Gesellschaft zum Schutz von Bürgerrecht und Menschenwürde e.V. - Zentraler Arbeitskreis Frieden
Europäisches Friedensforum epf Deutsche Sektion

Nr. 133

Elemente der Kriegsstrategie im 21. Jahrhundert

von

Klaus Eichner

Redaktionsschluss: 6. Februar 2014

c/o **Gesellschaft zum Schutz von Bürgerrecht und Menschenwürde e. V.**
Weitlingstrasse 89, 10317 Berlin
Tel.: 030/ 557 83 97 Fax: 030/ 555 63 55 E-mail: gbmev@t-online.de Homepage: www.gbmev.de/

Es ist eine alte Diplomatenweisheit: Staaten haben keine Freunde, Staaten haben Interessen.

Diese Interessen sind vor allem geostrategischer Natur, vorwiegend basierend auf wirtschaftlichen Zielen, insbesondere dem Zugang zu entscheidenden Ressourcen (neben Öl und Gas auch Wasser, Nahrung, seltene Erden etc.) oder zumindest Kontrolle des Zugangs zu diesen Ressourcen.

Unter diesen Gesichtspunkten lohnt es sich, einige der aktuellen öffentlichen Diskussionen intensiver zu hinterfragen.

Das Fazit vorweggenommen:
Fast im Verborgenen wird eine völlig neue Strategie der Kriegführung entwickelt und aufgebaut. Diese beruht entscheidend auf drei Säulen:

- Informationskrieg (Cyber Warfare);
- Einsatz ferngesteuerter/zunehmend automatisierter Systeme für Aufklärung und Waffeneinsatz (u. a. Drohnen);
- Vermischung von geheimdienstlichen und militärischen Sonderoperationen.

Informationskrieg (Cyber Warfare)

In den letzten Jahren hat es mehrfach sprunghafte qualitative Entwicklungen bei den technischen Möglichkeiten der Aufklärung, Erfassung und Verarbeitung von elektronischen Informationen gegeben.

Mit den aktuellen Veröffentlichungen über die so genannten Ausspähaffäre werden nur einige oberflächliche Erscheinungen einer neuen Qualität des Informationskrieges (= Cyber Warfare) publik gemacht. Der Begriff Cyber Warfare steht für „Kriegführung im virtuellen Raum“ (Cyber Space).

Damit wurde für die Kriegführung eine fünfte strategische Dimension (nach Land, Luft, See, Weltraum) eröffnet. Der Cyber-Krieg beinhaltet elektronische Angriffe auf Netzwerke und Server der gegnerischen Seite bzw. potentieller Feinde, mit denen deren Informationsbeziehungen blockiert bzw. ausgeschaltet oder manipuliert werden könnten.

Mehr noch, das Überleben der modernen Gesellschaften ist heute schon fast komplett abhängig vom Funktionieren der digitalisierten, computergestützten Systeme der Lebenserhaltung, der Infrastruktur und der Kommunikation. Störungen oder gar Ausschaltung dieser Systeme werden für ganze Staaten eine Frage des Überlebens, wenn sie nicht rechtzeitig erkannt und abgewehrt werden können.
Auch die Geheimdienste werden immer deutlicher von der Informations-Technologie abhängig. Experten gehen z. B. davon aus, dass nur ca. 25 Prozent des Informations-aufkommens der Geheimdienste von geheimen Quellen erbracht werden, von diesen Geheim-Informationen stammen wiederum drei Viertel aus der Fernmelde/Elektronischen Aufklärung. Das daraus entstehende Informationsaufkommen ist (wenn überhaupt) nur noch durch den Einsatz von Hochleistungscomputern beherrschbar. Mit den elektronischen Informationen wachsen aber auch die Möglichkeiten der Täuschung und Desinformation sowie die Anfälligkeiten für elektronische Angriffs- oder Störmaßnahmen.

Im Jahre 2009 erklärte Präsident Obama die digitale Infrastruktur der Vereinigten Staaten zu einer nationalen strategischen Angelegenheit, und im Mai 2010 kam es zur Etablierung des Cyber Space Command (US CYBERCOM) mit Sitz in Fort Meade/Maryland. Das Kommando ist unmittelbar dem zentralen Geheimdienst für elektronische Abwehr und Aufklärung (National Security Agency – NSA) unterstellt. Das US CYBERCOM ist vorrangig für die militärischen Komponenten der Cyber Warfare zuständig. Das Personal soll in den nächsten Jahren von 900 auf knapp 5.000 Mitarbeiter aufgestockt werden.

US-Verteidigungsminister Leon Panetta forderte im Oktober 2012 in einer Rede über das Schlachtfeld der Zukunft, eine Doktrin für künftige Cyberkriege zu entwickeln. Seine These: *Künftig werde der Krieg im Cyberspace ein normaler Bestandteil amerikanischer Militäroperationen sein.*
Was Panetta vornehm verschweigt: Das US-CyberCommand hat bereits im Jahr 2011 mindestens 231 offensive Operationen durchgeführt, von denen 18.000 meist hochgesicherte Computer

und Netzwerke betroffen waren – davon wurde keine Operation öffentlich bekannt. Das CyberCommand hat allein im Jahr 2011 rund 652 Millionen US-Dollar eingesetzt, um in weltweit genutzten Computersystemen Hintertüren einzubauen, die jederzeit von den USA für Angriffe genutzt werden können (ND vom 18. 11. 2013). Wir befinden uns also schon mitten drin im Informationskrieg!

