Dokumentation der öffentlichen Tagung vom 20.02.2015, Berlin

NatWiss
Verantwortung für Frieden und Zukunftsfähigkeit e.V.

Vernetzter Krieg

Inhalt

Vorwort:
Vernetzter Krieg
Von Lucas Wirl

Liebe LeserInnen,

moderne Technologie ermöglicht eine bessere Vernetzung und Netzwerke haben einen immer zentraleren gesellschaftlichen Stellenwert. Auch und gerade in den Kriegen des 21. Jahrhunderts spielt eine – meistens auf neuen Technologien basierende und „klassische“ Kriegsführungsbereiche ausdehnende - Vernetzung eine zentrale Rolle. Dies reicht von der Vernetzung der Gefechtsfelder zu Luft, Wasser, Boden, Weltraum und Cyberspace über Robotisierung und Automatisierung bis hin zur Stärkung der Heimatfront und „embedded journalism“; von enger Kooperation zwischen Wirtschaft/ Wissenschaft mit Militär bis hin zu zivil-militärischer Zusammenarbeit und Auswertung ziviler Daten für die Kriegsführung (siehe gezielte Tötung).

In der vorliegenden Broschüre haben wir die Beiträge der Veranstaltung „Vernetzter Krieg“, die am 20.02.2015 im AStA der TU Berlin mit über 70 Teilnehmenden stattfand, dokumentiert. Neben der genauen Analyse der Vernetzung zu kriegerischen Zwecken gilt es sich intensiver mit der Vernetzung für friedliche Zwecke zu beschäftigen. Es gilt aufzuzeigen welche Vernetzung besteht und es gilt auch Wege aufzuzeigen, wie eine solche Vernetzung gestaltet werden könnte. Diesem werden wir uns verstärkt widmen.

Wir wünschen Ihnen eine erhellende Lektüre.

Mit freundlichen Grüßen,

Lucas Wirl

Lucas Wirl,
Geschäftsführer der NaturwissenschaftlerInnen Initiative Verantwortung für Frieden und Zukunftsfähigkeit (NatWiss)

Vom vernetzten Krieg zum vernetzten Frieden: Die Rolle von Wissenschaft und Technik

Von Jürgen Scheffran

In Grenzbereichen des westlichen Zivilisierungsprozesses entstehen immer neue Muster von Gewalt und Krieg. Mithilfe von Technik durchdringen sie alle Räume und Dimensionen der Gesellschaft, von kleinsten Räumen über unsere Lebenswelt bis zum Planeten und in den Weltraum. Die Vernetzung zwischen Krieg und Gesellschaft betrifft die Ursachen und Folgen ebenso wie ihre Rechtfertigung und Realisierung, die Rolle zivil-militärischer Verflechtungen und die besondere Bedeutung der wissenschaftlich-technischen Entwicklung. Die Bewältigung damit verbundener Probleme bedarf neuer Konzepte nachhaltigen und vernetzten Friedens.

Ursachen, Folgen und Rechtfertigungen vernetzter Kriege

Die heutigen Krisen und Konflikte lassen sich nur verstehen, wenn die systemischen Ursachen in den Blick genommen werden. Im Prozess der expansiven Globalisierung, die die vergangenen Jahrzehnte und Jahrhunderte beherrscht hat, konnten die westlich geprägten Industriestaaten eine ökonomische und technologische Dominanz entwickeln, deren Akzeptanz durch universelle Prinzipien und Werte (Freiheit, Gleichheit, Demokratie, Wohlstand, Toleranz, Menschenrechte und Gewaltfreiheit) hergestellt wird. Während das westliche Erfolgsmodell eine hohe Anziehungskraft ausübt und für einen relevanten Teil der Menschheit Wohlstand bedeutet, ist es im globalen Maßstab widersprüchlich.

Basierend auf dem Prinzip permanenten Wachstums, gerät die kapitalistische Wirtschaft in Widerspruch zu natürlichen Grenzen, allen Versuchen der wissenschaftlich-technischen Naturbeherrschung zum Trotz. Zudem führt sie zur Akkumulation von Wohlstand in den Händen weniger auf Kosten vieler, die daran nur wenig oder gar nicht teilhaben. Dies steht in Widerspruch zum propagierten Wertesystem, das nur für einen Teil der Weltgesellschaft realisierbar ist. Das Versprechen von Wohlstand, Freiheit und Demokratie wird zwar über die Massenmedien in alle Welt transportiert, lässt sich aber bislang nicht überall einlösen. Aufgrund seiner Widersprüchlichkeit erzeugt das globalisierte Wachstumsmodel Differenzen, Grenzen und Spannungen, die Auslöser für Konflikte und Krisen sind.

In diesem Spannungsgefälle versucht das System eine Stabilisierung nach innen mit

einer Abgrenzung nach außen zu verbinden, wobei die Grenzen dynamisch auf Druck von beiden Seiten reagieren. Das westliche Entwicklungsmodell hat in den vergangenen Jahrzehnten eine beispiellose Expansion erlebt, wobei das Überschreiten von Grenzen mit teilweise gewalttätigen Konflikten verbunden war. Hierzu gehören die Konflikte im Gefolge des Ost-West-Konflikts im ehemaligen Jugoslawien und der Sowjetunion ebenso wie die Konflikte in Nahost und in Nordafrika im Gefolge des Arabischen Frühlings. Hier zeigten sich politische Grenzen der Expansion, etwa durch Konkurrenzen um Einflusszonen mit anderen Mächten wie Russland und China oder durch eine fehlende Akzeptanz gegenüber westlichen Werten. Zu nennen sind religiöse Differenzen, die zum Nährboden für Islamismus und Terrorismus werden, rechtspopulistische Strömungen gegen Gleichheit und Toleranz ebenso wie radikale Bewegungen gegen Ausbeutung und Ungerechtigkeit oder auch Differenzen zwischen „moderner" Stadtbevölkerung und „traditioneller" Landbevölkerung in vielen Teilen der Erde. Verstärkt werden solche Spannungen durch Krisenerscheinungen im kapitalistischen System, die dessen Attraktivität untergraben wie die Finanzkrise von 2008 oder die Griechenlandkrise, die tiefgehende Bruchlinien in Kernzonen des Systems offenbaren und Widerstände verstärken. Langfristig konfliktär sind die ökologischen Grenzen des Wachstums aufgrund der begrenzten Verfügbarkeit natürlicher Ressourcen und des Klimawandels, die dem Streben nach Wohlstand für alle im Wege stehen.

Das komplexe Ursachengeflecht heutiger Krisen schafft immer neue Gründe für Konflikte, die sich zu kaum lösbaren vernetzten Kriegen und Gewaltspiralen aufschaukeln können. Die Konfliktlinien verlaufen überall dort, wo das Spannungsgefälle widersprüchlicher Tendenzen am größten ist: im Mittelmeerraum zwischen Südeuropa, Nordafrika und Nahost, innerhalb der Ukraine zwischen Ost und West, in den Drogenanbaugebieten Afghanistans und Mittelamerikas und in den Rohstoffgebieten Afrikas, in den Regenwäldern der Welt und in ökologisch degradierten Zonen, ebenso in den Slumgebieten der Megastädte, an den Bruchlinien der Religionen und generell zwischen Arm und Reich.

Das System reagiert auf Krisenerscheinungen und damit verbundenen Risiken mit immer neuen Interventionen, die eine Kontrolle herstellen sollen. Wenn von einer Verantwortung Deutschlands in der Welt die Rede ist, geht es weniger um die eigene (Mit-) Verantwortlichkeit für die Krisen der Welt, sondern vielmehr um die Verantwortbarkeit von Eingriffen, ungeachtet der Frage, ob damit Öl ins Feuer gegossen wird oder eigene Prinzipien (etwa gegen Gewalt) über Bord geworfen werden. Der Verweis auf die moralische Verantwortung ermöglicht Handlungen gegen jedwede Bedrohung eigener Werte von außen und lenkt zugleich ab von den systemimmanenten Gefährdungen ebendieser Werte von innen, durch Demokratieabbau, Geheimdienste, Umweltzerstörung und Ungerechtigkeit. So wird es möglich, zur Abwehr von Terroristen oder Migranten einen größeren Sicherheitsapparat aufzubauen als zur

Vermeidung des Klimawandels oder ökonomischer Krisen, selbst wenn diese weit größere Probleme darstellen und Ursachen eben dieser Phänomene sind.

Netzwerke der Gewalt

So sehr bei vernetzten Kriegen die Ursachen, Folgen und Rechtfertigungen aufs Engste mit den gesellschaftlichen Strukturen verbunden sind, so sehr gilt dies für ihre Umsetzung und Durchführung. Wenn die gesamte Gesellschaft vom Krieg betroffen ist, verliert die klassische Trennung zwischen Soldat (lat. miles) und Bürger (lat. civilis) an Bedeutung. Die „Bürger"-Kriege in Ruanda und Ex-Jugoslawien ebenso wie die gewaltsamen Konflikte in Afghanistan, im Libanon, in Syrien oder im Irak durchziehen die Gesellschaften dieser Länder. Ohne klare Fronten agieren Streitkräfte innerhalb der Gesellschaften und sind damit deren Logiken unterworfen. Das Gegenstück eines entgrenzten, alles durchdringenden Krieges findet sich auch in den westlichen Industrienationen, trotz aller Versuche der Abgrenzung und Ausgrenzung. Die Terroranschläge des 11. September, die auch in den USA vorbereitet wurden, verwendeten zivile Passagierflugzeuge, um zivile Ziele inmitten einer Großstadt zu treffen. Der darauf erklärte „Krieg gegen den Terror" durchzieht die Zivilgesellschaften des Westens, lässt Koffer in einem Flughafen oder Bahnhof, jede Cyberattacke als möglichen Teil eines kriegerischen Gewaltakts erscheinen. Die Flüchtlinge aus den Krisengebieten, die nach Europa „vordringen", werden zu unfreiwilligen Kombatanden an einer „Heimatfront", an der innere und äußere Sicherheit verschmelzen, was im Begriff der „Homeland Defense" in den USA offenkundig wird. Bezeichnenderweise war die erste Belastungsprobe für die Heimatverteidigung in den USA nicht ein Terroranschlag, sondern eine Naturkatastrophe, der Wirbelsturm Katrina 2005. Sie ist gründlich schief gegangen.

Noch desaströser war der Versuch der USA, mit überwältigender Militärmacht den Irak besetzt zu halten, ignorierend dass eine Demokratisierung des Irak eine gesellschaftliche Aufgabe ist, die ganz andere, vor allem zivile Mittel erfordert. Statt den Irak zu „befrieden", wurde noch Öl ins Feuer gegossen. Der gewaltsame Widerstand gegen die als Besatzer empfundenen US-Truppen konnte sich an jeder Hausecke oder Straßenkreuzung entzünden und hat letztlich zur Entstehung des Islamischen Staates beigetragen.

Damit einher ging eine Privatisierung der Sicherheitsdienste, das Entstehen moderner Söldnerheere. Die Fraktionierung der Gewaltstrukturen bringt unermessliches Leid über die Zivilbevölkerung, sie zerstört soziale und politische Strukturen – u.a. in zahlreichen Ländern Afrikas. Dauerkriege, verbunden mit Massenmord und millionenfacher Flucht und Vertreibung, sind die Folge. An der gesellschaftlichen Basis wächst damit ein Potential der Verarmten und Entwurzelten, der Missachteten und Empörten heran, das einen Nährboden für jede Form der Radikalität bietet, dem Islamismus Menschen zutreibt. Durch Vernetzung kann die Unzufriedenheit auf der lokalen Ebene in nationale und globale Netzwerke der Gewalt einbezogen werden. Verbrecher- und Terrornetze agieren

weltweit, der Drogen- und Waffenhandel floriert und ist über eine Schattenwirtschaft mit der globalen Ökonomie verknüpft.

Zivil-militärische Verflechtungen

Die Vernetzung des Krieges betrifft auch die Vorbereitung, Planung und Durchführung von Gewalteinsätzen in Industrieländern, die sich gesellschaftliche Strukturen zunutze machen und mit struktureller Gewalt einhergehen kann. Dies erfolgt unter Ausnutzung fließender Übergänge zwischen zivilen und militärischen Infrastrukturen, inklusive Wissenschaft und Technik, Information, Kommunikation und Medien, Wirtschaft und kritischen Infrastrukturen bis hin zu den politischen Entscheidungsebenen.

Im Rahmen einer gesellschaftlichen Gesamtmobilisierung nutzt das Militär die zivil-militärische Zusammenarbeit, die dem Militär neue Spielräume eröffnet und zivile Ressourcen in die Militärplanung einbezieht. Entsprechend widmet sich die Bundeswehr verstärkt der Koordinierung zivil-militärischer Beziehungen und der Unterstützung von bewaffneten Streitkräften und der zivilen Umgebung. Hierzu gehören die Koordinierung von Planungen der zivilen und militärischen Verteidigung ebenso wie Vorsorgemaßnahmen für die Zivilbevölkerung und die Streitkräfte, die Einbindung der Streitkräfte in die Zivil- und Katastrophenschutzplanung und in die Einsatzplanung bei sogenannten Großschadensereignissen. Im weiteren geht es um die Zusammenarbeit in allen Bereichen des Umweltschutzes, der Raumordnung und der Konversion.

Dabei wird ausdrücklich zwischen Truppenführung im Kampf und bei Friedensmissionen unterschieden, wobei der Kampf nicht nur auf herkömmliche Kriege, sondern mit dem Oberbegriff des bewaffneten Konfliktes auf alle Erscheinungsformen sozialer Gewalt ausgedehnt wird, die mit Waffen ausgefochten werden. Bei der Informationsgewinnung wird auch auf internationale und Nicht-Regierungs-Organisationen zurück gegriffen, die über zusätzliche Information verfügen. Damit verbundene Probleme bei der Einbindung in militärische Befehlsstrukturen werden anerkannt, das unterschiedliche Selbstverständnis ziviler Organisationen und das Primat der Politik werden nicht bestritten.

