Ausgabe 3 - Juni 2016

14. Jahrgang, Nr. 78

Informationsstelle Militarisierung e.V.

AUSDRUCK

MAGAZIN DER INFORMATIONSSTELLE MILITARISIERUNG E.V.

Einzelpreis 3,50 € - ISSN 1612-7366

Editorial:

Es war schwer zu übersehen, dass dem Thema Cyber war seitens der Bundeswehr vermehrte Aufmerksamkeit geschenkt wird. Schließlich war halb Deutschland mit Werbeplakaten des „Projektes Digitale Kräfte“ vollgepflastert, mit denen IT-Nachwuchswuchs rekrutiert werden sollte. Obwohl NATO und Bundeswehr die defensive Natur ihrer Anstrengungen betonen, arbeitet der diesmalige Schwerpunkt heraus, dass es in mindestens ebenso großem Ausmaß darum geht, sich Angriffskapazitäten zu verschaffen. Außerdem gehen wir darauf ein, dass die aktuellen Versuche, den Cyberraum zu militarisieren, auch vor weiteren Bereichen wie etwa der Kryptologie nicht Halt machen. Neben dem Cyberschwerpunkt widmen wir uns in dieser Ausgabe auch ausführlich den NATO-Kompetenzzentren, die eine unterschätzte Rolle bei der „Fortentwicklung“ der Allianz für künftige Kriege spielen. Eine Langfassung der Studie, in der zwei weitere dieser Zentren untersucht werden, kann im Übrigen von der IMI-Internetseite heruntergeladen werden. Weitere Artikel beschäftigen sich mit der Weitergabe von Handydaten zum Drohnenkrieg, dem Jugendoffiziersbericht, den Auseinandersetzungen um die Bundeswehrkooperation mit der Hochschule Bremen, mit anti-russischer Propaganda und mit deutschen Rüstungsexporten. Schließlich findet sich in dieser Ausgabe noch ein Beitrag zum Krieg in Mali, in den auch die Bundeswehr verwickelt ist.

Die Redaktion

Impressum

Der **AUSDRUCK** wird herausgegeben von der Informationsstelle Militarisierung (IMI) e.V. Tübingen.

Redaktion: Das Aktiventreffen der Informationsstelle Militarisierung, Jürgen Wagner, Christoph Marischka, Andreas Seifert, Thomas Mickan, Jacqueline Andres, Thomas Gruber.

Erscheinungsweise: Der **AUSDRUCK** erscheint zweimonatlich jeweils zu Beginn des Monats.

Druck: Campus Druck, Hechinger Str. 203 (Sudhaus), 72072 Tübingen.

Bezugsbedingungen: IMI-Mitglieder und Mitglieder des IMI-Fördervereins erhalten den **AUSDRUCK** kostenlos (ab einem Beitrag von 5 €/Monat). Einzelpreis 3,50 €. Im Jahresabo (6 Hefte): 25 € bzw. Förderabo 37 €.

Bezugsadresse: Informationsstelle Militarisierung e.V., Hechinger Str. 203, 72072 Tübingen.

Hinweise zu einzelnen Texten: Δ Christian Stache, IT-Fachkräfte, in: junge Welt, 7.4.2016 (erweitert und aktualisiert); Δ Thomas Gruber, Die Militarisierung der kryptologischen Forschung in Deutschland, in: FIfF-Kommunikation 1/2016 (gekürzt und umgestellt); Δ Christopher Schwitanski, Nato-Exzellenzzentren – Planen für den nächsten Krieg, erschienen als: IMI-Studie 6/2016 (gekürzt).

Bildnachweise wie angegeben außer: Titelbild: Cybersoldat, Grafik: IMI; S. 26: Reaper, Grafik: IMI.

Hinweise zu den Autoren dieser Ausgabe: Thomas Gruber arbeitet im IMI-Büro mit. Christoph Marischka, Jürgen Wagner sind IMI-Vorstandsmitglieder. Mirko Petersen und Christian Stache sind IMI-Beiräte. Marius Pletsch und Christopher Schwitanski waren Praktikanten bei der IMI.

Hinweise zu Internetlinks in dieser Ausgabe: Alle enthaltenen Link-Verweise wurden von den jeweiligen Autoren/Autorinen zum Zeitpunkt der Drucklegung geprüft – für eine darüberhinausgehende Aktualität können wir keine Gewähr geben.

Spendeninformation

Die Informationsstelle Militarisierung und der IMI-Förderverein Analyse und Frieden sind eingetragene und als gemeinnützig anerkannte Vereine. Die Arbeit der Informationsstelle trägt sich durch Spenden und Mitgliedsbeiträge. Wenn Sie Interesse an der Arbeit der Informationsstelle oder Fragen zum Verein haben, nehmen Sie bitte Kontakt zu uns auf. Nähere Informationen, wie auch Sie IMI stützen können, erfahren Sie auf unserer Homepage (www.imi-online.de), per Brief, Mail oder Telefon in unserem Büro in Tübingen.

Spenden an IMI sind steuerabzugsfähig.

Unsere Spendenkontonummer bei der
Kreissparkasse Tübingen
IBAN: DE64 6415 0020 0001 6628 32
BIC: SOLADES1TUB.
Konto des IMI-Förderverein:
IBAN: DE54 6415 0020 0001 7669 96
BIC: SOLADES1TUB.

Kontakt: Informationsstelle Militarisierung (IMI) e.V.
Hechinger Str. 203 (Sudhaus)
72072 Tübingen
Telefon: 07071/49154
Fax: 07071/49159
e-mail: imi@imi-online.de
web: www.imi-online.de

Informationsstelle Militarisierung e.V.

Informationsstelle Militarisierung (IMI) e.V. - Hechinger Str. 203 - 72072 Tübingen

Die Militarisierung der kryptologischen Forschung in Deutschland

von Thomas Gruber

Die ganze Mathematik ist in drei Teile geteilt: die Kryptographie (bezahlt von der CIA, dem KGB und Ähnlichen), die Hydrodynamik (unterstützt von den Hersteller_innen von Atom-U-Booten) und die Himmelsmechanik (finanziert vom Militär und anderen Institutionen, die sich mit Raketengeschossen auseinandersetzen, wie die NASA).[1]

Vladimir Arnold

Für jede Form des Umgangs mit sensiblen Daten gilt eine zentrale Prämisse: Was nicht mitgehört und mitgelesen werden soll, wird verschlüsselt. Daher sind Techniken der Verschlüsselung auch in zahlreichen Bereichen des alltäglichen Lebens zu finden – in der privaten Kommunikation, bei bargeldlosen Geldtransfers, bei der Speicherung von personenbezogenen Daten (wie beispielsweise Patientenakten) und vielem mehr. Kaum verwunderlich also, dass sich das auch in der Forschung zu Verschlüsselungstechniken widerspiegelt: Die Kryptologie ist derzeit eines der am intensivsten behandelten Teilgebiete der angewandten Mathematik. Ebenso offensichtlich wie der individuelle und zivile Nutzen sicherer Verschlüsselung ist allerdings auch das staatliche, wirtschaftspolitische und militärische Interesse an der Kryptologie. Die Forschung an neuen Verschlüsselungstechniken wird dabei gepaart mit Angriffen auf bereits etablierte Systeme, was zur Abschirmung eigener kritischer Daten und der simultanen Abhörung des gewählten Feindes oder Gegners befähigt. Bei einem Blick auf die Arbeit deutscher Forschungseinrichtungen stellt sich die Frage, inwiefern sich ein militärischer Einfluss auf die Kryptologie auch in der hiesigen zivilen Forschungslandschaft abbildet und welche Konsequenzen sich daraus ergeben.

Militarisierungstendenzen innerhalb der kryptologischen Forschungslandschaft lassen sich oft nur schwer auf einzelne Staaten beschränken. Das liegt zum einen an den selbstverständlichen internationalen Kooperationsbestrebungen von Forscher_innen, zum anderen am transnationalen Agieren von Geheimdiensten, staatlichen Institutionen und Konzernen. Auch ist es oft nicht mehr möglich, militärische Interessen von staatlichen oder wirtschaftlichen zu trennen –zu nah liegen die (geo)politischen Ziele der jeweiligen Akteur_innen meist beisammen. Staatlich legitimierte (und oft mit der Wahrung von Menschenrechten begründete) Kriege dienen häufig wirtschaftlichen Interessen wie der Absatzmarkterschließung.[2] Einige Akteur_innen sind in der militärrelevanten Kryptologie an deutschen Forschungseinrichtungen besonders präsent: Die Bundeswehr und das Bundesministerium für Verteidigung (die sich meist auf direkte Drittmittelkooperationen mit Forscher_innen konzentrieren) sowie Institutionen und Behörden der USA (die sich eine subtilere Beeinflussung der kryptologischen Forschungslandschaft über Fachtagungen und Geheimdienstarbeit zu Eigen gemacht haben).

Nach einer kurzen begrifflichen und historischen Einordnung der Kryptologie soll hierzu anhand einiger exemplarischer Projekte die Militarisierung der kryptologischen Forschungslandschaft veranschaulicht werden. Es wird in jeweils zwei Beispielen auf die Verbindung der kryptologischen Forschung mit den US-amerikanischen Akteur_innen und den deutschen Institutionen eingegangen. Das Spektrum der militärrelevanten Kryptologie ist sehr breit gefächert. Die im Folgenden behandelten Beispiele können also nur einen Bruchteil der Militarisierung dieses Fachbereichs darstellen – sie sollen einen für die Kryptologie möglichst fachtypischen Einblick bieten. Dabei liegt der Fokus auf einer Darstellung nachvollziehbarer Forschungsprojekte, die gleichzeitig die wichtigsten Formen der Verquickung militärischer Interessen und der institutionellen Forschung zur Kryptologie in Deutschland verdeutlichen.

Begriffliche und historische Einordnung der Kryptologie

Fachlich teilt sich die Kryptologie in die *Kryptographie*, die Forschung zu möglichst sicheren Systemen der Verschlüsselung und die *Kryptoanalyse*, die Suche nach Erfolg versprechenden Angriffsschemata und Schwachstellen etablierter Kryptosysteme.[3] Beide Fachbereiche sind in der Kryptologie allerdings fast untrennbar eng verwoben – mit gutem Grund. Mathematisch lässt sich die Sicherheit eines Kryptosystems nicht beweisen – in endlicher Zeit ist jede Verschlüsselung zu brechen. Mithilfe der Kryptoanalyse kann aber verdeutlicht werden, ob dieser endliche Zeitraum für ein Menschenleben realistisch wäre. Das wissenschaftliche Abwägen und Ausprobieren neuer Angriffstaktiken auf Kryptosysteme sind also auch ständige Legitimationsfaktoren für die Güte der Verschlüsselung.

Der Namens- und Definitionsraum kryptologischer Forschung begründet sich weitgehend auf eine mathematisierte Darstellung von Strukturen und Algorithmen zur Ver- und Entschlüsselung von Nachrichten. Dabei sind die verschiedenen Verfahren in der Kryptologie so zahlreich wie vielfältig: Es existieren *symmetrische* (*Private-Key*) und *asymmetrische* (*Public-Key*) Verschlüsselungstechniken, Methoden zum sicheren Schlüsselaustausch, Identifikationsverfahren und vieles mehr. Auch kryptoanalytische Angriffe auf gesamte Kryptoverfahren oder auf verwundbare Teile der theoretischen Konzepte nehmen eine zentrale Rolle in der kryptologischen Forschung ein.

Schon die Stichworte „Mathematik" und „Krieg" verleiten oft zur Assoziation mit der von der nationalsozialistischen Wehrmacht im Zweiten Weltkrieg genutzten Chiffriermaschine *Enigma* und deren spektakulärer Entschlüsselung durch alliierte Mathematiker_innen in Bletchley Park. Und auch sonst ist die Militärgeschichte durchzogen mit der Entwicklung möglichst sicherer Kryptosysteme und feindlichen Angriffen auf dieselben. Einige nennenswerte Beispiele umfassen: die Skytale, die von den Spartanern 404 v. u. Z. benutzt wurde, um Kriegsbotschaften zu übermitteln;[4] die Caesar-Chiffre, mit der der römische Feldherr seine Kommunikation auf dem Schlachtfeld verschlüsselte;[5] die Nutzung der Vigenère-Chiffre durch die Südstaaten im US-amerikanischen Bürgerkrieg und die erfolgreichen kryptoanalytischen Angriffe der Nordstaaten;[6] die Entschlüsselung des Zimmermann-Telegramms, das zum Kriegseintritt der USA im Ersten Weltkrieg führte;[7] die kryptoanalytischen Angriffe des US-Militärs auf japanische

Militärcodes, die den Kriegsverlauf der 1940er Jahre im Pazifik grundlegend änderten[8] und vieles mehr.

Zu beachten ist dabei vor allem eine Parallele: Die taktisch relevanten Nachrichten, die innerhalb einer Kriegspartei versandt wurden, sollten so sicher als möglich verschlüsselt sein. Erfolgreiche feindliche Angriffe auf die verwendete Verschlüsselung veränderten andererseits nicht selten den Kriegsverlauf erheblich. Mit der zunehmenden Bedeutung der Kryptographie im zivilen Sektor der Kommunikation gerät oft die Tatsache in den Hintergrund, dass die Kryptologie ein Kind des Krieges ist. Denn die kryptologischen Anwendungen reichten in den ersten Jahrhunderten ihrer Entstehung kaum über die Ver- und Entschlüsselung kriegs- oder staatsrelevanter Nachrichten hinaus.

Die Rolle der USA in der kryptologischen Forschungslandschaft

An der Bedeutung der Kryptologie für die Kriegsführung hat sich selbstverständlich auch in modernen Kriegen nichts geändert. Allein die *National Security Agency* (*NSA*) dient in ihrer Geschichte und nach aktuellen Erkenntnissen über ihr Wirken als exemplarische Stellvertreterin für die zentrale Rolle der Kryptologie im militärischen und wirtschaftlichen Wettstreit zwischen Nationalstaaten.[9] Die NSA wurde auf Befehl des US-Präsidenten Harry S. Truman im Jahr 1952 unter Geheimhaltung und ohne Rücksprache mit dem Kongress als Zusammenschluss diverser militärischer Geheimdienste – zunächst zur *Armed Force Security Agency* – gegründet. Zwar blieb die NSA nach wie vor dem US-Verteidigungsministerium unterstellt, doch sollte sie nach Trumans ursprünglicher Intention der gesamten US-Regierung dienen; eine Aufgabe, die nach wie vor die Ziele der Behörde bestimmen. Die NSA akquiriert sensible elektronische Kommunikationsdaten, entschlüsselt diese und wertet sie schließlich unter militär- und wirtschaftspolitischen Gesichtspunkten aus. Geschichtlich hat sich allein die politische Lage, nicht die Zielsetzung der geheimdienstlichen Arbeit gewandelt: Ob im Kalten Krieg, dem selbsternannten Kampf gegen den Terrorismus oder der Spionage in „befreundeten" Staaten – es bleibt das Ziel der NSA, mit kryptologischen Mitteln einer militärischen und wirtschaftlichen Überlegenheit des US-amerikanischen Staates zuzuarbeiten.

Als äußerst vielversprechendes Mittel dient der NSA hierbei die Distribution kompromittierter Kryptostandards, die es dem Geheimdienst ermöglichen, die jeweilige Verschlüsselung zu brechen. Ein prominentes Beispiel der geheimdienstlichen Beteiligung bei der Verbreitung eines unsicheren Kryptosystems ist der Pseudozufallsgenerator *Dual_EC_DRBG*.[10] Im Jahr 2013 wurde via eines von Edward Snowden geleakten Dokuments bekannt, dass eine Sicherheitslücke im Dual_EC_DRBG existiert, die der Sicherheitsfirma RSA von der NSA mit 10 Millionen Dollar bezahlt wurde.[11] Zufallszahlen sind essenzieller Bestandteil vieler Kryptosysteme – so auch beispielsweise dem Diffie-Hellman-Schlüsselaustausch. Ein ausreichendes Zusatzwissen über die im Kryptosystem verwendeten Zufallszahlen würde es Angreifenden ermöglichen, gesamte Verschlüsselungsverfahren offenzulegen.

Aufgrund seiner weitgehend unbekannten Schwachstelle erfuhr der Pseudozufallsgenerator Dual_EC_DRBG weite Verbreitung in der kryptologischen Anwendung und der internationalen akademischen Forschung. Unterstützt wird die Anerkennung solch fehlerhafter Standards vornehmlich durch die Politik der US-Normierungsbehörde *NIST* (kurz für *National Institute of Standards and Technology*). Das NIST gibt Empfehlungen für die Normierung etablierter Kryptosysteme und beherzigt dabei geheimdienstlich und von Unternehmen entwickelte Implementierungen, wie die der NSA und des Sicherheitskonzerns RSA. Die NIST-Standards sind außerdem weitgehend alternativlos, die einzigen Ausnahmen bilden von Forscher_innen entwickelte, quelloffene Implementierungen, die als Antwort auf die Sicherheitslücken entstehen. Der Nutzen weit verteilter fehlerhafter Kryptosysteme für die moderne Kriegsführung ist also noch unmittelbarer als der einer bloßen Zurückhaltung von Informationen: Durch gut getarnte Hintertüren in den jeweiligen Implementierungen, die durch eine Veröffentlichung in NIST-Standards als sichere Verschlüsselungsschemata legitimiert werden, bleiben Abhöraktionen lange Zeit unbekannt. Die NIST-Kurven und -Algorithmen werden auch von feindlichen Akteur_innen genutzt und bieten damit eine willkommene, offene Flanke für kryptoanalytische Angriffe.

Neben der aktiven Sabotage neuer Kryptosysteme bietet sich für militärische und geheimdienstliche Akteur_innen auch der Besuch von internationalen Forschungskonferenzen an, die den derzeitigen Forschungsstand zur Kryptologie zuverlässig abbilden. Gerade bei der Suche nach neuen Kooperationsmöglichkeiten bieten die akademischen Konferenzen einen umfassenden Überblick in die aktuell beforschten Themengebiete. Die Teilnehmenden der meisten Konferenzen sind verschiedenster Nationalitäten. Und so teilen die Forscher_innen, egal welcher Herkunft, ihr Wissen mit den Zuhörer_innen aus Militär und Rüstungsindustrie. Die NSA nimmt aufgrund ihrer langjährigen Präsenz in der kryptologischen Forschungslandschaft eine Günstlingsrolle ein, die es ihren Mitarbeiter_innen ermöglicht, militärrelevante Fragen oft direkt in die zivile Forschung zu portieren.

Im Jahr 2009 wurde beispielsweise der NSA-Mitarbeiter J. F. Dillon vom Programmkomitee der *International Conference on Finite Fields and Their Applications* (z. Dt. *Internationale Konferenz zu endlichen Körpern und deren Anwendungen*) eingeladen, um über seinen Erkenntnisstand zur Existenz von *APN-Polynomen*[12] zu referieren.[13] Der Nutzen dieser Polynome besteht in der Kryptographie vor allem in ihrer Robustheit gegenüber kryptoanalytischen Angriffen (genauer: der Differenziellen Kryptoanalyse).[14] Dillon stellte in seinem Vortrag die Akquise neuer Erkenntnisse mit einer abschließenden Frage an die Forschungsgemeinde über die Existenz von APN-Polynomen vor.[15]

Die Sicherheit von Kryptosystemen gegenüber der Differenziellen Kryptoanalyse spielt für die NSA-Forscher_innen seit der Implementierung des *Data Encryption Standard* (*DES*) eine zentrale Rolle. Schon im Jahr 1974 legte die NSA dem Unternehmen IBM nahe, den diesbezüglichen Entwicklungsstand unveröffentlicht zu lassen, was erst im Jahr 1994 bekannt wurde.[16] Die Nutzung des exklusiven Wissens über die Angreifbarkeit und Sicherheit von Kryptosystemen für die Kriegsführung ist leicht nachvollziehbar: Während die NSA selbst sichere Kryptostandards verwendet, können die neu entdeckten Angriffsschemata für eine Kryptoanalyse der feindlichen militärischen Kommunikation genutzt werden. Bis heute hat sich an dieser Praxis nur wenig geändert – zu groß ist scheinbar der kalkulierte Nutzen von Hintertüren in aktuellen Verschlüsselungsschemata für den Geheimdienst.

Auftragsforschung des deutschen Militärs

Für eine geheime Kommunikation zwischen zwei Personen mittels eines symmetrischen Kryptosystems gilt es, sich

Informationsstelle Militarisierung (IMI) e.V. - Hechinger Str. 203 - 72072 Tübingen

Informationsstelle Militarisierung (IMI) e.V. - Hechinger Str. 203 - 72072 Tübingen

US-Cybersoldat_innen im Einsatz. Quelle: US Airforce

zunächst auf einen gemeinsamen Schlüssel zu einigen, mit dem die Nachrichten chiffriert werden können. Da aber Nachrichtenkanäle oft abhörbar sind, muss eine sichere Methode zum Schlüsselaustausch über jene Kommunikationswege gefunden werden. Der *Diffie-Hellman-Schlüsselaustausch* beispielsweise nutzt die diskrete Exponentialfunktion als sogenannte *Einwegfunktion*, also eine Funktion, deren Umkehrfunktion – der diskrete Logarithmus – nur unter enormem Rechenaufwand zu lösen ist.

An dieser Stelle knüpft die Fragestellung des Bundesministeriums der Verteidigung an, von dem die Universität Leipzig 2013 mit einer Studie zu den „Möglichkeiten und Grenzen der Berechnung des diskreten Logarithmus" beauftragt wurde.[17] Das militärische Interesse an der Berechenbarkeit einer Funktion, mit der die Sicherheit ganzer Kryptosysteme steht und fällt, ist denkbar vielseitig begründet: Einerseits bietet sie Ansatzpunkte für kryptologische Angriffe auf feindliche Kommunikationsstrukturen in deutschen Kriegseinsätzen oder auf andere selbstgewählte Ziele außerhalb kriegerischer Handlungen wie Privatpersonen, Staaten oder Unternehmen. Andererseits gibt eine solche Analyse Aufschluss über die derzeitige und zukünftige Sicherheit der eigenen Kryptosysteme, mit denen die Kommunikation in ebendiesen Konflikten verschlüsselt wird. Die Auslagerung einer solchen Studie in ein universitäres Forschungsprojekt scheint sinnvoll: Das Thema des diskreten Logarithmus entstammt direkt der theoretischen algebraischen Forschung. Im Falle der Leipziger Studie ist aufgrund fehlender Veröffentlichungen und der ausbleibenden Bewerbung der so prestigeträchtigen Drittmittelforschung von einer Verschwiegenheitsklausel für die beteiligten Forscher_innen auszugehen. Der Forschungsstand zu diskreten Logarithmen ist allerdings ein rege untersuchtes Gebiet der algebraischen Forschung und daher problemlos exemplarisch abzubilden.

Im mathematischen Sinne stellt die diskrete Exponentialfunktion mit einer gut gewählten strukturellen Basis eine äußerst vielversprechende Einwegfunktion dar – ein diskreter Logarithmus kann zunächst nicht in realistischer Zeit rechnerisch bestimmt werden. Die Angreifbarkeit einer Verschlüsselung hängt allerdings nicht allein von einer Berechenbarkeit des diskreten Logarithmus ab, sondern auch von möglichen Schwachstellen der zugrunde liegenden mathematischen Strukturen und der jeweiligen Umsetzung des Verschlüsselungsalgorithmus. Im Oktober 2015 stellten einige Kryptolog_innen auf der *Conference on Computer and Communications Security* (z. Dt. *Konferenz zur Computer- und Kommunikationssicherheit*) einen Angriff auf eine weit verbreitete Implementierung des Diffie-Hellman-Schlüsselaustauschs (namens *DHE_EXPORT*) vor – die *Logjam-Attacke*. Diese kryptoanalytische Attacke basiert auf einer massiven Vorberechnung von Werten gewisser diskreter Logarithmen und benötigt daher eine enorme Rechenleistung der verwendeten Infrastruktur.[18] Allerdings stehen gerade großen Unternehmen sowie staatlichen und militärischen Akteur_innen jene Hochleistungsrechner meist auch zur Verfügung. Die Analyse geleakter NSA-Dokumente legt nahe, dass der amerikanische Geheimdienst den Logjam-Angriff bereits durchführen kann, was bedeuten würde, dass ein erheblicher Teil einiger im Internet genutzter Verschlüsselungssysteme angreifbar wäre (genauer 66 % aller IPsec-VPNs und 26 % der SSH-Server).[19]

Einige der neuesten Angriffsschemata auf die diskrete Exponentialfunktion befassen sich mit der vergleichsweise jungen *Elliptic Curve Cryptography* (kurz *ECC*).[20] Gravierende Fehler in der Implementierung der ECC-Kryptosysteme wären zwar vermeidbar, sind allerdings keinesfalls immer offensichtlich – oft werden unsichere Algorithmen erst in diesbezüglichen mathematischen oder informatischen Forschungsprojekten aufgedeckt. Ein Beispiel für die Ausnutzung einer unzureichenden Implementierung sind sogenannte *Seitenkanalattakken*: Ein_e Angreifer_in kann bei einem ECC-System häufig schon über die Rechenzeit der Exponentialfunktion Informationen über den verwendeten Schlüssel gewinnen.[21]

Außerhalb des engeren universitären Kontexts finden sich Interessent_innen für kriegsrelevante Forschung auch an externen Forschungseinrichtungen. Institute zur Förderung angewandter Forschung – wie beispielsweise die Fraunhofer-,

Leibnitz- oder Max-Planck-Institute – verstehen sich meist auch als Dienstleister_innen für Staat, Militär, Industrie und Wirtschaft, in deren Kreisen sie Forschungsergebnisse als Produkte vermarkten und vertreiben. Allerdings überschneidet sich nicht selten die personelle Besetzung eines Instituts stark mit nahegelegenen Hochschulen – viele Projekte reichen daher in die staatlich wohlfinanzierte Bildungseinrichtung und die Forschungsinhalte werden von den Lehrstuhlinhaber_innen zur Weiterbearbeitung an den Mittelbau und die Studierenden herangetragen. So wird auch eine unproblematisierte Form der Rüstungsforschung an deutschen Forschungseinrichtungen möglich, die Mitglieder der Hochschulen mit einbezieht und einen Verweis auf den außeruniversitären Charakter der Projekte bei kritischen Nachfragen über kriegsrelevante Forschung zulässt.