Parallel dazu werden unter der Führung des US-Department of Homeland Security die innenpolitischen, zivilen und vor allem repressiven Aspekte dieses Krieges erforscht und in die Praxis der Überwachung des ganzen Landes umgesetzt. Außerdem installieren die großen Konzerne eigene Strukturen für Computersicherheit und virtuelle Angriffe auf Konkurrenten.

Eine der bekanntgewordenen aktuellen Operationen der virtuellen Kriegführung war der Einsatz des Computervirus „Stuxnet“ gegen die Urananreicherungsanlagen im Iran. Präsident Obama hatte diese Operation mit der Deckbezeichnung „Olympische Spiele“ (Olympic Games) persönlich angeordnet. Damit wurden rund 1.000 der 5.000 Zentrifugen zur Urananreicherung in der iranischen Atomfabrik Natanz zeitweilig außer Betrieb gesetzt bzw. in ihrer Funktionsweise manipuliert. Diese Manipulierung kann die Funktionsweise der Zentrifugen bis zur Katastrophe treiben. Dem Iran gelang es jedoch, den Virus in relativ kurzer Zeit unschädlich zu machen. Es gibt Hinweise, dass dieser Virusangriff gegen den Iran eine gemeinsame Operation der US-amerikanischen Geheimdienste und des israelischen Mossad war.

Aber selbst das Führungszentrum für den Einsatz der als „Drohnen“ verharmlosend umschriebenen Fliegenden Tötungsmaschinen (FTM) in der Luftwaffenbasis Creech war Zielobjekt eines Cyberangriffs. Die *Los Angeles Times vom 13. 10. 2001* berichtete, dass die Datenverbindungen des Kommandos lahmgelegt waren und die Experten zwei Wochen benötigten, um die Arbeitsfähigkeit der Systeme wieder herzustellen.

Europäische Union

Die EU bildete als eine zentrale Einrichtung die „Europäische Agentur für Netz- und Informationssicherheit“ („European Network and Information Security Agency – ENISA“) unter Leitung von Prof. Udo Helmbrecht. Sie definiert als ihre Aufgabe, gemeinsam mit EU-Institutionen und den staatlichen Behörden der Mitgliedsländer eine „Sicherheitskultur für EU-weite Informationsnetze“ zu entwickeln.

2013 veröffentlichte die Europäische Kommission eine neue Cybersicherheitsstrategie der EU für ein „offenes, freies und chancenreiches Internet“. In dem Strategiepapier heißt es: „Die EU wird mit internationalen Partnern und Organisationen, dem privaten Sektor und der Zivilgesellschaft zusammenarbeiten, um den Aufbau von Kapazitäten in Drittstaaten weltweit zu fördern. Dazu gehören ein verbesserter Zugang zu Informationen und einem offenen Internet sowie der Schutz vor Cyber-Bedrohungen.“
Im November 2011 spielten die Europäische Union und die USA in einem gemeinsamen Manöver (Cyber Atlantic 2011) den „Cyberwar-Ernstfall“ durch. Zum Übungs-Szenario gehörte u. a. eine „zielgerichtete verdeckte Cyber-Infiltration, um geheime Informationen aus den Rechnern der Cyber-Sicherheitsbehörden der EU-Staaten zu entwenden.“

Zur Verbesserung der öffentlichen Akzeptanz rief die ENISA für den Oktober 2013 zu einem „Europäischen Cybersicherheits-monat“ in 25 Ländern (22 EU-Mitgliedsstaaten und 3 Partnerländer) auf.

Bundesrepublik Deutschland

In der Bundesrepublik Deutschland spielen eigene Kapazitäten der Informations-Kriegführung ebenfalls eine wesentliche Rolle, vor allem mit dem Kommando Strategische Aufklärung der Bundeswehr (KSA). Offiziell wird für das KSA eine offensive militärische Funktion definiert: z. B. das Eindringen in gegnerische Netzwerke, um die Luftabwehr auszuschalten (Bln.Ztg. 10.5.13). Die volle Einsatzbereitschaft des KSA für den

Cyber-Krieg wird für ca. 2016 erwartet (es fehlen z. B. noch geeignete geschützte Fahrzeuge für mobile Cybertrupps).
Seit 2006 wird im KSA eine Abteilung „Informations- und Computer-Netzwerk-Operationen – CNO“ aufgebaut, CNO soll seit Ende 2011 einsatzbereit sein. CNO ist die offizielle Bezeichnung für alle Komponenten des „Cyber-War“ in der Bundeswehr.

Der BND baut eine eigene Abteilung zur Aufklärung und Abwehr von Angriffen gegen das Internet auf. Diese Aktivitäten werden öffentlich begründet als Abwehr gegen Hackerangriffe; vorwiegend von China und Russland aus. (Spiegel 13/2013)

Neben BND und Bundeswehr fordert das Bundesinnenministerium den Aufbau von Kapazitäten für die Kriegführung im virtuellen Raum. In Seminaren der Bundesakademie für Sicherheitspolitik wurden Vorschläge an die Bundesregierung zur systematischen Vernetzung der Repressionsbehörden verabschiedet. Dazu gehören auch Forderungen nach Veränderung des Völkerrechts und der „nationalen Rechtsordnung“, um den „neuen Bedrohungen“ durch Terrorismus und „Cyber-Angriffe“ gerecht werden zu können. Der Hauptangriff zielt dabei auf die im Grundgesetz der BRD noch verankerte „Grenzziehung zwischen der Bundeswehr und den Sicherheitsbehörden“. (german-foreign-policy, 1.8.2012)

Mitte 2011 wurde das erste Nationale Cyber-Abwehrzentrum (NCAZ) als Kommunikationsplattform der deutschen Sicherheitsbehörden gegründet. Es ist beim Bundesamt für Sicherheit in der Informationstechnik angesiedelt und kooperiert mit dem Verfassungsschutz, dem BND, dem Katastrophenschutz und diversen Internetanbietern.