Auch wenn eine Zusammenarbeit zwischen zivilen und militärischen Einrichtungen bei Friedensmissionen erfolgt, sind grundsätzliche Unvereinbarkeiten ziviler und militärischer Aufgaben und Einsatzmittel nicht zu übersehen. Nicht geeignet ist Militär für den Prozess der Staatenbildung und Demokratisierung, den Aufbau einer Volkswirtschaft, die nachhaltige Ressourcensicherung und den Umweltschutz. Genauso wenig lassen sich zivilgesellschaftliche Kräfte einfach in militärische Strukturen und den gewaltsamen Konfliktaustrag einbinden. Die Logik betriebswirtschaftlicher Rationalisierung verbirgt, dass sich auch das Militär ziviler Ressourcen bedient, um eigene Budgets zu schonen. Im Kontext von Krisenreaktionskräften und Antiterrorkriegen kann eine gesellschaftliche Mobilisierung unter militärischen Kalkülen eine Totalisierung von Konflikten befördern und Gewalteinsätze legitimieren. Statt Unterschiede zwischen zivil und militärisch

zu verwischen, sollten sie deutlicher gemacht werden.

Wissenschaft und Technik in vernetzten Kriegen

Wissenschaft und Technik spielen eine Schlüsselrolle in allen Bereichen der Gesellschaft und so auch im Netz globalisierter Gewalt. Getrieben von dem Streben nach militärischer Überlegenheit macht sich das Militär die Ergebnisse wissenschaftlicher Forschung immer umfassender zu Nutzen, von der Grundlagenforschung bis hin zur anwendungsnahen Entwicklung. Atomwaffen und Raketen, Satelliten, Anti-Satellitenwaffen, Raketenabwehr und Lasertechnologie, technische Intelligenz, Drohnen, Robotik und Cyberspace erlauben Macht- und Gewaltprojektionen über den ganzen Planeten und in den erdnahen Weltraum. Die ganze Hochtechnologie-entwicklung wird militärischen Verwertungs-interessen unterworfen, unter Ausnutzung des Dual-use des zivilen Technologiezweigs. Nach Ende des Ost-West-Konflikts wurde aufgrund der Notwendigkeit von Kosteneinsparungen und geringerer öffentlicher Akzeptanz für den Militärsektor die Ambivalenz der Forschungsergebnisse systematisch genutzt.

Dies betrifft zum einen die globale Vernetzung moderner Transport-, Informations- und Kommunikationssysteme ebenso wie die Verschmelzung von Mikro-, Nano- und Biotechnologien, die Macht- und Gewaltprojektionen in kleinsten Räumen ermöglicht. Sie verknüpfen die Globali-sierung der Gewalt mit der Miniaturisierung von Gewalt, was in den Informationskriegen auf unseren Computern ebenso zum Ausdruck kommt wie im Krieg der Mikroben oder Mini-Kampfroboter. Durch sie findet der Krieg weiter Einzug in unseren Nahbereich, unsere Wohnung, ja in den menschlichen Körper, der über technische Systeme mit globalen Strukturen vernetzt ist. Globale (Un-)Sicherheit und menschliche (Un-)Sicherheit sind so aufs engste verbunden.

Technisch vermittelte Netzwerke haben einen immer wichtigeren gesellschaftlichen Stellenwert. Auch und gerade in den Kriegen des 21. Jahrhunderts spielt eine technologisch realisierte Vernetzung eine zentrale Rolle, von der Vernetzung der Gefechtsfelder zu Luft, Wasser und Boden, im Weltraum und im Cyberspace über die Robotisierung und Automatisierung bis hin zur Heimatfront und zur Medienwelt.

Technikentwicklung zwischen Wirtschaftswachstum und Natur-zerstörung

Der Multiplikator- und Vernetzungseffekt der Technik hat eine besondere Bedeutung in der auf Wachstum ausgerichteten kapitalistischen Ökonomie, die technische Produktionsmittel in Form von Kapital anhäuft. Das baconsche Programm der wissenschaftsgeleiteten Technikentwicklung konnte in Teilen der Welt die Mühsal der menschlichen Existenz erleichtern und sorgte dafür, dass trotz begrenzter Ressourcen rund zehnmal so viele Menschen auf der Erde existieren können wie vor der Industriali-sierung. Es stellt sich die Frage, wie lange sich Wohlstand noch steigern lässt, ohne

dass die Folgen der Technik dessen Grundlagen untergraben. In der wirtschaftlichen Konkurrenz führen effektivere Produktionstechniken zu Wettbewerbsvorteilen durch Profitsteigerung und letztlich zur Ausschaltung von bzw. Fusion mit Konkurrenten, um deren Kapazitäten einzubinden – ein Äquivalent zur Konzentration in der Gewaltspirale.

Eine zentrale Rolle spielt Technik auch für den Konflikt zwischen Mensch und Natur. Dies betrifft zum einen die technischen Systemen zugrunde liegenden natürlichen Faktoren und Ressourcen, zum anderen die Wirkung des Technikeinsatzes auf die Natur, die zur Zerstörung von Ökosystemen, Lebensräumen und Artenvielfalt führt und diese zu Konfliktfeldern macht. Der von Malthus vor mehr als 200 Jahren prognostizierte baldige Zusammenbruch der menschlichen Population konnte mit neuen Erfindungen immer wieder verschoben werden. Ging es bei der Industrialisierung darum, Naturressourcen in großem Maßstab in die Erzeugung von Produktions- und Destruktionsmitteln zu schieben, so werden die Grenzen des expansiven und verschwenderischen Umgangs mit der Natur in Umwelt- und Ressourcenkonflikten sichtbar.

Neben dem Naturverbrauch auf der Verursacherseite tritt die destruktive Seite der Technik auch auf der Folgenseite hervor. Dies wird sichtbar bei der fossilen Energieversorgung, die ein breites Feld für Technikkonflikte aller Art war und ist, so bei der Einbeziehung von Kohle, Erdöl und Erdgas – als Ressource wie als Konfliktgegenstand – in die Kriegführung im Ersten und Zweiten Weltkrieg, im Kalten Krieg sowie in diversen Kriegen in Nahost und in der Kaukasusregion. Unkonventionelle Methoden der Gewinnung fossiler Energieträger sind nicht nur mit steigenden Kosten, sondern auch mit Umweltfolgen verbunden, so bei der Gewinnung von Ölsänden, Schiefergas oder Erdgas durch Fracking, was ebenso zu Protesten führt wie Ölbohrungen auf See oder in der Arktis.

Am deutlichsten wird dies beim Klimawandel, der durch die Freisetzung fossiler Treibhausgasemissionen das gesamte Erdsystem zu destabilisieren droht und damit neue Sicherheitsrisiken und Konfliktfelder eröffnet. Erscheint der Klimawandel zunächst noch als unbeabsichtigte Nebenfolge des fossilen Entwicklungspfades der Menschheit, so könnte der Versuch, mit Hilfe von Geoengineering im Anthropozän die Kontrolle über den Planeten zurückzugewinnen, zum Fiasko einer wider die Natur handelnden Technikgläubigkeit geraten.

Risikogesellschaft, technische Verwundbarkeit und gesellschaftliche Umbrüche

Auch das Versagen der Technik birgt erhebliche Risiken und Konfliktpotentiale, insbesondere in großtechnischen Systemen, in denen sich kleine Fehler zu Katastrophen aufschaukeln können. Spektakuläre Unfälle mit Risikotechnologien (Bhopal, Challenger, Tschernobyl) zeigten, dass Großtechnologien (Chemie- und Atomtechnik, Bio- und Gentechnologie, Luft- und Raumfahrt, Rüstungstechnik) nicht vollständig

beherrschbar sind und ein „Restrisiko“ schaffen, das mit Naturkatastrophen vergleichbar sein kann. Bei der Kernenergie treten Risiken über die gesamte nukleare Kette auf: von Uranminen über Unfälle und den Transport radioaktiver Materialen bis zur ungelösten Endlagerproblematik. Da bei komplexen Systemen nicht alle Eventualitäten vorherbestimmbar sind, genügt ein geringfügiges Ereignis, um eine Ereigniskette auszulösen, die bei gekoppelten Mensch-Maschine-Systemen als „normale Katastrophe“ erscheint.

Ein spektakuläres Beispiel für eine Risikokaskade, in der Natur und Technik zusammen wirkten, war das Erdbeben in Japan vom 11. März 2011, das eine Kette von Ereignissen mit globaler Wirkung in Gang setzte. Die Tsunami-Welle zerstörte in Fukushima mehrere Reaktoren, deren radioaktives Inventar sich über die Atmosphäre und den Ozean nicht nur lokal, sondern auch global ausbreitete. Direkt oder indirekt davon betroffen waren das japanische Stromnetz, die Nuklearindustrie, Aktienmärkte, der Ölpreis und die Weltwirtschaft. Autohersteller und Elektronikfirmen drosselten weltweit die Produktion, weil wichtige Teile aus Japan nicht mehr geliefert wurden. Die Schockwellen der Nuklearkatastrophe lösten in Deutschland die Energiewende aus. Diese Katastrophe zeigt eindrücklich, wie ein Einzelereignis kaskadenartig über globale Netzwerke verschiedene Prozessketten in Gang setzen und miteinander verknüpfen kann. Sie zeigt auch, wie die Risikohaftigkeit von Technik Widerstände und Proteste auslösen.

Neben Erdbeben oder technischen Unfällen können auch Klimawandel und Wetterextreme kritische Infrastrukturen und Versorgungsnetze treffen, die für die Aufrechterhaltung menschlicher Existenz wichtig sind. Hierzu gehören Systeme für die Versorgung mit Wasser, Nahrung und Energie, mit Gütern und Dienstleistungen, Systeme für die Bereitstellung von Kommunikations-, Gesundheits-, Transport- und Sicherheitsdienstleistungen sowie menschliche Siedlungen und politische Institutionen. Dabei ist nicht nur das Versagen von Teilsystemen von Bedeutung, sondern auch die Möglichkeit, dass sich das Versagen auf Kopplungen ausbreiten und das gesamte System gefährden kann. So führten Wetterextreme in Deutschland, wie die Hitzewelle 2003, die Sturmflut 2013 oder das Elbhochwasser im selben Jahr, zu Beeinträchtigungen des (Zug-)Verkehrs und der Energieversorgung. Im November 2005 ereignete sich nach heftigen Schneefällen in Nordrhein-Westfalen und Niedersachsen einer der größten Stromausfälle in der deutschen Geschichte.

Mit der wachsenden Abhängigkeit von technischen Infrastrukturen nimmt auch ihre Verwundbarkeit gegenüber Angriffen oder Missbrauch zu. Wenn der Mensch Teil der Maschine ist, kann er sie willentlich in den Untergang steuern, indem die eingebauten Wirkmechanismen einem von den Konstrukteuren nicht geplanten Zweck zugeführt werden. Durch den „Missbrauch“ wird aus der Möglichkeit einer nicht intendierten Nebenfolge die konkrete Gefahr, diese absichtlich auszunutzen. Flugzeuge, Fahrzeuge, Schiffe, Reaktoren, die Chemieindustrie, das Internet oder

Stromnetze können nicht nur Ziel von Gewalthandlungen sein, sondern auch selbst zur Waffe werden. Die von Allmachtsphantasien getriebene Wahnsinnstat wird nicht nur ergriffen, weil sie gewollt ist, sondern auch, weil sie durch den Verstärker- und Multiplikatoreffekt der Technik möglich wird und dazu verführt. Durch das Internet erhält das Individuum Zugriff auf riesige Informationsmengen und die Macht, gezielt Knoten des globalen Netzes nicht nur ausschalten, sondern für destruktive Zwecke einzusetzen. Das Netz wird Ziel von Gewalthandlungen, alle daran angebundenen Systeme werden zur potentiellen Waffe.

Durch technologische Umwälzungen beschleunigt sich die gesellschaftliche Entwicklung rasant und erlaubt es, Energie- und Informationsflüsse über wachsende Entfernungen in immer kleineren Zeiträumen auszutauschen. Alle jederzeit erreichen zu können, bedeutet auch, für Alle immer erreichbar zu sein. Der Prozess der permanenten Grenzüberschreitung durch Technik bestimmt so die menschliche Lebenswelt und macht immer mehr Lebensfunktionen von technischen Systemen abhängig. Die Beherrschung komplexer technischer Systeme bedarf eines fortwährenden Lernprozesses der Anpassung in technisch konstruierten Welten, die den Menschen zum Teil der Maschinerie machen.

Dies gilt für Individuen ebenso wie für staatliche Organe. Mit vernetzter Technik wird der Einflussbereich des Staates auf alle gesellschaftlichen Bereiche ausgedehnt. Polizei, Justiz, Militär und Geheimdienste nutzen die neuen Machtmittel und lassen sich nur widerwillig dabei einschränken, wie beim NSA-Skandal ersichtlich. Bei der Steuerung sozialer und politischer Prozesse kann Technik bestehende Macht- und Herrschaftsstrukturen verstärken, aber auch überwinden helfen. Technik dient als gesellschaftliches Herrschaftsinstrument, das die Macht staatlicher Institutionen stärkt und die Bereitschaft zur Machtteilhabe einschränkt, oft mit dem Argument, Technik dürfe nicht in „falsche“ Hände geraten. Dies gilt auch für die Mittel der Überwachung und Steuerung. Wer glaubt, die Welt durch Spionagesoftware, Drohnen oder Mikroroboter sicherer zu machen, wird sich am Ende durch diese selbst bedroht sehen.