Kryptologisch relevant ist in diesem Sinne beispielsweise die Zusammenarbeit zwischen der Arbeitsgruppe *Cyber Analysis and Defense* des *Fraunhofer-Instituts für Kommunikation, Informationsverarbeitung und Ergonomie* (*FKIE*) mit Sitz in Wachtberg-Werthhoven und den Hochschulen in Bonn.[22] Große Teile der Angestellten des FKIE und dessen Institutsleitung finden sich in der Personalstruktur des Instituts *Informatik 4* der Universität Bonn wieder und auch inhaltlich entsprechen sich einige Forschungsbereiche der beiden Einrichtungen.[23] Kriegsrelevante Forschungsergebnisse werden über das FKIE beworben, wie beispielsweise regelmäßig auf der stark militärisch geprägten Fachausstellung des *Anwenderforum für Fernmeldetechnik, Computer, Elektronik und Automatisierung* (*AFCEA*) – im Jahr 2015 unter dem Motto „IT ‚organisiert' – Bundeswehr und Behörden in der digitalen Welt".[24] Eines der laufenden kryptologisch orientierten Projekte am FKIE ist die Entwicklung eines Systems für den „sicheren Informationsaustausch zwischen militärischen Einheiten" in der „vernetzten Operationsführung" namens *IDP / MIKE*.[25] Die Zusammenarbeit zwischen dem FKIE und den Bonner Hochschulen wird hierbei nicht öffentlich benannt, sie findet sich aber thematisch in mehreren studentischen Abschlussarbeiten wieder.[26]

Das Ziel des IDP / MIKE-Systems ist es, ein *Virtual Private Network* (*VPN*) zu implementieren, das in militärischen Einsatzszenarien eine fehlerresistente und dynamische private Kommunikation innerhalb einer Kriegspartei ermöglicht. Ursprünglich ist ein VPN – wie schon der Name sagt – ein privates Netzwerk für ausgewählte Kommunikationspartner_innen, die sich in einem offenen oder unsicheren Netzwerk (z. B. im Internet oder einem öffentlichen lokalen Netzwerk) befinden. Innerhalb des VPN kann schnell und zuverlässig kommuniziert werden, nach außen wird die Kommunikation verschlüsselt. Herkömmliche VPNs fußen meist auf der Annahme eines während der Kommunikation feststehenden Rechners ohne plötzliche Verbindungsabbrüche und der Eigeninitiative der einzelnen Nutzer_innen beim Kommunikationsaufbau. Beide Voraussetzungen sind in Kriegsszenarien nicht immer erfüllbar, der taktische Mehrwert eines VPNs zwischen den militärischen Einheiten wäre allerdings unbestreitbar. Daher stehen bei der Entwicklung der IDP-MIKE-Software drei „wünschenswerte" Eigenschaften im Mittelpunkt:

– Das VPN soll von fachfremden Nutzer_innen (z. B. Soldat_innen)
– „unter schwierigen Einsatzbedingungen" (z. B. Krieg)
– möglichst wartungsfrei verwendbar sein.[27]

Für die Softwarelösung bedeutet das konkret, dass netzwerkfähige Geräte innerhalb einer Kriegspartei sich selbstständig erkennen, miteinander verbinden und bei einem Netzwerkausfall erneut die Kommunikation aufbauen können – insgesamt also eine mobile, dynamische VPN-Lösung. Tests zur Praktikabilität des IDP-MIKE-Systems wurden auf dem Kommunikationsserver *QUAKSBw* (*Querschnittlicher Anteil Kommunikationsserver Bundeswehr*) durchgeführt, der ein Bindeglied zwischen sprach- und datenbasierter Kommunikation sowie den Fernmeldemitteln der Bundeswehr darstellt.[28] Schließlich wurde IDP / MIKE auch auf der Rüstungsmesse der AFCEA vorgestellt und als militärische Kommunikationslösung beworben. Der Weg kryptologischer Methoden und Forschungsansätze von einem externen Institut über die universitäre Forschungslandschaft in die deutsche Kriegsplanung ist im Fall des VPNs am FKIE daher einwandfrei nachvollziehbar und unmissverständlich kommuniziert.

Gesellschaftliche Folgen einer militarisierten Forschungslandschaft

Ob historisch oder in der aktuellen Forschung – die Kryptologie ist eine wichtige Informationsquelle staatlicher und militärischer Interessenträger_innen bezüglich der Kommunikationssicherheit und der Datenakquise. Ein parasitär anmutender Informationsfluss von Seiten der Geheimdienste und die willentliche oder zumindest in Kauf genommene Sabotage universitärer Kryptologie für Geldmittel und infrastrukturelle oder personale Verbesserungen prägen dabei die Form der Militarisierung der Kryptologie.

Diese höchst bedenklichen Militarisierungstendenzen stehen allerdings jedweder wissenschaftlichen Intention einerseits und der Idee der gesamten Kryptologie andererseits krass entgegen. Wissenschaftliche Arbeit lebt von Transparenz und einer öffentlichen Diskussion von Forschungsergebnissen. Sollte außerdem die absichtliche Verbreitung fehlerhafter Kryptosysteme weiter um sich greifen, muss die Legitimation der gesamten institutionalisierten Forschung eines Bereiches, der sich mit einer sicheren und vertraulichen Kommunikation befasst, infrage gestellt werden. Als einzige Alternative verbleiben dann private Forscher_innenkollektive, die verlässliche und transparente Verschlüsselungsschemata erarbeiten. Jene Open-Source-Projekte werden dann parallel zu einem wohlfinanzierten, öffentlichen Forschungssektor entwickelt, der eigentlich genau dieser gesellschaftlichen Aufgabe dienen sollte, sich allerdings zunehmend zu einem Dienstleister für Wirtschaft, Industrie und Militär entwickelt.

Sowohl gesamtgesellschaftlich als auch wissenschaftlich wäre also ein grundlegendes Interesse begründet, sich der Militarisierung der kryptologischen Forschung zu widersetzen. Dieser Position entgegen stehen die Geldgeber_innen für militärrelevante Forschung, der Zwang zur Drittmittelakquise innerhalb der Hochschulforschung und die einzelnen Universitätsleitungen – all das im Sinne der staatlichen Bemühungen um eine immer weiter reichende Liberalisierung des Bildungs- und Forschungssektors. Zivil- und Transparenzklauseln – also die Selbstverpflichtung einer Institution, nur für friedliche Zwecke zu forschen und die aktuellen Drittmittelkooperationen zu veröffentlichen – in den Grundordnungen einzelner deutscher Universitäten stellen eine erste politisch erkämpfte Antwort auf die Militarisierung der Forschung dar. Gerade im Bereich der Kryptologie als stark transnational agierende Wissenschaft mit einem gewissen US-Zentrismus kann aber eine Zivilklausel oft nur Drittmittelprojekte an den jeweiligen Institutionen verhindern. Diese Einschränkung betrifft also nur einen kleinen Teil der militärrelevanten Forschung

Informationsstelle Militarisierung (IMI) e.V. - Hechinger Str. 203 - 72072 Tübingen

zur Kryptologie. Jede weitere Form des Widerstands bedarf daher einer kritischen Öffentlichkeit, sowohl einer zivilgesellschaftlichen – ausgedrückt im politischen Kampf – als auch einer wissenschaftlichen. Die Frage nach der Verantwortung richtet sich außerdem nicht nur an die politische Öffentlichkeit, sondern auch an die direkt involvierten Forscher_innen, die als Fachkundige am besten Forschungskooperationen auf den gesellschaftlichen Nutzen und die Verträglichkeit mit den Grundwerten der Wissenschaft prüfen können. Fern von monetären Interessen gälte es innerhalb der Forschungsgemeinschaft das Vertrauen gegenüber Akteur_innen aus dem Militär-, dem Staats- und dem Wirtschaftssektor in Frage zu stellen.

Anmerkungen

1 Übersetzung des Autors aus dem Englischen.

2 Das bestätigten auf Seiten der deutschen Politik auch der ehemalige Bundespräsident Horst Köhler und der ehemalige Verteidigungsminister Guttenberg. Köhler: Krieg für freien Handel, http://www.sueddeutsche.de/politik/bundeswehreinsaetze-koehler-wirtschaftsinteressen-militaerisch-durchsetzen-1.950594, 02.03.2016; Guttenberg auf Köhlers Spuren, http://www.taz.de/!5132558/, 02.03.2016.

3 Die Möglichkeiten zur Wahl eines Verschlüsselungsverfahrens und des Austausches eines Schlüssels sind so unterschiedlich wie zahlreich – im Verlauf des Artikels werden entsprechende Grundlagen umrissen.

4 Jordan, Craig: *Secret History: The Story of Cryptology*. Chapman & Hall/CRC, 2013. S. 4-5

5 ebd., S. 11-12

6 Kahn, David: *The Codebreakers: The Story of Secret Writing*. Simon & Schuster, 1996. S. 217-218

7 Jordan, Craig: *Secret History: The Story of Cryptology*. S. 185-187

8 ebd., S. 293-311

9 ebd., S. 342-367; United States SIGINT System, January 2007 Strategic Mission List, http://cryptome.org/2013/11/nsa-sigint-strategic-mission-2007.pdf, 29.02.2016.

10 Exclusive: Secret contract tied NSA and security industry pioneer, http://www.reuters.com/article/us-usa-security-rsa-idUSBRE9BJ1C220131221, 29.02.2016.

11 Hintertüren und Schwächen im kryptographischen Standard SP 800-90A, https://www.mathematik.de/ger/presse/ausdenmitteilungen/artikel/dmvm-2014-0012.pdf, 29.02.2016.

12 Almost Perfect Nonlinear Polynomial

13 Abstracts of the 9th International Conference on Finite Fields and their Applications, http://claudeshannoninstitute.ucd.ie/fq9/AllFq9Abstracts.pdf, 29.02.2016.

14 Wikipedia: substitution box, https://de.wikipedia.org/wiki/S-Box, 02.03.2016; Highly resistant Boolean functions for cryptography, http://iml.univ-mrs.fr/~ritzenth/AGCT/talks/rodier.pdf, 02.03.2016.

15 APN Polynomials: An Update, http://mathsci.ucd.ie/~gmg/Fq9Talks/Dillon.pdf, 02.03.2016.

16 Coppersmith, Don: *The Data Encryption Standard (DES) and its strength against attacks*. IBM Journal of Research and Development, 1994, 38. S. 243-250

17 Kleine Anfrage: Militärische und sicherheitstechnische Forschung in Sachsen seit 2009, http://edas.landtag.sachsen.de/viewer.aspx?dok_nr=12635&dok_art=Drs&leg_per=5&pos_dok=-1, 01.03.2016. S. 6

18 Adrian, David ; Bhargavan, Karthikeyan ; Durumeric, Zakir ; Gaudry, Pierrick ; Green, Matthew ; Halderman, J. Alex ; Heninger, Nadia ; Springall, Drew ; Thomé, Emmanuel ; Valenta, Luke ; VanderSloot, Benjamin ; Wustrow, Eric ; Zanella-Béguelin, Santiago ; Zimmermann, Paul: *Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice*. 22nd ACM Conference on Computer and Communications Security, 2015

19 Wobei bei der Nutzung von elliptischen Kurven ebenso auf eine fehlerfreie Implementierung zu achten ist, wie die oben stehenden Ergebnisse zeigen.

Logo zur Cyberpeace-Kampagne. Quelle: FIfF

20 Stinson, Douglas R.: *Cryptography: Theory and Practice, Third Edition*. Chapman & Hall/CRC, 2006. S. 254-267

21 Remote Timing Attacks are Still Practical, http://eprint.iacr.org/2011/232.pdf, 02.03.2016.

22 Beide Bonner Hochschulen besitzen eine seit 2015 in der jeweiligen Grundordnung verankerte Zivilklausel.

23 Fraunhofer FKIE: Institutsleitung, http://www.fkie.fraunhofer.de/de/ueber-uns/institutsleitung.html, 02.03.2016; Fraunhofer FKIE: Forschungsbereiche, http://www.fkie.fraunhofer.de/de/forschungsbereiche.html, 02.03.2016; Universität Bonn: Institute of Computer Science 4, https://net.cs.uni-bonn.de/start/, 02.03.2016.

24 AFCEA Fachausstellung 2015, https://www.afcea.de/29_fa-131.html, 02.03.2016; FKIE auf der AFCEA Fachausstellung 2015, https://www.afcea.de/1400.html?tx_mhbranchenbuch_pi1[detail]=29&cHash=6f0eb2587cd75b505dff8d2363a26a97, 02.03.2016.

25 IDP / MIKE – Sicherheit zwischen Kommunikationspartnern, http://www.fkie.fraunhofer.de/de/forschungsbereiche/cyber-analysis-and-defense/projekt-idp-mike.html, 02.03.2016.

26 Christof Fox: Konzeption eines SOA-konformen Discovery Mechanismus zur Verbesserung der Fehlertoleranz eines Gruppenschlüsselmanagements, http://www.leischner.inf.fh-bonn-rhein-sieg.de/aa/thesis/08_Fox_MIKE-IDP.htm, 10.2.2016; Shirish Negi: Evaluation and Optimization of the Group Key Management IDP-MIKE over VHF Data Links, https://net.cs.uni-bonn.de/de/nc/aktuelles/newsansicht/708/e8d00ec903a483e2f6d361bfa9b8438e/, 02.03.2016; Anastasia Danilova: Bewertung des IDP-MIKE-Systems in Bezug auf Replay- und DoS- Angriffe, http://net.cs.uni-bonn.de/nc/news/singleview/584/2ccfc86b9375cec3546458bceb644c07/, 02.03.2016.

27 http://www.fkie.fraunhofer.de/de/forschungsbereiche/cyber-analysis-and-defense/projekt-idp-mike.html, 02.03.2016.

28 http://www.leischner.inf.fh-bonn-rhein-sieg.de/aa/thesis/08_Fox_MIKE-IDP.htm, 10.2.2016; Oberst Warnicke: Das Kommunikationssystem der Bundeswehr für den Einsatz (KommSysBwEins), https://www.afcea.de/fileadmin/downloads/Fachausstellung/23._Fachausstellung_2009/Anmeldung/2 - 20101214_KommSysBw Eins - Vortrag AFCEA_SKUKdo - mit.pdf, 02.03.2016.

Nerd-Offensive

Der Cyberspace als militärischer Operationsraum

von Jürgen Wagner

Logo des Kommando Strategische Aufklärung der Bundeswehr. Quelle: Wikipedia

Um der gewachsenen Bedeutung des Bereiches Rechnung zu tragen, veröffentlichte die Bundeswehr am 26. April 2016 den „Abschlussbericht des Aufbaustabs Cyber- und Informationsraum“, mit dem der Bereich weiter militärisch „erschlossen“ wird. Dabei geht es ganz und gar nicht allein um „Verteidigung“, wie offiziell suggeriert wird. Schon länger hat die Bundeswehr damit begonnen, sich auch Offensivkapazitäten zuzulegen.

Militärischer Operationsraum

Im „Abschlussbericht des Aufbaustabs Cyber- und Informationsraum“ wird der Bereich als fünfte Bundeswehr-Streitkräftekategorie etabliert: „Der dargestellte strategische Kontext zeigt die militärische Relevanz des CIR [Cyber- und Informationsraum] als eigene Dimension neben Land, Luft, See und Weltraum auf. Dieser ist umfassend Rechnung zu tragen.“ Bis Oktober 2016 soll hierfür in einer Grundbefähigung im Verteidigungsministerium eine eigene Abteilung „Cyber/IT“ (CIT) geschaffen und ein militärischer Organisationsbereich für den Cyber- und Informationsraum bis spätestens April 2017 aufgestellt werden, dem ein eigener Inspektor vorstehen soll. Der CIT werden dann fast 14.000 bislang über verschiedene Abteilungen verstreute Dienstposten angehören. Im Abschlussbericht des Aufbaustabs Cyber- und Informationsraum heißt es dazu: „Mit dem Aufbau des militärischen Organisationsbereiches CIR soll der Cyber- und Informationsraum als Operationsraum bzw. militärische Dimension angemessen abgebildet werden. […] Dazu wandern in einem ersten Schritt ca. 13.700 Dienstposten mit ihren Aufgaben zum Organisationsbereich CIR. Darüber hinaus werden ca. 300 Dienstposten für die Führungsfähigkeit des KdoCIR, die Aufstellung eines Zentrum Cyber-Sicherheit der Bundeswehr und die Stärkung der Aufgabe Computer Netzwerk Operationen herangezogen.“

Offensivkapazitäten & Rekrutierung

Schon 2009 meldete der Spiegel (7.2.) die Bundeswehr sei dabei, eine „Abteilung Informations- und Computernetzwerkoperationen“ genannte Hackertruppe mit 76 Soldaten für Cyberangriffe aufzustellen: „Die Bundeswehr wappnet sich mit einer bislang nicht bekannten Einheit für künftige Internet-Konflikte. […] Die Soldaten, die sich vor allem aus den Fachbereichen für Informatik an den Bundeswehruniversitäten rekrutieren, beschäftigen sich dabei auch mit den neuesten Methoden, in fremde Netzwerke einzudringen, sie auszukundschaften, sie zu manipulieren oder zu zerstören – digitale Angriffe auf fremde Server und Netze inklusive.“

Mittlerweile sind die diesbezüglichen Bemühungen noch deutlich weiter fortgeschritten. Bei dem nun veröffentlichten Abschlussbericht Cyber- und Informationsraum handelt es sich nach Eigenangaben um „ergänzende Maßnahmen zur Umsetzung der Strategischen Leitlinie Cyber-Verteidigung“. Dieses geheime Dokument vom 16. April 2015, das u.a. von Netzpolitik.org (30.7.2015) eingehend analysiert wurde, veranschaulicht, dass es bei all diesen Bemühungen tatsächlich auch darum geht, sich Offensivkapazitäten zu verschaffen. Explizit heißt es in der Leitlinie Cyber-„Verteidigung“: „Offensive Cyber-Fähigkeiten der Bundeswehr sind als unterstützendes, komplementäres oder substituierendes Wirkmittel anzusehen. Sie haben zum Einen das Potenzial, in der Regel nicht-letal und mit hoher Präzision auf gegnerische Ziele zu wirken, zum Anderen kann diese Wirkung im Gegensatz zu kinetischen Wirkmitteln unter Umständen sogar reversibel sein. Offensive Cyber-Fähigkeiten der Bundeswehr haben grundsätzlich das Potenzial, das Wirkspektrum der Bundeswehr in multinationalen Einsätzen signifikant zu erweitern.“

Zu diesem Zweck will die Bundeswehr nun verstärkt IT-Fachkräfte rekrutieren; gesucht seien aktuell „eher Nerds als Sportskanonen“, fasst es tagesschau.de (26.4.2016) zusammen. Hierfür startete die Bundeswehr im Rahmen des „Projekts Digitale Kräfte“ eine massive Rekrutierungskampagne (siehe auch IMI-Standpunkt 2016/16b), deren Details die Bundeswehr zeitgleich mit der Vorstellung des neuen Cyberkonzeptes auf einer Folie veranschaulichte: „rund 60 Kampagnentage“; „Mitte März Plakate-Kampagnenauftakt im CeBIT-Umfeld“; „3 verschiedene Sprüchemotive (unter dem Aspekt ‚Sinnstiftung‘)“; „ 5 IT-Berufswelt-Botschafter/Botschafterinnen (unter dem Aspekt ‚Qualifizierung‘)“; „Anzeigen in 25 Printtiteln“; „knapp 18.000 Plakat-Flächen“; „45 Online-Banner“; „YouTube- und Facebook-Einsatz über die gesamte Kampagnenlaufzeit“; „Kosten 3,6 Mio. Euro“.

„Cyber-Gedöns“

Logo des Chaos Computer Club. Quelle: Wikipedia

Die Bundeswehr rüstet sich ganz offensichtlich für den Kampf um den Cyber- und Informationsraum. Scharf geht deshalb u.a. Frank Rieger vom Chaos Computer Club auf „Internationale Politik und Gesellschaft“ (2.5.2016) mit den Plänen des Verteidigungsministeriums ins Gericht: „Der Versuch, das Feld zu militarisieren und zu ‚vergeheimdienstlichen‘ geht am Kern des Problems vorbei: schlechte Software, mangelnde Ausbildung und fehlende Haftungsregeln für Unternehmen. Zu glauben, man könne hier mit militärischen Mitteln irgendetwas anderes als eine Eskalation bewirken, ist naiv. Die Lage fasste ein Bundeswehr-General mir gegenüber auf einer Veranstaltung treffend zusammen: ‚Solange ich über das Bundeswehr-Logistiksystem nicht einmal zuverlässig Toilettenpapier bestellen kann, brauche ich auch kein Cyber-Gedöns.‘“

Informationsstelle Militarisierung (IMI) e.V. - Hechinger Str. 203 - 72072 Tübingen

Informationsstelle Militarisierung (IMI) e.V. - Hechinger Str. 203 - 72072 Tübingen

Zu den Waffen, Nerds!

Bundeswehr rekrutiert IT-Fachkräfte für Krieg im Cyberspace

von Christian Stache

Derzeit zieren 18.000 Plakate des neuen Bundeswehr-Rekrutierungsfeldzugs „Projekt Digitale Kräfte“ nahezu unübersehbar die Werbeflächen in deutschen Städten. Von Mitte März bis Mitte Mai versucht das Bundesverteidigungsministerium nach Eigenangaben, „Talente und digitale Fachkräfte für den Bereich Informationstechnologie (IT)“ anzuheuern. Dazu lässt es „Anzeigen in 25 Printtiteln“ und Reklame auf „45 Online-Seiten mit Tagesfest- und Rotationsplatzierungen“ schalten. Zahlreiche Promotion-Videos und -Lebensläufe aktiver Soldaten und Soldatinnen im zivilen und militärischen Dienst, vom einfachen IT-Lanzer bis zur karriereorientierten Juniorprofessorin für Mensch-Maschine-Interaktion, schmücken die Internetseite der Kampagne. Selbstverständlich bespielt der Presse- und Informationsstab des Verteidigungsministeriums auch das gesamte Ensemble der „sozialen“ Netzwerke und Medien. Die Gesamtkosten liegen laut Angaben der Bundeswehr bei „rund 3,6 Millionen Euro“ aus dem Jahresgesamtetat 2016 für „Nachwuchswerbung“ von 35,3 Millionen Euro.

Die drei Kampagnenslogans sind provokativ. Mit der Losung „Gegen virtuellen Terror hilft kein Dislike-Button“ wird die Notwendigkeit militärischen Handelns im Internet und anderen virtuellen Netzwerken nahegelegt. Ähnliches gilt für die Suggestivfrage „Wie können wir Kriegstreiber im Netz deinstallieren?“. Die politische Marschrichtung der Werbe- und der Rekrutierungsoffensive gibt die Parole „Deutschlands Freiheit wird auch im Cyberraum verteidigt“ vor.

Das „Projekt Digitale Kräfte“ gründet auf der 12,5 Millionen Euro teuren „Arbeitgeberkampagne“ der Bundeswehr „Mach, was wirklich zählt“ aus dem vergangenen Jahr. Diese sollte laut Bundesverteidigungsministerium nur bis Februar 2016 laufen. Sebastian Wanninger vom Presse- und Informationszentrum Personal der Bundeswehr bestätigte auf Anfrage der Tageszeitung junge Welt (jW), dass es sich um „die zweite Phase der ›Mach, was wirklich zählt‹-Kampagne“ handele. Sie adressiere eine der Problemzonen der Militärs. „Auch für andere Teilbereiche der Bundeswehr“ seien Kampagnen geplant.

Wanninger bestätigte gegenüber der jW ebenfalls, dass das „Projekt Digitale Kräfte“ wie auch schon „Mach, was wirklich zählt“ in Zusammenarbeit mit der Düsseldorfer Werbeagentur Castenow umgesetzt werde. Zu Castenows Kunden zählen neben der Bundeswehr McDonald‘s Deutschland, die Leih- und Zeitarbeitsfirma DIS AG und der Fernsehsender Super RTL.

Lühr Henken, Sprecher des Bundesausschusses Friedensratschlag, kritisierte gegenüber der jW die Nachwuchswerbung dafür, dass mit LKW-Führerscheinen, Abenteurertum, Technikbegeisterung und guten Verdienstmöglichkeiten geworben wird, anstatt die harten Realitäten der Auslands- und Kampfeinsätze zu zeigen. Ralf Buchterkirchen, Bundessprecher der Deutschen Friedensgesellschaft-Vereinigte KriegsdienstgegnerInnen, pflichtete bei: „Die heile Welt der Videos ist nur Fassade.“ Bundeswehr-Vertreter Wanninger räumte ein, es sei im Rahmen einer Kampagne immer schwierig, alle Facetten des militärischen Berufs darzustellen. „Natürlich ist das Plakat erst einmal dazu da, Aufmerksamkeit zu erregen.“

Markus Gross vom Netzwerk Schule ohne Bundeswehr NRW sieht in der forcierten Anwerbung von IT-Arbeitskräften „im Kern eine Angriffsbefähigung der Bundeswehr im Cyberspace.“ Prononciert äußerte sich Sevim Dagdelen, Sprecherin für Internationale Beziehungen der Fraktion DIE LINKE im Bundestag und Mitglied des Auswärtigen Ausschusses: „Die Bundeswehr sucht ‚Laptop-Krieger‘. Die Soldaten von heute kämpften mit Keyboard und Maus. Ohne IT bleiben Killerdrohnen am Boden.“

Tatsächlich beabsichtigt die Hardthöhe, „die offensiven Fähigkeiten der Bundeswehr (…) als unterstützendes, komplementäres oder substituierendes Wirkmittel“ zu entwickeln und einzusetzen. „Das Potenzial und die Chancen des Cyber-Raums sind hier auch in der Ausrüstung und operativen Aufstellung zu nutzen, um die Wirksamkeit des Handelns der Bundeswehr zu steigern“, heißt es weiter in der im Jahr 2015 geleakten „Strategische Leitlinie Cyber-Verteidigung“ des Bundesverteidigungsministeriums. Auf eine kleine Anfrage der Bundestagsfraktion DIE LINKE zum „Krieg im ›Cyber-Raum‹“ antwortete das Ministerium in Drucksache 18/69689, dass den „Cyberfähigkeiten (…) eine Rolle zum Schutz der eigenen Kräfte oder zur Erhöhung eigener Wirkung“ zukomme. Auch in einem Ende April 2016 an die Öffentlichkeit gelangten internen Konzeptpapier der Bundeswehr, wird der Cyberspace als „militärischer Operationsraum“ bezeichnet.