USA-Geheimdienste in der BRD

1999 konzentrierte der Geheimdienst INSCOM (Intelligence and Security Command – Geheimdienst der US-Landstreitkräfte) rund 50 Einheiten und Dienststellen im Raum Griesheim bei Darmstadt (im sogen. Dagger Complex). Mit einem Aufwand von 18 Mio. US-Dollar wurde dort das deutsche Hauptquartier von INSCOM

aufgebaut. Auf den benachbarten August-Euler-Flugplatz verlegte INSCOM im Jahr 2003 unter der Projektbezeichnung „ICEBOX“ Antennenanlagen aus der früheren Großstation der NSA in Bad Aibling. Die Anlagen wurden zwischen 2006 und 2008 von Wiesbaden aus fernbedient betrieben und anschließend wieder zurückgebaut.
Gegenwärtig soll dort noch das „European Cryptologic Center“ mit rund 1.100 Mitarbeitern tätig sein.
Im Augenblick bereitet INSCOM eine erneute Verlegung vor. Im Bereich des Europa-Hauptquartiers der US-Landstreitkräfte (US-Army Europe – USAREUR) in der Lucius D. Clay-Kaserne in Wiesbaden-Erbenheim baut INSCOM bis 2015 für 124 Millionen Euro ein Gemeinsames Aufklärungs-Zentrum („Consolidated Intelligence Center - CIC“) auf.
Nach den bisher bekannten Dimensionen entsteht hier ein neues Abhörzentrum für Europa, ausgerüstet mit den modernsten Anlagen für die Erfassung von elektronischen Abstrahlungen aller Art und entsprechenden Kommuni-kationsanlagen.
Vordergründig soll das Consolidated Intelligence Center nach den vorliegenden Medieninformationen Aufklärungsdaten für die Einsätze der dem Europakommando der US-Army unterstellten Einheiten beschaffen und auswerten – das betrifft Spionageinformationen aus über 50 Ländern – von Russland bis Israel.
Die Bundesregierung ist über dieses Projekt ausreichend informiert, wie der BND-Präsident in einer Sondersitzung des Innenausschusses des Bundestages im Juli 2013 bestätigte. Im CIC wird die jahrzehntelange enge Zusammenarbeit der deutschen und US-amerikanischen Geheimdienste fortgesetzt.

Geheimdienstliche Partnerdienstbeziehungen

Unter dem Deckmantel des Kampfes gegen den Terrorismus erfolgt auch in Deutschland eine Zusammenfassung vielfältiger Informationen in zentralen Datenbanken sowie ein reger Austausch mit Partnerdiensten, vor allem der Vereinigten Staaten. Die bundesdeutschen Geheimdienste reagieren auf kritische Hinweise aus der Öffentlichkeit mit dem Hinweis, sie

„sichern sich gegen einen Missbrauch ihrer Daten für die Menschenjagd“ ab, indem sie an die amerikanischen Partnerdienste nur Telefon-Nummern ohne Ortsangaben weiterleiten und diese Hinweise mit den Zusätzen versehen: die Amerikaner dürften sie nur im „nachrichtendienstlichen Bereich“ oder nur zur „Gefahrenabwehr“ verwenden. (vgl. SPIEGEL 20/2011: „Feuer und Schwefel“) Damit haben die deutschen Behörden aber nur scheinbar feste Riegel gegen einen Missbrauch der deutschen Informationen vorgeschoben – jeder Insider ist sich darüber klar, welchen wirklichen Wert die Geheimdienste auf solche „Sperrvermerke“ legen.

Das Projekt ECHELON

Bereits 1998 entstand im Auftrag des Ausschusses für Bürgerrechte des Europaparlaments ein erster Bericht über ECHELON. Darin wurde es als weltweites Spionagesystem im Dienste der amerikanischen NSA vorgestellt, mit dem alle über Satelliten laufenden Telefongespräche, Faxe und E-Mails aufgefangen und ausgewertet werden können. Obwohl der damalige EU-Kommissar für Telekommunikation, Martin Bangemann, sagte, wenn es so etwas gäbe, wäre es „ein Skandal“, erregte dieser Bericht kaum Aufsehen. Einige Zeit später erschien dann einer weitere Studie des Amtes zur Bewertung von Technologiefolgen bei der EU (STOA-Scientific and Technological Options Assessment) aus der Feder des britischen Sicherheitsexperten Duncan Cambell. Er konzentrierte die Aussagen zu ECHOLON insbesondere auf die Funktion in der Wirtschaftsspionage - und nun ging es an und um das Geld, und die Politik und die Medien reagierten.

Weitgehend verschwiegen wurde in der Diskussion, dass ECHOLON ein Spionagesystem der NATO-Staaten unter strenger Führung durch die USA darstellt. Die beteiligten NATO-Partner werden von den USA relativ willkürlich und unter Beachtung ihres Nutzens für die USA und ihrer „Zuverlässigkeit“ an den Ergebnissen der weltumspannenden elektronischen Spionage beteiligt.