Vernetzter Frieden und soziale Bewegungen

Was kann getan werden, um die Teufelskreise vernetzter Kriege zu durchbrechen? Netzwerke können die Entstehung demokratischer und partizipativer Strukturen fördern und Chancen für Zusammenarbeit, Friedenssicherung und Konfliktlösung auf lokaler, regionaler und globaler Ebene eröffnen. Jedes Individuum ist Knoten im globalen Netzwerk und kann sich die Strukturen als Machtverstärker zunutze machen, auch Kritiker und Aktivisten. Netzwerke für den Frieden gab es auch ohne Internet, so die Friedensbewegung Anfang der achtziger Jahre, die weltweit die öffentliche Debatte beherrschte. Die globale Protestbewegung gegen den Irakkrieg konnte diesen 2003 zwar nicht verhindern, jedoch mithilfe digitaler Netze eine relevante Gegenmacht aufbauen. Beim Arabischen Frühling waren soziale Medien bereits ein bestimmendes Moment,

auch wenn die Bewegung einen friedlichen Umbruch nicht auf Dauer erreichen konnte. Statt auf Probleme nur zu reagieren, ist es für eine nachhaltige Friedenssicherung wichtig, Konfliktursachen präventiv zu vermeiden: durch Naturschutz und Ressourceneffizienz, Begrenzung des ökologischen Fußabdrucks, angepasste Technologien und Lebensweisen, gerechte Verteilung und Kooperation, Dialog und Partizipation.

Es gibt auch eine lange Geschichte sozialer Bewegungen, die sich kritisch mit den Folgen der Technik auseinandersetzten, von den Maschinenstürmern über die Arbeiterbewegung bis zur Studenten- und Umweltbewegung. Dabei geht es um den Streit, welche Richtung die technische Entwicklung nehmen oder nicht nehmen soll, um Interessensgegensätze und um den Umgang mit Risiken. Dabei können Protest, Widerstand und Whistleblowing helfen, negative Entwicklungen an die Öffentlichkeit zu bringen, inakzeptable Folgen und Risiken zu vermeiden oder Win-Win-Lösungen zu stärken.

Um mit solchen Fragen umzugehen, bedarf es geeigneter Entscheidungsprozesse im Lebenszyklus der Technikentwicklung, von der Grundlagenforschung über die Erprobung bis zu Einsatz, Recycling und Abfallverwertung. Es geht auch um Lern- und Aushandlungsprozesse, die Differenzen und Konflikte auf konstruktive Weise lösen und kooperative Strukturen schaffen. Verschiedene Konzepte können im Rahmen des vernetzten Friedens zusammenwirken: präventive Rüstungskontrolle und Zivilklauseln zur Eindämmung der militärischen Verwendung von Forschung und Technik; nachhaltige und effiziente Ressourcennutzung, um die Belastung für Mensch und Natur durch Technik auf der Verursacher- und Folgenseite zu verringern; die Nutzung von Technologien, die die soziale Kompetenz stärken und gemeinsames Handeln zur Problem- und Konfliktbewältigung ermöglichen; Partizipation der Bevölkerung an Entscheidungs- und Nutzungsprozessen, um demokratisch legitimierte Entscheidungen und einen Interessenausgleich zwischen gesellschaftlichen Gruppen und Stakeholdern zu ermöglichen; und politische Regulierungsmechanismen, die die Entwicklung einer verantwortlichen Technikfolgenabschätzung und Technikgestaltung erlauben.

Jürgen Scheffran ist Professor am Institut für Geographie der Universität Hamburg und leitet dort die Forschungsgruppe Klimawandel und Sicherheit. Er arbeitet in der Redaktion der Zeitschrift Wissenschaft und Frieden und ist Mitglied in verschiedenen Wissenschaftsorganisationen (u.a. Natwiss, FONAS, VDW, INES).

Dieser Beitrag erscheint in der Zeitschrift FIFF-Kommunikation 3/2015 und wurde leicht verändert (Stand August 2015). Er basiert auf:
Scheffran, J. (2015) Vernetzter Krieg, Vortrag bei der Beiratssitzung der Naturwissenschaftler-Initiative Verantwortung für den Frieden, Berlin, 20.02.2015.
Scheffran, J. (2015) Technikkonflikte in der vernetzten Welt, Wissenschaft und Frieden, 02/2015, S. 6-10.

Information Warfare: Der vernetzte Krieg und seine neuen Werkzeuge

Von Ute Bernhardt und Ingo Ruhmann

Keine Technologie verändert die Kriegsführung derart wie die Informationstechnik. Der Computereinsatz hat die Kriegsführung immens beschleunigt und erlaubt die Steuerung von Waffensystemen rund um den Globus. Die Informationstechnik ist aber selbst nicht nur Kriegswerkzeug, sondern wird zum Ziel von Angriffen. Es ist erst wenige Jahre her, dass mit Computerattacken auf Länder und staatlich entwickelten Computertrojanern handfeste Hinweise auf staatlich verantwortete Computerattacken publik wurden. Die durch Edward Snowden ermöglichten Enthüllungen zeigten der Öffentlichkeit, in welchem Ausmaß Cyberattacken heute zum Bestandteil militärisch-geheimdienstlicher Aktivitäten gehören und welchen Preis die Zivilgesellschaft dafür zahlt.

Die Entstehung des Computers in Großbritannien, den USA und Deutschland ist untrennbar mit seiner militärischen Nutzung verbunden: der Konstruktion von Atombomben und Lenkwaffen sowie der Entschlüsselung[1]. Auch die erste Phase der Computerentwicklung profitierte von militärischen Anforderungen. Erst durch vernetzte Computersysteme wurde die Kontrolle atomarer Waffensysteme in globalen militärischen Kommandonetzwerken möglich. Dier erste Generation integrierter Schaltungen – Computerprozessoren – diente in Atomraketen der stark verbesserten Zielgenauigkeit[2].

Das in den 1950er Jahren entwickelte globale System zur Lageüberwachung der atomaren Abschreckung wurde in den 1960er Jahren transformiert in ein taktisches Werkzeug zur vernetzten Kriegsführung. Im Vietnamkrieg entstand erstmals ein System, das Funkdaten von abgeworfenen Bodensensoren an ein Überwachungsflugzeug lieferte, von dem aus die Daten zur Auswertung durch Großrechner in ein Kontrollzentrum nach Thailand flossen. Von dort wurden nach wenigen Minuten automatisch neue Zielkoordinaten an Bomber über dem Zielgebiet übermittelt[3]. Mit diesem System einer automatisierten Entscheidungsfindung

[1] Die ersten programmierbaren digitalen Computer dienten in den USA der A-Waffenentwicklung, in Großbritannien der Entschlüsselung der Wehrmachts-Codes und in Deutschland dem Bau von V1-Abstandswaffen. Vgl. zur Geschichte: Reinhard Keil-Slawik: Die neue Waffe - Der Computer; in: Nehmer, J. (Hg.), GI - 12. Jahrestagung, Berlin Heidelberg New York 1982.

[2] Holger Iburg: Abschreckung und Software: Computertechnologie als Instrument der amerikanischen Sicherheitspolitik Frankfurt, 1991; Bernhelm Booß-Bavnbek; Jens Høyrup (Eds.): Mathematics and War; Basel, 2003.

[3] Paul N. Edwards: The Closed World. Computers and the Politics of Discourse in Cold War America, Cambridge, 1993, S. 3f. Siehe dazu auch den freigegebenen Bericht: Col. Jesse C. Gatlin: Project CHECO Southeast Asia Report. Igloo White , 31.

und militärischen Kontrolle hielt der Computer Einzug auf dem Schlachtfeld.

Diesem Muster folgend dient heute die militärische Nutzung von Computern und Datenkommunikation dem kontrollierbaren Einsatz einzelner zielgenau wirkender Waffen und einzelner Soldaten. Das in den Medien heute dargestellte moderne Gegenstück von „Igloo White“ ist die Suche nach Sprengfallen im Irak und Afghanistan. Mit Drohnen und dem Überwachungsflugzeug J-STARS werden Radar- und optische Daten gesammelt und an Bord mit leistungsfähigen Computern verarbeitet. Bei einem Anschlag mit einer Sprengfalle werden die Spuren verdächtiger Fahrzeuge, aus denen die Sprengfalle vermutlich abgelegt wurde, zurück verfolgt und Zielkoordinaten an Kampfdrohnen oder Bomber übermittelt. An dem Ablauf dieser Operationen hat sich seit „Igloo White“ vor 40 Jahren wenig geändert.

Was die mediale Darstellung nicht vermittelt, ist das räumliche Ausmaß, in dem diese Technik heute eingesetzt wird. Dieses IT-gestützte voll integrierte militärische Kommando- und Kontrollsystem umspannt heute den Globus. Der Einsatz von Kampfdrohnen überall in Krisengebieten auf dieser Welt beruht auf einer Sammlung von Daten für die taktische Entscheidungsfindung und deren Aufbereitung zur Steuerung militärischer Operationen. Ohne Unterbrechung wird der Globus auf allen Ebenen des optischen und elektronischen Spektrums mit Sensoren aufgeklärt; die Daten werden in Kommandozentralen wie etwa der im Weißen Haus übermittelt. Die durch vernetzte Computer ermöglichte Geschwindigkeit dieses Systems bestimmt die Intensität global vernetzter Kriegsführung.

Ein Ergebnis dieser Vernetzung war die bessere Kenntnis der militärischen Lage vor Ort. Die Zunahme der produzierten Sensordaten vermittelt an zentrale Kommandostellen eine bessere Lagebewertung, Koordinierung und erhöhte Operationsgeschwindigkeit von Kampfeinsätzen. Die Datenvernetzung der Kommandostellen mit den Soldaten verbessert deren Kenntnis der eigenen unmittelbaren Umgebung („situational awareness“) und stärkt ihre Kampfkraft. Der Computerverbund auf dem Schlachtfeld ist damit heute auch bei dem einzelnen Soldaten angekommen.

Während die seit 20 Jahren diskutierte „Revolution in Military Affairs“ – also die Vernetzung kleiner Einheiten und ihre stärkere Autonomie – sich in der Praxis trotz vieler Anläufe gegen hierarchische militärische Strukturen nicht durchgesetzt hat, ist das zur selben Zeit formulierte Paradigma der Vernetzung als „Information Warfare“ heute etabliert.

Die umfassende und systematische Nutzung vernetzter Computer für militärische Operationen hat ihren Ursprung in der 1982 für die US-Streitkräfte formulierten AirLand-Battle-Doktrin, die von der NATO 1984 übernommen wurde[4]. AirLandBattle war der Auslöser für massiv ausgeweitete Kapazitäten

July, 1968, http://www.dtic.mil/dtic/tr/fulltext/u2/a485055.pdf . Der Name der „Operation Igloo White“ entstand aus der weißen Außenfarbe des riesigen Datencenters.

4 Konzeption: Department of the Army: The AirLand Battle and Corps. TRADOC Pamphlet 525-5. In: Militärpolitik Dokumenta-

computergestützter Aufklärung. Angewendet wurde dies erstmals bei der Operation „Desert Storm", dem ersten Irakkrieg 1991. Die Ergebnisse dieses Krieges und der gezielte Einsatz von Präzisionswaffen führten wiederum zur Weiterentwicklung und Formulierung des Field Manuals 100-6 „Information Operations"[5].

Damit ist Information Warfare seit nun 20 Jahren reguläre militärische Doktrin der USA. Mit dieser Doktrin basiert die Kriegsführung der US-Streitkräfte und seit der Jahrtausendwende auch zahlreicher NATO-Staaten auf dem Einsatz vernetzter Computer, Datenerhebung aus der permanenten Aufklärung und der elektronischen Kriegsführung.

Sicherheitspolitische Folgen

Die vorhersehbaren sicherheitspolitischen Folgen[6] sind heute evident: Zur globalen Projektion und Ausübung militärischer Macht werden als Vorbereitungshandlung insbesondere potentielle Krisengebiete einer intensiven dauerhaften Überwachung unterzogen. Die technischen Grundlagen dafür sind global einsetzbare Aufklärungs- und Spionage-Ressourcen sowie kleine, aber schnell und global einsetzbare mobile Truppenteile. Die durch Information Warfare bereit gestellten Grundlagen für den Einsatz von Abstands- und Präzisionswaffen erfordern immer weniger eine physische Truppenpräsenz. Das heutige Ergebnis ist eine auf Dauer angelegte und globale Projektion und Ausübung militärischer Gewalt.

Mit ihrer wachsenden Bedeutung wurden IT-Systeme selbst ebenso zum Mittel wie auch zum Ziel in Konflikten: Der Schutz von Computern in Kommandonetzen und der Angriff auf solche IT-Systeme ist eine logische Konsequenz aus der großen Bedeutung, die Computer für die Kriegsführung haben. Nachdem Computer in den 1980ern zu genuinen Werkzeugen und Zielen der Kriegsführung wurden, hat sich heute das Anwendungsfeld digitaler Technik - oder „Cyberwelt" - zu einem genuinen Kampfraum mit denselben Denkmustern entwickelt: Eine Aufklärung rund um die Uhr, Informationsdominanz und Manipulation in einem „Cyberspace" als Kampfraum[7].

Die vorgesehenen Mittel in diesem Kampf – „Information Operations"[8] – beginnen mit der Beeinflussung der Medien, gehen über zum Ausspionieren von Daten und weiter zum Einsatz von Schadsoftware gegen Computer. Weiterer Eskalationsschritt ist die „physische Destruktion" von Infrastrukturen, im Extremfall sogar unter Einsatz von Atomwaffen zur Erzeugung eines

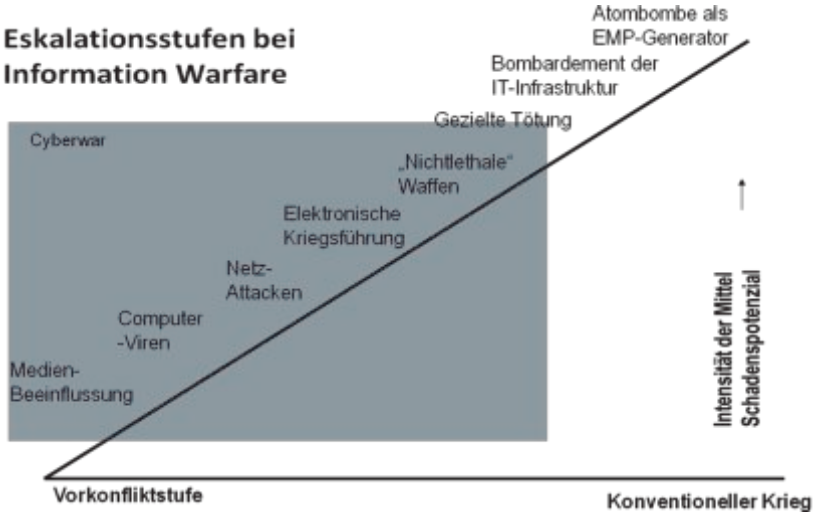
tion, Heft 34/35, (1982) S.13-40, umgesetzt in: Departement of the Army: Field Manual 100-5. Operations, 5 May 1986.