Falk Grabsch, ein Sprecher des Chaos Computer Clubs, sagte gegenüber dem Internetportal netzpolitik.org, dass „digitale Angriffe den Charakter von Streubomben“ besäßen und „ein hohes Risiko für weite Bereiche der Zivilbevölkerung darstellen“. Er fügte hinzu: „Wir brauchen keine neuen Wege, noch mehr Kriege zu führen.“ Das Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung fordert von der Bundesregierung in einem Appell entsprechend, auf eine offensive Cyberstrategie zu verzichten, keine Cyberwaffen zu entwickeln und anzuwenden und sich für ein internationales Abkommen zur weltweiten Verbannung von Cyberwaffen einzusetzen (www.cyberpeace.fiff.de).

Patrik Köbele, Vorsitzender der Deutschen Kommunistischen Partei (DKP), ordnete die Kampagne der Bundeswehr ein und wies gegenüber der jW darauf hin, dass die IT-Kämpfer, die über das „Projekt Digitale Kräfte“ rekrutiert werden, für dieselben Ziele eingesetzt würden wie alle anderen Soldaten. Bei den Reklame-Offensiven gehe es um nichts anderes, als ums „Werben fürs Töten und Sterben für die Interessen des Imperialismus“. Entsprechend rät Ulla Jelpke, innenpolitische Sprecherin der Fraktion die LINKE im Bundestag und Obfrau für ihre Fraktion im Innenausschuss: „Macht, was wirklich zählt und sagt Nein zu Militarismus und Krieg!“

Werbeplakat des Projekts Digitale Kräfte. Quelle: IMI

Cyberwar und Inforaum

Die NATO und der Krieg auf dem fünften Schlachtfeld

von Thomas Gruber

„Der erste Schuss im nächsten großen Krieg wird im Web fallen". Rex Hughes, Sicherheitsberater der NATO im Bereich der Cyber-Verteidigung, weiß die zentrale Bedeutung der Cyber-Kriegsführung für die Mitglieder des Nordatlantikbündnisses in Szene zu setzen.[1] Neben klassischen militärischen Schauplätzen wie dem Krieg zu Land, in der Luft, im Meer und im Weltall wird der Cyberspace innerhalb der NATO längst als neues fünftes Schlachtfeld gehandelt. Der Begriff Cyberwar bezeichnet dabei kriegerische Aktionen im virtuellen Raum. Diese neuen Angriffstaktiken umfassen unter anderem Attacken auf feindliche Infrastruktur über das Internet, das Einschleusen fehlerhafter Hardware in Kommunikationsnetze und die gezielte Störung elektronischer Geräte durch Mikrowellen- oder elektromagnetische Strahlung.[2] Das Bedrohungsszenario, dem sich die NATO-Verbündeten bei der Thematisierung des Cyberkriegs bedienen, reicht von der bloßen industriellen oder diplomatischen Spionage bis zur vollständigen Sabotage kritischer ziviler und militärischer Infrastruktur. Die politischen und militärischen Entscheidungsträger_innen suggerieren, dass Cyberangriffe auf Krankenhäuser, Kraftwerke oder Kriegsgerät – vor allem jene, die über das Internet erfolgen – äußerst niedrigschwellig, „kostengünstig und effektiv"[3] und daher auch von Staaten mit begrenzten militärischen Mitteln oder Hacker_innenkollektiven durchführbar sind. Suleyman Anil, der Leiter des NATO-Zentrums zur Reaktion auf Computerzwischenfälle, konstatiert: „Cyberverteidigung wird nun in den höchsten Rängen zusammen mit der Raketenabwehr und der Energiesicherheit in einem Atemzug genannt".[4] Dass allerdings eine Struktur zur Cyberverteidigung auf NATO-Seite jemals ohne die gleichzeitige Planung von Cyberangriffen gedacht wird, ist höchst unwahrscheinlich – denn innerhalb der NATO dominiert folgende Auffassung zum „Wert" solcher Offensivkapazitäten: „[K]ann irgendeine militärische Macht glaubwürdig versichern, dass sie zukunftsweisende Fähigkeiten besitzt, wenn sich in ihrem Arsenal nicht auch offensive Cyberoperationen befinden?"[5]

Öffentliche Darstellung und Kooperationsstrukturen

Angriffe im Informationsraum werden auf Seite der NATO umfassend als Verteidigungsfall dargestellt. Ebenso defensiv orientiert berichtet auch die westliche Presse vornehmlich von Cyberangriffen auf NATO-Verbündete durch russische und chinesische Hacker_innen oder durch politische Aktivist_innen (wie das Kollektiv Anonymous). Die einzelnen Ziele der Angriffe auf die jeweilige Staats- und Wirtschaftsordnung sind dabei in klare Feindbilder abgegrenzt: Chinesische Angreifer_innen beschränken sich demnach auf die Wirtschaftsspionage,[6] russische Hacks dagegen auf die politische Vergeltung gegenüber einzelnen Staaten oder NATO-Strukturen[7] und aktivistische Hacker_innen zielen aus ideologischen Gründen auf die Offenlegung von empfindlichen Staatsgeheimnissen ab.[8] Gegen die erdrückende Flut von Cyberattacken kann sich die NATO also als Retterin – und zu gegebener Zeit gar als Rächerin – der westlichen Werte- und Wirtschaftsunion hervortun. Doch für schlagkräftige Wehrhaftigkeit werden Strukturen und Technologie benötigt, Personal muss ausgebildet, eingestellt und Stellen müssen verstetigt werden – kurz: Der Verteidigungsetat der einzelnen NATO-Staaten wird entsprechend erhöht und es entstehen nationale und transnationale Kompetenzzentren zum Cyberwar. Dabei zeichnet sich auf Seiten der Staatsregierungen und deren Bündnissen ein Ringen um die Kontrolle des virtuellen Raumes ab. Waren gezielte Großangriffe im Cyberspace vor 10 bis 15 Jahren noch den mächtigen und reichen Staaten oder Konzernen vorbehalten, bangen diese nun zunehmend um ihren exklusiven Status und befürchten gegenüber Kleinstgruppen gekonnter Hacker_innen Informations- und Raumverluste im Cyberkrieg hinnehmen zu müssen.

Auf nationaler Ebene befassen sich traditionell meist Geheimdienste mit der Abwehr und der Durchführung von Cyberattacken (so beispielsweise im Falle der USA die National Security Agency und in Deutschland der Bundesnachrichtendienst). Der „Vorteil", solch intransparent agierende Organisationen zu unterhalten, ist die Möglichkeit, selbst klandestine Spionage oder Sabotage-Angriffe durchführen zu können, ohne diese öffentlich thematisieren zu müssen. Nicht immer ist allerdings ein geheimer Schlagabtausch im Cyberspace politisch erwünscht: Es kann aus nationaler und geopolitischer Sicht durchaus sinnvoll sein, einen Cyberangriff als Kriegsakt zu stilisieren. Denn würde eine Cyberattacke als vollwertige kriegerische Aktion gegen einen NATO-Staat klassifiziert, so ließe sich daraufhin der in einer Politik der militärischen Eskalierung oft ersehnte Bündnisfall ausrufen. Auf dem NATO-Gipfel in Wales 2014 wurde konstatiert: „Ein Beschluss darüber, wann ein Cyber-Angriff zur Erklärung des Bündnisfalls nach Artikel 5 führen würde, wäre vom Nordatlantikrat fallweise zu fassen."[9] Mit ebendieser Prämisse arbeitet auch das 2008 in Estland gegründete Kompetenzzentrum für Cyberabwehr der NATO.[10] Nach eigener Auffassung soll es die „Fähigkeit [...] bieten, Bündnismitglieder auf Verlangen bei der Abwehr eines Cyberangriffs zu unterstützen".[11] Auch auf nationaler Ebene entstanden militärische Abteilungen zur Abwehr und zur Durchführung von Cyberangriffen. Die im Jahr 2008 gegründete *Abteilung Informations- und Computernetzwerkoperationen der Bundeswehr* soll neben einer Analyse des Bedrohungspotentials feindlicher Cyberattacken auch die Möglichkeiten offensiver digitaler Kriegsführung durch die Bundeswehr bearbeiten.[12] In Frankreich wurde im Jahr 2009 die regierungsamtliche Cybersicherheitsbehörde *ANSSI* ins Leben gerufen, die sich mit der Sicherheit französischer Informationssysteme befassen soll und dem Sekretariat zur nationalen Verteidigung und Sicherheit unterstellt ist.[13] Das US-amerikanische *United States Cyber Command* entstand im Jahr 2010 und setzt sich unter Führung *United States Strategic Command* mit den Möglichkeiten und Strategien des Cyberwars auseinander.[14]

Neben dem Aufbau eigener Strukturen und der Ausbildung militärischen Personals für Cyberaufgaben greift das NATO-Bündnis vor allem auf bereits bestehende Expertise aus der Privatwirtschaft zurück. Auf dem NATO-Gipfel 2014 in Wales wurde die Gründung einer *NATO Industry Cyber Partnership*

(NICP) beschlossen, die beim Aufbau einer engen Kooperation zwischen dem Nordatlantikbündnis und Unternehmen der Kommunikationsindustrie behilflich sein soll. Bereits knapp zwei Wochen später trafen sich NATO-Vertreter_innen mit Personen aus der Industrie, um die NICP offiziell einzugehen. Das Ziel der NATO innerhalb der NICP besteht in der Akquise von „Expertise" und „Innovation" aus dem privaten Sektor. Koen Gijsbers, Geschäftsleiter der *NATO Communications and Information Agency* (NCIA), fügt hinzu: „Hier geht es um ein Bündnis mit der Industrie und der Schlüssel zu diesem Bündnis ist Vertrauen – sensible Informationen miteinander auszutauschen, um auf Bedrohungen reagieren zu können".[15] Zum einen erhoffen sich die NATO-Funktionär_innen also technologische und innovative Unterstützung von den kollaborierenden Unternehmen, zum anderen sollen sensible Informationen (wie beispielsweise Kommunikationsdaten oder Schwachstellen in den eigenen Sicherheitssystemen) von den Konzernen an die militärischen Akteur_innen weitergegeben werden. Dass dabei erhebliche Summen an die beteiligten IT-Sicherheits- und Kommunikationsunternehmen fließen werden, ist selbstverständlich. Sie verkaufen an die NATO neben den neuesten Angriffs- und Verteidigungsschemata im Cyberwar auch private Daten ihrer Kunden, oder zumindest Wege, diese zu akquirieren.[16]

NATO-Aktionen im Cyberwar

Die Aktionen der NATO-Staaten im Cyberwar werden öffentlichkeitswirksam verkauft. Die Berichte umfassen militärische Übungen wie beispielsweise einen simulierten Großangriff auf Computernetzwerke im NATO-Kompetenzzentrum in Tallinn – bei dem Methoden zur Cyberverteidigung eine ebenso große Rolle spielten wie Angriffsschemata im Cyberspace[17] – oder die Einbettung von Cyberkonzepten in die Großübung Trident Juncture im Jahr 2015. Trident Juncture behandelte eine Intervention in einer Region in Afrika, in der zwei Kleinstaaten um den Zugang zu Trinkwasser streiten und die es nach NATO-Maßstäben militärisch zu stabilisieren gilt.[18] In diesem Sinne fanden während der Übung auch Cyberkonzepte ihre offensive Anwendung. Von minder technologisierten Kleinstaaten kann kaum ein Cyberangriff ausgehen, der für die NATO-Verbündeten gefährlich würde. Stattdessen muss sich ein solches Manöver auf Cyberattacken gegen zivile und militärische Infrastruktur, Überwachung, Spionage und die Möglichkeiten der Verbreitung von westlicher Kriegspropaganda – der sogenannten „strategischen Kommunikation" – fokussieren.[19] Offensive Taktiken im Cyberspace werden von NATO-Seite nach alter Manier in ein Verteidigungsszenario eingebettet und als legitime Abschreckungsmanöver gerechtfertigt: „Eine klare Artikulation der Art, wie die NATO offensive Cyberstrategien als Teil jeder defensiven Operation nutzen würde, würde auch die Risikoabschätzungen der Feinde dahingehend ändern, dass sie gezwungen wären zu bedenken, dass jede offensive Aktion, auch wenn sie verdeckt stattfinden sollte, nicht risiko- oder kostenfrei ist."[20]

Eine weitere Möglichkeit, die öffentliche Meinung zu manipulieren, ist die Kopplung geheimdienstlicher Cyberangriffe und offen kommunizierter Cyberabwehr. Denn die westlichen Großmächte können die Herkunft ihrer geheimdienstlichen Cyberattacken weitaus besser verschleiern als Staaten wie der Iran oder China. So wurden beispielsweise im Jahr 2010 mittels des Internetwurms Stuxnet, der vermutlich aus den USA stammt, iranische Atomanlagen angegriffen[21] und die anschließenden Vergeltungsschläge iranischer Hacker_innen in den westlichen Medien als Angriff dargestellt und verurteilt.[22] Da die US-Behörden und -Geheimdienste allerdings nicht offenlegen, auf welcher Grundlage sie die Ursprünge der neuen Cyberangriffe im Iran verorten, ist auch nicht auszuschließen, dass die iranischen Hacks von den USA selbst fingiert wurden. Denn falls auf die US-amerikanischen Cyberangriffe keine militärische oder geheimdienstliche Reaktion aus dem Iran folgt, wäre auch die fälschliche Darstellung eines feindlichen Cyberangriffes denkbar, um den Konflikt zu eskalieren. Während die Sabotage bei Cyberangriffen meist gegen politische Feinde außerhalb des NATO-Bündnisses beschränkt ist, greifen Spionagebemühungen auch unter den NATO-Staaten um sich. Eines der jüngsten Beispiele ist die NSA-Abhöraffäre, die aufgrund der von Edward Snowden geleakten Dokumente im Jahr 2013 an die Öffentlichkeit gelangte: Unter dem Deckmantel der Terrorbekämpfung wurden von den USA global und verdachtsunabhängig Kommunikationswege überwacht, private Kommunikation offengelegt und auch staatliche Institutionen von NATO-Verbündeten sowie Vertretungen der Vereinten Nationen ausspioniert.[23]

Logo des Kompetenzzentrums. Quelle: Wikipedia

Die Auswirkungen des Cyberwar auf die Zivilbevölkerung

Das Bedrohungsszenario, das von der NATO stetig aufrechterhalten wird, birgt neben der Möglichkeit einer Eskalation internationaler Konflikte aber auch eine erhebliche Gefahr für die Zivilgesellschaft. Ziele wie Krankenhäuser oder die Stromversorgung eines Landes stehen sowohl auf der Liste der bei einem Cyberangriff gefährdeten Objekte, als auch auf der Agenda bei Angriffen von Seiten der NATO-Staaten, wie die vermutliche US-amerikanische Attacke auf das iranische Atomprogramm eindrucksvoll zeigt. Die immer weiter reichende Digitalisierung und Technologisierung von Städten bis hin zur Planung sogenannter *Smart Cities* öffnet den neuartigen Cyberattacken sukzessive eine breitere Flanke. Die Absichten, den öffentlichen Nahverkehr zu automatisieren, intelligente Produktionslinien bereitzustellen und die Stromversorgung

Verlegungsschiff für Transatlantikkabel „Nessie II“. Quelle: Friflash/Wikipedia

über Netze von Kleinkraftwerken (teil)autonom zu steuern, sind nur einzelne Beispiele angreifbarer Infrastruktur, deren Abschaltung in Zukunft ganze Landstriche zum Stillstand zwingen würde und in ein handfestes Chaos stürzen könnte.[24] Die Wahl des Schlachtfeldes ist von ebenso großer gesamtgesellschaftlicher Bedeutung: Bei den meisten Cyberangriffen wird ein vorwiegend zivil verwendeter Kommunikationsweg genutzt – das Internet. Knotenpunkte der Datenübertragung sind vermehrt Ziel von Sabotage- und Spionageaktionen. *TAT-14*, eines der weltweit wichtigsten Transatlantikkabel, wurde in Ägypten mehrmals durchtrennt und in der englischen Küstenstadt Bude vermutlich vom britischen Geheimdienst *GCHQ* angezapft.[25] Auch russischen U-Booten wird von NATO-Seite inzwischen die Fähigkeit attestiert, Transatlantikkabel durchtrennen zu können.[26] Eine weit verbreitete Praxis bei Cyberattacken ist außerdem die Infizierung zahlreicher Computer mit Viren, die anschließend unbemerkt Befehle auf den Privatrechnern ausführen und sie so zu einem kollektiven Netzwerk, einem sogenannten *Botnetz*, machen. Auf diese Weise können beispielsweise Internetseiten und Server von Firmen oder staatlichen Institutionen überlastet werden, indem mehrere tausend Rechner gleichzeitig auf die Webpräsenz zugreifen.[27] Öffentliche Kommunikationswege werden also zu Kriegsschauplätzen, private Technologie zu Waffensystemen und die Zivilgesellschaft steht schließlich im digitalen Kreuzfeuer. Nach Konstanze Kurz wird „die Zivilbevölkerung […] als Geisel genommen und ihre zivile Infrastruktur Schlachtfeld und unreguliertes Operationsgebiet.”[28] Zum einen schürt diese Kriegstaktik das Klima der Angst in der Bevölkerung und erleichtert damit die Legitimation neuer militärischer Aktionen unter dem Deckmantel der nationalen Verteidigung, zum anderen bietet der zivile Sektor eine angenehme moralische Pufferzone bei feindlichen Angriffen.

Im selbsternannten Kampf gegen den Terror wird die Gefahr von in der Mitte der Gesellschaft verdeckt agierenden Terrorzellen instrumentalisiert, um staatliche Überwachungsmechanismen auszuweiten und damit die Privatsphäre der Bürger_innen einzuschränken. Neben der stetigen geheimdienstlichen Überwachung soll nun auch dem Militär ein breiterer Zugriff auf die zivile Kommunikation gewährt werden. Dabei kommen sowohl propagandistische Methoden gegen vermeintliche terroristische Werbung zum Einsatz, als auch komplexe Algorithmen zur automatisierten Analyse staatsgefährdender ziviler Kommunikation. Dass bei einer solchen verdachtsunabhängigen Überwachung auch subversive politische Gruppen in das Raster der Streitkräfte passen, ist kein Novum. Dieser Rhetorik bedienen sich beispielsweise auch die Entscheidungsträger_innen des für Anfang 2017 geplanten *Cyber- und Informationsraum-Kommandos* (CIRK) der Bundeswehr. Rekrutierungsbemühungen terroristischer Gruppierungen wie des IS über die sozialen Netzwerke werden als Angriff auf den Informationsraum gewertet und sollen ebenso aktiv überwacht und offen gelegt werden wie gezielte Cyberangriffe auf deutsche staatliche Institutionen und Unternehmen.[29] Neben der Löschung unliebsamer Inhalte wird der Bundeswehr damit auch die propagandistische Beeinflussung öffentlicher Diskussionen erleichtert, das CIRK kann also auch als Knotenpunkt strategischer Kommunikation fungieren. Dass der Bundeswehr mit der Begründung präventiver Terrorbekämpfung empfindliche Eingriffe in die private Kommunikation von Nutzer_innen sozialer Netzwerke und damit die Privatsphäre deutscher Staatsbürger_innen ermöglicht werden, tut der Planung bisher keinen Abbruch. Die deutsche Beteiligung an der digitalen Aufrüstung der NATO-Streitkräfte ist nicht zu unterschätzen: Neben den überaus präsenten US-amerikanischen Spionagebehörden, wie beispielsweise der NSA oder der US Airforce, kann kaum ein NATO-Staat so umfassende Wachstumsbestrebungen im Cyberkrieg vorweisen wie die Bundesrepublik. Begründet mit der veralteten Technologie der Bundeswehr und dem unmissverständlichen Wunsch der Politik, die deutsche Position in weltweiten Konflikten zu stärken, werden so militärische Umstrukturierungen und damit einhergehende Budgeterhöhungen im Cybersektor durch den parlamentarischen Entscheidungsprozess gewinkt.

Der NATO den virtuellen Raum nehmen!

Das Vorgehen des Nordatlantikbündnisses im Cyberkrieg zeigt vielfältige Parallelen zur übrigen NATO-Kriegsführung auf: Während NATO-Staaten selbst Angriffe planen und durchführen, werden öffentlich nur Verteidigungsszenarien beworben. Außerdem wird die augenscheinliche Einigkeit in Verteidigungsfragen innerhalb der NATO auch von den nationalistischen Aktionen der Einzelstaaten überlagert, die sich gegenseitig misstrauen und ausspionieren. Privatwirtschaftliche Akteur_innen wie IT-Sicherheitsunternehmen, die ursprünglich für die Sicherheit der ihnen anvertrauten Daten sorgen sollten, lassen sich von der NATO kaufen und kompromittieren dabei ihre eigenen Produkte. Allein dieser Umstand zeigt, dass IT-Sicherheit nicht in einem marktwirtschaftlichen Kontext funktionieren kann; die einzige sinnvolle Alternative bleibt quelloffene, kollektiv entwickelte Software, die unabhängig von Markt- und Machtinteressen entsteht. Die wahre Bedrohung für die Zivilgesellschaft, die von der NATO wie von jeder imperialistisch handelnden Militärinstitution ausgeht, fällt gegenüber der ständig präsenten Angst vor feindlichen Cyberattacken kaum ins Gewicht. Doch gerade aus

Smart City. Quelle: pixabay.com

den Angriffen auf die Privatsphäre und der Einbeziehung ziviler Infrastruktur in kriegerische Aktionen gälte es Motivation für vielfältige Formen des Widerstandes und des Protests zu schöpfen. Dass selbst kleine Kollektive von Hacker_innen eine nennenswerte antimilitaristische und antikapitalistische Rolle im digitalen Wettrüsten einnehmen können, wird schon allein durch die offensiven Anfeindungen deutlich, mit denen die NATO aktivistisch motivierte Hacker_innen zu legitimen Zielen im Cyberwar erklärt: „Sogenannte ‚Hacktivists', die sich an Cyberattacken während eines Krieges beteiligen, können legitime militärische Ziele darstellen, obwohl sie Zivilist_innen sind."[30] Hier zeigt sich auch der eigentliche Grund für das von der NATO beschworene Bedrohungsszenario im Cyberraum: Die Sabotage von Kommunikationsnetzen der NATO-Staaten oder die Offenlegung von Staats- und Unternehmensgeheimnissen bedarf im virtuellen Raum keiner schwer beizukommenden Waffentechnologie oder persönlicher Spionage mehr. Gruppen von Hacker_innen, die sich dezidiert friedvoll und jenseits jedweder Großmachtinteressen positionieren, können so der Eroberung des virtuellen Raumes durch macht- und wirtschaftspolitische Interessenträger_innen entgegenstehen. Die wahre Gefahr für eine Zivilgesellschaft geht dagegen nicht von politischen Kleingruppen aus, sie entsteht im internationalen virtuellen Wettrüsten, an dem sich die NATO-Staaten beispiellos beteiligen. Eine Cyberattacke auf wirklich kritische zivile Infrastruktur wie Krankenhäuser oder die Energieversorgung eines Landes benötigt Mittel, die nur den militärischen Großmächten zur Verfügung stehen. Denn im Gegensatz zu großen Teilen der NATO-Kommunikation und der Kommunikation großer Unternehmen oder staatlicher Behörden, sind die Gesundheits- und Energieversorgung meist nicht im Internet vernetzt und muss gezielt über das Einschleusen kompromittierter Hardware oder eigens zu diesem Zweck implementierten Computerviren attackiert werden. In ihren Bemühungen um den Schutz der eigenen militärischen Kommunikationsnetze und den einzelnen nationalen oder wirtschaftlichen Interessen erzeugen die NATO-Staaten also die Gefahr für ihre jeweilige Bevölkerung selbst. Dieser gefährlichen Scheinheiligkeit gilt es gesamtgesellschaftlich entgegen zu wirken und die Argumentation der rüstenden Großmächte muss systematisch dekonstruiert werden.

Anmerkungen

1 *Cyberwar: Nato-Staaten rüsten für das fünfte Schlachtfeld*, Spiegel online, 20.04.2016.
2 *Cyberkrieg*, Wikipedia, 20.04.2016.
3 Katrin Suder, Staatssekretärin des BMVg in: BMVg, 20.04.2016.
4 *Das Cooperative Cyber Defence Centre of Excellence der NATO*, Wikipedia, 20.04.2016.
5 Übersetzung des Autors aus dem Englischen; *The Role of Offensive Cyber Operations in NATO's Collective Defence*, NATO CCDCOE, S. 2, 05.05.2016.
6 *Is China still hacking US? This cyber firm says yes*, CNBC, 20.04.2016.
7 *Russische Hacker spionieren angeblich NATO aus*, heise.de, 20.04.2016.
8 *NATO report threatens to 'persecute' Anonymous Hacktivist grouped named as threat by military alliance*, serpent's embrace, 20.04.2016.
9 *Cyber-Kommando für die Bundeswehr*, NDR.de, 05.05.2016
10 *Krieg in der fünften Dimension*, Neue Züricher Zeitung, 20.04.2016.
11 *Das Cooperative Cyber Defence Centre of Excellence der NATO*, Wikipedia, 20.04.2016.
12 *Die Abteilung Informations- und Computernetzwerkoperationen, Cyber-Einheit der Bundeswehr*, Wikipedia, 20.04.2016.
13 *ANSSI, die erste regierungsamtliche Cybersicherheitsbehörde in Frankreich*, Wikipedia, 20.04.2016.
14 *United States Cyber Command*, Wikipedia, 20.04.2016.
15 Übersetzung des Autors aus dem Englischen; *NATO launches Industry Cyber Partnership*, NATO, 21.04.2016.
16 Besonders eindrucksvoll lässt sich diese Entwicklung am Beispiel des IT-Sicherheitskonzerns *RSA* nachvollziehen, der sich eine vorsätzlich implementierte Sicherheitslücke im eigenen Verschlüsselungssystem vom US-Geheimdienst *NSA* mit 10 Millionen Dollar bezahlen ließ: *Exclusive: Secret contract tied NSA and security industry pioneer*, Reuters, 21.04.2016.
17 *Verteidigungsministerin von der Leyen: Angriff der Cyber-Krieger*, Spiegel online, 20.04.2016.
18 *„Trident Juncture 2015": Machtdemonstration gegenüber Russland?*, IMI, 20.04.2016.
19 *Trident Juncture 2015 kicked off*, NATO, 20.04.2016.
20 Übersetzung des Autors aus dem Englischen; *The Role of Offensive Cyber Operations in NATO's Collective Defence*, NATO CCDCOE, S. 7, 05.05.2016.
21 *Obama ordnete Stuxnet-Attacken an*, taz.de, 20.04.2016.
22 *DDoS gegen Banken: USA klagen iranische Hacker an*, heise newsticker, 20.04.2016.
23 *Globale Überwachungs- und Spionageaffäre*, Wikipedia, 20.04.2016.
24 vgl. dazu beispielsweise Florian Rötzer: *Smart Cities im Cyberwar*, Westend Verlag, 2015.
25 *Die Kabel-Krake, die alles weiß*, Zeit online, 20.04.2016.
26 *Russian Ships Near Data Cables Are Too Close for U.S. Comfort*, New York Times, 20.04.2016.
27 *DDoS und Botnetze*, Wikipedia, 20.04.2016.
28 *High-Tech-Kriege*, Heinrich Böll Stiftung, S.21, 20.04.2016.
29 Katrin Suder in *Streitkräfte und Strategien*, NDR Info, 17.10.2015.
30 Übersetzung des Autors aus dem Englischen; *Tallinn Manual: NATO veröffentlicht Handbuch mit Cyberwar-Regeln*, netzpolitik.org, 05.05.2016.