Das System ECHELON erfasst Informationen auf mehreren Ebenen:

- Es werden die internationalen und regionalen Telekommunikationssatelliten (z.B. INTELSAT) angezapft.
- Dann stehen die Überseekabel unter Kontrolle, entweder durch Verteilerknoten an ihren landseitigen Schnittstellen oder durch elektronische Erfassungssysteme direkt an den Kabeln.
- Alle Richtfunkstrecken, über die immer mehr Fernmeldeverkehre abgewickelt werden, werden überwacht.
- Hochleistungsfähige Antennen- und Peilsysteme erfassen weiterhin die Funkverkehre, insbesondere Funk-Fernverbindungen.

Die politische Aufklärung richtet sich u. a. auch und nicht zuletzt gegen die politische Opposition oder andere politisch missliebige Personen oder Organisationen. So konnten sich vor einiger Zeit die Engländer darüber aufregen, dass ihre Prinzessin Diana ebenfalls Objekt der Echelon-Überwachung war und in den Speichern der NSA erfasst wurde. Das geschah vor dem Hintergrund der Überwachung solcher Organisationen wie Amnesty International, Christian Aid oder Greenpeace. Nach Aussagen des ehemaligen Mitarbeiters der NSA, Wayne Madsen, wird „jeder, der politisch aktiv ist, früher oder später von Radarschirm der NSA erfasst werden."

Nun stehen dem geheimdienstlichen Einsatz gegen die politische Opposition in einigen Staaten rechtliche Regelungen entgegen, die solche Aktivitäten offiziell verbieten oder bestimmten Einschränkungen unterwerfen. Gehen wir einmal positiv davon aus, dass die Geheimdienste ihr innerstaatliches Recht achten und angeblich auch einhalten. Dann bietet ihnen der Datenverbund in ECHOLON immer noch die Möglichkeit, dieses Recht scheinbar legal zu brechen. Dann erfassen die Stationen in Kanada Daten über USA-Bürger, die Amerikaner in Bad Aibling hören Gespräche britischer Bürger ab etc. – und im Informationsaustausch landen diese Daten dort, wo sie gebraucht werden.

Das erinnert sehr klar an die aktuellen Diskussionen in der deutschen Politik, die auf die strikte Einhaltung der deutschen Datenschutzrichtlinien bei den Aufklärungsoperationen der USA pochen.

Die öffentliche Diskussion war aufgrund des STOA-Berichts sehr stark auf das Problem der **Wirtschaftsspionage** focusiert. Man nutzt dazu auch gern Beispiele, wo Konkurrenten sich mit Hilfe der Geheimdienste gegenseitig lukrative Aufträge abgejagt haben. Dazu ist anzumerken, dass die Orientierung auf die Geheimnisse von Firmen und Konzernen zu eng ist.
Wirtschaftsspionage umfasst auch die Überwachung finanzieller Transaktionen (nicht nur zur Bekämpfung der Geldwäsche!), die Erfassung wissenschaftlich-technischer Entwicklungen, die Lage auf den Rohstoffmärkten (auch Wasser und Getreide) und die Entwicklung der Ressourcen weltweit.
Aber Wirtschaftsspionage ist nicht erst durch ECHELON zum Problem geworden. Bereits 1994 haben Erich Schmidt-Eenboom und Jo Angerer in „Die schmutzigen Geschäfte der Wirtschafts-spionage“ dazu umfangreiche Rechercheergebnisse veröffent-licht. 1999 hat Udo Ulfkotte mit „Marktplatz der Diebe“ die deutsche Wirtschaft als Opfer der internationalen Wirtschafts-spionage beschrieben, ohne die deutschen Täter zu benennen.

Gravierender erscheinen jedoch die immens gewachsenen Möglichkeiten und Gefahren, dass **Privatpersonen** in den Strudel dieser Überwachung gezogen werden – und sie bleiben mit all ihren Querverbindungen und persönlichen Eigenheiten (man sollte nur an die Möglichkeiten denken, die die Auswertung diverser Chipspeicher über Reisetätigkeit, Gesundheitszustand, Bankkonten, Kaufverhalten, Interessen und Neigungen durch Internet-Zugänge etc. bieten!) in den Speichern der Geheim-dienste. Hintergrund dieser Gefahren sind die verschwommenen Regelungen, die den Geheim-diensten Befugnisse zur Auf-klärung der sogen. Organisierten Kriminalität (OK) erteilen. Die sehr willkürlich gefassten Definitionen der OK gehen meist weiter als die öffentlich genannten, wie Drogenhandel, Geld-

wäsche, Waffenhandel oder Terrorismus und bedienen damit die Speicherwut der Geheimdienste.

Zu den vielen Vorschlägen, wie einem solchen Überwachungs-System zu begegnen sei, gehört auch, mehr Verschlüsselungs-Technologien einzusetzen, die Telekommunikation also abhörsicher zu machen. Dazu ist anzumerken, dass in den USA seit den 80er Jahren die technischen und rechtlichen Möglichkeiten geschaffen werden, um durch einen intern eingebauten „Zugangsschlüssel“ die Verschlüsselungs-Software für den Inhaber dieses Zugangsschlüssels – und das ist die NSA – zugänglich zu machen. Die großen Software-Anbieter wie Microsoft, Oracle oder SAP haben sich den Forderungen der NSA gebeugt. Wenn kleinere Software-Entwickler nicht spuren, werden sie vom Markt gedrängt.

