rüstungskonzern *Northrop Grumman* entwickelt derzeit Drohnen mit einer automatisierten Zielerkennung, die aus den im Einsatzgebiet gesammelten Oberflächendaten selbstständig potenzielle militärische Ziele erkennt und identifiziert.[6] Eine solche Zielerkennung erfordert zuverlässige Klassifikatoren, die lernfähig sind und fehlertolerant arbeiten – eine typische Problemstellung im Forschungsbereich des Maschinellen Lernens und der Künstlichen Intelligenz. Hier lässt sich auch ohne genaue Kenntnis des Forschungs- und Entwicklungsstands der Drohnenkomponenten ein unmittelbarer Bezug zur Forschung in der Informatik herstellen, ohne die ein so mächtiger Klassifikator nicht realisierbar wäre.

Als weitere Beispiele könnten die Steuerung autonomer Fahrzeuge, die Forschung an *augmented reality* für das Militär, die Verschlüsselung kriegsrelevanter Daten oder das Brechen etablierter Kryptosysteme genannt werden. All dies sind Beispiele für die vielfältigen Anwendungen informatischer und informationstechnologischer Forschung in der modernen Kriegsführung. Dabei würde eine vollständige Analyse der Verflechtung zwischen Informatik und moderner Kriegsführung ins Uferlose führen.

Der gesellschaftliche Diskurs

Die Methoden der modernen Kriegsführung sind von der Informatik geprägt. Erkennbar ist dies nicht nur für die beteiligten Wissenschaftler.innen, sondern auch bei der Analyse der Kriegstechnologie aus einer gesellschaftskritischen Sicht. Die gesellschaftlichen Auswirkungen dieser Technologie stehen dem gesellschaftlichen Grundwert Frieden entgegen. Gelte es dann nicht, die Rolle von Informatiker.innen in aktuellen Kriegen in den allgemeinen Diskurs um den Krieg einzubinden? Was sind die Punkte, auf die sich dieser Diskurs stützen würde? Wo gestaltet sich ein breiter gesellschaftlicher Diskurs schwierig? Und welche Lösungsansätze gibt es für diese Problematik?

Eine der zentralen Fragestellungen für die Diskussion um friedliche Forschung ist zunächst die Verantwortlichkeit von Forscher.innen: Sind Informatiker.innen für die Nutzung ihrer Forschungsergebnisse verantwortlich, vielleicht sogar, wenn die Anwendung gar nicht ihrer Intention entsprach? Eine militärische (Mit-) Nutzung der Forschungsergebnisse in den Grundlagen oder für zivile Anwendungen (*Dual-Use*) ist kein Novum, doch könnten gerade die Wissenschaftler.innen fachlich am kompetentesten gegen die militärische Nutzung ihrer Forschungsergebnisse argumentieren. Eine solche Ausweitung der Verantwortung wäre also keine utopische Forderung der Gesellschaft an die Forschenden, es wäre die logische Konsequenz einer in allen Teilen nach Frieden strebenden Gesellschaft.

Natürlich gibt es Wissenschaftler.innen, die bewusst und gewollt für militärische Zwecke forschen. Insofern ist außerdem die Rangfolge der Werte *Frieden* und *Wissenschaftsfreiheit* zu klären. Denn sollte die Gesellschaft die Kriegsforschung für unverträglich mit ihren Werten erklären, dann ließe sich diese auch von der Wissenschaftsfreiheit ausnehmen, wie es beispielsweise bereits beim Embryonenschutzgesetz der Fall ist.

Auf Grundlage dieser Diskursansätze ließe sich die universitäre Militärforschung auch in die aktuelle Diskussion um Kriegseinsätze und so genannte Friedensmissionen einbinden. Das wäre ein wichtiger politischer Faktor, um auch auf universitärer Ebene gegen die Forschung für militärische Zwecke argumentieren zu können.

Problematik und Lösungsansätze

Während einige Ideen zur Ausgrenzung militärischer Forschung an Universitäten auf institutioneller Ebene existieren, fehlt für einen breiten gesellschaftlichen Diskurs vor allem eines: die Transparenz. Zivilklauseln, Ethikkommissionen und wissenschaftsethische Reflexion sind institutionelle Lösungsansätze, die zwar dem Ziel friedlicher Forschung zuarbeiten, die öffentliche Diskussion allerdings weitgehend unbeachtet lassen. Mit Geheimhaltungsklauseln versehene oder anderweitig intransparente Forschungsprojekte verhindern bisher die oben geforderte öffentliche Anfechtbarkeit von Forschungsprojekten, die in diesem Sinne fragwürdig sind. Transparenzklauseln zur Offenlegung von Drittmittelförderung oder Landesgesetze zur Transparenz von Forschungsprojekten[7] scheinen daher unabdingbar.