Nato-Exzellenzzentren

Planen für den nächsten Krieg

von Christopher Schwitanski

Im Zuge des 2002 auf dem Nato-Gipfeltreffen in Prag eingeleiteten Umbaus der Nato-Kommandostruktur wurde die Neugründung des Alliierten Kommando Transformation (ACT) beschlossen, mit der Aufgabe, die Transformation der Allianz hin zu einem international agierenden militärischen Interventionsbündnis voranzutreiben. Unterstützt wird das ACT dabei durch die Etablierung einer neuen Struktur militärischer Denkfabriken, sogenannten Exzellenzzentren[1] (Centre of Excellence – COE). Deren Anzahl ist inzwischen auf 24[2] solcher Einrichtungen angewachsen (Tendenz steigend), womit die Frage in den Vordergrund rückt, welche Bedeutung diese für die Nato haben.

In einer ersten Kleinen Anfrage der Partei die Linke 2015 äußerten die Abgeordneten bezüglich der Nato-Exzellenzzentren die Befürchtung, „dass mit den Exzellenzzentren gezielt und mit Steuergeldern finanziert Foren für Militärs und angehende Führungskräfte geschaffen werden, um außerhalb der militärischen Befehlskette, politischen Kontrolle und kritischen Öffentlichkeit auch in Spezialfeldern, wie der Cyber-kriegsführung und der strategischen Kommunikation, eine offensivere Doktrin der NATO zu entwickeln und dass dabei das Völkerrecht kaum Beachtung findet.“[3]

Die vorliegende Arbeit wird u. a. der Frage nachgehen, inwieweit diese Bedenken berechtigt sind und welche Bedeutung den Nato-Exzellenzzentren innerhalb der Militärallianz zukommt.

Es gilt zu beachten, dass neben der genannten Kleinen Anfrage bislang wenige neutrale oder kritische Quellen zu den Exzellenzzentren zu finden sind. Wer sich die Quellenangaben genauer anschaut, wird feststellen, dass die verwendete Literatur größtenteils von der Nato oder ihr nahestehenden Einrichtungen stammt. Eine objektive oder gar kritische Betrachtung ist nahe liegenderweise in solcher Literatur kaum zu finden. Entsprechend sind viele der gezogenen Schlussfolgerungen aus bestehenden Nato-Darstellungen abgeleitet. Die vorliegende Arbeit soll einen ersten Ansatzpunkt für eine kritische Problematisierung der Exzellenzzentren als Teil der Nato bieten in der Hoffnung, dass dies zu einer notwendigen weiteren Auseinandersetzung mit dem Thema anregt.

Hierfür werden im Folgenden zunächst die Exzellenzzentren im Allgemeinen, ihre Entwicklung, Finanzierung und Arbeitsprinzipien beschrieben. Anschließend werden einzelne Einrichtungen unter deutscher Beteiligung konkret in den Blick genommen, ehe abschließend eine kritische Bewertung der Exzellenzzentren als Teil des Alliierten Kommando Transformation vorgenommen wird.

Nato-Exzellenzzentren: Teil des Nato Transformationsprozess

Im Rahmen ihres Gipfeltreffens in Prag 2002 beschlossen die Nato-Staaten die Neuausrichtung der Nato-Kommandostruktur und die fortlaufende Transformation der Allianz. Ziel war es u. a., die Nato zu einer flexibleren Interventionsstreitmacht auszubauen, um besser auf die neuen „Bedrohungen“ des 21. Jahrhunderts reagieren zu können und im Zuge dessen die Nato-Kommandostruktur deutlich zu verschlanken.[4] Bereits nach dem Zerfall der Sowjetunion war es zu einer Straffung der Kommandostruktur gekommen, im Rahmen derer die Anzahl der Nato-Hauptquartiere von 78 auf 20 reduziert worden war. Infolge des Gipfeltreffens 2002 wurden die bisherigen Nato Oberkommandos in Europa (Allied Command Europe) und den USA (Allied Command Atlantic) im Alliierten Kommando Operation (Allied Command Operation – ACO) mit Sitz im ehemaligen europäischen Oberkommando in Mons, Belgien zusammengeführt; ihm obliegt die Führung sämtlicher weltweiter Nato-Einsätze.[5] Zweiter Teil der neuen Kommandostruktur wurde das ebenfalls neugegründete Alliierte Kommando Transformation (ACT), welches in den Räumlichkeiten des ehemaligen Allied Command Atlantic in Norfolk, Virginia stationiert ist und die Förderung und Kontrolle sämtlicher Transformationsprozesse des Bündnisses zur Aufgabe hat.[6] An der Spitze des ACT steht der Supreme Allied Commander Transformation (SACT), einer der beiden strategischen Kommandeure der Nato. Gemeinsam bilden ACO und ACT die Nato-Kommandostruktur, welche den beiden obersten militärischen und zivilen Gremien der Nato unterstellt ist, dem Militärkomitee und dem Nordatlantikrat. Letzterer setzt sich aus ständigen Vertretern sämtlicher Nato-Mitgliedsstaaten zusammen und ist die oberste Entscheidungsinstanz innerhalb der Nato. Das Militärkomitee dagegen ist die oberste militärische Instanz, bestehend aus militärischen Vertretern der Mitgliedsstaaten, welche dem Nordatlantikrat und weiteren zivilen Institutionen in militärischen Fragen beratend zur Seite steht.[7]

Bei einem weiteren Treffen des Verteidigungsausschusses (dieser wurde 2010 aufgelöst und seine Kompetenzen vom Nordatlantikrat übernommen) und der Nuklearen Planungsgruppe (NPG) 2003 in Brüssel wurde der Beschluss gefasst, das neu gegründete Alliierte Kommando Transformation durch eine Struktur von Exzellenzzentren zu unterstützen, mit der Aufgabe, koordiniert durch das ACT den anhaltenden Transformationsprozess der Nato voranzubringen.[8] Hierbei handelt es sich um international finanzierte und geförderte Einrichtungen, die trotz ihrer Bedeutung für die Nato nicht Teil ihrer Kommandostruktur sind. So soll explizit die Möglichkeit gegeben werden, innovativ zu arbeiten, ohne durch die bestehenden Nato-Doktrinen übermäßig eingeschränkt zu werden.

Bereits zwei Jahre nach dem Beschluss des Verteidigungsausschusses und der Nuklearen Planungsgruppe in Brüssel wurde das Joint Air Power Competence Centre (JAPCC), das erste Exzellenzzentrum, in Deutschland von der Nato anerkannt und nahm in Kalkar offiziell seine Arbeit auf. 2006 folgte das Defence Against Terrorism Centre of Excellence (DAT COE) in der Türkei. Innerhalb der letzten zehn Jahre ist diese Struktur deutlich angewachsen, so gibt es heute bereits 24 Nato-Exzellenzzentren, 23 davon in Europa (Stand April 2016).[9]

Einrichtung eines Nato-Exzellenzzentrums

Die groben Voraussetzungen für die Einrichtung von Exzellenzzentren seitens der Nato umfassen einige allgemeine Anforderungen: Zunächst sollen sie innerhalb der Allianz einen Mehrwert schaffen und nicht in Konkurrenz zueinander treten,

Informationsstelle Militarisierung (IMI) e.V. - Hechinger Str. 203 - 72072 Tübingen

weswegen jedes Zentrum einen eigenen inhaltlichen Arbeitsschwerpunkt hat. Innerhalb dessen sind sie ausdrücklich aufgefordert, über den eigenen Tellerrand hinauszudenken und neue innovative Konzepte zu entwickeln. Des Weiteren soll jedem Nato-Mitglied die Partizipation an einem Exzellenzzentrum freistehen und über diese und nicht den Nato-Haushalt läuft auch ausschließlich die Finanzierung. Zuletzt sind klar definierte Beziehungen zwischen Exzellenzzentrum, Nato und beteiligten Nationen von Bedeutung, welche mittels verschiedener Vereinbarungen (Memoranda of Understanding – MOU) definiert werden. Der Zweck der Exzellenzzentren besteht laut Nato darin, die Lehre und Ausbildung zu verbessern, die Interoperabilität und Einsatzmöglichkeiten zu erweitern, die Entwicklung und Erprobung neuer Konzepte und Doktrinen zu ermöglichen und Lessons-Learned-Analysen anzubieten.[10] Dabei sind die Exzellenzzentren passend zu ihrem jeweiligen Arbeitsschwerpunkt in verschiedene Nato-Arbeitsgruppen eingebunden und ihre Tätigkeit kann so in die Bearbeitung von Nato-Konzepten sowie Doktrinen einfließen und zum Transformationsprozess beitragen.[11]

Staatliche Beteiligung und Finanzierung

Um ein neues Nato Exzellenzzentrum zu gründen, braucht es zunächst eine sogenannte Rahmennation, einen Staat, der die nötigen Örtlichkeiten und Ressourcen zur Verfügung stellt und den Arbeitsschwerpunkt der Einrichtung festlegt. Diese leistet üblicherweise den höchsten finanziellen Beitrag und stellt im folgenden Prozess auch den formalen Antrag auf Anerkennung durch die Nato. Die Initiative zur Gründung des Zentrums muss dabei nicht zwingend von der Rahmennation ausgehen, möglich wäre auch eine Gruppe von Mitgliedsstaaten oder die Nato selbst. Das vorläufige Konzept wird anschließend mit dem ACT abgestimmt und sofern es dessen Zustimmung erhält, kann die Rahmennation anderen Staaten die Beteiligung an dem Projekt anbieten, die bereit sind, das Exzellenzzentrum finanziell mitzutragen. Alle Staaten, die sich finanziell und/oder personell an einem Exzellenzzentrum beteiligen wollen (Sponsoring Nations), haben damit die Möglichkeit, Einfluss auf die Arbeit der Einrichtung zu nehmen. Wenn auch üblich, so ist es doch nicht zwingend, dass es sich bei einer Sponsoring Nation um ein Nato-Mitglied handelt. Möglich sind auch Staaten, die Teil des Programms Partnership for Peace[12] sind, oder auch nichtstaatliche Organisationen.[13] Weiterhin besteht auch die Möglichkeit, sich als Contributing Nation/Participant an einem Exzellenzzentrum zu beteiligen. Contributing Nations können sich neben Sponsoring Nations ebenfalls durch Bereitstellung von Ressourcen an dem Projekt beteiligen. Im Unterschied zu diesen haben sie innerhalb des Exzellenzzentrums allerdings kein Mitbestimmungsrecht und gehen auch keine (finanziellen) Verpflichtungen ein. Ihre Beteiligung wird unter Zustimmung durch das ACT mittels einer technischen Vereinbarung zwischen den Contributing Nations, dem COE und wahlweise den Sponsoring Nations festgelegt.[14] So beteiligt sich Georgien seit 2014 als erster nicht-Nato Staat als Contributing Nation am Energy Security Centre of Excellence (ENSEC COE) im litauischen Vilnius.[15]

Da die COEs keine Gelder von der Nato selbst kriegen, finanzieren sie sich vollständig multinational über die Beiträge der beteiligten Nationen. Ein COE stellt daher i. d. R. jährlich einen Finanzierungsantrag an das Führungskomitee (Steering Commitee – SC). Dieses setzt sich aus Vertretern sämtlicher Sponsoring Nations zusammen und stellt das wichtigste Instrument zur Steuerung eines Exzellenzzentrums dar. Das Komitee trifft sich halbjährlich, beschließt die Verteilung des Budgets und entscheidet über das Arbeitsprogramm (Programm of Work – POW) des Exzellenzzentrums und legt somit fest, wie die Arbeit der Einrichtung aussehen soll. Dabei wird das POW in Abstimmung zwischen Sponsoring Nations und ACT entwickelt und anschließend vom Führungskomitee formal gebilligt. Die Arbeitsergebnisse des Exzellenzzentrums stellt dieses über das Führungskomitee den beteiligten Nationen zur Verfügung und auch „[d]ie fachliche und politische Kontrolle der auf Grundlage des ‚Programme of work' erzielten Arbeitsergebnisse erfolgt in erster Linie über die im Lenkungsausschuss [Führungskomitee] des COE vertretenen Nationen."[16] Die nationalen Vertreter sind in den Führungskomitees der Exzellenzzentren weiterhin für die Überprüfung des nationalen Engagements innerhalb der Einrichtungen zuständig. Neben dem Führungskomitee haben auch andere Organisationen – allen voran die Nato – die Möglichkeit, sich mit Aufträgen an ein Exzellenzzentrum zu wenden.

Die Beteiligung an einem Exzellenzzentrum kann für die jeweilige Nation verschiedene Vorteile bieten. Zunächst kann ein Land von der im COE gebündelten multinationalen Expertise und den entwickelten Konzepten und Strategien profitieren und darüber hinaus auf diese über die Beteiligung im Führungskomitee einwirken. Weiterhin kann eine internationale militärische Organisation auf dem eigenen Boden als Prestigeobjekt dienen und die Beteiligung an einem solchen insbesondere neuen Nato-Mitgliedern die Möglichkeit bieten, größeren Einfluss innerhalb der Nato Kommandostruktur zu gewinnen.[17] Auf der Website der Bundeswehr findet sich diesbezüglich folgende Einschätzung: „Neben ihrer fachlichen Rolle erfüllen [die Exzellenzzentren] auch eine Präsenzfunktion: Vor allem den jüngeren NATO-Bündnispartnern in Osteuropa […] bieten sie die Möglichkeit, ihre NATO-Zugehörigkeit sichtbar zu unterstreichen und eine NATO-Flagge auf ihrem Territorium zu hissen."[18]

Neben den an Exzellenzzentren beteiligten Nationen und Organisationen pflegen diese darüber hinaus im Einzelnen noch Beziehungen zu anderen Exzellenzzentren und Nato-Einrichtungen, wie z. B. der Nato-Schule in Oberammergau, wo neue Konzepte direkt in die Lehre einfließen können. Daneben gibt es Kooperationen mit anderen Staaten, wie z. B. Mitgliedern der Partnership for Peace oder den Ländern des Mediterranean Dialogue, aber auch mit zivilgesellschaftlichen Akteuren, internationalen Organisationen, der Industrie, NGOs, Schulen, Universitäten und Forschungszentren. Ein solches Geflecht von Beziehungen wird offiziell als Community of Interest (COI) bezeichnet und die Exzellenzzentren sind angehalten, diese auszubauen und zu pflegen.[19] Hierfür hat die Nato ein eigenes Online-Portal eingerichtet, um die Vernetzung mit verschiedenen Partnern zu erleichtern.[20] Da es sich hierbei nicht ausschließlich um militärische Partner handelt, werden auf diesem Wege auch zunehmend zivilgesellschaftliche Akteure in die Nato-Militärstrukturen eingebunden.

Die rechtliche Beziehung zwischen einem Exzellenzzentrum, den Sponsoring Nations und dem Supreme Allied Commander Transformation (SACT) werden mittels zweier Memoranda of Understanding (MOU) festgelegt. Das Operational MOU definiert das Verhältnis zwischen Exzellenzzentrum und Sponsoring Nations, deren Vertreter es unterzeichnen. Es werden Vorschriften für die Gründung, Arbeit, Finanzierung, Personalausstattung, Sicherheit und die Leistungen der beteiligten Nationen festgelegt. Das Functional MOU auf der anderen Seite regelt die Beziehung zwischen dem Hauptquartier des Alliierten Kommando Transformation (HQ SACT in Norfolk), den

Sponsoring Nations, weiteren Nato-Einrichtungen und dem Exzellenzzentrum.

Akkreditierung

Damit ein Exzellenzzentrum den Status einer Nato-Organisation erhält, muss es zunächst durch die Nato akkreditiert werden. Die notwendigen Akkreditierungskriterien werden vom SACT entwickelt und ihre Einhaltung in regelmäßigen Abständen von drei bis vier Jahren überprüft. Dabei gibt es zwei unterschiedliche Arten von Kriterien: verpflichtende Kriterien (Mandatory Criteria) und wünschenswerte Kriterien (Highly Desirable Criteria).

Die verpflichtenden Kriterien müssen konstant aufrechterhalten werden und sehen vor, dass das Exzellenzzentrum den Anforderungen der Nato genügt, diese in ihrem Transformationsprozess gewinnbringend zu unterstützen. Hierzu soll es Fähigkeiten, Expertise und Ressourcen zur Verfügung stellen, die nicht schon anderswo im Bündnis angesiedelt sind und so den bereits genannten Mehrwert liefern. Weiterhin dienen sie der Ausbildung und dem Training von Nato-Personal, welche fortlaufend mit dem HQ SACT abgestimmt werden. Neben diesen eher inhaltlichen Kriterien besteht die Verpflichtung, für die Sicherheit der Anlage und dem dort befindlichen Personal und Material zu sorgen. Der Nato wird oberste Priorität eingeräumt, wenn es um den Zugriff auf Unterstützungen und Leistungen durch ein Exzellenzzentrum geht, und der Kontakt zwischen Nato und Exzellenzzentrum muss jederzeit möglich sein.[21]

Die wünschenswerten Kriterien stellen eine Ergänzung zu den verpflichtenden Kriterien dar und sollten in größtmöglichem Ausmaß aufrechterhalten werden. Auch hierbei geht es darum, dem Transformationsanspruch der Nato gerecht zu werden und die Arbeit und Organisationsstruktur des Exzellenzzentrums dementsprechend auszurichten. Weiterhin wird erwartet, dass sämtliche Tätigkeiten der Nato gegenüber transparent gehalten werden und so eine funktionierende Arbeitsbeziehung mit dem SACT ermöglicht wird. Hierfür sollen effektive Informations- und Kommunikationssysteme eingerichtet werden, welche die Kommunikation mit und Verbindung zu bestehenden Nato-Netzwerken ermöglichen.[22]

Bei der Akkreditierung wird ein neues Exzellenzzentrum durch eine Abteilung des Supreme Allied Commander Transformation unterstützt, die Transformation Network Branch (TNB), welche u. a. die Bewerber auf die Prüfung durch das Militärkomitee vorbereitet und kontrolliert, inwieweit die genannten Kriterien erfüllt sind. Neben der Vorbereitung der Akkreditierung ist die TNB im Anschluss auch dafür zuständig, die Einhaltung der Nato-Kriterien zu überwachen. Wird das Exzellenzzentrum vom Militärkomitee akzeptiert, erhält es die Anerkennung als Nato-Organisation durch den Nordatlantikrat. Mit der Akkreditierung wird der Einrichtung darüber hinaus durch den Nordatlantikrat der Status einer internationalen militärischen Organisation gemäß Artikel 14 Absatz 1 des sog. Pariser Protokolls verliehen (eines der rechtlichen Grundlagendokumente der Nato, welches den rechtlichen Status der internationalen Hauptquartiere der Allianz regelt). Damit verfügt ein akkreditiertes Exzellenzzentrum über die gleichen Rechte und Privilegien wie ein Nato-Hauptquartier.[23]

Tätigkeit

Mit Abschluss der Akkreditierung nimmt ein Exzellenzzentrum offiziell seine Arbeit auf. Im Rahmen dieser wird in ihm meist an verschiedenen Projekten und zu unterschiedlichen Themenschwerpunkten gearbeitet, an denen jeweils verschiedene Experten, sog. „Subject Matter Experts“ (SME) arbeiten, die häufig in weitere über das Exzellenzzentrum hinausgehende Nato-Arbeitsgruppen eingebunden sind. Die jeweiligen Projekte reichen von der Entwicklung neuer Doktrinen und strategischer Konzepte und Empfehlungen, der Bewertung und Erprobung neuer Technologien bis hin zur Unterstützung und Zuarbeit für laufende Nato-Einsätze. Beispielsweise wurden im Joint Operations from the Sea COE (CJOS COE) Konzepte für die Bekämpfung von Piraten entwickelt, die aktuell vor der Küste Somalias zum Einsatz kommen. Ein Schwerpunkt liegt im Bereich „Education and Training“: Exzellenzzentren bieten häufig selbst Kurse und Weiterbildungen an und kooperieren mit Nato-Schulungseinrichtungen wie der Nato-Schule in Oberammergau. Solche Weiterbildungsmaßnahmen richten sich großteils an Militärs, es finden sich aber auch Angebote für nicht-militärische und nicht-Nato-Angehörige. Je nach Themenschwerpunkt werden auch externe Akteure und Experten einbezogen, beispielsweise wenn es um Rechtsfragen geht. Dem Zusammenführen unterschiedlicher Akteure dienen auch zahlreiche Konferenzen und Workshops, die von Exzellenzzentren veranstaltet werden und zu denen in Abhängigkeit vom Thema u. a. auch Vertreter aus Politik, Wissenschaft und Wirtschaft (häufig Rüstungsindustrie) eingeladen werden. Nicht selten tritt gerade die Rüstungsindustrie bei solchen Veranstaltungen auch als Sponsor auf. Arbeitsergebnisse werden z. T. in Form von Studien und Artikeln veröffentlicht und einzelne Exzellenzzentren publizieren regelmäßig Infobroschüren über ihre laufende Arbeit. Das Ausmaß, in dem solche Publikationen auf den jeweiligen Webseiten auch der Öffentlichkeit zugänglich gemacht werden, schwankt zwischen den einzelnen Einrichtungen teils erheblich und auch da, wo öffentlicher Zugang besteht, muss man sich vor Augen führen, dass es sich hier nur um einen sehr „ausgewählten“ Einblick handeln dürfte.

Der stetige Zuwachs an Nato-Exzellenzzentren seit 2003 auf inzwischen 24 ist beachtlich und wirft die Frage auf, welche Bedeutung diese Einrichtungen neben den offiziellen Verlautbarungen für die Nato konkret haben bzw. was genau sich hinter dieser Struktur verbirgt. Dabei ist davon auszugehen, dass der Einfluss, den die einzelnen Exzellenzzentren innerhalb der Allianz haben, verschieden ist. Das zeigt sich u. a. schon in der sehr unterschiedlichen Anzahl beteiligter Nationen, welche von einer einzelnen Nation bis hin zu 17 im Falle des JAPCC in Kalkar und des MILENG COE in Ingolstadt reichen können. Dabei bietet die Anzahl der Unterstützer einen ersten Anhaltspunkt bezüglich der Größe und des finanziellen Gewichts der Einrichtungen. So äußerte sich der ehemalige Direktor des Exzellenzzentrums Combined Joint Operations from the Sea (CJOS COE) 2008 über das Luftwaffen-Exzellenzzentrum (JAPCC) in Kalkar: „Dieses war bemerkenswert erfolgreich, in der Produktion mehrerer Joint Air Power Produkte für die Nato, von denen die meisten akzeptiert wurden und direkt in die Doktrin einflossen.”[24] Dabei dürfte die Bedeutung der einzelnen Zentren auch stark von der Relevanz ihrer jeweiligen Themenschwerpunkte für die Nato abhängen. So wird z. B. auch das Cooperative Cyber Defence Centre of Excellence (CCD COE) in Tallinn von 15 Nato-Mitgliedstaaten gefördert und setzt u. a. durch Arbeit zu einem völkerrechtlichen Rahmen für den Umgang mit Cyberangriffen, ebenso wie der Forderung nach offensiven Cyber-Kapazitäten innerhalb der Nato (Tallinn Manual) deutliche Akzente in der aktuellen Debatte zur Cyberkriegsführung.[25]

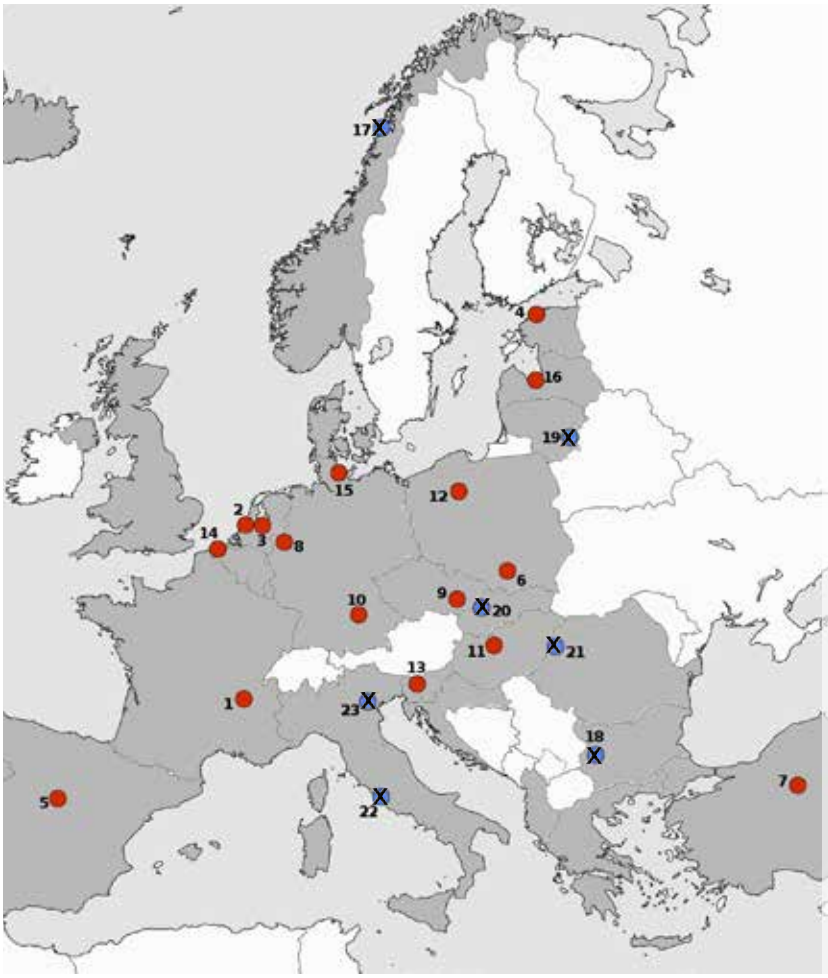
Beteiligung und Finanzierung Deutschlands

Aktuell ist Deutschland an 17 der 24 akkreditierten Exzellenzzentren als Rahmennation bzw. Sponsoring Nation beteiligt, bei dreien davon als alleinige Rahmennation: dem Joint Air Power Competence Centre (JAPCC) in Kalkar, dem Military Engineering Centre of Excellence (MILENG COE) in Ingolstadt und dem Centre of Excellence for Operations in Confined and Shallow Waters (COE CSW) in Kiel. Am Civil-Military Cooperation Centre of Excellence (CCOE) in Den Haag beteiligt sich Deutschland zusammen mit den Niederlanden als Rahmennation. Darüber hinaus betätigt es sich an 13 weiteren Exzellenzzentren als Sponsoring/Participating Nation. [26]

Die Finanzierung der Exzellenzzentren unter deutscher Beteiligung erfolgt aus Kapitel 1422 des Bundeshaushalts („Verpflichtung im Rahmen der Mitgliedschaft zur NATO und zu anderen internationalen Organisationen und Stellen“). In den Jahren 2011-2014 wurden elf Exzellenzzentren mit jährlich insgesamt ca. 900.000 bis 1 Mio. Euro finanziert. Der Anteil der vier Exzellenzzentren, die Deutschland als Rahmennation unterstützt, an den gesamten Ausgaben für COEs lag in diesem Zeitraum bei 70-80%, zwischen 2011 und 2014 waren das jährlich ca. 100.000-300.000 Euro für jedes der vier Exzellenzzentren.[27] Dabei muss berücksichtigt werden, dass die übrigen Sponsoring Nations ebenfalls ihren Beitrag leisten, das Gesamtbudget der einzelnen Zentren also deutlich höher liegt. Dies lässt sich am Beispiel des JAPCC nachvollziehen, welches in seinem jährlichen Report einen Einblick in seinen Haushalt gewährt: Seit 2007 stehen dem Exzellenzzentrum durchschnittlich ca. 950.000 € zur Verfügung, wovon der überwiegende Anteil (55-63%) unter den Posten „Reisen, Versorgung und Service“ fällt. Deutlich kleiner fallen die beiden übrigen Posten aus: Personelle Ausgaben (24-26%) und „Automated Information System (AIS)“ (12-18%).[28] Eine konkretere Aufschlüsselung lässt sich allerdings nicht finden. Im genannten Budget nicht berücksichtigt sind die Personalkosten für die von den beteiligten Staaten entsendeten Militärs. Im Fall des JAPCC und der anderen beiden in Deutschland ansässigen Einrichtungen kommt hinzu, dass die Bundesregierung ihnen die nötigen Liegenschaften kostenlos zur Verfügung stellt.