Das 1995 verabschiedete EU-Memorandum über „ die rechtmäßige Überwachung des Fernmeldeverkehrs“ verlangt von jedem Kommunikationsanbieter die feste Einrichtung einer Abhör-Schnittstelle, die nach dieser Regelung natürlich nur für gesetzlich vorgesehene Abhörmaßnahmen Gültigkeit haben soll. Aber: Nichts ist unmöglich!

Automatisierte Tötungsmaschinen

Der in der öffentlichen Diskussion benutzte Begriff „Drohnen“ verharmlost diese neue Stufe der Kriegsvorbereitung durch den Einsatz Fliegender Tötungsmaschinen (FTM). Entwicklungen werden auch für ähnliche Systeme im Einsatz am Boden oder im Unterwasser-Einsatz vorangetrieben.
Gleichzeitig geht der Trend immer massiver auf die Ablösung der menschlichen Steuerung dieser Systeme auf Softwareentwicklungen, die den Maschinen selbständige Entscheidungen über Zielerfassung und Waffeneinsatz ermöglichen.

Bereits unter US-Präsident George Bush jr. hatten die USA begonnen, eine neue Doktrin der „modernen Kriegführung“ auszuarbeiten und aktiv anzuwenden. In dieser Doktrin sollten zwei geheime Kriegführungsprogramme vereinigt werden - der

Einsatz von unbemannten Waffensystemen und der Krieg der Informationssysteme (Cyber-War).
Diese Doktrin wurde zum grundlegenden Operationsprinzip des nach dem 11. September 2001 verkündeten „Krieg gegen den Terror“. Damit erklärten sich die Vereinigten Staaten als im permanenten Kriegszustand befindlich und suchten sich aus dem Kriegsvölkerrecht alle jene Regelungen heraus, die ihrer Kriegspolitik einen scheinbar legalen Anstrich vermitteln könnten.
Die alte Kanonenbootdiplomatie sollte abgelöst werden von der Durchsetzung der Interessen der amerikanischen Monopole mittels unbemannter Killermaschinen und von einem Schattenkrieg.

Präsident Obama erweiterte und effektivierte die Kriegführungsdoktrin seines Vorgängers Bush jr. Sein erklärtes Ziel besteht darin, Kriegseinsätze mit Zehntausenden von Soldaten, Panzern etc. zu beenden. Anfang 2012 erklärte er in einer Rede im Pentagon*: <<er werde die überholten Systeme aus der Zeit des Kalten Krieges abschaffen*>>.
Kriege der Zukunft sollen in einem leeren Schlachtfeld, im Verborgenen, mit einem Joystick oder Mausklick aus der Ferne ohne eigene Verluste realisiert werden. Ab und zu werden sie ergänzt durch gezielte Kommandounternehmen von Spezialeinsatzkräften. Gezielte Tötungen mit unbemannten Killermaschinen werden damit zu einem Merkmal der Militärdoktrin des Friedens-nobelpreisträgers Obama.
Obamas aktuelle Kriegführung ist die Verhängung der Todesstrafe auf Verdacht – ob für Verdächtige oder Unschuldige ist den Verantwortlichen dafür gleichgültig. Es ist dieser permanente „Krieg gegen den Terror“, der die Anwendung tödlicher Gewalt nach unbewiesenen Behauptungen an jedem Ort und gegen jedermann erlaubt. Hiermit wird aus dem Völkerrecht wieder einmal das angemaßte Recht des Stärkeren, ein Faustrecht.
Waren das die Meriten, die das Nobelpreis-Komitee veranlassten, Präsident Obama den Friedensnobelpreis zu verleihen?

Die Fliegenden Tötungsmaschinen sind nicht nur ein neues, höchst effektives Waffensystem, sie sind vor allem Instrumente zur massenhaften Tötung von Menschen außerhalb jeder Rechtsprechung. Wenn z. B. ein angeblicher Al-Qaida-Führer von einer Hellfire-Rakete in seinem Auto oder seinem Haus getötet wird, dann nehmen die verantwortlichen Einsatzleiter billigend in Kauf, dass seine dort befindlichen Angehörigen oder auch zufällige Besucher mit ermordet werden. Noch perfider wird es durch die internen Einsatzgrundsätze der sogen. „double-tap"-Angriffe, nach denen in ca. 30 Minuten ein erneuter Raketenangriff auf das gleiche Ziel erfolgt, um Angehörige von Rettungsdiensten bzw. Helfer aus der Nachbarschaft, die Überlebende suchten oder Leichen bergen wollten, ebenfalls zu vernichten.
Die Todeslisten werden angeblich von Präsident Obama persönlich bestätigt, meist auf der Grundlage von Informationen der US-Geheimdienste. Koordinator war der bisherige Berater des Präsidenten für Terrorabwehr, John Brennan, der nach der Wiederwahl von Obama für sein neues Kabinett zum Direktor der CIA berufen wurde.

In keinem der Fälle liegen jedoch der Angriffsentscheidung der Operatoren, die einen Joystick in ihren vollklimatisierten Einsatzräumen bedienen, rechtlich gesicherte Informationen über die Angriffsziele zugrunde. Oft darf der Operationsoffizier den Abschuss einer todbringenden Rakete auch schon entscheiden, wenn er „der Meinung" ist, bei dem Zielobjekt könnte es sich um einen Terroristen handeln.
Obama konnte in seinen Wahlkämpfen jedoch mit den Argumenten punkten, durch den Einsatz von Drohnen brauche kein US-Soldat sein Leben aufs Spiel setzen, d.h. übersetzt: Die Zahl der in der Heimat eintreffenden Zinksärge könne damit drastisch reduziert werden.