[5] U.S. Department of the Army: Field Manual 100-6. Information Operations. Washington, 27. August 1996. http://fas.org/irp/doddir/army/fm100-6/index.html. Dies wurde 2003 ersetzt durch Field Manual 3-13 und Field Manual 3-0 „Operations", 2001.

[6] Ute Bernhardt, Ingo Ruhmann: Der digitale Feldherrnhügel. Military Systems – Informationstechnik für Führung und Kontrolle. Wissenschaft und Frieden, Dossier Nr. 24, Februar 1997.

[7] Ausführlich dazu: Ingo Ruhmann, Ute Bernhardt: Information Warfare und Informationsgesellschaft. Zivile und sicherheitspolitische Kosten des Informationskriegs; in: Wissenschaft und Frieden, Heft 1, 2014, Dossier Nr. 74, S. 1-16; http://wissenschaft-und-frieden.de/seite.php?dossierID=078.

[8] Ursprünglich definiert in: U.S. Department of the Army: Field Manual 100-6. Information Operations. Washington, 27. August 1996, 2003 ersetzt durch: U.S. Department of the Army: FM 3-13 (FM 100-6) Information Operations: Doctrine, Tactics, Techniques, and Procedures, November 2003, und schließlich durch: U.S. Department of Defense: Field Manual 3-13. Inform and Influence Activities Jan. 2013.



elektromagnetischen Impulses, der großflächig elektronische Geräte überlastet und zerstört.

Psychologische Kriegsführung, Spionage, elektronische Kriegführung und die Destruktion von Kommunikations-knotenpunkten sind schon lange militärische Taktik. Ein Beispiel dafür war der Überfall auf den Irak 2003, der medial als erster »digitaler Krieg« angekündigt wurde. Er sollte durch die psychologische Wirkung massiver Luftschläge zu Beginn der Kampfhandlungen („shock and awe") und eine überlegene alliierte Truppenführung binnen kurzer Zeit gewonnen werden.

Ein typisches Element für den Information Warfare ist die herkömmliche psychologische Kriegsführung, d.h. die Beeinflussung des heimischen und gegnerischen Publikums. In diesem Sinne wurden Medienberichte lanciert, US-Militärs hätten bereits vor Kriegsbeginn mit wichtigen irakischen Truppenkommandeuren die Bedingungen für ihre Kapitulation ausgehandelt[9]. Die Medien berichteten damals weiter, „nahezu Allwissenheit plus intelligente Munition" werde die US-Truppen in die Lage versetzen, die meisten wichtigen Ziele simultan anzugreifen und zu zerstören. Die USA könnten, so hieß es, bis zum Ende der ersten Woche dem gesamten irakischen Militärapparat einen vernichtenden Schlag versetzen und 75% des irakischen Territoriums besetzen[10]. Auch bei sehr vorsichtiger Bewertung der Medienberichte über den Irakkrieg lassen sich zahlreiche Argumente dafür finden, dass die militärische Machtausübung durch den breiten Einsatz vernetzter IT im Sinne des Information Warfare real gestärkt wurde. Der entscheidende Faktor war dabei nicht der Einsatz vereinzelter Präzisionswaffen, sondern die Integration der Einzelteile in eine komplexe Infrastruktur, mit der Kommando und Kontrolle verbessert wurde.

[9] Evan Thomas und Daniel Klaidman: The War Room. Newsweek, 31.3.2003, S.24-29, hier S.28.
[10] Mark Thompson: Opening With a Bang. Time, 17.3.2003, S.30-33, hier S.30f.

Dieses Konzept erwies sich allerdings als untauglich für den nachfolgenden Guerillakrieg.

Die klassischen Ziele der elektronischen Kriegsführung sind die Ermittlung und Lokalisation der Kommunikationspartner - also die Kommunikationsnetze -, und die Entschlüsselung und Auswertung der Inhalte. Zivile Mobilnetze und Internet-kommunikation haben diese Aufgaben der Aufklärung durch leicht entschlüsselbare oder erst gar nicht verschlüsselte digitale Kommunikation im Internet ganz erheblich vereinfacht. Da die NSA durch enorme Finanzmittel und Investitionen in Supercomputer und riesige Datenspeicher in der Lage war, die rasante Zunahme des Kommunikationsaufkommens zu kompensieren, kommt die NSA ihrem Anspruch des „How can we monitor everything?“ heute sehr nahe. Erfasst und zumindest vorübergehend gespeichert wird jede Art von Kommunikation, Datenaustausch oder in der Cloud gespeicherte Daten. Ausgewertet wird zusätzlich natürlich auch Sprach- und Videokommunikation oder Google-Suchanfragen.

Klassischer Bestandteil der elektronischen Kriegsführung ist auch die Entschlüsselung von Kommunikationsinhalten, da die militärische Kommunikation schon seit Ende des Ersten Weltkriegs nicht mehr im Klartext übermittelt wird. Die NSA hatte nach Veröffentlichung des Prinzips der asymmetrischen Verschlüsselung Mitte der 1970er Jahre fast zwei Jahrzehnte intensiv daran gearbeitet, Verschlüsselungsverfahren zu behindern durch ein Verhindern von wissenschaftlichen Veröffentlichungen, Patenten, die Beschränkung der Reisefreiheit für Forscher und die intensive Kontrolle von Exporten[11]. Die NSA-Dokumente lassen erkennen, dass auch heute ein großer Teil der Ressourcen der NSA für Entschlüsselungs-aufgaben aufgewendet wird.

Mit der Information Warfare-Doktrin kamen zu den klassischen Aufgaben des Spionierens, Entschlüsselns und Überwachens auch die systematische Manipulation von Computern und Netzwerken - „Information Operations“ - hinzu. Schon seit den 80er Jahren wird über Angriffe auf gegnerische Computernetze berichtet, damals vielfach noch durch Einbruch und Einspielen vor Ort[12]. In den 1990er Jahren kam die systematische Nutzung von Computerviren gegen vernetzte IT-Systeme hinzu. Diese Cyber-Kriegsführung, die Manipulation von Computern und Rechnernetzen, richtet sich zunächst gegen den Computereinsatz für militärische Zwecke auf militärischen Infrastrukturen. Durch die Vernetzung des offenen Internets mit militärischen Netzwerken bedeutet „Informations-kriegsführung“ aber auch die potenzielle Bekämpfung aller, die im Internet Daten und Informationen sammeln und verarbeiten.

Dazu wurden seit den 1990er Jahren offensive und defensive Information-Warfare-Einheiten des US-Verteidigungsministeriums

[11] Ingo Ruhmann, Christiane Schulzki-Haddouti: Kryptodebatten. Der Kampf um die Informationshoheit; in: Christiane Schulzki-Haddouti (Hg.): Bürgerrechte im Netz, Bundeszentrale für politische Bildung, Bonn, 2003, S. 162-177.
[12] Jay Peterzell: Spying and Sabotage by Computer; in: Time, March 20, 1989, S. 41; Oberstleutnant Erhard Haak: Computer-viren – ein Kampfmittel der Zukunft?; in: Soldat und Technik, Nr. 1, 1989, S. 34-35.

aufgebaut, die 2009 im „U.S. Cyber Command“ zusammengefasst wurden, dessen Leiter der jeweilige Direktor des für elektronische Spionage zuständigen US-Geheimdienstes NSA ist[13]. Die NSA erhielt diese zentrale Aufgabe im U.S. Cyber Command, weil sie gegründet worden war als spezialisierter Dienst für die elektronische Kriegsführung. Nimmt man die herkömmliche elektronische Kriegsführung als Blaupause für Information Warfare, lassen sich an den Aktivitäten und Schwerpunkten sehr einfach ablesen, in welchem Kontext die durch die Enthüllungen von Edward Snowden bekannt gewordenen Spionageoperationen zu sehen sind. Seine Enthüllungen haben uns Einblicke in die Aktivitäten der USA erlaubt. Nicht vergessen werden darf jedoch, dass etwa 100 Staaten heute über Militär- oder Geheimdienst-einheiten verfügen, deren Aufgabe der umfassende Information Warfare von der Aufklärung und Überwachung bis zur Zerstörung von IT-Infrastrukturen ist. So wurde in der Bundeswehr 2002 das strukturell dem Cyber Command vergleichbare „Kommando Strategische Aufklärung“ (KSA) gegründet, um dort jede Form der Aufklärung, sowie die elektronische und psychologische Kriegsführung zusammenzuziehen. Auf Computerangriffe spezialisiert ist im KSA die 2009 gegründete Abteilung „Informations- und Computer-netzwerkoperationen“[14].

Im Jahr 2007 wurden die digitalen Infrastrukturen Estlands durch Cyberattacken gestört, was letztlich dort die Einrichtung eines Cyber-Sicherheitszentrums der NATO zur Folge hatte[15]. 2008 begann der Krieg zwischen Georgien und Russland mit gezielten Cyber-Manipulationen in Georgien durch Angreifer, die im Voraus über russische Militäraktionen informiert waren[16]. Schließlich wurde 2010 mit „Stuxnet“ ein Computerwurm zur Manipulation eines Anlagensteuerungssystem der Firma Siemens identifiziert. Die Analyse von Stuxnet zeigte Aufwände weit außerhalb der Möglichkeiten gewöhnlicher Krimineller. Zwei Jahre nach der Entdeckung erklärten Vertreter der US-Regierung, Stuxnet sei zusammen mit Israel entwickelt worden, um die Urananreicherung in iranischen Anlagen zu sabotieren[17]. Weitere Analysen haben seither gezeigt, dass Stuxnet nur ein Teil einer ganzen Familie von Schadsoftware mit derselben Code-Basis ist, die vor allem in Nahen Osten Schäden in einer Höhe verursacht hat wie herkömmliche Cyber-Kriminelle[18].

---

[13] Center for Strategic and International Studies (CSIS): U.S. Cybersecurity Policy and the Role of U.S. Cybercom. Transcript einer Veranstaltung der »CSIS Cybersecurity Policy Debate Series« mit General Keith Alexander, Washington, 3.6.2010, S.4. http://www.nsa.gov/public_info/_files/speeches_testimonies/100603_alexander_transcript.pdf.

[14] Informationsprofis arbeiten enger zusammen; Bundeswehr-Pressemeldung vom 29.06.2010; http://www.opinfo.bundeswehr.de/portal/a/opinfo/!ut/p/c4/04_SB8K8xLLM9MSSzPy8xBz9CP3I5EyrpHK94uyk-PyCzLyofL3SvOLUotT4HLoqqACIyC_QK01NSi1KT0xK1S_IdlQEAJFZpok!/. Zur Abteilung „Computernetzwerk-operationen“ vgl. die Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Jan van Aken, Andrej Hunko, Christine Buchholz, weiterer Abgeordneter und der Fraktion DIE LINKE. Elektronische Kampfführung der Bundeswehr, Bt.-Drs. 18/3963.

[15] Eneken Tikk, Kadri Kaska, Kristel Rünnimeri, Mari Kert, Anna-Maria Talihärm, Liis Vihul: Cyber Attacks Against Georgia: Legal Lessons Identified. Tallinn, 2008.

[16] Und: Overview by the U.S. Cyber Consequences Unit (CCU) of the Cyber Campaign against Georgia in August of 2008. US-CCU Special Report, August 2009.

[17] David E. Sanger: Obama Order Sped Up Wave of Cyberattacks Against Iran. New York Times, 1.6.2012, S. A1. http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html

[18] Vgl. Kapersky Lab: Resource 207 -Kaspersky Lab Research Proves that Stuxnet and Flame Developers are Connected. 11.6.2012 http://www.kaspersky.com/about/news/virus/2012/

Edward Snowden schließlich ermöglichte Einblicke in Cyber-Aktivitäten der NSA in neuer Qualität. Lange wurden diese Dokumente vor allem als Bericht einer ausufernden Überwachung gelesen. Das viel diskutierte NSA-System „XKeyScore“ erlaubt es, Daten- und Kommunikationsverkehr in Echtzeit zu durchsuchen[19]. So lassen sich etwa alle verschlüsselten Kommunikationsverbindungen in einer Region oder die Suche bei Google mit „verdächtigen“ Schlüsselworten herausfiltern. IT-Sicherheitsfachleuten erschloss sich jedoch, dass XKeyScore zusätzlich sicherheitsspezifische Daten zu den Zielsystemen erhebt und dazu beispielsweise gezielt die Systeminternas der Absturzberichte von Softwarepaketen auswertet. Aus Referenzdatenbanken werden bekannte Schwachstellen abgerufen. Je nach Auftrag versucht XKeyScore, Zielsysteme daraufhin automatisiert mit Schadsoftware zu infizieren[20]. XKeyScore ist daher – neben einer ganzen Reihe anderer bekannt gewordener Systeme - nicht nur ein Spionage - sondern auch ein Angriffssystem für den „Alltagsgebrauch“ von Cyber-Spionage und Sabotage. Andere Systeme wie „Turbulence“ und „QFire“ dienen dazu, den Datenverkehr eines Zieles zu manipulieren und Schadcodes in dessen Datenstrom einzuschleusen. Der mit solchen Werkzeugen durchgeführte Angriff des eng mit der NSA kooperierenden britischen Geheimdienstes GCHQ auf Systemadministratoren der belgischen Telekommunikationsgesellschaft BELGACOM hatte das Ziel, zuerst deren Rechner zu infizieren, um dann Schadsoftware in die Systeme der BELGACOM und zuletzt deren Kunden - die EU-Kommission - einzuschleusen[21]. Dies dokumentiert ebenso wie das Kapern von Botnetzen nichtsahnender Nutzer[22], dass Jede und Jeder im Internet Operationsziel der NSA und ihrer Verbündeten werden kann.