Mit einer Beteiligung an insgesamt 17 Exzellenzzentren ist Deutschland von allen Nato-Mitgliedern in die meisten dieser Einrichtungen involviert, gefolgt von Italien (15), den Niederlanden, Polen und den USA (jeweils 13) sowie Frankreich, Rumänien und Tschechien (jeweils 12). Es liegt die Vermutung nahe, dass Staaten mit einer breiten Beteiligung an verschiedenen Exzellenzzentren einen entsprechend größeren Einfluss auf den Transformationsprozess der Nato und die militärische Kommandostruktur haben. Die umfassende deutsche Beteiligung kann somit in Übereinstimmung mit dem zunehmenden militärischen Engagement Deutschlands innerhalb der Nato gesehen werden. Weiterhin ist denkbar, dass man versucht, hierüber auf die Vergabe von Aufträgen für die heimische Rüstungsindustrie einzuwirken, etwa im Rahmen der Forschung zu neuen Technologien innerhalb der Exzellenzzentren.

Um einen groben Überblick über das Spektrum der verschiedenen Exzellenzzentren zu erhalten, werden im Folgenden kurz die unterschiedlichen Einrichtungen aufgelistet und anschließend vertiefend auf zwei Exzellenzzentren eingegangen, an denen sich Deutschland als Rahmennation beteiligt.



1 - Analysis and Simulation
2 - Civil-Military Cooperation
3 - Command and Control
4 - Cooperative Cyber Defense
5 - Counter- Improvised Explosive Devices
6 - Counter Interlligence
7 - Defence Against Terrorism
8 - Joint Air Power
9 - Joint CBRN Defense
10 - Military Engineering
11 - Military Medicine
12 - Military Police
13 - Mountain Warfare
14 - Naval Mine Warfare
15 - Operations in Confined and Shallow Waters
16 - Strategic Communication
17 - Cold Weather Operations
18 - Crisis Management and Disaster Response
19 - Energy Security
20 - Explosive Ordanance Disposal
21 - Human Intelligence
22 - Modelling and Simulation
23 - Stability Policing

● mit deutscher Beteiligung
X ohne deutsche Beteiligung

Die Nato Exzellenzzentren im Überblick. Graphik: Christopher Schwitanski nach Daten der Nato

Deutschland als Rahmennation

Joint Air Power Competence Centre (JAPCC)*Standort*

Das Kompetenzzentrum für gemeinsame Luftoperationen (JAPCC) ist in den Räumlichkeiten der Von-Seydlitz-Kaserne der Bundeswehr in Kalkar untergebracht und seit seiner Akkreditierung 2005 das erste und größte Exzellenzzentrum der Nato. Dabei ist das JAPCC räumlich und organisatorisch in die Strukturen der deutschen bzw. der Nato-Luftwaffe eingebunden, woraus sich auch die Verortung der Anlage in Deutschland, insbesondere in Kalkar erklären lässt.

In der Von-Seydlitz-Kaserne befindet sich neben dem JAPCC u. a. auch das Zentrum Luftoperationen der deutschen Luftwaffe, welches an der Führung der Luftwaffe im Inland ebenso wie in Auslandseinsätzen beteiligt ist. Für letztere betreibt das Zentrum Luftoperationen auch ein verlegbares Luftwaffen-Hauptquartier (Joint Force Air Component Headquarters – JFAC HQ) zur Führung multinationaler Einsätze. In unmittelbarer Nähe zu Kalkar, im benachbarten Uedem, befindet sich das Combined Air Operations Center (CAOC) der Nato, einer von zwei taktischen Gefechtsständen der Nato-Luftwaffe in Europa und zuständig für die Überwachung des Luftraums von 14 Nato-Mitgliedsstaaten, für die hier Luftlagebilder erstellt werden. „Der Zuständigkeitsbereich reicht [damit] vom Baltikum bis nach Großbritannien und von den Alpen bis nach Island.“[29]

An das CAOC angeschlossen ist das Nationale Lage- und Führungszentrum für Sicherheit im Luftraum, in dem Soldaten der Bundeswehr, Beamte von Bundespolizei und deutscher Flugsicherung und das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe an der Überwachung des deutschen Luftraums arbeiten. Dabei besteht eine der Hauptaufgaben in der Abwehr möglicher Terrorangriffe mittels ziviler Flugzeuge.

Ebenfalls geographisch nicht weit entfernt beim Rheinland-Pfälzischen Ramstein, befindet sich das US- und Nato-Oberkommando der Luftwaffe. Während vom Standort Uedem/Kalkar aus der Luftraum nördlich der Alpen kontrolliert wird, werden von Rammstein aus Luftwaffeneinsätze südlich der Alpen befehligt.

Führt man sich die Ballung luftwaffenrelevanter Standorte der Bundeswehr und der Nato in Deutschland vor Augen, so ist die Eingliederung des JAPCC in Kalkar wenig verwunderlich, da es mit seiner Arbeit den umliegenden Einrichtungen zuarbeiten und mit diesen kooperieren kann. Begünstigt wird diese Zusammenarbeit auch durch eine gemeinsame Führungsebene, so ist der Direktor des JAPCC, General Frank Gorenc, gleichzeitig auch der Oberkommandierende der US-Luftwaffe in Europa und Afrika und der Nato-Luftwaffe in Ramstein. Der ihm untergeordnete geschäftsführende Direktor des JAPCC, Generalleutnant Joachim Wundrak, ist weiterhin der Kommandeur des Zentrum Luftoperationen der Bundeswehr und des Nato-Gefechtsstands (CAOC) im nahegelegenen Uedem.

Arbeit

Laut der offiziellen Web-Präsenz besteht der Auftrag des JAPCC in der „[…] Entwicklung innovativer Konzepte und Lösungen, benötigt für die Transformation von Air und Space Power innerhalb der Allianz und den Nationen.”[30] Etwas griffiger formuliert es die Bundeswehr-Luftwaffe auf ihrer Website, welche darauf verweist, dass die Einrichtung „in der Lage ist, Problemstellungen aus dem gesamten Spektrum der Führung und des Einsatzes von Luftkriegsmitteln erfolgreich zu bearbeiten.“[31]

Um diesen Aufgaben gerecht zu werden, wird im JAPCC an der Entwicklung neuer Doktrinen und Konzepte gearbeitet, welche thematisch nicht nur dem Bereich Luftwaffe zuzuordnen sind, sondern darüber hinaus auch den Einsatzfeldern Weltraum und Cyberspace sowie der Interoperabilität mit den übrigen Akteuren der Kriegsführung (Heer, Marine). Die konkreten Ergebnisse der einzelnen Projekte werden – soweit öffentlich nachvollziehbar – zumeist in Form von Studien und White Papers veröffentlicht. Dabei ist das Exzellenzzentrum mit zahlreichen weiteren Nato-Einrichtungen vernetzt, so heißt es im jährlich erscheinenden Bericht der Einrichtung für das Jahr 2012, Experten des JAPCC „[…] beteiligten sich aktiv an über 70 Nato-Gremien, Panels und Ausschüssen sowie als Vorsitzende von drei Nato-Arbeitsgruppen.“[32]

Zu den originär luftwaffenrelevanten Arbeitsschwerpunkten zählen z. B. Luftbetankung, Luftaufklärung, Transport von Truppen und Ressourcen und der Einsatz von Drohnen. Daneben liegt ein großer Stellenwert auf der Nutzung des Weltraums, insbesondere zur Überwachung und Informationsgewinnung, und es wird daran gearbeitet, diesen als militärisch relevantes Feld (neben Boden, See und Luft) zunehmend innerhalb der Nato zu verankern. Gleiches gilt für den Cyberspace, dessen zunehmende Bedeutung ebenfalls mit Nachdruck thematisiert wird und der (so heißt es im halbjährig erscheinenden Journal des JAPCC) neben dem Weltraum als eine „[der] fünf Domänen der Kriegsführung (Luft, Land, See, Weltraum und Cyber)“[33] verstanden wird. Auch in der Weiterentwicklung der Drohnenkriegsführung wirkt das JAPCC aktiv mit, so wurden hier u. a. Drohnen-Flugpläne und Konzepte zur Implementierung und zum Einsatz innerhalb der Nato erarbeitet und empfohlen, die Entwicklung dieser Technologie auch in Zukunft weiter voranzutreiben. Die vielen zivilen Opfer, die mit dem Einsatz von Drohnen einhergehen, oder völkerrechtliche Bedenken finden dabei kaum Beachtung. Hingegen wird die erhöhte politische Akzeptanz von Einsätzen aufgrund ausbleibender Gefährdung für die Piloten gelobt. So heißt es in einem vom JAPCC veröffentlichten White Paper zum Einsatz unbemannter Flugsysteme (Unmanned Air System - UAS) innerhalb der Nato: „[…] UAS können das Risiko senken und die politische Akzeptanz und das Vertrauen steigern, dass hochriskante Missionen erfolgreich sein werden.“[34]

Neben der Entwicklung theoretischer Konzepte wird auch konkret laufenden Nato-Einsätzen zugearbeitet. So wird z. B. der Afghanistaneinsatz mit Leitfäden für die luftgestützte Bekämpfung von Sprengfallen (IED) unterstützt oder der Anti-Piraten-Einsatz am Horn von Afrika mit Konzepten für die Luftunterstützung der Marine weitergedacht. Dabei bleibt die Arbeit nicht nur auf die Entwicklung von Leitfäden und Doktrin beschränkt, sondern es werden auch Experten in die Einsatzgebiete geschickt, um dort die Umsetzung der erarbeiteten Konzepte zu unterstützen.[35]

Weiterhin werden Veranstaltungen organisiert, um verschiedene Experten und relevante Akteure für einzelne Themengebiete zusammenzuführen. Am wichtigsten ist dabei die jährlich stattfindende Air and Space Power Conference, die von zahlreichen Rüstungskonzernen finanziert wird (u. a. Airbus, General Atomics, Thales-Raytheon-Systems) und an der 2015 ca. 200 hochrangige Militärs sowie Vertreter aus Politik und Wirtschaft teilnahmen.

Ein besonders umfangreiches Projekt stellt die 2014 erarbeitete Studie Future Vector dar, welche auch Thema der im gleichen Jahr veranstalteten Air and Space Power Conference in Kleve war. Hierfür erarbeiteten im Rahmen des „Future Vector Project“ verschiedene Nato-Experten aus dem Bereich Luft-

waffe Empfehlungen für die leitenden politischen und militärischen Führer der Nato bezüglich der zukünftigen Entwicklung der Luftwaffe innerhalb des Bündnisses. Auffällig ist dabei die Forderung nach erhöhten Rüstungsausgaben der europäischen Nato-Staaten (insbesondere für die Luftwaffe), denn: „[D]ie Fähigkeit der NATO, weiterhin Air und Space Power einzusetzen und zu erhalten, um unsere Bevölkerungen zu schützen und NATO-Einsätze zu ermöglichen, ist in Gefahr."[36] Warum der Schutz der Bevölkerung Aufgabe der Luftwaffe sein soll, die in den letzten Jahren primär fernab der Landesgrenzen von Nato-Mitgliedsstaaten eingesetzt wurde, wird nicht weiter thematisiert. Aber mit der Forderung nach erhöhten militärischen Ausgaben liegt das JAPCC ganz im Trend der Zeit, wenn man sich vor Augen führt, in welchem Ausmaß in den letzten Jahren in Deutschland die angebliche Unterfinanzierung der Bundeswehr in den Medien diskutiert wurde.

Neben der Empfehlung der Future Vector Studie, den Einsatz unbemannter Drohnen weiter voranzutreiben, ist die Forderung erwähnenswert, im Hinblick auf Russland und die Ukraine-Krise an einer Strategie der Abschreckung „basierend auf einem angemessenen Mix nuklearer und konventioneller Potenziale"[37] festzuhalten und darüber hinaus die „aktuelle Politik der nuklearen Abschreckung [der Nato] nochmals zu bekräftigen und ein zuverlässiges ‚Dual Capable Aircraft' (DCA) Potenzial in Europa beizubehalten."[38]

Hier zeigt sich also einmal mehr, dass man innerhalb der Nato von einer atomaren Abrüstung weit entfernt ist. Doch auch die Haltung gegenüber konventionellen Bomben, wie sie sich in den Veröffentlichungen des JAPCC ausdrückt, ist denkbar problematisch. So wird innerhalb des Future Vector Projects auch auf die bisherigen Nato-Einsätze und die hieraus zu ziehenden Lehren eingegangen. Ausgehend vom Jugoslawien-Krieg über den Irak-, Libyen- und Afghanistan-Krieg wird eine positive Bilanz der Luftwaffeneinsätze gezogen und ihre entscheidende Rolle für den „Erfolg" der Nato-Missionen betont. Die immensen zivilen Opfer, die Folgen zerstörter ziviler Infrastruktur und der anschließende Zerfall staatlicher Ordnung finden dagegen keinen Raum in der „kritischen" Aufarbeitung der verschiedenen Bombardierungen. Tatsächlich werden Kollateralschäden eher dahingehend problematisiert, dass sie die Unterstützung von Einsätzen innerhalb von Politik und Bevölkerung gefährdeten, anstatt dass der Tod von Zivilisten als solcher im Vordergrund steht. Diese Tendenz findet ihren Ausdruck auch in einer aktuellen Studie des JAPCC („Mitigating the Disinformation Campaigns against Airpower"), die sich der Frage widmet, was man gegen „Desinformationskampagnen" unternehmen könne, welche die Akzeptanz der Luftwaffe gefährden, wie z. B. falsche Informationen über zivile Opfer, welche u. a. die Ablehnung von Luftangriffen in Auslandseinsätzen oder des Einsatzes von unbemannten Drohnen zur Folge hätten. Untersuchungen zur Einstellung der Bevölkerung zeigten demnach, dass insbesondere in Deutschland große Vorbehalte gegenüber dem Einsatz der Luftwaffe bestehen (im Unterschied zu den USA und Großbritannien), ein Umstand, der darauf zurückgeführt wird, dass pazifistische Überzeugungen in Deutschland infolge des Zweiten Weltkrieges besonders ausgeprägt sind: „[…] die Deutschen sind deutlich empfänglicher für Desinformations-Kampagnen und anti-militärische Kampagnen als die meisten anderen NATO-Nationen."[39] Ausgehende von der Problematik mangelnder Unterstützung, werden Vorschläge gemacht, wie die Kommunikation von Kriegseinsätzen verbessert werden kann, um deren Akzeptanz zu erhöhen und gegnerischen „Falschinformationen" offensiv entgegenzuwirken.

Die Bedeutung dieses Themas für die Nato-Luftwaffe wird dadurch unterstrichen, dass es auch von der letzten Air and Space Power Conference aufgegriffen wurde, welche unter dem Titel „Air Power and Strategic Communication – Nato Challenges for the Future" 2015 in Essen stattfand. Hier lag der Fokus auf strategischer Kommunikation als Mittel, um unliebsamen Überzeugungen in der Bevölkerung zu begegnen. Im Vorfeld der Konferenz veröffentlichte das JAPCC – in Zusammenarbeit mit dem Exzellenzzentrum für strategische Kommunikation (StratCom COE) in Riga – einen Einführungstext, welcher die Teilnehmenden auf das Thema einstimmen und zum Nachdenken anregen sollte. Darin findet sich u. a. folgende Äußerung: „Die Lawfare Bewegung, welche zivile Verluste als Rechtfertigung nutzt, hat nicht nur Luftmunitionen, die für zukünftige Konflikte benötigt werden, verboten (Streubomben sind sehr wichtig, wenn ein Feind bekämpft wird, der als konventionelle Kraft organisiert ist), sondern versucht auch die Regel zu etablieren, dass JEDER Verlust von Zivilisten oder ziviler Kollateralschaden ein Kriegsverbrechen ist. Die NATO wird alle verfügbaren Ressourcen nutzen, um zivile Verluste zu vermeiden."[40] Der Hinweis, die Nato werde alle Ressourcen nutzen, um zivile Opfer zu vermeiden, kann nur noch als verlogen bezeichnet werden, wenn im vorangegangenen Satz die Notwendigkeit von Streubomben betont wird – Kriegsmittel, die nicht umsonst wegen der Verursachung grausamer Verletzungen, unter denen größtenteils die Zivilbevölkerung leidet, inzwischen von über 100 Staaten – darunter auch Deutschland – geächtet werden. Die Argumentation, mit der die Akzeptanz der Nato-Luftwaffe verbessert werden soll, ist, wie das vorherige Beispiel zeigt, perfide. Die Kritik der Gegner von Luftwaffeneinsätzen und besonders an deren hohen zivilen Opferzahlen wird als illegitim und falsch dargestellt, diese Argumentation diene primär dazu, die Luftwaffe zu schwächen. Auf diesem Weg werden zivile Opfer auf eine bloße instrumentelle Argumentationshilfe von Kriegsgegnern reduziert, anstatt das kaum zu ermessende menschliche Leid, das (Bomben-)Kriege mit sich bringen, zu problematisieren und hierfür Verantwortung zu übernehmen. Wichtiger als die Vermeidung ziviler Opfer scheint tatsächlich die Vermeidung einer entsprechenden Berichterstattung. Es bleibt zu hoffen, dass „die Deutschen"[41] auch in Zukunft ihre kritische Haltung gegenüber Lufteinsätzen bewahren bzw. diese ungeachtet von strategischen Bemühungen um eine bessere Reputation der Luftwaffe noch zunimmt.

Centre of Excellence for Operations in Confined and Shallow Waters (COE CSW)

Standort

Eingerichtet auf Initiative Deutschlands, befindet sich das Exzellenzzentrum für Einsätze in begrenzten und seichten Gewässern (Operations in Confined and Shallow Waters – CSW) an einem der zentralen Standorte der deutschen Marine, dem Marinestützpunkt in Kiel am Tirpitzhafen. Hier befindet sich das Exzellenzzentrum im Stabsgebäude der Einsatzflottille 1, welche ebenfalls für maritime Operationen in Küstengewässern und Randmeeren zuständig ist. Vor diesem Hintergrund sind ihr primär kleine bewegliche Einheiten zugeordnet, wie z. B. Schnellbootgeschwader, Minensuchgeschwader, U-Boot-Geschwader und auch das Kommando Spezialkräfte Marine (SEK M). Neben der Einsatzflottille 1 sind am Standort Kiel auch die Minensucher der Marine und die Forschungsanstalt der Bundeswehr für Wasserschall und Geophysik ansässig.[42] Man kann davon ausgehen, dass zwischen dem Exzellenzzen-

trum und der Einsatzflottille 1 eine enge Kooperation besteht, dies zeigt sich nicht nur in der räumlichen und inhaltlichen Überlappung, sondern auch auf der Führungsebene: Der Direktor des COE CSW ist gleichzeitig der Kommandeur der Einsatzflottille 1.

Arbeit

Was die Rolle des Exzellenzzentrums betrifft, so unterstreicht es auf seiner offiziellen Website die Bedeutung seiner Arbeit mit dem Hinweis, dass 70% der Erdoberfläche mit Wasser bedeckt sind, 80% der Weltbevölkerung in Küstennähe leben und 90% des internationalen Handels zur See erfolgen.[43] Berücksichtigt man darüber hinaus die enorme Bedeutung des maritimen Außenhandels für die deutsche Wirtschaft[44] – woraus die Bundeswehr-Marine ableitet, dass die „Maritime Sicherheit […] für Deutschland lebenswichtig"[45] sei – so ist es wenig verwunderlich, dass Deutschland sich hier als Rahmennation beteiligt. Weiterhin kommt eine vom Exzellenzzentrum angefertigte Studie zu dem Ergebnis, dass die zu erwartende Zunahme des globalen Handels „[i]nsbesondere in den folgenden Regionen: Intra-Fernost; zwischen Fernost und Ozeanien, Lateinamerika und dem Mittleren Osten […] die Bedeutung der zentralen internationalen Schifffahrtsrouten weiter erhöhen [wird], welche unweigerlich durch CSW führen, da sie unverzichtbare Verbindungen zwischen den (bedeutenden) Häfen ebenso wie den (Mega-)Städten sind. Daher ist die Sicherung dieser SLOCS [Sea Lines of Communication] in CSW-Umgebung essenziell."[46] Demnach wird also auch in Zukunft eine zentrale Aufgabe der Marine in der militärischen Sicherung von Handelswegen bestehen, hier mit spezifischem Fokus auf seichte und Küstengewässer.

Neben solchen grundlegenden Argumenten für die gewichtige Rolle der Marine umfassen die Arbeitsschwerpunkte des Exzellenzzentrums verschiedene Projekte wie die Entwicklung rechtlicher Rahmenbedingungen für zukünftige Marineeinsätze, die Bekämpfung von Seeminen und improvisierten Sprengfallen im Wasser (auch mittels Autonomer Unterwasser-Fahrzeuge (AUV)), Konzepte für die Bekämpfung von Piraterie und die Verknüpfung mit verschiedenen weiteren Domänen wie Luftwaffe, Cyberspace und Weltraum.

Im Rahmen dieser Projekte kooperiert das CSW einerseits mit zahlreichen Einrichtungen der Nato, insbesondere mit dem in den USA beheimateten maritimen Exzellenzzentrum Combined Joint Operations from the Sea (CJOS COE) und der Bundeswehr, darüber hinaus bestehen auch Kooperationen mit dem Institut für Transformationsstudien der Europäischen Universität Viadrina in Frankfurt Oder und dem Institut für Sicherheitspolitik der Universität Kiel (ISPK; siehe auch Kiel-Konferenz weiter hinten im Text).

Einen interessanten Einblick in die zukünftigen Einsatzbereiche der Nato-Marine in Küstengewässern und damit die Arbeitsschwerpunkte des Exzellenzzentrums bietet ein dort entwickeltes Arbeitspapier mit dem Titel „Zukünftige Einsätze in begrenzten und seichten Gewässern", in dem globale Entwicklungen und ihre Folgen für die Küstenregion als „Schlachtfeld" diskutiert werden. In diesem Dokument finden sich einige interessante Passagen bezüglich der antizipierten „Herausforderungen" der Zukunft. Zunächst wird bezüglich der urbanen Entwicklung Folgendes festgestellt: „Städte werden bis 2040 65% der Weltbevölkerung beherbergen. Die Mehrheit dieser konzentrierten städtischen Cluster wird sich in der Nähe oder direkt an der Küste in Ufernähe und damit in Nähe zu CSW befinden."[47] Damit befinden sich Großstädte also im potentiellen Einsatzgebiet von Marine-Operationen und gerade in Städten wird von einer Verschärfung von Konflikten ausgegangen: „Verknappung lebensnotwendiger Ressourcen, gescheiterte Infrastruktur, erhöhte Wahrscheinlichkeit ansteckender Krankheiten und Einkommensunterschiede könnten zu Unzufriedenheit und gesteigerter Kriminalität bis hin zu zivilen Unruhen in urbanen Gebieten führen. Folglich werden möglicherweise Marine-Kräfte benötigt, um Friedens-Unterstützung, humanitäre Hilfe und Stabilisierungs-Einsätze in städtischer Umgebung in der Nähe von und innerhalb von CSW zu leisten."[48] Die hier bereits angesprochene globale Ungleichheit, insbesondere in der Verteilung lebenswichtiger Ressourcen wird noch weiter ausgeführt: „[D]ie wachsende Nahrungsnachfrage bleibt ein lebensnotwendiges Thema für die Menschheit, während Hunger und Unterernährung zentraler Antrieb für Unruhen, Aufstände und Revolten sind, welche leicht Gebiete mit geschwächter Regierung bis hin zu gescheiterten Staaten hinterlassen."[49]

Dass eine Vielzahl der Marine-Einsätze dem Schutz von Handelswegen und damit der westlichen Wirtschaft dient, ist inzwischen fast schon eine Binsenweisheit. Die zuvor zitierten Passagen machen darüber hinaus deutlich, dass man sich der verheerenden Folgen einer ungleichen globalen Verteilung von Wohlstand bis hin zu lebenswichtigen Ressourcen wie Nahrung und Trinkwasser auch in militärischen Kreisen wohl bewusst ist und diese auch konkret benennt. Das eigentliche Problem wird dabei aber nicht angegangen: anstatt die Politik und das System, welches solch ein Ungleichgewicht produziert, zu hinterfragen und politische Lösungen anzustreben, sieht man hierin bloß den Rahmen zukünftiger militärischer Interventionen. Diese werden an den eigentlichen Problemen nichts ändern, sondern im Gegenteil auch weiterhin eben jene Strukturen stützen, die für das globale Elend mitverantwortlich sind.