Die Operationsgebiete für die Drohneneinsätze werden immer mehr ausgeweitet. Neben Pakistan, Afghanistan und dem Jemen ist Somalia zunehmend Zielgebiet für die US-Drohnen.

Das US-South Command forderte die Stationierung von Drohnen für den Bereich Lateinamerika. Als offizielle Begründung dient die Aufklärung von Drogenschmugglern – aber ganz verschleiert erscheint auch die Unterstützung der „Aufstandsbekämpfung“. Dazu erwähnen Insider die logistische Unterstützung der kolumbianischen Armee in ihrem Kampf gegen die Revolutionären Streitkräfte Kolumbiens (FARC).

Der Ersteinsatz der neuen Waffensysteme erfolgte am 4. Februar 2002 in Afghanistan, seitdem sind bis Anfang 2013 allein in Pakistan mehr als 400 Drohneneinsätze bekannt geworden, davon mehr als 350 (90 Prozent) in der Amtszeit Obamas. Die vorsichtigen Schätzungen der Opferzahlen gehen von 2.500 bis über 3.300 getöteten und um 1.300 verletzten Personen aus. Unter den Toten sollen zwischen 474 bis 884 „Zivilisten“, darunter 176 Kinder gewesen sein. Aber auch unter den offiziell als „Kombattanten“ ausgewiesenen Opfern waren in der Mehrzahl örtliche Stammeskrieger, von denen keinerlei terroristische Bedrohung gegen die Vereinigten Staaten ausging (jW vom 24.10.2012; Knut Mellenthin: Krieg ohne Regeln).

Die militärische Führung liegt in den USA in den Händen des für Sonderoperation (Joint Special Operations Command - JSOC), die militärische Leitzentrale ist auf dem Luftwaffenstützpunkt Creech in Nevada stationiert. Bis 2020 sollen allein 28 Milliarden Dollar für die Ausrüstung der Streitkräfte mit Fliegenden Tötungsmaschinen (ohne Geheimdienste!) ausgegeben werden.
Natürlich nutzt die Obama-Administration ihren Einfluss, damit diese Kriegführung auch in der Operationsplanung der NATO ihren entsprechenden Platz findet (abgesehen davon, dass die US-amerikanischen Rüstungskonzerne sich damit neue riesige Absatzmärkte erschließen).
Die NATO hat auf ihrem Gipfel im Mai 2012 in Chicago das NATO-Programm einer Allianzeigenen Bodenüberwachung mit Großdrohnen („Alliance Ground Surveillance – AGS“) und dafür die Beschaffung von fünf Drohnen vom Typ „Global Hawk“ beschlossen. Die Bundesregierung trägt dafür ein Drittel der Gesamtkosten von 1,5 Milliarden Euro – aufgestockt von

ursprünglich nur 400 Millionen Euro auf vorläufig 483 Millionen Euro.

Fliegende Tötungsmaschinen in der BRD

Die Bundesregierung legte am 21. Februar 2008 ein Grundsatzdokument unter dem Titel: „Konzeptionelle Grundvorstellungen (KGv) zum Einsatz unbemannter Luftfahrzeuge in der Bundeswehr“ vor. Darin wurde erstmalig öffentlich als Einsatzoption auch die Bewaffnung derartiger fliegender Tötungsmaschinen aufgeführt. In vorhergehenden Dokumenten wurde seit Anfang der 90er Jahre immer lediglich die Funktion als Mittel der Aufklärung – insbesondere bei Auslandseinsätzen der Bundeswehr – formuliert.
Immer noch verschlüsselt charakterisieren Bundeswehrautoren die Bedeutung von Kampfdrohnen im Rahmen der Bundeswehrreform z. B. mit folgenden Worten: „Die Nutzung von unbemannten Luftfahrzeugsystemen oder Unmanned Aicraft Systems (UAS) gewinnt vor dem Hintergrund aktueller und zukünftiger Einsätze der Bundeswehr erheblich an Bedeutung.“ (Europäische Sicherheit 8/2010, S. 20)
In den Grundprinzipien der Bundeswehrreform wird der „vernetzten Operationsführung“ die Rolle eines „zentralen Weiterentwicklungsschrittes für die Streitkräfte der Zukunft“ zugewiesen.
In der Zeitschrift „*Wehrtechnik*“ (V/2010, S. 108) formulieren die Autoren zu den universellen Grundfunktionen der Tötungsmaschinen: „Die klassischen Aufgabenfelder für UAV werden in der Zukunft in den Bereichen Aufklärung (zivil und militärisch), Waffeneinsatz und als Mikro/Mini-Sensorenträger bei verdeckten Operationen liegen. […] UAV eignen sich grundsätzlich als Waffenplattform zur Bekämpfung von Zielen an Land, in der Luft und im Wasser sowie zum Wirken im Informationsraum.“

Seit einiger Zeit testet die Bundeswehr eine eigene Version des US-amerikanischen Modells „Global Hawk“ – den „Euro Hawk“, der von 2016 an zum Einsatz kommen soll.

Die Bundeswehr hat in Afghanistan drei Drohnen vom Typ „Heron“ (Reiher) im Einsatz. Diese wurden von Israel geleast (Kosten unbekannt).