In komplizierten Fällen, wenn ein automatischer Angriff nicht möglich oder das Zielsystem gar nicht mit dem Internet verbunden ist, ist das »Office for Tailored Access Operations« (TAO) gefordert. Dessen Aufgaben sind „neben der Aufklärung auch Attacken in Computernetzen als integrierter Teil militärischer Operationen“, so eine frühere Leiterin[23]. Neben Schadsoftware – wie etwa Stuxnet - hat das TAO seit 1998 Techniken zur Infektion von Zielrechnern entwickelt mit Erfolgsquoten von bis zu 80 Prozent und verschafft sich durch Besuche vor Ort auch einen „physischen Zugang“[24].

Verglichen mit allen anderen Akteuren, verfügen NSA und GCHQ über fast

Resource_207_Kaspersky_Lab_Research_Proves_that_Stuxnet_and_Flame_Developers_are_Connected.

[19] So die Guardian dokumentierte NSA-Präsentation »XKeySore« vom 25.2.2008, http://www.documentcloud.org/documents/743252-nsa-pdfs-redacted-ed.html.

[20] Konrad Lischka und Christian Stöcker: NSA-System XKeyScore – Die Infrastruktur der totalen Überwachung. Spiegel Online, 31.7.2013.; http://www.spiegel.de/netzwelt/netzpolitik/xkeyscore-wie-die-nsa-ueberwachung-funktioniert-a-914187.html.

[21] Ryan Gallgher: Operation Socialist. The inside Story of How British Spies Hacked Belgium's Largest Telco; in: The Intercept; 13. Dez. 2014, https://firstlook.org/theintercept/2014/12/13/belgacom-hack-gchq-inside-story/.

[22] Kevin Poulsen: NSA has been Hijacking the Botnets of Other Hackers; In: Wired, 3. Dez. 2014, http://www.wired.com/2014/03/nsa-botnet/; Darlene Storm: NSA secretly uses scapegoats, data mules and innocent victims' PCs for botnets; in Computerworld, http://www.computerworld.com/article/2872292/nsa-secretly-uses-scapegoats-data-mules-and-innocent-victims-pcs-for-botnets.html.

[23] Jacob Appelbaum, Laura Poitras, Marcel Rosenbach, Jörg Schindler, Holger Stark, Christian Stöcker: Die Klempner aus San Antonio. Der Spiegel Nr. 1/2014, S.100-105.

[24] Appelbaum et al., a.a.O., S.104. Dieser „physische Zugang“ wurde schon Mitte der 1980er Jahre beschrieben, siehe Jay Peterzell: Spying and Sabotage by Computer. Time, 203.1989, S.41.

unbegrenzte Möglichkeiten, Kommunikationswege und Computersysteme zu überwachen und Schadsoftware zu verbreiten. Allein 2013 wandten diese Dienste über zwölf Milliarden Dollar auf für Datensammlung, -analyse sowie zum Brechen von Codes und Sicherheitsvorkehrungen[25]. Hier erübrigt sich jeder Vergleich mit privaten Hackern oder Kriminellen: NSA und der verbündete britische Geheimdienst GCHQ sind die weltweit wichtigsten Hackerorganisationen mit Zugangswegen, die alles andere auf diesem Gebiet in den Schatten stellen.

Eigenen Aussagen zufolge befindet sich die NSA mitten im Information Warfare. Die Ziele von NSA und GCHQ sind verbündete Militärs wie etwa die Bundeswehr[26] ebenso wie UNO, EU-Kommission, befreundete Regierungen und Privatpersonen. Die NSA – dies machen die verfügbaren Dokumente deutlich - befindet sich im unbegrenzten Cyberkrieg gegen Freund und Feind.

Folgen für die Zivilgesellschaft

Information Warfare sieht das Internet als Kampfraum. Diese organisatorische und operative Verquickung von Spionage und Computersabotage mit militärischen Operationen gegen Kommunikations- und Informationsinfrastrukturen ist eine allgegenwärtige Bedrohung auch ziviler IT-Systeme. Das IT-Sicherheitsunternehmen McAfee sah darin schon 2009 die größte Gefahr durch eine „so gut wie eingeläutete" Cyber-Kriegsführung[27]. Militärs und Geheimdienste sind die derzeit größte Gefahr für Datenschutz und IT-Sicherheit. Eine Abhilfe ist kaum zu erwarten: Internationale Abkommen nehmen die Zusammenarbeit bei Cyberspionage und –sabotage aus, wenn Militärs und Geheimdienste involviert sind[28].

Allerdings ist die Diskussion über die von Edward Snowden zugänglich gemachten Dokumente auf der Ebene von Spionage und Datenschutz eine Verharmlosung. Die Spionagedebatte lässt die Bevölkerung unbeteiligt, weil es vordergründig um die Ausspähung von Regierung, Verwaltung und Wirtschaft geht. Es wird nicht nachvollziehbar, wenn Regierungshandeln durch Spionage von außen gesteuert wird und Unternehmen durch Wirtschaftsspionage Schaden nehmen. Doch Spionage als Teil von vernetzter Kriegsführung im Information Warfare ist lediglich eine Vorbereitungshandlung.

Das eigentliche Ziel des Information Warfare heutzutage sind Sicherheit und Zuverlässigkeit der zivilen IT-Infrastuktur. Erst die gründliche Analyse der Angriffshandlungen zeigt die Folgen und die notwendigen Konsequenzen. Der NSA-Skandal zeigt nichts weniger als die vollständige Kompromittierung der IT-

[25] Barton Gellman und Ellen Nakashima: U.S. Spy agencies mounted 231 offensive cyber operations in 2011, documents show. Washington Post, 31.8.2013. http://articles.washingtonpost.com/2013-08-30/world/41620705_1_computer-worm-former-u-s-officials-obama-administration.

[26] So beantwortet das CERT der Bundeswehr die Frage „Wer bedroht uns eigentlich?" nicht mit dem Hinweis auf Hacker, sondern auch mit „Traditionelle Geheimdienste (Freund und Feind)". Siehe z.B. Norbert Wildstacke: Cyber Defense – Schutzlos in einer vernetzten Welt? Das CERT Bundeswehr. Folienvortrag vom 16.2.2009, S.3. http://www.afcea.de/fileadmin/downloads/Young_AFCEAns_Meetings/20090216%20Wildstacke.pdf.

[27] McAfee: Virtual Criminology Report 2009. Virtually Here: The Age of Cyber Warfare, Santa Clara, 2009, http://resources.mcafee.com/content/NACriminologyReport2009NF.

[28] Artikel 27 Absatz 4 des »Übereinkommens über Computerkriminalität«, abgeschlossen in Budapest am 23.11.2001, nimmt beide Bereiche explizit von den Kooperationspflichten aus.

Infrastruktur[29]. Für IT-Sicherheitsexperten lässt sich heute keine gesicherte Aussage mehr darüber treffen,

- welches Verschlüsselungssystem zuverlässig und sicher gegen Angriffe ist – und damit, welche Verfahren für Telebanking, Telemedizin und andere sichere und vertrauenswürdige Transaktionsverfahren im Internet noch einsetzbar sind;
- welches IT-Produkt frei von Hintertüren ist, die auf staatliche Veranlassung eingebaut wurden;
- welche IT-Systeme für kritische Infrastrukturen – von der Energie- und Wasserversorgung, dem Finanzwesen und der Kommunikationsinfrastruktur bis zur Steuerung von Anlagen mit Gefahrstoffen – heute zuverlässig arbeiten und sicher gegen Angriffe nach dem Muster von Stuxnet sind.

Für eine auf dem Funktionieren ihrer IT-Systeme fußende Gesellschaft wie die unsere ist es keine Option, dass Militärs und Geheimdienste diese zivile Infrastrukturen als potenzielle Ziele begreifen. Die einzige Möglichkeit des Umgangs ist die intensive Weiterentwicklung von sicheren IT-Systemen anstelle einer militärischen Logik aus Eskalation und Rüstungsspirale.

Begrenzung von Information Warfare

Die ressourcenstärksten Hackertruppen sind heute bei Militär und Geheimdiensten wie der NSA angesiedelt. Die heute systematischen Information Warfare-Attacken sind eine Bedrohung der zivilen Infrastruktur der Informationsgesellschaft. Die USA haben in ihrer jüngsten Cyberwarfare-Doktrin verkündet, dass sie Hackerangriffe als militärische Erstschlagoption vorsehen[30].

Weltweit wird dabei nicht zwischen zivilen und militärischen IT-Infrastrukturen unterschieden. Wichtig ist, auch hier die Perspektive über die USA hinaus auszuweiten. Auf die parlamentarische Anfrage, ob die in der Bundeswehr zur Ausübung von Cyberattacken 2007 eingerichtete Gruppe „Computer Netzwerk Operationen“ innerhalb des Kommandos Strategische Aufklärung (KSA) auch dafür trainiere, in zivile IT-Netzwerke kritischer Infrastrukturen einzudringen und diese zu manipulieren und zu schädigen, antwortete der Parlamentarische Staatssekretär bei der Bundesministerin der Verteidigung:

> „Aus rechtlicher Sicht gelten auch elektronische Systeme während eines bewaffneten Konflikts als militärische Ziele, wenn sie entsprechend der Definition des humanitären Völkerrechts aufgrund ihrer Beschaffenheit, ihres Standorts, ihrer Zweckbestimmung oder ihrer Verwendung wirksam zu militärischen Handlungen beitragen und deren gänzliche oder teilweise Zerstörung oder Neutralisierung einen eindeutigen militärischen Vorteil darstellt. [...] Das humanitäre Völkerrecht bestimmt keinen absoluten Schutz von Energieversorgungseinrichtungen, des Transportwesens oder der Telekommunikation. Ob ein elektronisches System ein ziviles Objekt oder aber ein militärisches Ziel darstellt, kann nur unter Berücksichtigung aller Umstände des

[29] Vgl. Ingo Ruhmann: NSA, IT-Sicherheit und die Folgen. Eine Schadensanalyse; in: DuD Nr. 1, 2014, S. 40-46.
[30] The DoD Cyber Strategy, Washington, April 2015, http://www.defense.gov/home/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.

konkreten Einzelfalls bestimmt werden.“ [31]

Aus Sicht der IT-Sicherheit sind die Hintergründe dieser Antwort klar: Hier geht es darum, IT-Systeme in zivilen Umgebungen, die von Angreifern kompromittiert sind und für Angriffe genutzt werden – also als Ausgangspunkte für Attacken missbraucht werden —, ebenso anzugreifen, wie etwa ein ziviles Gebäudeziel, das Operationsbasis von gegnerischen Militärs ist. Der ganz wesentliche und in der parlamentarischen Antwort nicht geklärte Unterschied besteht hier allerdings darin, legitime einzelne virtuelle oder realweltliche Ziele auszuschalten oder – der Frage gemäß - ganze zivile Infrastrukturen als Antwort auf Cyberattacken lahmzulegen. Das Ausschalten ziviler Infrastrukturen als Teil des Information Warfare ist eine Stufe militärischer Konfliktaustragung mit gravierenden Folgen.

Abrüstung und Rüstungskontrolle für Information Warfare muss daher dringender denn je auf die politische Agenda. Schon 1995 ließ der „Unterausschuss für Abrüstung und Rüstungskontrolle“ des Deutschen Bundestags das Thema Rüstungskontrolle und Information Warfare durch das Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V. (FIfF) eingehend untersuchen.[32] Kaum etwas ist davon bis heute umgesetzt, die Diskussion darüber ist nur wenig weitergekommen. Zur Aufklärung der Öffentlichkeit über die mit Information Warfare verbundenen Gefahren hat das FIfF 2014 die „Cyberpeace-Kampagne“ gestartet. Das Ziel ist, den militärischen Missbrauch des Internets und der Informationstechnik einzudämmen und dazu u.a. den offensiven Einsatzes des Information Warfare zu ächten und die zivile IT-Sicherheit zu stärken[33].

Die vernetzte Kriegsführung hat sicherheitspolitisch zu keinem Zugewinn an Stabilität geführt und nicht geholfen, Konflikte zu vermeiden. Information Warfare ist weltweit zu einer Option der computergestützten Konfliktaustragung geworden. Sie birgt erhebliche Eskalationsrisiken. Die umfassende Beschädigung der IT-Sicherheit ist eine gravierende Gefahr für jede zivile Informationsgesellschaft.

Ute Bernhardt, Informatikerin, wissenschaftliche Referentin, Gründungsmitglied und ehemalige stv. Vorsitzende des Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V., Arbeiten zu Datenschutz, Bürgerrechte sowie Informatik und Militär.

Ingo Ruhmann, Informatiker, wissenschaftlicher Referent und Lehrbeauftragter, Gründungsmitglied und ehemaliges Vorstandsmitglied im Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V., Arbeiten zu Datenschutz, IT-Sicherheit, sowie Informatik und Militär.

[31] Plenarprotokoll der Fragestunde der 16. Sitzung des Deutschen Bundestages vom 19.02.2014, Antwort auf Frage Nr. 8, S. 1165f.
[32] Ralf Klischewski und Ingo Ruhmann: Ansatzpunkte zur Entwicklung von Methoden für die Analyse und Bewertung militärisch relevanter Forschung und Entwicklung im Bereich Informations- und Kommunikationstechnologie. Gutachten für das Büro für Technikfolgenabschätzung des Deutschen Bundestages, Bonn, März 1995.
[33] Weitere Informationen zum FIfF sind zu finden unter www.fiff.de, zur Cyberpeace-Kampagne unter cyberpeace.fiff.de

Drohnen: Eine unaufhaltsame Entwicklung?