Um den anstehenden Entwicklungen auf einem „Schlachtfeld steigender Komplexität" zu begegnen, empfiehlt das COE CSW: „Innovative Technologien wie künstliche Intelligenz, intelligente Netzwerke, fortgeschrittene Computertechnologie, Automation, Miniaturisierung, Nanotechnologie, Robotik, Bionik, generative Fertigung und fortschrittliche Schiffbau-Technologien müssen hinsichtlich ihres Potentials, operative Anforderungen in CSW zu unterstützen, bewertet werden."[50] Es ist anzunehmen, dass eine kritische Berücksichtigung möglicher damit einhergehender gesamtgesellschaftlicher Risiken (sofern sie überhaupt stattfindet) bei der Bewertung derartiger Technologien durch eine Einrichtung wie das COE CSW zu kurz kommen wird. Passend stellte man in der abschließenden Veröffentlichung der Kiel-Konferenz bezüglich autonomer U-Boote fest: „Von diesen wird erwartet, dass sie bald bis zu 6.000 t schwer sind und einen Einsatzradius von über 7.500 Seemeilen haben, inklusive der Fähigkeit, automatisch Ziele anzugreifen, ohne dass dabei ein Soldat involviert ist. In den Augen europäischer Staaten bringt ein solcher Einsatz potentielle ethische und rechtliche Probleme mit sich, während die USA, Russland oder China mit solchen Themen anscheinend offener umgehen."[51]

Teil der Arbeit des COE CSW ist die Organisation verschiedener Konferenzen, hierzu gehört u. a. die Conference on Operational Maritime Law, die Maritime Security Conference in Zusammenarbeit mit dem CJOS COE und die vom COE CSW und dem Institut für Sicherheitspolitik der Universität Kiel im Juni 2015 erstmals ausgerichtete Kiel-Konferenz. Auf dieser trafen sich rund 80 internationale Experten aus den Bereichen Militär, Politik, Wissenschaft und Wirtschaft. Zukünftig wollen die Veranstalter die Konferenz dauerhaft in der Kieler Woche verankern und auf lange Sicht als maritimes Pendant

zur Münchener Sicherheitskonferenz etablieren. Offizielles Thema ist die maritime Sicherheit mit wechselnden regionalen Schwerpunkten. In der ersten Konferenz lagen diese auf der Ostsee und dem Umgang mit dortigen Seeminen. Im abschließenden Bericht der Konferenz wird u. a. auf die Bedrohung der Ostsee-Anrainerstaaten durch die angeblich zunehmenden militärischen Aktivitäten Russlands eingegangen: „Neben wiederholten aggressiven russischen Signalen ist die erhöhte Präsenz russischer Mittel für den Transport nuklearer Waffen in der Region […] besonders besorgniserregend.“[52] In diesem Zusammenhang werden zwar auch „kritische“ Stimmen erwähnt, die die Bedrohungslage weniger problematisch einschätzen, der Grundtenor spiegelt sich aber beispielhaft in Überlegungen, wie, „[…] ob und in welchem Ausmaß das Konzept der Abschreckung mit nuklearem Schwerpunkt, angesichts einer neuen Facette russischer Militärstrategie hybrider Natur, tragfähig ist.”[53] Diese mündet wie so oft in der Forderung, die westlichen Militärausgaben weiter anzuziehen: „Westliche Staaten scheinen kontinuierlich die Beschneidung ihrer Verteidigungs-Anstrengungen fortzusetzen, primär aufgrund von Budget-Beschränkungen, anstatt sie der steigenden aktuellen Bedrohung anzupassen.”[54] Eine differenzierte Betrachtung der Rolle beider Seiten, wozu auch eine Problematisierung der massiven Aufrüstung der Nato-Ostflanke, der Nato-Präsenz im Schwarzen Meer und zahlreicher Nato-Manöver gehören müsste, sucht man hingegen vergeblich. Wenn man sich eine derart einseitige militärische Herangehensweise an mögliche Konflikte in der Ostsee vor Augen führt, scheint es absurd, dass der zweite Veranstalter neben dem CSW, das Institut für Sicherheitspolitik der Universität Kiel, auf seiner Website schreibt, es sehe sich dem Motto der Universität „[…] ‚Der Frieden ist das wichtigste Gut‘, zutiefst verpflichtet.“[55] Neben der Beteiligung an der Kiel-Konferenz macht auch die Arbeit des Instituts die Widersprüchlichkeit dieses Mottos deutlich, so wurde etwa für das Bundesministerium für Verteidigung eine Studie über die Effektivität der Aufstandsbekämpfung in Afghanistan und vergleichbarer Einsätze erstellt. Wirft man weiterhin einen Blick auf die Institutsleitung, so wird die Nähe des Instituts zum Militär noch deutlicher. Prof. Dr. Joachim Krause wird u. a. mit folgenden Einschätzungen zur Ukraine-Krise zitiert: „Besser wäre eine Politik, die auf Eskalationsdominanz zielt und dabei auch realistische militärische Maßnahmen nicht ausschließt. Dazu können Waffenlieferungen an die Ukraine ebenso gehören wie amerikanische Luftunterstützung für die Ukraine im Kampf gegen irreguläre Truppen […].“[56]

Betrachtet man diese aggressive Rhetorik und die Arbeitsschwerpunkte des ISPK, so überrascht die Zusammenarbeit der beiden Einrichtungen wenig. Vielmehr scheinen sich zwei „Partner im Geiste“ gefunden zu haben. Denn genauso wenig wie das ISPK folgt das Exzellenzzentrum für Einsätze in begrenzten und seichten Gewässern dem Motto „Der Friede ist das wichtigste Gut“. Anstelle des Friedens steht vielmehr die militärische Wahrung einseitiger (Sicherheits-)Interessen in den Küstenregionen der Welt im Vordergrund.

Fazit

Die im vorliegenden Artikel getroffene Auswahl der zwei von Deutschland als Rahmennation geförderten Exzellenzzentren bildet nicht das vollständige Spektrum aktiver Nato-Exzellenzzentren ab. Sie bietet vielmehr einen ersten Anhaltspunkt dafür, wie die eingangs geschilderten Arbeitsprinzipien und Schwerpunkte dieser wachsenden Nato-Struktur konkret aussehen können und ermöglicht einen Einblick in die militärische Logik, auf Basis derer sich in den jeweiligen Denkfabriken mit verschiedenen Themen befasst wird. Abschließend sollen hiervon ein paar wiederkehrende Aspekte kurz zusammengefasst werden.

Bemerkenswert ist zunächst die Bewertung vergangener Konflikte unter Nato-Beteiligung. Dabei ist es geradezu symptomatisch, dass der Fokus ausschließlich auf kurzfristigen militärischen Erfolgen liegt – die enorme Anzahl ziviler Opfer und die anhaltenden strukturellen Folgen zerstörter Infrastruktur werden dagegen nicht berücksichtigt. Eine solche unreflektierte Betrachtung spiegelt sich auch in der Auseinandersetzung mit sogenannten gescheiterten oder instabilen Staaten wider. Unabhängig von der Frage, ob eine derartige Einteilung von Staaten sinnvoll ist, gilt es anzumerken, dass diese als aktuelle und zukünftige Problemherde gesehen werden. Die eigene Mitverantwortung für den Zustand einzelner Länder infolge von Nato-Interventionen oder westlicher Außen- und Wirtschaftspolitik findet dabei allerdings systematisch keinerlei Berücksichtigung. Dementsprechend werden zu erwartende Konflikte aufgrund zerstörter Staaten, Armut und globaler Ungleichheit, wie sie in verschiedenen Publikationen vorhergesagt werden, ausschließlich als potentielle Schauplätze zukünftiger Kriegseinsätze bewertet.

Um auf diese vorbereitet zu sein, wird sowohl vom JAPCC als auch vom COE CSW die für die Nato schon als symptomatisch zu bezeichnende Forderung nach höheren Investitionen in die jeweilige Streitkräfte-Gattung vorgetragen. Die parlamentarische Kontrolle der Haushalte und gesellschaftspolitischen Umstände wie massive Verschuldung und Sparzwang – verschärft nicht zuletzt in Folge der Finanzkrise – werden dabei völlig ignoriert, ebenso wie die bereits laufenden, massiven Rüstungsausgaben der einzelnen Staaten oder der Nato als Ganzes. Sowohl die internationale Beteiligung an bereits bestehenden Exzellenzzentren als auch die fortlaufende Akkreditierung neuer Anlagen vermag einen ersten Aufschluss über das Gewicht der jeweiligen Themenschwerpunkte innerhalb der Allianz zu bieten. So drückt sich der aktuelle Ausbau von Kompetenzen im Bereich „Strategischer Kommunikation“ innerhalb der Nato auch in der Einrichtung des eigens hierfür zuständigen Exzellenzzentrums aus, welches Anfang 2014 im litauischen Riga seine Arbeit aufnahm. Dabei bleibt die strategische Kommunikation nicht auf die Tätigkeit des StratCom COE beschränkt, sondern findet sich ebenso in der Arbeit des JAPCC. Führt man sich in diesem Zusammenhang vor Augen, wie die Planungen bezüglich des kommunikativen Umgangs u. a. mit zivilen Opfern von Luftschlägen aussehen, so wird einmal mehr deutlich, was sich eigentlich hinter diesem Begriff verbirgt: militärische Propaganda mit dem Ziel, die Akzeptanz der eigenen Position in der Öffentlichkeit zu erhöhen.

Der in den Exzellenzzentren der Nato betriebene Militarismus beschränkt sich nicht auf die einzelnen Einrichtungen, sondern wird von diesen auch offensiv nach außen, in ihr ziviles Umfeld getragen und zeigt sich im Ausmaß, in dem sich darum bemüht wird, die Zivilgesellschaft in die jeweiligen Aktivitäten mit einzubeziehen. Während dieser Aspekt im Fall des Civil-Military Cooperation Centre of Excellence bereits im Namen der Einrichtung deutlich wird, sind auch die übrigen Exzellenzzentren nicht untätig, sei es durch zivile Gäste auf Konferenzen, Veranstaltungen, die gezielt die Zivilgesellschaft einbinden, oder Kooperationen mit verschiedenen Universitäten.

Die Fragesteller, der in der Einleitung erwähnten kleinen Anfrage, äußerten die Sorge, es könne sich bei den Nato-Ex-

Proteste bei der Kieler Woche. Quelle: warstartsherekiel.noblogs.org

zellenzzentren um eine Struktur handeln, die abseits von militärischer Befehlskette, politischer Kontrolle und kritischer Öffentlichkeit eine offensivere Nato-Doktrin vorantreibt, in welcher das Völkerrecht kaum Beachtung findet. Abschließend lässt sich sagen, dass diese Sorge nicht nur berechtigt ist, sondern die Problematik noch deutlich weitergeht. Wie die ausgewählten Publikationen der einzelnen Exzellenzzentren zeigen, findet die Entwicklung offensiver Doktrinen bereits innerhalb der COEs statt. Seien es Empfehlungen des JAPCC zu Abschreckungspotentialen atomarer Waffen und Weiterentwicklung von Drohnentechnologie oder die Überlegungen des COE CSW bezüglich zukünftiger Einsätze in Küstengewässern: Es lässt sich sagen, dass es sich hier in Übereinstimmung mit dem derzeitigen Vorgehen der Nato nicht um Planungen zur Landesverteidigung, sondern um Interventionen außerhalb des Bündnisgebiets handelt. Aber auch die Arbeit des CCOE und des MILENG dienen u. a. der gezielten Unterstützung von Auslandseinsätzen, die CIMIC-Doktrinen im Rahmen der „vernetzten Sicherheit“ beispielsweise sind derzeit wohl kaum zur Aufstandsbekämpfung in Europa oder Nordamerika gedacht.

Mit verschiedenen Konzepten und Planungen zukünftiger Einsatzfelder in internationalen Krisenherden wird der ideologische Boden für weitere Nato-Einsätze bereitet und gleichzeitig durch die vermehrte Einbeziehung der Zivilgesellschaft höhere Akzeptanz für diese angestrebt. Der Fokus liegt dabei primär auf der militärischen „Lösung“ internationaler Konflikte und Probleme, mögliche politische Lösungen werden dagegen ebenso ausgespart wie die finanzpolitische Situation einzelner Mitgliedstaaten. Diese Entwicklung ist bedenklich, da auf diesem Weg suggeriert wird, dass Konflikte primär mit militärischen Mitteln gelöst werden könnten und so ein einseitiger außenpolitischer Diskurs gefördert wird, der politische und zivile auf Kosten von militärischen Lösungen verdrängt. Diese Tendenz, einer Abkehr vom Politischen zugunsten des Militärischen zeigt sich in den letzten Jahren auch zunehmend in der deutschen Außenpolitik. Zwar liegt der Ursprung dessen nicht in den Nato-Exzellenzzentren, aber sie erweisen sich als Förderer einseitiger militärischer Ideologie, die in außenpolitischen Fragen das Primat des Militärischen vertritt, das durch zahlreiche Veranstaltungen an Politik und Zivilgesellschaft herangetragen und mittels strategischer Kommunikation auch zunehmend in den medialen Diskurs gebracht wird.

Diese Entwicklungen innerhalb einer Struktur von Exzellenzzentren, deren Ziel ausdrücklich darin besteht, den Transformationsprozess der Nato zu befördern, macht deutlich, in welche Richtung sich die Nato konsequent entwickelt: Hin zu einem zunehmend offensiven und aggressiven militärischen Interventionsbündnis, eine Tendenz die auch in der seit einiger Zeit beliebten Bezeichnung 360°-Nato deutlich wird. Konkret äußerte sich hierzu der General der Deutsch-Niederländischen Brigade mit dem Hinweis, die Nato müsse „einen 360-Grad-Blick [haben], also rundherum. Und sich darauf einstellen, in allen möglichen denkbaren Einsatzgebieten und in allen denkbaren Einsatzszenarien eingesetzt zu werden. Das sagt sich einfach, ist aber schwer umzusetzen.“[71] Bei der Erleichterung dieser Umsetzung dürften die Nato-Exzellenzzentren ein geeignetes Mittel darstellen.

Man sollte sich daher keinen Illusionen über die Natur der Nato hingeben. Auch wenn sie sich laut Selbstdarstellung als Verfechter demokratischer Werte der friedlichen Lösung von Konflikten verschrieben hat, handelt es sich um ein militärisches Interventionsbündnis, dessen Einsätze den Interessen seiner Mitglieder dienen und von friedlichen Lösungen und demokratischen Werten meilenweit entfernt sind.

Glücklicherweise gehen diese Entwicklungen nicht ganz unbemerkt vonstatten. Sowohl gegen einzelne Nato-Exzellenzzentren als auch gegen die von diesen ausgerichtete Veranstaltungen regt sich in den letzten Jahren Widerstand. 2015 formierte sich in Kiel ein breites Bündnis aus regionalen politischen, gewerkschaftlichen und universitären Gruppen gegen die Kiel-Konferenz, die im Rahmen des Volksfests „ Woche“ vom Center of Excellence for Operations in Confined and Shallow Waters und dem Institut für Sicherheitspolitik an der Universität Kiel abgehalten wurde. Unter dem Motto „War starts here – Keine Kriegs-Konferenz in Kiel!“ wurde zur Demonstration gegen die Veranstaltung aufgerufen. Ein Aufruf, dem über 400 Menschen folgten und der sich neben der Konferenz auch gegen die Kooperation der Universität mit militärischen Einrichtungen wie dem COE CSW richtete.

Im gleichen Jahr folgten über 700 Demonstrierende dem Aufruf „Kein Nato-Kriegsrat in Essen“, der sich gegen die dort stattfindende Konferenz des Joint Air Power Competence Centre (JAPCC) richtete und u. a. „[k]eine Nato-Planung neuer Kriege – Kein Werben fürs Inferno!“ forderte sowie die „Abschaffung des JAPCC und umfassende Aufklärung der Öffentlichkeit!“.

Man kann nur hoffen, dass diese Proteste in den kommenden

Jahren noch zunehmen und gerade Veranstaltungen wie die Kiel-Konferenz, die als maritime Sicherheitskonferenz etabliert werden soll, in Zukunft wachsendem Widerstand gegenüberstehen.

Der vorliegende Artikel ist eine gekürzte Version der IMI-Studie 6/2016, aufzurufen unter: www.imi-online.de

Anmerkungen

1 Alternativ auch Kompetenzzentren. Im Folgenden wird der Begriff Exzellenzzentrum sowie die englische Abkürzung COE gleichbedeutend verwendet.
2 Aktuelle existieren 23 akkreditierte Exzellenzzentren und das Counter Intelligence Centre of Excellence (CI COE) befindet sich im Akkreditierungsprozess (Stand April 2015). Es ist anzunehmen, dass auch hier die Akkreditierung erfolgen wird, daher wird im Text von 24 Exzellenzzentren gesprochen und keine weitere Differenzierung vorgenommen.
3 Deutscher Bundestag, Drucksache 18/4567, dip21.bundestag.de, 09.04.2015
4 Nato Press Releases: Prague Summit Declaration, nato.int, 21.11.2002
5 Nato: Topics. Allied Command Operations, nato.int, 11.11.2014
6 Nato: Topics. Allied Command Transformation, nato.int, 11.11.2014
7 Structure of NATO, Wikipedia.org
8 Nato Press Releases: Final Communiqué - Ministerial Meeting of the Defence Planning Committee and the Nuclear Planning Group held in Brussels on Thursday, nato.int, 12.06.2003
9 NATO Lessons Learned Portal: Centres of Excellence, nllp.jallc.nato.int
10 Zdenek Hybl und Zelenák János: Centres of Excellence, portal.zmne.hu, 2001
11 Drucksache 18/4567, 09.04.2015
12 Hierbei handelt es sich um 22 europäische und asiatische Staaten, die in unterschiedlichem Ausmaß militärisch in die Nato eigebunden sind. Ausgewählten Mitgliedsstaaten kann das PfP u. a. als Vorstufe zu einer Nato-Mitgliedschaft dienen.
13 Guy B. Roberts: NATO's Centers of Excellence: A Key Enabler in Transforming NATO to Address 21st Century Challenges, stanleyfoundation.org, 08.10.2014
14 Ebd.
15 Ministry of National Defence Republic of Lithuania: News releases. Georgia joins NATO Energy Security Centre of Excellence in Vilnius, kam.lt, 17.10.2014
16 Drucksache 18/4567, 09.04.2015, S. 14
17 Roberts: NATO's Centers of Excellence, 2014
18 Streitkräftebasis: Vernetztes Wissen. Das ABC-Abwehr-Kompetenzzentrum in Tschechien, kommando.streitkraeftebasis.de, 18.03.2014
19 Roberts: NATO's Centers of Excellence, 2014
20 NATO Lessons Learned Portal: Communities, nllp.jallc.nato.int
21 Hybl und János: Centres of Excellence, 2001
22 Ebd.
23 Ebd.
24 Department of the Navy information technology magazine CHIPS: Q&A with Royal Navy Commodore R. J. Mansergh Deputy Director, U.S. Second Fleet. Combined Joint Operations from the Sea Center of Excellence, CHIPS Magazine, July-September 2008, S. 11
25 siehe z. B.: James A. Lewis: The Role of Offensive Cyber Operations in Nato's Collective Defence, Tallinn Paper No. 8, CCD COE, ccdcoe.org, 2015
26 NATO Lessons Learned Portal: Centres of Excellence, nllp.jallc.nato.int
27 Die genannten Zahlen ergeben sich aus der Antwort der Bundesregierung auf die kleine Anfrage der Linken (Drucksache 18/4567). Die gesamten Ausgaben dürften inzwischen deutlich höher liegen, da Deutschland seit besagter Anfrage Anfang 2015 sechs weitere Exzellenzzentren finanziell unterstützt.
28 Siehe JAPCC-Reports 2008-2015
29 So Brigadegeneral Nolte gegenüber der Rheinischen Post. (Marc Cattelaens: Der Luftwaffenstandort Kalkar wächst, rp-online.de, 06.03.2014)
30 Joint Air Power Competence Center: About JAPCC, japcc.org
31 Bundeswehr Luftwaffe: Joint Air Power Competence Centre, luftwaffe.de
32 JAPCC Report 2012, japcc.org
33 JAPCC Journal Edition 17, Spring/Summer 2013, japcc.org, S. 44
34 White Paper 2010-01: Strategic Concept of Employment for Unmanned Aircraft Systems in NATO, japcc.org, S. 2
35 JAPCC: Report 2011, japcc.org
36 JAPCC: Future Vector Project, Present Paradox – Future Challenges 2014, japcc.org, S. 61
37 JAPCC: Air & Space Power in Nato – Future Vector Part I, japcc.org, Juli 2014, S. 70
38 Ebd.
39 JAPCC: Read Ahead, Air Power and Strategic Communications – NATO Challenges for the Future, japcc.org, 2015, S. 35
40 Ebd., S. 46 f.
41 So die Formulierung in der Studie Mitigating the Disinformation Campaigns against Airpower
42 Attac-Kiel, Avanti-Kiel, GEW-Kreisverband Kiel: Militär und Rüstung in Kiel - antimilitaristische Stadtrundfahrt, gegenwind.info, 2014
43 COECSW: OUR COE: Our Expertise, coecsw.org
44 Laut Jahresbericht der Marine zur maritimen Abhängigkeit Deutschlands - Zusammenfassung 2015:
„Der Export hatte hier mit 76,26 Mio. t zwar nur einen Mengenanteil von 31,3%, erzielte aber mit 283,3 Mrd. € einen Wertanteil von 62,2 %"
45 Bundeswehr Marine: Der Auftrag der Marine, marine.de
46 COE CSW: Study Paper (First Edition) on Prospective Operations in Confined and Shallow Waters, coecsw.org, 2015, S. 22
47 Ebd., S. 2
48 Ebd.
49 Ebd., S. 3
50 Ebd., S. 4
51 COE CSW: Kiel Conference 2015 Baltic Sea Focus – Conference Documentation, kielconference.com, S. 22
52 Ebd., S. 12
53 Ebd., S. 15
54 Ebd., S. 14
55 Institut für Sicherheitspolitik: Kiel Conference, ispk.uni-kiel.de
56 Prof. Dr. Joachim Krause: Droht der „große Krieg"? Erschienen in der FAZ am 04.09.2014 „Fremde Federn"
57 Standort Ingolstadt wird ausgebaut, onetz.de, 17.09.2008
58 European Security and Defense, 5/2015
59 Ebd., S. 41
60 The Transformer: Vol. 2, Issue 3, act.nato.int, Oktober 2006
61 CIMIC Messenger Vol. 6 Issue 4, cimic-coe.org, 2014
62 Drucksache 18/4567, S.11
63 Nato: Topics. A ‚comprehensive approach' to crises, nato.int
64 MC 411/1 NATO Military Policy on Civil-Military Cooperation, nato.int
65 Venro-Postitionspapier, 7/2009
66 Ebd.
67 Michael Paul: CIMIC in the ISAF Mission – Conception, Implementation and Development of Civil-Military Cooperation in the Bundeswehr Abroad, swp-berlin.de, April 2009, S. 23
68 Siehe hierzu auch die IMI-Studie 2015/10: Benjamin Hirschfeld: Ethnologie im Kriegseinsatz - Die Geschichte einer Zusammenarbeit zwischen Wissenschaft, Geheimdiensten und Militär
69 Nato CIMIC-Doktrin: AJP 3.4.9, cimic-coe.org, Februar 2013, S. 42
70 CIMIC Messenger Vol. 6, Issue 5, cimic-coe.org, Dezember 2014
71 Informationen am Morgen: Abschreckung mit Mängeln, deutschlandfunk.de, 28.12.2015.

Drohnenkrieg

Die Weitergabe von Handydaten

von Marius Pletsch

In der Anhörung von Zeugen des Bundesamtes für Verfassungsschutz im NSA-Untersuchungsausschuss im Bundestag vom 28. April 2016 ging es unter anderem auch um die Weitergabe von Handydaten, die von deutschen Diensten erhoben wurden, an ausländische Stellen (siehe auch einen Artikel „NSA-Ausschuss und Drohnenkrieg“ bei Heise.de, 29.4.16). Die beiden Zeugen vom Bundesamt für Verfassungsschutz (BfV) räumten ein, dass ihre Dienststelle Handydaten an US-Stellen weitergab und immer noch weitergibt. Diese Daten spielen für die Zielfindung im US-Drohnenkrieg eine wichtige Rolle.

Eine Handynummer reicht aus, damit eine Rakete oder Bombe ihren Weg ins Ziel finden kann. Zum einen ist da das Programm Skynet zu nennen, das Metadaten auswertet und anhand von besuchten Orten, kontaktierten Personen und weiterer Muster (z.B. große Menschenansammlungen), die als verdächtig gelten, diejenigen Nummern nennt, die zu Terrorverdächtigen gehören könnten. Diesen Prozess nennt man auch Data-Mining. Auf Basis dieser Daten, die von einem Algorithmus berechnet werden, werden dann die Ziele definiert und nicht selten auch getötet. Der Name des Verdächtigen muss dabei nicht bekannt sein; nur, weil er sich vielleicht verdächtig verhält, könnte er bereits Opfer eines Drohnenangriffs werden. Und die Genauigkeit des Algorithmus wird angezweifelt. So ist die Befürchtung, dass zehntausende Nummern fälschlicherweise als terrorverdächtig klassifiziert werden. Das hat ein Informatiker für den Technikblog ArsTechnica.co.uk (16.2.16) hervorgehoben (auch c’t 3/2016 beschäftigte sich mit dem Programm Skynet und dem Data-Mining für den Drohnenkrieg). Je nach Fehlerwahrscheinlichkeit werden allein in Pakistan, wo von insgesamt rund 120 Millionen Handys 55 Millionen für das Data-Mining verwendet werden können, 15.000 bis 99.000 Personen fälschlich von Skynet als Terroristen klassifiziert. Von möglichen „Kollateralschäden“ bei konkreten Angriffen aufgrund dieser Daten ganz zu schweigen.