Für die Operationen mit den fliegenden Tötungsmaschinen ist in der Bundeswehr ebenfalls (wie auch für Cyber Warfare) das Kommando Strategische Aufklärung (KSA) zuständig. Das KSA wurde am 17. Januar 2002 in Rheinbach in Dienst gestellt und ist jetzt in Gelnhausen bei Bonn stationiert. Das Kommando entstand nicht zuletzt aus der Überlegung heraus, sich bei militärischen Einsätzen von den Informationen der US-Aufklärung unabhängig zu machen.
Das KSA vereinigt bisherige Einzelkomponenten der Teilstreitkräfte für technische Aufklärung zu einer zentralen Dienststelle der Bundeswehr, die im Bereich des militärischen Nachrichtenwesens mit technischen Mitteln Aufklärung betreibt. Das betrifft sowohl die Unterstützung der Einsätze von Bundeswehrkontingenten im Ausland als auch die als „Krisenfrüherkennung“ bezeichnete militärstrategische Aufklärung.
Kommandeur ist seit 2012 Brigadegeneral Jürgen Setzer, zuvor Chef des Stabes des Heeresführungskommandos in Koblenz.

Das KSA ist zuständig für

- die „Satellitengestützte Abbildende Aufklärung“ (unter Nutzung der Bundeswehr-Radarsatelliten „SAR-Lupe“),
- die „Fernmelde- und Elektronische Aufklärung“,
- den „Elektronischen Kampf“ (Cyber Warfae) und die „Objektanalyse“.

In diese Aufgabenstruktur eingebettet ist der Einsatz von unbemannten Flugobjekten („Drohnen“).
Das KSA hat einen Personalbestand von rund 7.000 Soldatinnen und Soldaten, von denen ständig 150 bis 180 in den ausländischen Einsatzgebieten der Bundeswehr stationiert sind.

Nach wie vor umstritten ist die rechtliche Bewertung des Drohneneinsatzes zur gezielten Tötung von Personen. Letzten Endes vollziehen die Leitoffiziere der Drohnen an ihren Monitoren extralegale Todesstrafen, nur auf Verdacht und ohne

jede Rechtsgrundlage. Zugleich nehmen sie billigend den Tod einer Vielzahl unschuldiger Zivilisten, vielfach von Kindern, in Kauf.
Wissenschaftler von zwei US-amerikanischen Eliteuniversitäten haben im Herbst 2012 eine äußerst kritische Bewertung der Drohnenangriffe vorgelegt. Diese Art der Kriegführung sei politisch kontraproduktiv, rechtlich fragwürdig und koste Hunderten von Zivilisten das Leben. Sie betonten: „Alle Angriffe auf Personen oder Gruppen, die keine Verbindung zu den Terroranschlägen vom 11. September 2001 hätten und die die USA nicht unmittelbar bedrohen, seien rechtlich zweifelhaft“ (zitiert in Berliner Zeitung, 26.9.2012)
Dagegen wendet sich ein „Völkerrechtsexperte“ der Viadrina-Universität in Frankfurt/Oder. Dieser behauptet, die Kameras und Sensoren in den Drohnen garantierten, dass die vom humanitären Völkerrecht geforderte Unterscheidung zwischen Zivilpersonen und Angehörigen organisierter bewaffneter Gruppen gewährleistet sei (jW 16.11.2012). Damit gibt dieser Wissenschaftler die erwartete Unterstützung für die Forderungen der Bundeswehr nach Anschaffung und Einsatz von Kampfdrohnen.

Wehrpflichtarmee – Berufsarmee - Söldnerarmee

In den imperialistischen Hauptländern und darüber hinaus erfolgt ein rasanter Umbau der Streitkräfte von den klassischen Verteidigungs- und Angriffsformationen auf die „Krisen-reaktionskräfte“ (Rapid Employment Forces) mit hoher und globaler Einsatzbereitschaft. Damit lassen sich auch angebliche Abrüstungsfortschritte begründen (z. B. die Abschaffung schwerer Verbände und Ausrüstungen) oder die Abschaffung der Wehrpflicht als politischen Erfolg darstellen (durch den notwendigen Aufbau einer Berufsarmee).

All das ist Bestandteil der Bundeswehrreform, deren Ziel sein soll, die Bundeswehr professioneller, schlagkräftiger, moderner und attraktiver zu machen (so der ehemalige Generalinspekteur der Bundeswehr, Harald Kujat und in der letzten Zeit fast alle

verantwortlichen Politiker der BRD). Mit dieser Reform wird ein Fähigkeitsprofil der Bundeswehr angestrebt, das im Rahmen der Interventionsstrategie der NATO gleichzeitig die Durchführung von zwei großen Operationen hoher Intensität und mehrerer kleiner Operationen ermöglichen soll. Der Auftrag der Bundeswehr besteht nicht mehr in der im Grundgesetz verankerten Landesverteidigung (z. B. Art. 12a Wehrpflicht …; Art. 26: Verbot des Angriffskrieges; Art. 87a Streitkräfte; Kapitel X a Verteidigungsfall) sondern im Führen weltweiter imperialistischer Interventionskriege.