Von Roland Reimers

Seit Beginn des dritten Jahrtausends sind Drohnen in zunehmenden Maße in die Streitkräfte verschiedener Staaten eingeführt worden. Auslöser war vordergründig der nach dem 11.9.2001 von den USA einseitig verkündete „Krieg gegen den Terror". Tatsächlich ist die Forschung und Entwicklung an Drohnen aber deutlich älter. Der Urtyp einer Drohne kam schon im 2. Weltkrieg von Deutschland aus in den Einsatz. Es handelte sich um die Fieseler Fi-103, besser bekannt unter der Kurzbezeichnung „V1" (Vergeltung 1). Und auch im ersten Irakkrieg der USA[1] 1991 kamen schon drohnenähnliche Flugkörper zum Einsatz, die Marschflugkörper. Ihnen gemeinsam ist, dass sie einen vorprogrammierten Kurs abfliegen, der sie zu ihrem Ziel führt, das sie am Ende vernichten sollen.

Wie genau lässt sich der Begriff „Drohne" definieren? Wenn heutzutage von Drohnen die Rede ist, ist in der Regel mehr gemeint als nur das Abfliegen eines vorprogrammierten Kurses. Drohnen werden assoziiert mit unbeschränkter Manövrierfähigkeit, Fernsteuerung, teilweise autonomer Kursfindung und einer Vielzahl von Aufgaben, die mit ihnen erledigt werden können. Drohnen sind dabei nicht nur auf den Bereich der Luftfahrzeuge beschränkt; es gibt ebenso land- und seegestützte Drohnen. Letztere haben aber aus verschiedenen Gründen gegenwärtig eine geringere militärische Bedeutung. Als Arbeitsdefinition für den vorliegenden Artikel gehe ich beim Begriff „Drohne" von ferngesteuerten, teilautonom operierenden Fluggeräten und Fahrzeugen aus, deren Einsatzzwecke unterschiedlich sein können. Ballistische Raketen fallen ausdrücklich nicht unter diese Definition. Marschflugkörper sind eng verwandt, aber ihr Einsatzprofil ist ein anderes als das von Drohnen. Ein entscheidender Unterschied ist auch die Weiterverwendbarkeit: Nach Beendigung ihrer Mission landen Drohnen in der Regel auf einem Flugplatz (Flugdrohnen) bzw. kehren zum Mutterschiff/Hafen zurück (Schiffsdrohnen) oder werden eingesammelt (fahrende Drohnen). Marschflugkörper und Raketen sind hingegen Einwegflugkörper.

Im militärischen Bereich haben bisher nur fliegende Drohnen in größerem Ausmaß Einzug gehalten. An ihnen spitzt sich zur Zeit die Diskussion exemplarisch zu. Diese

1 Dieser Krieg wird auch manchmal zweiter Golfkrieg genannt, weil in den 1980er Jahren Iran und Irak miteinander im Krieg lagen. Jener Krieg zwischen Iran und Irak wäre in dieser Zählung dann der erste Golfkrieg.

Diskussion betrifft aber in gleichem Maße Schiffsdrohnen und fahrende Drohnen. Dies sollte immer berücksichtigt werden, auch wenn im Folgenden meist nur von Flugdrohnen die Rede ist.

Politische Relevanz fliegender Drohnen

Drohnen in ihrer Ausprägung als Flugzeug, sind in den letzten Jahren in den Fokus des allgemeinen Interesses gerückt, weil mit ihrer Hilfe gezielte Tötungen durchgeführt werden. Zur Zeit tun dies die USA, Großbritannien[2] und Israel[3]. Es ist aber absehbar, dass andere Länder vergleichbare Kapazitäten entwickeln, die sie in die Lage versetzen werden ebenso zu agieren wie diese Länder.

Woran entzündet sich die Kritik an diesen Drohnen? Zunächst ist dies nicht klar ersichtlich, wenn nur das Fluggerät an sich betrachtet wird: Ein unbemanntes, ferngesteuertes Flugzeug. Flugzeuge gibt es seit Jahrzehnten und niemand regt sich darüber auf. Was macht also die geringere Akzeptanz von Drohnen aus?

Entscheidend ist die Art, wie Drohnen eingesetzt werden. Offensichtlich ist die Schwelle für ihren militärischen Einsatz wesentlich geringer als die Einsatzschwelle für (bemannte) Flugzeuge. Diese Niederschwelligkeit macht es für Politiker einfacher, militärische Konfliktlösungen zu suchen.

Im Vergleich der politischen Implikationen anhand konkreter Beispiele wird dies klarer. 1960 wurde ein US-amerikanisches Spionageflugzeug des Typs U-2 über der Sowjetunion abgeschossen[4]. Der Pilot überlebte und wurde gefangen genommen. Es gab weitreichende diplomatische Verwicklungen mit einer diplomatischen Niederlage für die USA. Die Sowjetunion konnte den überlebenden Piloten präsentieren, so dass ein Zweifel an der Verletzung des sowjetischen Luftraums durch die USA nicht möglich war. Im Gegensatz dazu hielten sich die diplomatischen Verwicklungen in Grenzen als im Dezember 2011 der Iran meldete eine Drohne vom Typ RQ-170 „Sentinel“ abgeschossen zu haben[5]. Die USA konnten zunächst dementieren und den Vorfall herunterspielen. Mit einer gewissen Zeitverzögerung gaben dann „Regierungskreise in Washington“ zu, dass die Drohne zum Ausspähen iranischer Atomanlagen eingesetzt worden war[6]. Ein derartiger diplomatischer Erfolg, wie ihn seinerzeit die Sowjetunion hatte, war dem Iran nicht vergönnt.

Auch innenpolitisch lassen sich Drohneneinsätze leichter vertreten als Flugzeugmissionen. In Flugzeugen sitzen Menschen, die getötet oder gefangen genommen werden können. Eine unbemannte Drohne erfordert keine Rechtfertigung gegenüber der eigenen Bevölkerung, warum Soldaten in Einsätze

[2] BBC-News: Armed drones operated from RAF base in UK, says MoD, 27.4.2013. abrufbar unter http://www.bbc.com/news/uk-england-lincolnshire-22320275. Link verifiziert am 25.7.2014.
[3] Atef Abu Saif: Sleepless in Gaza - Israeli drone war on the Gaza Strip, Rosa Luxemburg Stiftung, 2014.
[4] https://de.wikipedia.org/wiki/Francis_Gary_Powers, Link verifiziert am 24.7.2014.
[5] http://www.airforcetimes.com/article/20111209/NEWS/112090311/Iran-s-captured-RQ-170-How-bad-damage-, Link verifiziert am 24.7.2014.
[6] http://www.nytimes.com/2011/12/08/world/middleeast/drone-crash-in-iran-reveals-secret-us-surveillance-bid.html, zitiert nach http://www.spiegel.de/politik/ausland/verlorene-us-drohne-iran-praesentiert-das-biest-von-kandahar-a-802618.html weil NY Times nur kostenpflichtig zugänglich. Links verifiziert am 24.7.2014.

geschickt werden. Auch parlamentarische Zustimmungen lassen sich leichter erreichen, wenn eigene Soldaten nicht gefährdet werden. Die Drohnenpiloten befinden sich im Heimatland und allenfalls in Nachbarländern des Einsatzgebiets, sind also nicht in Gefahr.

Das politische Kalkül ist also entscheidend. Innenpolitisch sind Drohneneinsätze leichter zu vertreten. Außenpolitisch stellen Drohnen, die in den Luftraum eines anderen Landes eindringen, eine geringere Verletzung der nationalen Souveränität dar als Flugzeuge.

Die wichtigsten Einsatzländer

Aktuell werden Drohnen von etlichen Staaten zur Aufklärung eingesetzt und, soweit bekannt, nur von den USA, Großbritannien und Israel auch zur gezielten Tötung von Personen. Die gezielten Tötungen der USA sind es, die jedweder internationalen Rechtsprechung zuwider laufen. Die USA haben nach dem 11.9.2001 einseitig den „Krieg gegen den Terror" erklärt ohne genau zu spezifizieren, gegen wen er sich eigentlich richtete. Der damalige Vize-US-Außenminister Wolfowitz drückte das kurz nach dem 11.9.2001 so aus, dass es dabei nicht nur darum geht Personen zu verhaften und sie zur Verantwortung zu ziehen, sondern auch darum ihre „[...] Zufluchtsorte wegzunehmen, die unterstützenden Systeme auszuschalten, Staaten zu beenden, die Terrorismus unterstützen."[7] Die bewaffneten Drohnen werden jetzt so eingesetzt, als befänden sich die USA im Krieg. Diesen Krieg haben sie jedoch keiner völkerrechtlich fassbaren Einheit erklärt. Der Gegner, gegen den er sich richtet, bleibt diffus und so ist es nicht weiter erstaunlich, dass Tötungen mit Kampfdrohnen in ganz unterschiedlichen Ländern stattfinden: Afghanistan, Pakistan, Jemen, Somalia. Im Bedarfsfall nehmen sich die USA das Recht heraus weitere Länder als Operationsgebiet ihrer bewaffneten Drohnen hinzu zu nehmen[8]. Allesamt sind dies Staaten mit schwachem oder gar keinem staatlichen Gewaltmonopol, in denen zum Teil Warlords den Ton angeben.

Großbritannien setzt Drohnen vor allem in Afghanistan zur Aufklärung und als Luftstreitkräfte ein. Schon 2009/10 wurden dort etwa die Hälfte aller britischen Luftangriffe von Drohnen ausgeführt, 2014 waren es bereits 80%[9]. Die Angaben der britischen Regierung sind spärlich. Immerhin kann hier von einem Drohneneinsatz in einem Kriegsgebiet ausgegangen werden, was aber nicht ausschließt, dass dort auch gezielte Tötungen nach US-Muster durchgeführt werden.

Der israelische Kampfdrohneneinsatz ist vor dem Hintergrund zu bewerten, dass Israel ein in seiner Existenz unmittelbar gefährdeter Staat ist. Er befindet sich, so sehen es die Israelis mehrheitlich selbst, im Krieg mit militanten Organisationen der Palästinenser und Araber wie der Hamas und

---

[7] Zitiert nach http://www.pbs.org/wgbh/pages/frontline/shows/iraq/etc/cron.html (eigene Übersetzung aus dem Englischen). Link verifiziert am 5.3.2015.

[8] Chris J. Dolan: The Bush Doctrine and U.S. Interventionism, American Diplomacy, 2004, verfügbar unter http://www.unc.edu/depts/diplomat/archives_roll/2004_04-06/dolan_bush/dolan_bush.html. Link verifiziert 24.7.2014.

[9] Ch. Cole: New figures show UK increasingly relying on drones for strikes in Afghanistan, verfügbar unter http://dronewars.net/2014/07/22/new-figures-show-uk-increasingly-relying-on-drones-for-strikes-in-afghanistan. Link verifiziert am 1.10.2014.

der Hisbollah. Perioden ohne bewaffnete Auseinandersetzung werden nicht als Frieden sondern als Waffenstillstand angesehen, in dem der Kriegszustand weiter besteht. In diesem Kontext sieht es die israelische Führung als gerechtfertigt an, Führungspersonen der Gegenseite zu töten. Ob diese Einschätzung juristisch tragfähig ist, darf mit Recht bezweifelt werden. Diese innerisraelische Sichtweise führte schon früh dazu, sich mit den Möglichkeiten des Einsatzes von Drohnen intensiv zu beschäftigen. Das Resultat ist heute, dass Israel eine Technologieführerschaft bei Drohnen hat und israelische Technologie auch in vielen Drohnen steckt, die in anderen (vor allem westlichen) Ländern entwickelt worden sind[10]. Der Einsatz von Drohnen hat an der israelischen Politik der Luftaufklärung und der gezielten Tötungen nichts Grundsätzliches geändert. Israel hat schon immer Luftschläge ausgeführt wenn es im nationalen Interesse schien, ungeachtet der Verletzung der Souveränität anderer Staaten. Vor der Einführung der Drohnen wurde dies mit Flugzeugen bewerkstelligt. Drohnen haben die Kosten dafür (wahrscheinlich) verringert und die Verfügbarkeit erhöht. Insbesondere für die Aufklärung ist dies wichtig: Unbemannte Flugkörper sind nur durch ihren Treibstoffvorrat begrenzt, weswegen sie wesentlich länger als bemannte in der Luft bleiben können. Die Entfernungen spielen in der Regel keine Rolle weil sie so gering sind, dass Flugzeuge oder Drohnen in Minuten dort sind, wo sie eingesetzt werden sollen (z.B. über dem Gaza -Streifen). Gelegentlich hat Israel aber auch schon in weiter entfernten Regionen Drohnen eingesetzt, so z.B. im Januar 2009 im Sudan, wo ein LKW-Konvoi mit iranischen Raketen vernichtet wurde[11].

Drohnentechnologie: Worauf baut sie auf?

Das Konzept einer Drohne ist nicht neu. Neu ist vielmehr, dass jetzt ein technischer Stand erreicht worden ist, der es gestattet, das Konzept auch zu realisieren. Technologien aus unterschiedlichen Bereichen sind nötig, um eine Drohne zu bauen. Die Integration dieser Technologien in ein neues Produkt ist es, was heutige Drohnen auszeichnet. Und das hat zur Folge, dass Vieles, was an Technologie in Drohnen steckt, nicht in unmittelbarem Zusammenhang mit der Drohnenforschung entwickelt wurde.