Zum Zweiten kann für die Ausführung eines Drohnenangriffs eine Technik zum Einsatz kommen, die den Namen Gilgamesh trägt und ähnlich wie ein ISMI-Catcher funktioniert, nur, dass hier der Standort der SIM-Karte mit einem speziell für diesen Zweck entwickelten Algorithmus der NSA ermittelt wird. Eine kleine Box ist an der Drohne angebracht, die sich für Mobilfunkgeräte als Funkmast ausgibt. Handys können nun gezwungen werden, sich hier einzuwählen und wenn eine Nummer, die zuvor, z.B. durch das Programm Skynet als Ziel definiert wurde, entdeckt wird, kann das Mobilfunkgerät geortet und dann die Person, die es bei sich führt, angegriffen werden. (Zu Gilgamesh siehe The Intercept, 10.2.16)

Somit sind Mobilfunkdaten ein zentraler Bestandteil, damit der Drohnenkrieg der USA überhaupt geführt werden kann. Und diese Daten stammen nicht nur von US-Diensten, sondern kommen auch von Partnerdiensten. Die Frage, ob hier auch deutsche Dienste, wie das Bundeskriminalamt (BKA), das BfV sowie der Bundesnachrichtendienst (BND) Handynummern weitergeben, wurde zum ersten Mal breiter diskutiert, als der Wuppertaler Bünyamin Erdoğan durch einen Drohnenangriff in Pakistan 2010 ums Leben kam. (Zum Fall Bünyamin: stern.de, 29.3.12; BT-Drucksache 17/8088) Hatten hier deutsche Stellen Daten weitergegeben und wurde so der Angriff erst ermöglicht?

Die Frage nach der Datenweitergabe allgemein war am 28.4.2016 im Untersuchungsausschuss des Bundestages zur NSA-Affäre Thema. Hier werden einige Stellen aus dem Liveblog, der bei Netzpolitik.org (28.4.16) zu finden ist, zitiert:

***Renner**: Haben sie Handynummern weitergegeben?*

***Berfuß**: Öffentlich nur allgemein. Ja, kommt vor.*

***Renner**: Auch aus G-10?* [G10 = Grundgesetzartikel 10: Brief-, Post- und Fernmeldegeheimnis; gemeint sind also Daten, die nach dem G10-Gesetz, welches ein Eingriff in die Grundrechte des GG-Artikels 10 erlaubt, von den Diensten erhoben wurden, Anm. d. Autors]

***Berfuß**: Nicht sicher. Aber könnte sein.*

Diese Befragung nahm die Obfrau der Linksfraktion im Untersuchungsausschuss, Martina Renner, vor. Sie befragte u.a. Folker Berfuß, Referatsgruppenleiter in der Abteilung 6 des BfV, die für „Islamismus und islamistischen Terrorismus“ zuständig ist. Im Anschluss an Renner war der Abgeordnete Tankred Schipanski von der Unionsfraktion an der Reihe; dieser stellte folgende Fragen:

***Schipanski**: Für Weitergabe Handynummer gibt es Rechtsgrundlage. Ist das so?*

***Berfuß**: Ja.*

***Schipanski**: Also klare Grundlage. Dürfen sie machen.*

***Berfuß**: Ja.*

***Schipanski**: Gab es Gründe, dass sie misstrauisch waren, dass sich an irgendwas nicht gehalten wurde?*

***Berfuß**: In UG und UZ nein.* [UG = Untersuchungsgegenstand, UZ = Untersuchungszeitraum, Anm. d. Autors]

***Schipanski**: Also auch keinen Anlass anzunehmen, dass sich Partner nicht an Vorgaben hält?*

***Berfuß**: So ist es.*

***Schipanski**: Also Disclaimer hinreichendes Mittel, um das abzusichern. Muss man ja mal sagen.*

[Disclaimer = hier soll es sich um die Einschränkung handeln, dass die weitergegebenen Daten nur zu nachrichtendienstlichen Zwecken verwendet werden dürfen, Anm. d. Autors]

Mit diesen Fragen unterstützte Schipanski den Zeugen, indem er hervorhebt, dass es eine rechtliche Grundlage für die Weitergabe gäbe. Doch ob diese Grundlage so eindeutig ist, daran lässt das erst letzte Woche gefällte Urteil des Bundesverfassungsgerichts (BVerfG) Zweifel, wie später aufgezeigt werden wird.

Bei der späteren Befragung durch den Obmann der Fraktion Bündnis 90/Die Grünen Konstantin von Notz ging es dann noch um die Frage, ob es sich bei den Einsätzen von Drohnen durch die CIA um nachrichtendienstliche Tätigkeiten handle. Da auch dieser Abschnitt sehr kurios ist, soll er auch hier in entsprechender Länge zitiert werden:

***Notz:** In Disclaimer: Daten nur für ND-Zweck?* [ND = Nachrichtendienstlichen, Anm. d. Autors]

***Berfuß**: Ja.*

***Notz**: Im Gegensatz zu welchem anderen Zweck?*

***Berfuß**: Polizeilich z.B.*

***Notz**: Militärisch?*

Informationsstelle Militarisierung (IMI) e.V. - Hechinger Str. 203 - 72072 Tübingen

***Berfuß**: Jeder andere Zweck.*

***Notz**: Aber die CIA. Wenn die Drohnenoperationen durchführt. Wäre das erfasst?*

***Berfuß**: KA.* [KA = Keine Angabe, Anm. d. Autors]

***Notz**: Aha, also kann es sein, dass die doch für Drohnenoperationen bei CIA genutzt werden?*

***Berfuß**: KA.*

***Notz**: Also, würde ihr Disclaimer helfen, dass das nicht passiert?*

***Berfuß**: Kann ich nicht beantworten.*

***Notz**: Also: Erfasst der Disclaimer CIA ja oder nein?*

***Berfuß**: Ja.*

***Notz**: Wenn CIA eine Operation durchzieht, ist das eine nachrichtendienstliche Operation?*

Akmann [Ministerialrat des Bundesministeriums für Inneres (BMI) für die Projektgruppe „Untersuchungsausschuss“, Anm. d. Autors]: *Das müssen sie die CIA fragen, nicht den Zeugen.*

***Notz**: Das BMI sagt mir also, dass die CIA Drohnentötungen durchführt.*

***Akmann**: Das wissen wir nicht aktiv.*

***Notz**: Das wissen sie nicht?*

***Akmann**: Nein. Das steht in den Medien.*

***Notz**: Geht darum, ob Daten für Drohnentötungen verwendet. Zeuge sagt, nein, kann nicht sein, weil Disclaimer. Aber CIA ist ein ND. Und Einsatz der CIA mit Drohnen ist ein ND-Einsatz. Also sagt der Disclaimer überhaupt nichts. Dass sie hier sagen, sie wüssten nicht, was die CIA tut, Herr Akmann, ist eine absurde Behauptung.*

***Akmann**: Ob der Drohneneinsatz eine ND-Maßnahme ist, kann der Zeuge nicht beantworten.*

***Notz**: Was dann? Haben sie das mal geprüft? Kann ja sein, dass der Disclaimer nichts hilft.*

Anwlat [sic! Gemeint ist der Anwalt von Berfuß, Anm. d. Autors]: *Von ihnen wird juristische Subsumption abgefragt.*

***Notz**: Herr Berfuß, sie wurden gefragt, was sie dagegen tun, dass Daten für Drohnenangriffe verwendet wurden. Sie haben gesagt: Disclaimer. Ich hinterfrage das Argument. Das muss möglich sein. Er hat das ins Spiel gebracht, nicht ich. Der Zeuge kann ja sagen: „Wenn Drohne von CIA geflogen wird, ist das militärisch, dann funktioniert Disclaimer.“*

***Berfuß**: Sie verlangen rechtliche Bewertung, für die ich nicht zuständig bin. Habe versucht, zu erklären, wie wir arbeiten. Bin qua Amt nicht der Richtige, um diese Fragen zu beantworten.*

***Notz**: Also sie können die Frage nicht beantworten?*

***Berfuß**: Nein.*

***Notz**: Ok. Das ist ja eine andere Antwort.*

***Akmann**: Aus Sicht des BfV ist eine ND-Maßnahme immer eine Maßnahme im Sinne der Informationsgewinnung.*

***Notz**: Interessante Aussage. Wenn sie sagen, der Zeuge meinte, dass wenn CIA eine Drohne fliegt und Terroristen tötet, dann ist das keine ND-Aktion?*

***Akmann**: Würd ich so sagen.*

Erst kurz zuvor, am 20. April 2016, hat sich das Bundesverfassungsgericht in seinem Urteil zum BKA-Gesetz vom 20. April 2016 relativ eindeutig zu der Weitergabe von Informationen, die auch zur Lokalisierung und Tötung von Terrorverdächtigen dienen könnten, geäußert. Denn die im Gesetz getroffenen Bestimmungen würden den verfassungsrechtlichen Ansprüchen teilweise nicht genügen und seien zu „unbestimmt“. Die Verfassungsrichter_innen fordern eine verbesserte Kontrolle, zu welchem Zweck die Daten vom Empfängerland genutzt würden. Dazu hier einige einschlägigen Abschnitte aus dem Urteil:

„[Es] ergeben sich Grenzen in Blick auf die Nutzung der Daten durch den Empfängerstaat, wenn dort Menschenrechtsverletzungen zu besorgen sind. Zwingend auszuschließen ist danach jedenfalls die Datenübermittlung an Staaten, wenn zu

Boden-Kontrollstation für Drohnen-Einsätze. Quelle: Gerald Nino/Wikipedia

befürchten ist, dass elementare rechtsstaatliche Grundsätze verletzt werden […]. Keinesfalls darf der Staat seine Hand zu Verletzungen der Menschenwürde reichen. […] Die Übermittlung personenbezogener Daten ins Ausland setzt weiter einen datenschutzrechtlich angemessenen und mit elementaren Menschenrechtsgewährleistungen vereinbaren Umgang mit den übermittelten Daten im Empfängerstaat (1) und eine entsprechende Vergewisserung hierüber seitens des deutschen Staates (2) voraus.“

Heribert Prantl, Journalist der Süddeutschen Zeitung (20.2.16) und ehemaliger Richter kommentierte das Urteil überwiegend optimistisch und schrieb: „Das heißt: Deutsche Daten, die für US-Drohnenangriffe verwendet werden könnten, dürfen wohl künftig nicht mehr herausgegeben werden.“

Doch nach der Anhörung im Untersuchungsausschuss am 28.4.2016 lässt sich kaum auf eine Veränderung der Praxis hoffen, unabhängig davon, ob es nun ums BKA, das BfV oder den Bundesnachrichtendienst (BND) geht. Denn die Nachrichtendienstler scheinen sich ihre eigene Realität zu schaffen. Drohnenangriffe seien „spekulativ“, der Sensor-Operator Brandon Bryant ein „angeblicher“ ehemaliger „Drohnenpilot“. Diese Aussagen stammen vom zweiten Zeugen der gestrigen Anhörung im Untersuchungsausschuss, Klaus Rogner, des Leiters der Abteilung 6 beim BfV, die für „Islamismus und islamistischen Terrorismus“ zuständig ist. Bei der Nachfrage, ob sich die weitergegebenen Daten zur Lokalisierung einer Person eignen würden, zeigte der Zeuge, wie wenig Wissen man in den deutschen Nachrichtendiensten über die Fähigkeiten der US-Dienste zu haben scheint.

***Renner**: Schon viel zu Disclaimer gefragt. Erlass BMI 24.11.2010. Regelt, dass keine Übermittlung dabei, die für geografische Ortung geeignet sind. Kennen sie den? [17/8088]*

***Rogner**: Können sie den mal zeigen?*

***Renner**: Habe ich nicht, kenne ihn nur aus Kleiner Anfrage. Dachte, sie kennen ihn.*

***Rogner**: Bei der Vielzahl von Erlassen kann ich mich nicht an jeden einzelnen erinnern.*

***Renner**: Dass Weitergabe von Daten zu Geolokation unterlassen werden soll, ist nicht bekannt?*

***Rogner**: Nein.*

***Akmann**: Wir haben Erlass dabei. Könnten ihnen den übergeben.*

***Renner**: Dann können wir den auch dem Zeugen zeigen. Können wir dann kurz Pause machen?*

[Dokument wird vorgelegt.]

Ist ihnen das Schreiben bekannt?

***Rogner**: Damals nicht. War nicht AL, sondern Referatsgruppenleiter.* [AL = Abteilungsleiter, Anm. d. Autors]

***Renner**: Und dann Anfang 2011?*

***Rogner**: Ja, im Rahmen Beantwortung parlamentarischer Anfragen bekannt geworden. Ob ich Dokument als solches mal gesehen habe, KA. Hätte mich erinnert, wenn es meinerzeit eingegangen wäre. Dann wäre es wahrscheinlich über meinen Schreibtisch gegangen. Äußerung wurde mir dann berichtet.*

***Renner**: Welche Daten sind für unmittelbare geografische Ortung geeignet?*

***Rogner**: Keine solchen, die wir übermitteln.*

***Renner**: Welche?*

***Rogner**: GPS-Daten.*

***Renner**: Mobilfunk?*

***Rogner**: Bloße Nummern nicht afaik.* [afaik = soweit ich weiß, Anm. d. Autors]

***Renner**: Postadresse?*

***Rogner**: Postadresse in D. Wo die dann in AFG, PAK wohnen KA.* [AFG = Afghanistan, PAK = Pakistan, Anm. d. Autors]

***Renner**: Haben Handynummern übermittelt, die in Transit- oder Zielländern.*

***Rogner**: Afaik bloße Handynummer nicht geeignet.*

***Renner**: Damaliger Wissensstand oder heute?*

***Rogner**: Habe auch heute keinen Grund daran zu zweifeln.*

Also auch Veröffentlichungen zu Skynet und Gilgamesh scheinen hier kein Anlass zur Überprüfung dieses Wissensstandes gewesen zu sein.

Die Bundesregierung zieht sich gern auf die Formulierung zurück, zu Drohnenangriffen durch die USA hätte man keine „eignen gesicherten Erkenntnisse“. Da die zuständigen Stellen in der Bundesregierung sowie in den polizeilichen, wie nachrichtendienstlichen Behörden Berichte über Drohneneinsätze und die Möglichkeiten der US-Dienste zwar wahrnehmen, aber wenig Bemühungen erkennen lassen, zu eigenen Erkenntnissen zu kommen, ist eine Veränderung der Praxis der Weitergabe der Daten nicht zu erwarten. Ob das Urteil des BVerfG an dieser Weitergabepraxis etwas wird ändern können, bleibt abzuwarten. Zwar sind die Forderungen der Richter für eine bessere Kontrolle der Verwendung der Daten durch die Empfängerstaaten ein klares Signal; doch wie dies letztlich umgesetzt wird, darauf muss wohl auf die Art und Weise der Umsetzung der gerichtlichen Vorgaben gewartet werden. Für eine klare und deutliche Abkehr könnten wohl Urteile mit klarem Bezug zu den Staaten sorgen, die Drohnen für Tötungen einsetzen. Zwar sind und waren einige Klagen gegen die USA, bzw. gegen die Bundesregierung, meist wegen Vernachlässigung ihrer Schutzpflicht, weil Sie den Drohnenkrieg über die Relaisstation Ramstein zulassen würden, vor deutschen Gerichten anhängig. Ob es aber zu Urteilssprüchen kommt, in denen den Kläger_innen Recht gegeben wird, ist mehr als fraglich. Die Bundesregierung beteuert stets, keine „eigenen gesicherten Erkenntnisse“ zu haben; und mit einer Mitarbeit der von den Klägern beschuldigten US-Diensten ist auch nicht zu rechnen. Die Geheimhaltung der US-Seite, bzw. das offen zur Schau gestellte Unwissen der Bundesregierung wird eine rechtliche Bewertung eher erschweren, wenn nicht gar unmöglich machen. Und dieses Spiel scheint vor den Gerichten aufzugehen. So stellte das Kölner Verwaltungsgericht im Mai 2015 fest, dass die Bundesregierung den Beteuerungen der USA, dass Drohnen aus der US-Air Force Base in Ramstein weder gesteuert noch Drohnen von dort starten würden, durchaus Glauben schenken dürften (hierzu Pressemitteilung VerG Köln, 27.5.16). Und wie eine aktuelle schriftliche Anfrage des grünen Abgeordneten Hans-Christian Ströbele zeigt, werden die Beteuerungen der US-Seite nicht in Zweifel gezogen (Drucksache 18/8191). In der hier angesprochenen Klage dreier Jeminiten, die bei der Klage von den Menschenrechtsorganisationen Reprieve und dem European Center for Constitutional and Human Rights (ECCHR) unterstütz wurden, geht und ging es um diese beiden Punkte aber freilich nicht. Stattdessen wird in den Fällen aber auf die zentrale Funktion Ramsteins als Relaisstation Bezug genommen. Eine weitere Klage eines Somaliers, der vor dem Bundesverwaltungsgericht in Köln wegen der Tötung seines Vaters geklagt hatte, wurde erst vor zwei Tagen abgewiesen (hierzu die Süddeutsche Zeitung, 27.4.16). All das sind Anzeichen, dass es wohl erheblichen Drucks Bedarf, damit die skandalöse Praxis der Weitergabe von Handydaten und damit der Beihilfe zur Tötung ein Ende finden wird.

Propaganda an der Heimatfront

Verteidigungsministerium veröffentlicht Bericht der Jugendoffiziere 2015

von Christian Stache

Der Presse- und Informationsstab des Bundesverteidigungsministeriums hat jüngst den Tätigkeitsbericht der Jugendoffiziere für das Kalenderjahr 2015 veröffentlicht. In ihren Reporten dokumentieren die derzeit 80 aktiven von potentiell 94 hauptamtlichen „Öffentlichkeitsarbeitern“ (vgl. jugendoffizier.eu) der Bundeswehr einerseits ihre Propaganda- und Indoktrinationsarbeit in Schulen und anderen Institutionen sowie ihre Kontakte zu zivilen Organisationen in der Bundesrepublik, wie etwa zum Unternehmerverband Berlin-Brandenburg und zur SPD Hamburg im vergangenen Jahr. Andererseits fassen die Mitglieder der 1958 geschaffenen militärischen Einheit jährlich ihre Erkenntnisse über die politische Haltung der Zivilbevölkerung gegenüber der Bundeswehr und der deutschen Sicherheits- und Verteidigungspolitik zusammen, die sie während ihrer Einsätze in Klassenzimmern und andernorts sammeln. „Die Jugendoffiziere erfüllten somit eine wichtige Brückenfunktion zwischen Bundeswehr und Gesellschaft“ (Alle Zitate sind folgendem Bericht entnommen: Jahresbericht der Jugendoffiziere der Bundeswehr (Ausgabe 2015), Berlin, 13. April 2016).

Hauptsächlich arbeiten die Auftragspropagandisten mittels Vorträgen (3.189). Hinsichtlich der Qualität ist das Strategiespiel Politik und Internationale Sicherheit (POL&IS) hervorzuheben. Zum einen überschreitet die Nachfrage regelmäßig das personal- und kostenintensive Angebot. Zum anderen fungiert es als „Türöffner“ und „als Mittel des Ausbaus wichtiger bestehender Kontakte“. Im Jahr 2015 hat es rund 400 solcher mehrtägigen Seminare gegeben.

Im Jahr 2015 haben die Militärs insgesamt 5.569 Veranstaltungen durchgeführt. Dies entspricht dem Niveau der beiden Vorjahre. Bei den verschiedenen Vorträgen, Podiumsdiskussionen, Seminaren und Seminarfahrten, Besuchen bei der Truppe, Informationsveranstaltungen über die Arbeit der Jugendoffiziere und Großveranstaltungen erreichten sie 149.966 Teilnehmer. Das sind rund 12.000 weniger als 2014 und 2.500 weniger als 2013. Die Hauptzielgruppe waren wie gehabt Schüler und Studierende (115.111).

Unter den Schulformen bildeten Gymnasien und Realschulen die „Arbeitsschwerpunkte“. An Gymnasien wurden die Jahrgangsstufen 12 (24.923) und an Realschulen die zehnten Klassen (20.434) am meisten aufgesucht. Schließlich handelt es sich bei diesen Schülern um Schulabgänger und um Berufsanfänger mit höherer Bildung. Diese Jugendlichen finden aufgrund besserer Berufsaussichten ihren Weg seltener zum Militär, das sie in der Regel mit freundlichem Desinteresse links liegen lassen.

Die zweite große Zielgruppe der Jugendoffiziere sind die sogenannten Multiplikatoren, wie z.B. Referendare. 34.258 solcher „Multiplikatoren“ nahmen Angebote der Jugendoffiziere im Berichtsjahr 2015 wahr. In Hamburg wurde etwa „erneut eine Weiterbildung für Pädagogen aus Hamburg, Niedersachsen und Schleswig-Holstein gemeinsam mit dem Ernst Klett Verlag durchgeführt“.

Besondere Verunsicherung unter den Jugendoffizieren hatte offenbar die Inauguration der ersten Landesregierung unter Leitung eines Linkspartei-Ministerpräsidenten ausgelöst. Die Angst hat sich aber als unbegründet erwiesen. Im rot-rot-grünen Koalitionsvertrag heißt es zwar, dass an Schulen keine Veranstaltungen „in alleiniger Durchführung der Bundeswehr“ mehr stattfinden sollten. Aber die rot-rot-grüne Landesregierung in Thüringen habe „bis dato keine Auswirkungen auf das Anfrageverhalten der Schulen und die Durchführung der Jugendoffiziereinsätze“ gehabt. „Laut Bericht sind die Einsätze sogar um 16 Prozent gestiegen und dies ›ohne nennenswerte zusätzliche‹ Anstrengungen“, empört sich Markus Gross vom Netzwerk Schule ohne Bundeswehr NRW. „Eine ›links‹ geführte Landesregierung muss also für das Agieren des Militärs im Klassenzimmer überhaupt kein Hindernis sein.“ Ralf Buchterkirchen, Bundessprecher der Deutschen Friedensgesellschaft – Vereinigte Kriegsdienstgegner, fordert deswegen ein „rigoroses Verbot für Armee-Werbung an Schulen“. „Die Einheit der Jugendoffiziere gehört aufgelöst.“

Zudem sei die „in Baden-Württemberg entbrannte Debatte über das Für und Wider der Tätigkeit der Jugendoffiziere (…) erfolgreich beigelegt“ worden. „Eine vom Kultusministerium herausgegebene Handreichung für Schulleiterinnen und Schulleiter sorgt nunmehr für Handlungssicherheit im Umgang mit den Jugendoffizieren.“

Bedauerlich, aber kaum überraschend sei es, so Markus Gross vom Netzwerk Schule ohne Bundeswehr NRW, dass „in Thüringen laut dem Bericht der Jugendoffiziere abermals die Evangelische Kirche neben nicht namentlich genannten Vertretern der ‚Friedensbewegung‘ das Vorgehen der Landesregierung abgesegnet hat. Die gleiche schmerzhafte Erfahrung mussten wir schon hier in NRW, in Rheinland-Pfalz und vor allem in Baden-Württemberg machen.“

Im Vergleich zu den Vorgängerberichten wird die Kritik an deutschen und den Kriegseinsätzen der NATO bemerkenswert offen wiedergegeben. „Allgemein war die Tendenz festzustellen, dass Kampfeinsätze der Bundeswehr eher abgelehnt wurden.“ In Bezug auf den Ukraine-Konflikt sei argumentiert worden, „dass die USA und die NATO durch die Osterweiterung des transatlantischen Bündnisses Russland in die Enge getrieben haben“. Diese Position denunzieren die Jugendoffiziere in ihrem Bericht ohne Angabe von Gründen als „Antiamerikanismus“.

Die deutsche Außen- und Sicherheitspolitik im Syrien-Krieg und der militärische Einsatz gegen den IS würden „oft kritisch hinterfragt und negativ bewertet. Auch der Beschluss des Deutschen Bundestages zum Einsatz der Bundeswehr konnte nicht alle Zweifel an der völkerrechtlichen Legitimation des Einsatzes zerstreuen. Zudem erscheint es vielen Menschen grundsätzlich fraglich, ob man Terrorismus mit militärischen Mitteln sinnvoll und wirksam begegnen kann.“

Damit diese Haltungen sich nicht durchsetzten, predigten die Jugendoffiziere »die alternativlose Notwendigkeit einer militärisch abgestützten Außen- und Sicherheitspolitik“, meint Alexander Neu, Obmann im Verteidigungsausschuss des Bundestags für die Fraktion DIE LINKE. „Entgegen aller Beteuerungen rekrutiert die Bundeswehr auch vor allem besser ausgebildete Jugendliche in den Klassenzimmern“, so Lühr Henken, Sprecher des Bundesausschusses Friedensratschlag. „Deshalb“, schlussfolgert Denise Wilken vom Hamburger Bündnis Bildung ohne Bundeswehr (BoB), „brauchen wir auch in den Schulen eine starke Bewegung gegen imperialistische Kriege und die Militarisierung der Gesellschaft.“

Offizierinnenausbildung an der zivilen Hochschule

Der Frauenstudiengang Informatik der Hochschule Bremen und die Bundeswehr

von Thomas Gruber

Die Hochschule Bremen geht für den internationalen Frauenstudiengang Informatik (IFI) eine enge Kooperation mit der Bundeswehr ein. Neun der 38 Studienplätze werden jährlich für Offiziersanwärterinnen der Bundeswehr im Rahmen eines dualen Studiums geblockt.[1] Die HS Bremen übernimmt damit eine wichtige Rolle in der Ausbildungsoffensive des deutschen Militärs, sie verschafft der im Cyberkrieg und dem digitalen Wettrüsten scheinbar so weit abgehängten Bundeswehr[2] Zugriff auf aktuelle informatische Forschungsergebnisse und essentielles technisches Know-How. Dass dabei erhebliche Geldmittel vom Militär in die Hochschule fließen werden, betont auch der Hochschulsprecher Ulrich Berlin, laut dem die Bundeswehr sich am IFI mit Verwaltungskosten beteilige. Darüber hinaus dürfen „Kooperationspartner […] keinen Einfluss auf die Inhalte nehmen." Und weiter: „Es gibt also auch keine inhaltlichen Änderungen im Studiengang." Dass eine solche Entscheidung allerdings sehr wohl zu einschneidenden Änderungen von Studieninhalten im IFI führen kann, muss inzwischen wohl auch der Hochschulsprecher feststellen: Ralf Streibl, der seit der Gründung des Studienganges im Jahr 2000 als Lehrbeauftragter des Fachgebietes „Informatik und Gesellschaft" an der Hochschule Bremen angestellt war, gibt aufgrund der Kooperation der HS Bremen mit der Bundeswehr seine Lehrtätigkeit auf. In einem offenen Brief[3] an die Hochschulrektorin begründet der Dozent seine Entscheidung und zeigt damit auf, wie sich die Hochschule als Wegbereiterin einer militarisierten zivilen Forschungslandschaft der eigenen Profilierung einer selbstreflektierenden wissenschaftlichen Institution beraubt.