Der allgemeine Trend geht zum Einsatz hochqualifizierter Berufssoldaten und zur Rückkehr des privaten Unternehmertums im Krieg (Eric S. Hobsbawm), verbunden mit dem Einsatz von Söldnern.
Damit verzichten die Staaten zunehmend auf ihr Gewaltmonopol als Kern der staatlichen Souveränität.
Unternehmertum und Kapitalinteressen treten an die Stelle des Staates. Ein früherer Justitiar der CIA verweist auf das unvermeidliche Dilemma bezüglich der Loyalität der Söldner: „Gilt sie der Fahne? Oder gilt sie der Bilanz?“ (zitiert in Mark Mazzetti: „Killing Business“, Berlin-Verlag, 2013).

Hinzu kommt, dass die Entwicklung der modernen Militärtechnik Massenarmeen und massive Waffenkonzentrationen zunehmen überflüssig macht, womit man auch auf die Wehrpflicht verzichten kann.
Mit der Verlagerung der staatlich organisierten Gewalt auf private Unternehmer in Krisen- und Kriegsgebieten ist eine Camouflage der Interventionsabsichten und –ziele verbunden. Wenn offiziell erklärt wird, dass die Truppenkontingente abgezogen werden (Beispiele Irak und Afghanistan), dann bleiben in den besetzten Ländern immer noch genügend Konzentrationen von Söldnern, mit all ihren unberechenbaren Reaktionen und Folgen. Diese privatwirtschaftlichen Dienstleister der US-amerikanischen Geheimkriege werden meist von ehemaligen Geheimdienst-Offizieren oder früheren Angehörigen

von Spezialeinsatzgruppen betrieben. Ihre Einsatzgebiete werden immer weiter ausgedehnt.

Moderne Streitkräfte und geheime Kriege

Parallel zu dieser Entwicklung schuf die US-Administration vereinigte Kommandostrukturen, wodurch die Grenzlinien zwischen militärischen Einsätzen und geheimdienstlichen Sonderoperationen immer weiter verwischt werden. Damit wurden geheime Kriege zu einem Grundpfeiler der Außenpolitik des Friedensnobelpreisträgers Obama und es kommt zur Bildung eines militärisch-geheimdienstlichen Komplexes, einer immer engeren Verflechtung zwischen Geheimdienst und Militär durch geheimdienstliche Sonderoperationen.

Ein Paradebeispiel, das uns der Pulitzer-Preisträger Mark Mazzetti in seinem Buch „Killing Business“ ausführlich darlegt, ist die Aufklärung des Wohnsitzes von Osama bin Laden in Abbottabad, einem Ort mitten in Pakistan, und letzten Endes die militärische Operation zu seiner Liquidierung. Der Autor nennt sie die größte und kostspieligste Menschenjagd in der Geschichte (S. 320), die unter bewusster Verletzung der Souveränität eines partnerschaftlich verbundenen Staates erfolgte.
Man muss sich dabei an die Fernsehübertragung aus dem Weißen Haus erinnern, wie die Führungsriege um Präsident Obama das Ergebnis dieser Operation feierte.

Als die amerikanische Öffentlichkeit Mitte der 70er Jahre durch die Untersuchungen von Ausschüssen des Kongresses und des Senats über illegale Praktiken der CIA – z. B. Planung und Durchführung von blutigen Staatsstreichen, Ermordung von führenden ausländischen Politikern, Überwachung der eigenen Bevölkerung – aufgeschreckt wurde, führte das schnell zu drastischen Reaktionen: Der Präsident der USA verbot per Verwaltungsanordnung („Executive Order“) – verbindlich für alle US-amerikanischen Geheimdienste - grundsätzlich solche Praktiken. Zumindest offiziell wurde dieses Verbot auch eingehalten – bis die „Große Wende“ kam.

Als unmittelbare Reaktion auf die Attacken vom 11. September 2001 erklärte der Präsident der USA, George Bush jr., den „Krieg gegen den Terror“ und hob damit alle bisherigen Restriktionen der Geheimdienstarbeit auf – die Hunde wurden von der Kette gelassen. Aber diese Entscheidung betraf nicht nur eng begrenzt die Aktivitäten der USA-Geheimdienste. Damit wurde insgesamt eine qualitativ neue Phase der imperialistischen Kriegführung eingeleitet.

Mit den dazu ergangenen Entscheidungen der US-Administration erhielt der US-Präsident die Vollmacht, überall auf dem Erdball, in jedem Lande, in dem nach den vorliegenden Informationen angeblich al-Qaida operierte, Krieg zu führen. In den ersten Jahren nach 2001 realisierte die CIA diese Vollmacht vorwiegend über ein geheimes – und illegales - Inhaftierungs- und Folterprogramm. Verdächtige Personen wurden entführt und ohne jede Rechtsgrundlage weltweit in geheime Foltergefängnisse verbracht. Partner dafür waren meist Diktatoren, bei denen völkerrechtliche (z.B. die Anti-Folter-Konvention der Vereinten Nationen) und rechtsstaatliche Standards keine Rolle spielten.

Nach einer kritischen Analyse des Generalinspekteurs der CIA im Mai 2004 wurde diese rechtswidrige Strategie der „Terrorbekämpfung“ in den nächsten Jahren Schritt für Schritt zurückgefahren. Statt aufwändiger Entführungen und Verhöre gingen CIA und zunehmend auch das Pentagon dazu über, Terrorverdächtige durch ein umfassendes Tötungsprogramm direkt zu eliminieren.

Die damit verbunden strukturellen und operationellen Veränderungen führen zur Herausbildung eines militärisch-geheimdienstlichen Komplexes mit qualitativ völlig neuen Dimensionen.

V. i. S. d. P. – Arbeitskreis Frieden der GBM, Helga Hörning