In Drohnen stecken unter Anderem die folgenden Technologien:

- Computerhardware: Mikroprozessoren, deren Aufgabe es ist das Fluggerät zu stabilisieren und zu steuern.
- Computersoftware: Algorithmen, die von den Programmen in der Computer-hardware ausgeführt werden. Unter Anderem kommen neuronale Netze und Kryptographieprogramme zum Einsatz.
- Sensorik: In jeder Drohne sind eine Menge Sensoren verbaut. Das fängt an bei Lagesensoren und geht, bei militärischen Drohnen, weiter zu Infrarotsensoren und

[10] M. Dobbing, Ch. Cole: Israel and the Drone Wars, Examining Israel's production, use and proliferation of UAVs, publiziert von „Drone Wars UK", Oxford, 2014, verfügbar unter http://dronewarsuk.files.wordpress.com/2014/01/israel-and-the-drone-wars.pdf. Link verifiziert am 1.10.2014.

[11] Yaakov Katz: Israel's eye in the sky, Jerusalem Post vom 10.7.2011, verfügbar unter http://www.jpost.com/Magazine/Features/Israels-eye-in-the-sky. Link verifiziert am 1.10.2014.

Radar zur Zielerfassung.

- Navigationstechnik: Zentral ist das US-amerikanische Global Positioning System (GPS), dessen Konzeption auf die Zeit des Kalten Krieges zurückgeht und als dessen Hauptaufgabe damals das präzisere Lenken von atomaren Interkontinentalraketen auf ihre vorbestimmten Ziele angesehen wurde. Daneben enthalten militärische Drohnen auch Trägheitsnavigationssysteme wie sie in der Luftfahrt gebräuchlich sind.

- Neue Werkstoffe, die hochfest und gleichzeitig leicht sind, z.B. Kohlefaser und die auch in anderen Bereichen zunehmend eingesetzt werden.

- Flugzeugtechnologie: Aerodynamik, Avionik, ggf. Stealth-Eigenschaften, Antriebstechnik (Düsenantrieb oder Propeller).

- Eine Kommunikationsinfrastruktur und Leittechnik zur Kommunikation mit den Drohnen und zu ihrer Steuerung. Im militärischen Fall ein umfassendes System, das größtenteils schon existiert und nur an die Drohnen, wie an jedes neu eingeführte System, angepasst werden muss. Bei zivilen Drohnen reicht manchmal schon ein Handy mit einer speziellen App, aber für umfangreichere Projekte, wie das synchrone Steuern mehrerer Drohnen, ist ein höherer Aufwand nötig.

Zunächst ist festzustellen, dass die meisten dieser Technologien sowohl für militärische als auch zivile Drohnen genutzt werden (können). Wird also über die Weiterentwicklung von Technologien für Drohnen gesprochen, so muss das nicht zwangsläufig militärische Gründe haben, kann es aber. Dies ist ein klassisches Dual Use Problem.

Viel wichtiger ist aber, dass die oben aufgeführten Technologien zunächst einmal gar nichts mit Drohnen zu tun haben. Sie wurden nicht primär für den militärischen Einsatz sondern für zivile Zwecke entwickelt. Dies trifft in besonderem Maße auf die Computertechnologie (Hard- und Software) zu. Die Entwicklung schreitet, unabhängig von militärischen Interessen, voran. Insbesondere die Informationstechnik ist eine offene Technologie. Gekoppelt mit entsprechenden Sensoren und programmiert mit angepasster Software sind Computer so ziemlich für Alles einsetzbar, eben auch für Drohnen. Die Entwicklung zu kleineren, schnelleren Prozessoren[12], ausgefeilteren Algorithmen und niedrigerem Energieverbrauch findet auf jeden Fall statt. Für Drohnenbauer gleicht dies einem Selbstbedienungsladen, dessen Produkte sie für ihre Zwecke anpassen aber nicht mehr neu entwickeln müssen. Betrachtet man Drohnen als führerlose Fahrzeug, so drängt sich eine Parallele zum zivilen Kontext auf: In letzterem gehen durch Automatisierung Arbeitsplätze verloren[13], bei Drohnen wird der Führer/Pilot durch eine computerisierte Steuerung ersetzt und aus der Drohne heraus verlagert mit der Perspektive, eines Tages ganz ersetzt zu werden.

Parallel zur Entwicklung der

[12] Laut Gordon Moore, einem der Gründer von Intel, die Anzahl der Transistoren auf einem Chip exponentiell mit Verdoppelung ungefähr alle 18 Monate. Vergleiche https://de.wikipedia.org/wiki/Gordon_Moore.
[13] C.A.Frey, M.A.Osborne: The Future of Employment: How Susceptible are Jobs to Computerisation? Oxford University, UK, 2013. Abrufbar unter http://ct.de/yqfv . Link verifiziert am 10.3.2015.

Computertechnologie hat in den letzten Jahren eine Miniaturisierung und Integration verschiedenster Sensoren stattgefunden. In jedem Handy sind solche miniaturisierten Sensoren verbaut. Ein Chip wie der „InvenSense MPU-9250“ hat nur die Abmessungen 3x3x1 mm³ und enthält ein dreiachsiges Gyroskop, einen dreiachsigen Beschleunigungsmesser, ein Magnetometer sowie eine digitale Signalverarbeitungseinheit zur Datenaufbereitung für das Endgerät[14]. Solche Chips sind heutzutage in Handys verbaut, aber ihre Anwendungsmöglichkeiten gehen weit darüber hinaus.

Die Navigationstechnik wird ebenfalls weiterentwickelt. Neben dem US-System GPS gibt es das russische Glonass-System. Europa ist auch dabei ein eigenes System („Galileo“) zu stationieren ebenso wie China („Beidou“).

Über Flugzeugtechnologie lässt sich Ähnliches sagen, wobei hier auch die militärische Flugzeugtechnologie eine herausragende Rolle spielt. Systeme zur Entlastung der Piloten sind allgegenwärtig. Moderne militärische Kampfjets sind aerodynamisch instabil und müssen aktiv durch Computersteuerung stabilisiert werden. Fällt diese Steuerung aus, fallen sie wie ein Stein vom Himmel. Kurse zum Einsatzgebiet werden automatisch, ohne Piloteneingriff geflogen, im Bedarfsfall im Tiefstflug, den Geländekonturen folgend. Dies lässt sich leicht auf Drohnen übertragen.

Zusammenfassend lässt sich feststellen, dass die Technologien, um Drohnen zu bauen, existieren und ständig weiterentwickelt werden. Zum Teil ist das auch gesellschaftlich wünschenswert, wenn sie für Produkte nötig sind, die unseren Alltag erleichtern.

Das militärische Drohnensystem und die Rolle Deutschlands

In den Armeen dieser Welt wird die Einführung der Drohnen durch bereits bestehende Strukturen unterstützt, die ursprünglich nicht für Drohnen eingeführt wurden aber gut zu ihnen passen. Zu nennen ist vor allem das militärische Kommando-, Kommunikations- und Steuerungssystem (engl. C3I: command, control, communication, intelligence), das, wie alle Bereiche der Gesellschaft in den letzten 20 Jahren, umfassend durchcomputerisiert worden ist. Die genaue Navigation lässt sich darunter subsumieren.

In den Luftstreitkräften der NATO-Staaten ist es Standard, zum Einsatzort und zurück einen vorher festgelegten Kurs computergesteuert zu fliegen. Die Piloten sind nur noch erforderlich, um zu starten und zu landen und um im Zielgebiet ihre Waffen einzusetzen. Die Einsatzmodi für Drohnen haben das gleiche Muster: Es gibt Piloten am Start/Zielflugplatz, die die Drohne starten und landen. Teile des Kurses zum Einsatzgebiet werden automatisiert geflogen und im Zielgebiet übernimmt dann wieder ein Pilot, der den Befehl zum Einsatz der Waffen gibt. Dieser Pilot sitzt in der Regel in den USA und steuert die Drohne über eine verschlüsselte digitale Funkverbindung, die über militärische Kommunikationssatelliten und/oder Glasfaserkabel verläuft. Start und

[14] Laut Beschreibung der Herstellerfirma http://www.invensense.com/mems/gyro/mpu9250.html. Vergleiche auch http://www.androidmag.de/report/ein-wahres-sensibelchen-handy-sensoren. Links verifiziert am 9.3.2015.

Landung kann von diesen Piloten nicht ausgeführt werden, wegen der Zeitverzögerung („Latenz"), mit der Steuersignale bei der Drohne ankommen und sensorische Signale von der Drohne zum Piloten zurückkommen.

Die Latenz ist in der Tat ein Problem, wenn Pilot und Drohne durch mehrere Tausend km voneinander getrennt sind. Im Fall der USA befinden sich die Einsatzgebiete (Pakistan etc.) auf der gegenüberliegenden Seite der Erde, knapp 20.000 km entfernt. Bevorzugte Kommunikation ist diejenige über Glasfaserkabel, denn der Weg, den die Signale zurücklegen müssen, wenn sie über geostationäre Satelliten laufen, ist wesentlich länger. Eine kurze Überschlagsrechnung verdeutlicht dies: Jeder geostationäre Satellit befindet sich (aus physikalischen Gründen) in 36.000 km Höhe über der Erdoberfläche. Vereinfacht angenommen, die Satellitenverbindung könnte über einen einzigen Satelliten hergestellt werden, dann würde sich eine Übertragungsstrecke von 84.000 km ergeben, für die das Signal 0,28 s braucht[15]. Im Gegensatz dazu ist eine Glasfaserleitung um den halben Globus nur etwa 20.000 km lang, ein Fünftel. Unter Berücksichtigung der Tatsache, dass sich das Signal durch die Glasfaser nur mit zwei Dritteln der Geschwindigkeit bewegt, die es im Weltraum hat, ergibt sich eine Signallaufzeit von 0,1 s. D.h. die Glasfaserübertragung ist etwa dreimal so schnell, wie die Satellitenübertragung.

Aufgrund der vergleichsweise langen Signallaufzeiten ist Deutschland im US-Drohnensystem ein Schlüsselstaat. Über die US-Basis in Ramstein läuft die Drohnenkommunikation für den Nahen Osten. Die Signale werden über Satellit von den Steuerungszentren in den USA nach Ramstein übertragen und dann in ein Glasfaserkabel eingespeist. Ohne diese Infrastruktur wären die USA zur Fortsetzung ihres Drohnenkriegs gezwungen Steuerungszentren in Drittländern näher am Einsatzort der Drohnen zu betreiben, um die Latenz in Grenzen zu halten.

Technologische Perspektiven

Neben der eingangs geschilderten politischen Niederschwelligkeit gibt es auf Seiten der Militärs auch Motive, die eine Entwicklung zu Drohnen vorantreiben. Der gewichtigste ist die erhöhte Flexibilität: Es kann auf die lebenserhaltenden Systeme für die Piloten verzichtet werden, woraus sich eine beträchtliche Gewichtsersparnis ergibt, wodurch mehr Treibstoff und ggf. Waffen mitgeführt werden können. Die Piloten, die die Drohne fernsteuern, können unproblematisch ausgetauscht werden, so dass menschliche Ruhezeiten keine Rolle mehr spielen. Dadurch können Drohnen viel länger in der Luft bleiben als Flugzeuge, was eine militärische Einsatzplanung deutlich erleichtert.

Auf zivilem Gebiet schreitet die Entwicklung von Drohnen für Privatleute stürmisch voran. Stand der Technik sind inzwischen Quadrokopter (Hubschrauber mit vier

[15] Dies ist überoptimistisch, denn es sind mindestens zwei geostationäre Satelliten erforderlich, um von einer zur anderen Seite der Erde ein Signal zu übertragen. Damit würde sich der Weg auf ca. 150.000 km verlängern wenn eine Bodenstation zwischengeschaltet werden muss, von der aus zu beiden Satelliten eine Sichtverbindung besteht. Unter der Voraussetzung, dass zwischen beiden Satelliten eine direkte Verbindung hergestellt werden kann, ohne den Umweg über eine Bodenstation, wäre der Weg immer noch ca. 137.000 km lang.

Rotoren), die computerstabilisiert starten und landen und dem (unerfahrenen) Piloten die unfallträchtigsten Flugphasen abnehmen. Sie haben den Status eines hippen Spielzeugs, was sie zu einem Gegenstand, selbst von Kunstprojekten macht: So hat z.B. die österreichische Firma Voest Alpine (die auch das österreichische Bundesheer beliefert) auf dem Festival „Ars Electronica" 2012 in Linz 49 Quadrokopter gleichzeitig computergsteuert fliegen lassen[16]. Die Koordination von 49 Drohnen auf engem Raum allein ist schon eine Leistung, die auch im militärischen Bereich interessant sein kann.

Angesichts der verwendeten Technologien ist es logisch, das nicht nur luftgestützte unbemannte Systeme entwickelt werden: Genauso gut kann die Navigations- Steuer- und Waffentechnologie in land- oder seegestützte Fahrzeuge integriert werden. So hätte man z.B. einen unbemannten Panzer. Allerdings sind die Anforderungen an die Navigation (Ausweichen vor unerwarteten Hindernissen etc.) an Land ungleich höher als das Abfliegen einer doch ziemlich linearen Trajektorie in der Luft, so dass hier militärisch einsatzfähige landgestützte Vehikel nur eingeschränkt nutzbar sind. Für die Zukunft zeichnet sich ab, dass immer mehr, bislang noch von den Piloten wahrgenommene Funktionen, in die unbemannten Vehikel integriert werden. Im zivilen Bereich ist z.B. angedacht, die Piloten von Frachtflugzeugen durch eine automatisierte Steuerung zu ersetzen. Miniaturisierung der computerisierten Steuerung spielt hier keine Rolle, denn Flugzeuge wie eine Boeing 747 können schwere Lasten tragen. Die Hürden, die verhindern, dass solche Flugzeuge heute schon fliegen, sind im Wesentlichen rechtlicher und nicht technischer Natur[17].

Münden kann das in Vehikel, bei denen auch die Entscheidung zum Waffeneinsatz nicht mehr von Menschen getroffen wird, sondern von einem Computer (an Bord oder, zunächst wahrscheinlicher, am Boden bzw. in der Basis) aufgrund bestimmter Algorithmen. Käme es soweit, dann hätte man Killerroboter konstruiert.