Anmerkungen

1 *Aus dem Fernsehprogramm „NDR Info" vom 25.11.2013*
2 *Vgl. hierzu beispielsweise: David Jordan et al., Understanding Modern Warfare, Cambridge University Press, 2008*
3 *Vgl. hierzu: Thomas Gruber, Verquickung mathematischer und informationstechnologischer Forschung an deutschen Forschungseinrichtungen mit der modernen Kriegsführung, Dissertation im Fachbereich Mathematik an der Universität Bremen, noch unveröffentlicht*
4 *Vgl. hierzu: http://www.bloomberg.com/news/articles/2011-11-03/syria-crackdown-gets-italy-firm-s-aid-with-u-s-europe-spy-gear, aufgerufen am 22.7.2015*
5 *https://www.wikileaks.org/spyfiles/docs/UTIMACO-2010-UtimLIMSLawf-en.pdf, aufgerufen am 22.7.2015*
6 *http://www.northropgrumman.com/Capabilities/Triton/Documents/pageDocuments/Triton_data_sheet.pdf, aufgerufen am 23.7.2015*
7 *Wie beispielsweise im März 2015 vom Bremer Senat verabschiedet: http://landesportal.bremen.de/senat/44488385, aufgerufen am 24.7.2015*

Ute Bernhardt und Ingo Ruhmann

Das Blaumilch-System

Der unerklärte *Information Warfare*

1940 knackten die Briten erstmals mit programmierbaren Rechnern die deutsche ENIGMA-Verschlüsselung. Dieses Wissen wurde bis 1974 als Staatsgeheimnis gehütet. In den dazwischenliegenden 30 Jahren wurde die auf der ENIGMA beruhende kompromittierte Verschlüsselungstechnik weiter von staatlichen Stellen genutzt – und von den Briten geknackt. Dank Edward Snowden haben die Angreifer heute diesen Zeitvorsprung verloren. Wenig mehr als zehn Jahre nach der Entwicklung von digitalen Überwachungs- und Angriffswerkzeugen wie Turmoil, Turbulence *und deren Schwestersystemen wie* XKeyscore *wissen wir heute, in welchem Umfang Datenkommunikation weltweit überwacht und Computer mit solchen Werkzeugen angegriffen und manipuliert werden. Was macht den Unterschied aus?*

Otto Leiberich, lange Jahre Leiter der westdeutschen Zentralstelle für das Chiffrierwesen und nach deren Umwandlung in das Bundesamt für Sicherheit in der I… dessen erster Präsident, konnte si… Verlauf von Interviews, Gespräch… darüber echauffieren, dass erst 19… ENIGMA-Verschlüsselungsverfahren kompromittiert war[1]. Heute sorgt es hingegen kaum noch für Aufregung, dass aktuelle und ehemalige Kabinettsmitglieder im Dutzend und Regierungsmitarbeiter in Kohortenstärke abgehört wurden, dass Verschlüsselungsverfahren und grundlegende IT-Sicherheitsmechanismen ausgehebelt sind. Und dass das alles nicht einmal bemerkt wurde.

Liegt es daran, dass zum Glück kein Krieg mehr herrscht und Politiker sowieso all ihre Kommentare an die Medien geben? Und wir alle dann weiter nur das Glück haben, diese ungefilterte Mitteilungswut der Politik nicht erdulden zu müssen, weil wohlmeinende Journalisten uns nicht damit behelligen? Oder liegt es doch eher daran, dass Politiker auch nur Menschen sind und mit vielerlei missliebigen und politisch inkorrekten Äußerungen aus vielfältig belauschter Kommunikation genauso kompromittierbar sind wie ihre IT-Systeme? Was sollten denn sonst die Anlässe und …nten Angriffe auf die Server des …enn nicht die aus der Überwa… über Absprachen oder persönli… …rungen von Politikern, die nicht mit deren öffentlicher Kommunikation übereinstimmen?

Das Schöne Neue daran ist: Wir werden es erfahren! Und zwar nicht erst in 30 Jahren, sondern bei passender Gelegenheit. Denn zur Kernkompetenz der Geheimdienste gehört nicht nur das Ausspähen, sondern auch das Nutzen der erlangten kompromittierenden Informationen.

Der Rücktritt von Roderich Kiesewetter, CDU-Obmann im NSA-Untersuchungsausschuss, wegen BND-Informanten in seinem Umfeld – oder doch wegen russischer Agenten? – lupft die Decke ein ganz kleines Stückchen von diesem schmuddeligen Tun[2]. Zum Vorschein kommt die munter betriebene Manipulation des politischen Betriebs durch die Dienste, zum Vorschein kommen

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