Allerdings steckt die Forschung zu autonom entscheidenden Systemen noch am Anfang. Bisherige Versuche basieren auf vergleichsweise wenig komplex strukturierten neuronalen Netzen[18]. Es ist schwer vorhersagbar, wie sich dieses Gebiet weiter entwickeln wird. Verlängert man die Entwicklungstrends weiter, dann ist zu erwarten, dass Hard- und Software immer komplexere Aufgaben übernehmen und auf unerwartete Störungen sinnvoll reagieren kann.

Was wollen wir für die Zukunft?

Angesichts der stürmisch verlaufenden Technologieentwicklung auf allen Ebenen, ist es wohl illusorisch ein Verbot von Drohnen durchzusetzen. Die Perspektive auch der Verlagerung der letzten Entscheidung, der über Leben und Tod, auf eine Maschine, ist bedrohlich, abgesehen von den damit verbundenen völkerrechtlichen Problemen.

[16] Siehe http://www.aec.at/klangwolke/de. Link verifiziert am 9.3.2015.
[17] Detlev Borchers: Deutschland, deine Drohnen, ct 14(2014), S.64.
[18] Vortrag von Prof. Noel Sharkey im März 2014 in Berlin (im Magnus-Haus der Deutschen Physikalischen Gesellschaft) zum Thema Drohnen im Rahmen der FONAS-Fachgespräche.

Auf der Ebene der Rüstungskontrolle praktikabel erscheint der Ansatz eine Drohne als Integration verschiedener (ziviler und militärischer) Technologien in ein Gerät zu betrachten. Dann kann man fragen: Was wollen wir an Technologien in einer Drohne haben und was besser nicht? Dieser Ansatz wird von den Gruppen stopkillerrobots.org und dem International Committee for Robot Arms Control (http://icrac.net) verfolgt. Es ist wichtig, dass dieser Ansatz von der Funktion der Technologien für die Drohne ausgeht, um sicher zu stellen, dass eine Technologie nicht durch eine andere ersetzt werden kann, die das Gleiche tut. Solch eine Rüstungsbegrenzung muss umfassend und global angelegt sein, wobei aber immer die Möglichkeit besteht, dass durch neue Technologien plötzlich Dinge möglich werden, die niemand vorausgesehen hatte. Daher müsste ein solcher Vertrag in regelmäßigen Abständen überprüft und ggf. angepasst werden.

Aber zurück zur derzeitigen Situation der durch Menschen ferngelenkten Drohnen. Der US-geführte „Krieg gegen den Terror" beinhaltet ein hohes Maß an politischer Willkür, was einen gefährlichen Präzedenzfall für das Völkerrecht setzt. Mit fortschreitendem technischen Fortschritt ist es nur eine Frage der Zeit, bis auch andere Länder die gleichen Fähigkeiten wie die USA entwickelt haben werden. In erster Linie sind hier China, Russland, die europäischen Staaten und Japan zu nennen. Sollte es einem dieser Länder in den Sinn kommen, seinen machtpolitischen Ambitionen mit Hilfe bewaffneter Drohnen Nachdruck zu verleihen, dann droht eine Eskalation des Schreckens. Letztlich zeichnet sich eine Welt ab, in der niemand mehr seines Lebens sicher sein kann, weil stets wie aus heiterem Himmel eine Kampfdrohne kommen und alles ausradieren kann.

Hier ist also auch unbedingt politischer Regelungsbedarf nötig, am besten in Form eines völkerrechtlich bindenden Abkommens. Es sollte aber dabei berücksichtigt werden, dass dies kein exklusiv an Drohnen gekoppeltes Problemfeld darstellt. Interventionismus gibt es viel länger. In den 1980er Jahren wurde z.B. in den USA das Konzept der „Konflikte niedriger Intensität" entwickelt. Damals bediente man sich Guerillatruppen zum Teil zweifelhafter Zuverlässigkeit. In den Bürgerkriegen Mittelamerikas wurden z.B. in Nicaragua die „Contras" von den USA unterstützt, ein Zusammenschluss verschiedener Oppositionsgruppen gegen die revolutionäre Regierung in Nicaragua, denen immer wieder schwere Menschenrechtsverletzungen vorgeworfen wurden und die sich zum Teil über den Drogenhandel finanzierten[19]. Drohnen ersetzen heute diese Guerillatruppen und haben den Vorteil, dass sie nicht aus dem Ruder laufen können.

Es geht also letztlich um Einmischung in die Angelegenheiten anderer Staaten. Und da stehen die USA nicht allein da, Russland hat ebenso eine imperialistische Vergangenheit, wie die z.B. die Besetzung der baltischen Länder im 2. Weltkrieg und in neuerer Zeit die Besetzung Abchasiens und Ossetiens in Georgien zeigen. Solange nationalstaatliche Eigeninteressen dominieren, ist die Versuchung der unilateralen Regelung

[19] http://www.brown.edu/Research/Understanding_the_Iran_Contra_Affair. Link verifiziert am 24.7.2014.

solcher Konflikte sehr groß.

Als erster Schritt sollte daher der Einsatz der jetzt schon existierenden Vehikel, insbesondere der Drohnen, völkerrechtlich oder mit einer internationalen Konvention eingeschränkt werden. Es wäre bereits ein Fortschritt, wenn die außergerichtlichen Tötungen in unbeteiligten Drittstaaten international geächtet werden könnten. Das Problem, das sich durch Interventionismus generell stellt, ist damit aber noch nicht gelöst.

Dr. rer. nat. Roland Reimers, Lehrer in Berlin, Vorstandsmitglied von Natwiss.

NatWiss
NaturwissenschaftlerInnen-Initiative
Verantwortung für Frieden und Zukunftsfähigkeit e.V.

„Wir sind nicht nur verantwortlich für das was wir tun, sondern auch für das, was wir widerspruchslos hinnehmen."
Ernst Bloch (Philosoph, 1885-1977)

Im Februar 1988 haben sich NaturwissenschaftlerInnen in der Initiative "Verantwortung für Frieden und Zukunftsfähigkeit" zusammen gefunden, um als Teil der Friedensbewegung ihre spezifischen professionellen Kompetenzen für eine Welt ohne Krieg und Gewalt, für die Kontrolle und Beseitigung atomarer, chemischer, biologischer und konventioneller Waffensysteme, für Friedens- und Abrüstungsforschung und für soziale, ökologische und humane Technikgestaltung einzusetzen.

NaturwissenschaftlerInnen und IngenieurInnen sind die Protagonisten des Industriesystems: Sie erforschen, entwickeln und bauen die naturwissenschaftlich-technischen Geräte und Systeme, die seit der industriellen Revolution die Welt verändert haben. War bisher Analyse, Kritik und Kontrolle der Rüstungs- und Waffentechnik das Hauptarbeitsgebiet unserer Initiative, ist in den letzten Jahren die zivile „Alltagstechnik" und das materielle Wachstum als Gefahr für die Biosphäre und damit für die menschliche Existenz in ihr verstärkt in den Blick gekommen. Öffentlich diskutiert wird derzeit fast nur das Klimaproblem, das im Wesentlichen mit dem weiter steigenden Verbrauch fossiler Energieträger zusammenhängt. Wir sehen aber generell einen Raubbau an den anorganischen und biologischen Ressourcen der Natur, der inzwischen die Reproduktivität der nutzbaren Flächen auf dem Land und im Meer akut gefährdet. Der infolge des materiellen Wachstums stetig wachsende Rohstoffverbrauch hat entsprechend dem Entropiegesetz auch negative Folgelasten, welche die Biosphäre belasten: Emission von Klimagasen, Müllproduktion von Elektronikschrott bis zu Chemieabfällen, freigesetzte chemische und pharmazeutische sowie biologisch aktive und radioaktive Stoffe, Verlust der Artenvielfalt und Artensterben, Zerstörung der produktiven Flächen, der Wälder und der Wasserversorgung für große Teile der Erdbevölkerung.

Wir engagieren uns deshalb auch gegen das ökonomische Paradigma des ständigen „Mehr" der marktradikalen, globalisierten Geldwirtschaft und bemühen uns um Aufklärung von Öffentlichkeit, Politik, Gewerkschaften und Unternehmen über die

systemischen Gefahren durch weiteres materielles Wachstum und dessen Grenzen.

Naturwissenschaft und Technik haben sich seit der industriellen Revolution der Aufgabe verschrieben, dieses „Mehr“ technisch, energetisch und stofflich möglich zu machen. Wir wissen und erleben heute, dass die Ideologie ständigen ökonomischen Wachstums in der bisherigen, durch Ressourcen-Raubbau und fossile oder atomare Energie angetriebenen Form geschichtlich bald überholt und heute mehr Teil des Problems als Teil der Lösung ist. Die technische Nutzung der Kernspaltung ist eines von vielen Beispielen dafür, dass Naturwissenschaft und Technik Konzepte angeboten haben, die nicht nur mit illusionären Versprechen verbunden waren, sondern sich in der militärischen und zivilen Variante gleichermaßen als gefährlich und zerstörerisch erwiesen haben.

Nach dem Ende der militärischen Konfrontation von Kapitalismus und „real existierendem“ Sozialismus, zweier politisch unterschiedlicher, in der Ausbeutung der Natur und ihrer Technikgläubigkeit aber sehr ähnlicher Systeme, werden „moderne“ Kriege bei fortdauerndem Wachstumsanspruch heute verschärft um immer knapper werdende energetische und stoffliche Ressourcen geführt. Das Ungleichgewicht zwischen den reichen und den armen Ländern führt auch wegen der stofflichen Geschlossenheit unserer Geobiosphäre zunehmend zu Konflikten. Unser Engagement für Frieden und Abrüstung kann deshalb nur wirksam sein, wenn Ökonomie und Technik den natürlichen Gegebenheiten angepasst, die begrenzten Ressourcen international gerecht verteilt werden und die Belastung der Biosphäre drastisch eingeschränkt wird.

Deshalb arbeiten wir gemeinsam mit anderen Nichtregierungsorganisationen neben unserem gesellschaftlichen Engagement für Frieden, Abrüstung und Nachhaltigkeit an praktischen Projekten einer an Humanität und Nachhaltigkeit orientierten Naturwissenschaft und Technik, die stofflich und ökonomisch eingebettet ist in die Natur und in die soziale und kulturelle Diversität menschlicher Gesellschaften. Solche Projekte wachsen auch durch das Engagement von NaturwissenschaftlerInnen und IngenieurInnen, die grundsätzlich, spätestens aber seit dem ersten Bericht des Club of Rome, um die Grenzen des Wachstums wissen und folglich ihre professionelle Kompetenz statt zur ständigen Steigerung des stofflichen und energetischen Umsatzes zu dessen Minimierung bei größtmöglichem Nutzen für alle Menschen einsetzen.

Unsere Ziele sind:

- Information der Gesellschaft über die Fakten,
- eine Welt ohne ABC-Waffen und Atomenergie,
- schnellstmöglicher Ausstieg aus der fossilen Energiewandlung durch Umsteuerung auf regenerative Energiequellen,
- Suffizienz in Energieverbrauch und Konsum,

- globale Gerechtigkeit bei der Nutzung von natürlichen Ressourcen,
- Ausstieg der NaturwissenschaftlerInnen und IngenieurInnen aus der militärischen Forschung, Waffenentwicklung und -produktion weltweit,
- Friedens- und Umwelterziehung in der naturwissenschaftlichen Lehre und
- internationale Kooperationen für eine friedliche Welt.

Wir wollen die Rolle der „erfinderischen Zwerge, die für alles gemietet werde können“ (B. Brecht, „Galilei“) überwinden und fühlen uns als WissenschaftlerInnen und BürgerInnen dazu verpflichtet, mit unseren Arbeiten und Überlegungen über die traditionellen Grenzen der Fachwissenschaft in Forschung, Lehre und Praxis hinauszugehen. Deshalb engagieren wir uns in Zusammenarbeit und im Zusammenwirken mit anderen berufsbezogenen Initiativen politisch und gesellschaftlich entsprechend dem Vorbild von NaturwissenschaftlerInnen und IngenieurInnen wie Klara Immerwahr, Albert Einstein, Josef Rotblat, Dorothy Hodgkin, Joseph Weizenbaum, Hans-Peter Dürr und vielen anderen.

Die NaturwissenschaftlerInnen-Initiative (NatWiss) ist ein unabhängiger, überparteilicher und nicht konfessionell oder weltanschaulich gebundener gemeinnütziger Verein von WissenschaftlerInnen vor allem, aber nicht nur aus dem Bereich der Naturwissenschaften.

NatWiss arbeitet unter anderem zusammen mit der Vereinigung Deutscher Wissenschaftler (VDW) und den Internationalen Ärzten für die Verhütung des Atomkrieges (IPPNW), ist u.a. Mitglied im Trägerkreis des Grüner Strom Label e.V. und beteiligt sich an Aktionen und Veranstaltungen wie beispielsweise dem Internationalen Friedensaktionstag.

NatWiss hat zur Zeit ca. 500 Mitglieder und finanziert sich durch deren Beiträge und durch Spenden.

Kontakt:

NaturwissenschaftlerInnen-Initiative—
Verantwortung für Frieden und Zukunftsfähigkeit
c/o IALANA
Marienstraße 19-20
10117 Berlin
Tel: 0049 (0)30 31 99 66 86
Fax: 0049 (0)30 31 99 66 89
geschaeftsfuehrung@natwiss.de
www.natwiss.de

Dank an:

Allgemeiner Studierendenausschuss
Technische Universität Berlin

FIfF
Forum Informatikerinnen und Informatiker
für Frieden und gesellschaftliche Verantwortung e.V.

Öffentliche Veranstaltung im Plenarsaal des AStA TU Berlin

Impressum:

NaturwissenschaftlerInnen-Initiative—Verantwortung für Frieden und Zukunftsfähigkeit e.V.
c/o IALANA
Marienstraße 19-20
10117 Berlin
www.natwiss.de

V.i.S.d.P.: Lucas Wirl

Redaktion: Hester Samoray, Lucas Wirl