Was hat die Informatik mit der Gesellschaft zu tun und was will die Gesellschaft von der Informatik?

Der informatischen und informationstechnologischen Forschung kann aus zwei sehr unterschiedlichen Perspektiven begegnet werden. Zum einen befasst sich die wissenschaftliche Arbeit in der Informatik oft mit der Formulierung und der Lösung programmierlogischer oder hardwaretechnischer Fragestellungen, die Forscher_innen können daher die Motivation ihrer Arbeit in der theoretischen Bearbeitung komplexer mathematisierter oder technischer Probleme finden, ohne einen Anwendungsbezug herstellen zu müssen. Zum anderen sind viele ethisch problematische Technologien und Programme ohne Forschungsergebnisse aus der Informatik schlicht undenkbar. Seien es kryptologische Konzepte zur Bereitstellung von Überwachungstechnologie, die Programmierung und Steuerung militärisch genutzter Satellitensysteme oder die automatische Zielerkennung einer Kampfdrohne mit Methoden des maschinellen Lernens – viele Prozesse in der polizeilichen Überwachung oder der modernen Kriegsführung sind auf die Forschung in der Informatik angewiesen. Da die Informatik damit einige drastische Auswirkungen auf die Zivilgesellschaft, wie die Verletzung der Privatsphäre von Bürger_innen durch immer weiter umgreifende Überwachung oder die Bedrohung von Menschenleben durch moderne Kriege, erst möglich macht, werden Forschungsschwerpunkte und -projekte von Informatiker_innen zunehmend zu einem Politikum. Die Konzepte im Cyberwar, wie beispielsweise die Verbreitung von Schadprogrammen auf Privatrechnern, die Bedrohung ziviler Infrastruktur oder die Offenlegung privater Kommunikation, fußen zudem oft auf der militärischen Instrumentalisierung von Bürger_innen oder dem Missbrauch vorwiegend zivil genutzter Kommunikationsstrukturen als militärisches, geo- und wirtschaftspolitisches Schlachtfeld.

Dass die Auswirkungen informatischer Forschung unter diesen Gesichtspunkten Gegenstand eines gesamtgesellschaftlichen Diskurses sein müssen, ist selbstverständlich. Die Forderung nach einer solchen Debatte kann auch die Hochschulen, von denen die Forschungsergebnisse ausgehen, nicht aussparen – Hochschulen sind weder ein abgeschotteter Elfenbeinturm, in dem die Forscher_innen sich ihrer eigenen Verantwortung stellen und dieser ohne Wechselwirkung mit der Gesellschaft nachkommen können, noch sind sie Institute, die zur reinen Auftragsforschung missbraucht werden dürfen. Ralf Streibl schreibt in seinem offenen Brief: „Verantwortung in der Wissenschaft endet nicht bei Forschung. Die Identifikation, Betrachtung, Analyse, Bewertung und Reflexion von Rahmenbedingungen, divergierenden Interessen, gesellschaftlichen Wirkungen, ethischen Fragen und Dilemmata, Entwicklungspfaden, Handlungsspielräumen und Gestaltungsoptionen im offenen kommunikativen Miteinander und im gegenseitigen kritischen Diskurs muss wesentlicher Teil von Hochschullehre und Studium sein."[4]

Peacebuilding mal ernst gemeint – eine zentrale Aufgabe der Hochschule

Während Frieden als gesellschaftlicher Grundwert unbestreitbar scheint, drängen militärische und staatliche Akteur_innen auf eine immer aktivere Umprägung von Konfliktlösungen in der öffentlichen Wahrnehmung. „Friedensmissionen" im Rahmen politischer Konflikte, „humanitäre Interventionen" gegen gesellschaftliche Krisen und nicht zuletzt nationale Sicherheit durch Terrorismusbekämpfung – der Duktus wie die konkrete Außen- und „Sicherheitspolitik" rutschen immer stärker ins Militärische ab. Ralf Streibl dazu: „Kriterium für Frieden ist die Fähigkeit, mit Konflikten umzugehen […]. Erforderlich hierfür ist gleichermaßen eine Friedensstruktur wie auch eine Friedenskultur. Dem entgegen steht jedoch die bis heute in vielen Köpfen fest verwurzelte Überzeugung, Frieden sei nur durch Stärke erreichbar. Diese Überzeugung zu hinterfragen und in einem offenen Diskurs jenseits militärisch geprägter Sichtweisen den Weg zu einer echten Friedensfähigkeit zu eröffnen ist eine große Herausforderung für Politik und Gesellschaft und damit eine zentrale Aufgabe für Bildung und Wissenschaft."[5]

Dabei ist wohl die wichtigste Frage, wie der Übergang zu einer solch reflektierten Bildungs- und Forschungspraxis aussehen soll. Professor_innen, Dozent_innen und wissenschaft-

Informationsstelle Militarisierung (IMI) e.V. - Hechinger Str. 203 - 72072 Tübingen

liche Mitarbeiter_innen geraten inzwischen immer stärker unter den Druck der Liberalisierung des Forschungssektors. Die Einwerbung kompetitiver Drittmittel ist längst ein fester Bestandteil von Stellenausschreibungen und die Ablehnung eines Forschungsthemas aufgrund ethischer Bedenken kann schlimmstenfalls als Arbeitsverweigerung eingestuft werden – zumindest schadet es mit großer Wahrscheinlichkeit dem internationalen Ansehen der Forscher_innen. Dem entgegen steht die Möglichkeit ebenjene Missstände innerhalb der Bildungs- und Forschungseinrichtung auf allen Ebenen zu diskutieren und kritisch zu begleiten. Die Fragen, mit welchen eine Hochschule im Kontext dieser Anforderungen konfrontiert wird, formuliert Ralf Streibl wie folgt:[6]

- „Ermutigt und unterstützt sie ihre Mitglieder, regelmäßig im Sinne praktizierter gesellschaftlicher Verantwortung die Auswirkungen und Folgen eigenen wissenschaftlichen Handelns in Forschung und Lehre zu prüfen und zu hinterfragen?"
- „Werden Studierende angeregt und eingeladen, sich mit entsprechenden Fragen und Problemen als Teil ihres Studiums zu beschäftigen?"
- „Ermöglicht die Institution einen öffentlichen Diskurs über die Bedeutung und Folgen der dort betriebenen Forschung?"
- „Schafft sie Transparenz durch eine Verpflichtung zur Bekanntgabe von Forschungsthemen, Kooperationen und Herkunft von Fördermitteln sowie die Verpflichtung zur Veröffentlichung von Forschungsergebnissen?"
- „Fördert sie Diskurse in den Gremien und Fächern hinsichtlich der Ambivalenz wissenschaftlicher Erkenntnisse und Entwicklungen?"

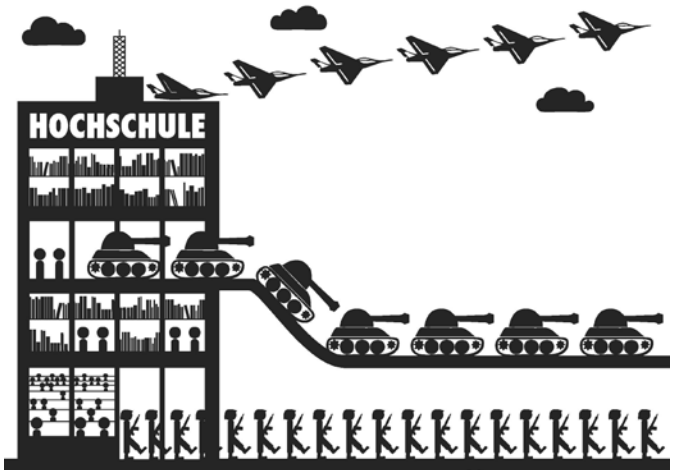
„Unsere Gesellschaft braucht mehr Menschen, die Rückgrat zeigen!"

Den Lehrbeauftragten, der diese Fragen als Aufgabe an eine verantwortungsbewusste Bildungseinrichtung stellt, ist die HS Bremen damit los. Der Hochschulsprecher Ulrich Berlin verargumentiert die Kooperation der Hochschule mit der Bundeswehr damit, dass neue Zielgruppen für den Studienfang erschlossen werden sollen, da die Nachfrage für den IFI nicht besonders stark war.[7] Dass Berlin dabei eher wie ein PR-Berater für Großunternehmen klingt als ein Vertreter einer zivilen Bildungseinrichtung, passt zur „Zielgruppe", die erschlossen werden soll: Es wird sich nicht mit interessanten Inhalten oder einem innovativen Bildungsangebot um neue Studentinnen bemüht und damit das Profil des Informatikstudiums an der Hochschule gestärkt, sondern es werden Studienplätze an die Bundeswehr verkauft, die damit Soldatinnen zu Expert_innenwissen verhilft. Eine wirkliche Profilierung würde die Stärkung eines wissenschaftsethischen und politischen Diskurses innerhalb der Hochschule bedeuten und gerade nicht die offene Einladung für die Bundeswehr, den IFI in einen militärischen Kontext zu setzen. Ralf Streibl beschließt seine Entscheidung folgendermaßen: „Als Reaktion auf den Beschluss der Hochschule Bremen, den besagten Kooperationsstudiengang mit der Bundeswehr einzurichten, werde ich […] meine langjährige Mitwirkung in diesem Studiengang beenden. […] Mein Bemühen galt der Schaffung eines anregenden Lern- und Studienambiente, in welchem – geprägt durch Offenheit, Wertschätzung und Reflexion – die Studentinnen die Möglichkeit erhalten sollten, Szenarien und Entwicklungen aus unterschiedlichen Perspektiven zu betrachten und zu bewerten, ihre und anderer Leute Sichtweisen in Frage zu stellen und vor allem kontrovers zu diskutieren. In der Presse wurde berichtet, dass – laut Leitung der Hochschule Bremen – die Bundeswehr keinen Einfluss auf Inhalte des Studiums nehmen könne. Dies mag formal auch so sein. Durch die strukturelle und finanzielle Verbindung zwischen Hochschule und Bundeswehr verändert sich aber der Gesamtkontext. Ich selbst bin nicht dazu bereit, als Person und mit meiner Lehrveranstaltung Teil solch einer Konstruktion zu sein".[8]

Ob die HS Bremen Ralf Streibls alte Stelle noch einmal neu vergibt, ist bislang unklar; sie führt den Studieninhalt zu „Informatik und Gesellschaft" zumindest an prominenter Stelle in der Beschreibung der Studieninhalte des IFI auf.[9] Dass bei einer Neubesetzung der Lehrstelle die ergebnisoffene Diskussion über ethisch fragwürdige und diskutable Forschung eine untergeordnete Rolle spielen dürfte, ist dagegen absehbar. Abschließend steht vor allem eines fest: An deutschen Forschungseinrichtungen wie in der Öffentlichkeit muss ein lebhafter Diskurs über die zunehmende Militarisierung und die Liberalisierung des Bildungs- und Forschungssektors stattfinden. Dabei ist dem Bremer AStA, wenn er über das Ausscheiden von Ralf Streibl aus der Hochschule schreibt, nur wenig hinzuzufügen: „Unsere Gesellschaft braucht mehr Menschen, die Rückgrat zeigen!"[10]

Anmerkungen

1 Hochschule will mit Bundeswehr zusammen arbeiten, https://weserreport.de/2016/04/28/weser/sued/hochschule-will-mit-bundeswehr-zusammen-arbeiten/, aufgerufen am 23.5.2016.
2 *Von der Leyens später Eintritt in den Cyberwar*, http://www.faz.net/aktuell/politik/inland/ursula-von-der-leyen-stellt-cyberarmee-kdocir-auf-14200457.html, aufgerufen am 23.5.2016.
3 Offener Brief von Ralf Streibl an die Hochschulrektorin der HS Bremen, http://www.kramschubla.de/hsb/HSB.pdf, aufgerufen am 23.5.2016.
4 Ebd., S. 4-5.
5 Ebd., S. 3.
6 Ebd., S. 7.
7 Geplanter dualer Studiengang in der Kritik, http://www.duales-studium.de/news/geplanter-dualer-studiengang-in-der-kritik, aufgerufen am 23.5.2016.
8 Offener Brief, S. 8-9.
9 *Studieninhalte des Internationalen Frauenstudiengangs Informatik*, *http://www.hs-bremen.de/internet/de/studium/stg/ifi/inhalte/*, aufgerufen am 23.5.2016.
10 Facebook-Eintrag des AStA Bremen am 19.5.2016, https://www.facebook.com/astahsb/?fref=nf, aufgerufen am 23.5.2016.



Keine Wissenschaft für den Krieg!
Quelle: AK Zivilklausel Frankfurt am Main

Eintausend deutsche Soldaten in Mali

von Christoph Marischka

Mit überwältigender Mehrheit (503 zu 66 Stimmen bei sechs Enthaltungen) hat der Bundestag am 28. Januar der „Fortsetzung und Erweiterung der Beteiligung“ der Bundeswehr an der MINUSMA-Operation in Mali zugestimmt. Anfang März dann besuchte die Verteidigungsministerin von der Leyen mit hochrangiger Delegation für drei Tage das Land und auch die im Aufbau befindlichen deutschen Container im von der niederländischen Armee übernommenen Camp Castor im umkämpften Norden des Landes. Das sorgte kurzfristig für etwas Berichterstattung über den Bundeswehreinsatz, die danach aber schnell wieder abebbte. Das ist erstaunlich, denn die Mission in Mali könnte bald Afghanistan als gefährlichsten Einsatz der Bundeswehr ablösen.

Als von der Leyen Camp Castor besuchte, waren bereits etwa 200 Soldat_innen der Bundeswehr vor Ort. Mit als Erste waren bereits im Februar Sanitätskräfte dort stationiert worden, die künftig verletzte Bundeswehrangehörige versorgen sollen. Insgesamt umfasst das Mandat des Bundestages den Einsatz von 650 Kräften der Bundeswehr, von denen etwa 400 im Norden, der Rest überwiegend in der Hauptstadt Bamako im Süden stationiert sein werden. Dem Sanitätstrupp folgten Spezialpioniere aus Husum, die für den Aufbau der Container und deren Sicherung u. a. mit insgesamt 320.000 Sandsäcken zuständig waren. Ende Februar dann übernahmen Objektschutzkräfte der Luftwaffe u. a. von bewaffneten Wachtürmen aus den Schutz des Lagers. Mittlerweile hinzugekommen sind Heeresaufklärer des einsatzerprobten Aufklärungsbataillons „Holstein“ aus Eutin. Falls die Spähtrupps außerhalb des Feldlagers in Gefechte geraten, steht dort ein „Mobile Reaction Team“ mit etwa 40 Kräften in Bereitschaft, um schnell und robust vor Ort sein und mitkämpfen zu können. Wie hoch die Wahrscheinlichkeit bewaffneter Auseinandersetzungen eingeschätzt wird, zeigt sich auch daran, dass die Bundeswehr in diesem Einsatz nur mit gepanzerten Fahrzeugen – insgesamt etwa 60 überwiegend vom Typ „Fennek“ und „Dingo“ sowie „Eagle IV“ und Transportpanzer „Fuchs“ – unterwegs ist.

Die Heeresaufklärer sind neben dem Spürpanzer „Fennek“ v. a. mit Drohnen ausgestattet. Dazu gehört die „Mikro-Aufklärungsdrohne für den Ortsbereich“ (MIKADO), die mit einer Reichweite von etwa 1 km mit handelsüblichen Kameradrohnen vergleichbar ist, sowie die gut 4 m breite LUNA-Drohne. Die LUNA wird von einem Katapult gestartet und bei der „Landung“ mit einem Netz aufgefangen. Insgesamt sind mehrere Fahrzeuge und über 20 Personen notwendig, um sie zum Einsatz zu bringen, dann kann sie in einem Radius von ca. 80 km mit verschiedenen Kameras das Gebiet aufklären und in Echtzeit Bilder liefern. Nach ersten Tests im Camp Castor soll die Drohne zukünftig auch außerhalb eingesetzt werden, um Verbindungsstraßen zu überwachen und Bewegungen bewaffneter Gruppen zu verfolgen. Die Luna-Drohne wird bereits seit Jahren in Afghanistan eingesetzt und vom Fraunhofer-Institut für Optronik, Systemtechnik und Bildauswertung (IOSB) wurde ihre Bilderkennung optimiert, sodass sie z. B. eigenständig Fahrzeuge identifizieren und verfolgen kann. Die Verteidigungsministerin kündigte bei ihrem Besuch in Mali außerdem an, dass bis Ende des Jahres noch deutlich größere Drohnen des Typs Heron I in Mali stationiert werden sollen, wie sie bislang von der Bundeswehr nur in Afghanistan eingesetzt wurden und werden. Die Heron I ist eine Drohne der MALE-Klasse (Medium Altitude, Long Endurance) und kann mit einer Einsatzreichweite von etwa 400 km über 24 Stunden in der Luft bleiben. Sie gehört nicht der Bundeswehr, sondern wird vom Hersteller (IAI) über das deutsche Rüstungsunternehmen Airbus Defence and Space geleast, das auch für die Ausbildung, Wartung und Teile der Steuerung verantwortlich ist.

Nach Angaben der Zeit sollen zwei oder drei Heron-Drohnen nach Mali verlegt werden und die Verteidigungsministerin begründet dies so: „Mit kleineren Drohnen könne die Bundeswehr zwar die unmittelbare Umgebung ihres Standortes in Gao überblicken, aber nicht die vielen hundert Kilometer langen Straßen zwischen den Städten in der dünn besiedelten Region... ‚Es ist in dieser Wüstenregion so: Wer die Straße beherrscht, der kann den Zugang zu einer Stadt ermöglichen oder die Stadt von der Versorgung abschneiden‘, sagte von der Leyen in Gao“.[1]

Ein wesentlicher Teil der Arbeit des deutschen Kontingents besteht tatsächlich darin, die „Rettungskette“ im Fall von Verwundeten und die eigenen Versorgungswege unter Kontrolle zu halten. Diesem Ziel dienen letztlich auch die sog. CIMIC-Teams, die „Erkundungsfahrten“ nach Gao und in andere Siedlungen unternehmen um – neben vielen Fotos mit Kindern und Frauen – „einen Beitrag zum zivilen Lagebild“ zu liefern, damit entsprechende Erkenntnisse „bei militärischen Entscheidungen mit berücksichtigt werden können.“[2]

Zur Sicherheitslage in und um Gao

Von der malischen Hauptstadt Bamako aus dem Fluss Niger folgend ist Gao nach Timbuktu die letzte große Stadt vor der Grenze zum Staat Niger. Von hier aus führen wichtige und traditionelle Verbindungsrouten in und durch die Sahara. Wesentliche Teile des Transsahara-Handels und selbst die Migration wurden jedoch in den letzten Jahren verstärkt illegalisiert und entsprechend werden diese Routen heute von kriminellen, oft auch als terroristisch eingestuften Gruppen kontrolliert. Während Gao aus Sicht der Regierung im Süden Malis und auch der UN-Truppe MINUSMA über die Versorgungswege entlang des Niger versorgt und kontrolliert wird, bestehen wichtige und bislang kaum kontrollierbare Verbindungen in den von Wüste geprägten Süden Algeriens, den Niger und hierüber auch nach Libyen. Im Grenzgebiet zwischen Algerien und Mali befindet sich das unübersichtliche Ifoghas-Gebirge, in dem sich seit 2013 verschiedene als terroristisch oder sezessionistisch eingestufte Kräfte verbarrikadiert und verlustreiche Kämpfe mit französischen und tschadischen Truppen geliefert haben. Von Mali aus liegt der Zugang zu diesem Gebirge in Kidal, das zugleich eine Provinz, ein weiträumiges Siedlungsgebiet und eine Stadt ist. Trotz intensiver Bemühungen haben es bislang französische Spezialeinheiten mit Luftunterstützung und die v. a. aus dem Tschad und anderen Nachbarstaaten stammenden Soldaten der MINUSMA nicht geschafft, diese Region auch nur annähernd unter Kontrolle zu bringen. Eine

Informationsstelle Militarisierung (IMI) e.V. - Hechinger Str. 203 - 72072 Tübingen

MINUSMA-Operation im Osten Malis. Quelle: UN

große Offensive mit 60 gepanzerten Fahrzeugen fand offenbar am 10. April 2016 statt und wurde dadurch bekannt, dass mindestens drei französische Soldaten starben, als sie auf eine Mine fuhren, was auch in deutschen Medien berichtet wurde. Über weitere Verluste ist wenig bekannt, laut Statistik der UN sind jedoch bislang 86 Menschen, davon 80 Soldaten, seit Juli 2013 im Rahmen der MINUSMA-Mission ums Leben gekommen. Damit ist MINUSMA bereits jetzt die gefährlichste UN-Mission weltweit, wobei unklar ist, welche Opfer überhaupt der MINUSMA zugeordnet werden, da Frankreich mit Kontingenten aus denselben afrikanischen Staaten, welche einen Beitrag zu MINUSMA leisten, auch im Zuge seiner Operation Barkhane operiert, die die gesamte Region von Mauretanien an der Westküste bis zum Tschad umfasst. In Mali unterstützen die MINUSMA-Truppen die malische Armee bei der Rückeroberung des Nordens. Deren Verluste werden ebenfalls nicht erfasst, sollen sich jedoch alleine bis zum Jahr 2014 auf etwa 500 belaufen haben. Die Zahl der offiziell bestätigten Gefallenen der französischen Armee beläuft sich mit dem Vorfall am 10. April bislang auf sieben, wobei in Wirklichkeit deutlich mehr französische Soldaten gefallen sein dürften.

Insofern ist es allenfalls Ausdruck (neo)kolonialer militärischer Arbeitsteilung, wenn Verteidigungsministerin von der Leyen für die Bundeswehr in Mali von keinem „Kampfauftrag“ sprechen möchte und versichert, dass die Bekämpfung von Terroristen keine Aufgabe der Bundeswehr sei. Ziel ist es vielmehr, jene Aufklärung zu leisten, mit der dann französische Spezialeinheiten mit Luftunterstützung und ihre afrikanischen Hilfstruppen ins Gefecht geschickt werden; und eben die Sicherung der Nachschubwege, der Aufklärungstrupps (durch Mobile Reaction Teams) und des Camps selbst. Dass auch die 320.000 Sandsäcke und die rund um die Uhr bemannten Wachtürme dabei alles andere als symbolisch sind, wird u. a. daran deutlich, dass eben jenes Camp Castor, das nun von der Bundeswehr geschützt wird, erst im Dezember 2015 – damals noch unter niederländischer Führung – mit Granaten beschossen wurde und bis heute nicht einmal das unmittelbare Umfeld – und schon gar nicht Gao selbst – als sicher gelten kann.

Aufgrund seiner Lage und Funktion als Tor zur Sahara ist es wenig verwunderlich, dass die im Oktober 2011 u. a. von aus Libyen zurückgekehrten Tuareg gegründete MNLA (Mouvement National de Libération de l‘Azawad) Gao zur Hauptstadt des „Staates“ Azawad kürte, als sie im April 2012 den Norden Malis für unabhängig erklärte. Gut zwei Monate später gewannen jedoch islamistische Gruppen nach heftigen Gefechten in der „Schlacht um Gao“ (26.-28.6.2012) die Oberhand in Gao, Timbuktu und Kidal. Im Januar 2013 dann erfolgte die Intervention Frankreichs, mit der Gao und Timbuktu zurückerobert wurden. Den französischen Soldaten folgten Truppen der MINUSMA-Vorgängermission AFISMA aus den Nachbarstaaten und anschließend Truppen der malischen Armee. Gerade durch diese Truppen aus dem Süden Malis kam es im Zuge der Rückeroberung im Schatten der französischen Intervention zu schweren Übergriffen auf Tuareg als „Vergeltung“ für den Vormarsch der MNLA ein Jahr zuvor. Die MNLA hat sich zwar von den Islamisten distanziert und bekämpft diese nun in Koordination mit den französischen Truppen, will aber die Präsenz der malischen Armee im Norden nicht dulden.

Wer aktuell die Oberhand und den Rückhalt der Bevölkerung in Gao selbst hat, lässt sich schwer sagen. Nach dem französischen Vormarsch gab es zwar viele Presse- und Radioberichte über jubelnde Bewohner, die französische Fahnen schwenkten und von Aufbruchsstimmung war die Rede. Mittlerweile aber ist die Berichterstattung aus Gao und Timbuktu wieder zum Erliegen gekommen. Neben den Bildern der CIMIC-Teams der Bundeswehr, die (stets mit Handschuhen bekleidete) Soldaten im harmonischen Miteinander mit Frauen und Kindern zeigen, gibt es kaum Nachrichten aus Gao, was schlicht damit zu tun hat, dass die Sicherheitslage für (westliche) Journalist_innen zu gefährlich ist. Konvois mit Waren, UN-Mitarbeiter_innen und anderen Zivilisten werden häufig auf den Straßen von und nach Gao überfallen oder angegriffen. In der Stadt dürfte weiterhin die MNLA sehr einflussreich sein, Islamisten aus dem Umland können einsickern und Anschläge verüben. In den entlegeneren Gegenden kann durchaus von Arrangements der MNLA mit islamistischen Gruppierungen ausgegangen werden, von einer Zusammenarbeit mit eher kriminell/ökonomisch motivierten bewaffneten Gruppen ohnehin. Der Krieg ist hier zum Geschäft geworden.

Logistik vom Süden und von Niger aus

Das Mandat zur Beteiligung der Bundeswehr an MINUSMA sieht neben den genannten Komponenten (sanitätsdienstliche Versorgung, Aufklärung, Sicherung und Schutz, zivil-militärische Zusammenarbeit (CIMIC)) auch Personal aus den Bereichen Führung(sunterstützung), militärisches Nachrichtenwesen, Luftbetankung und Lufttransport sowie in Stäben

und Hauptquartieren vor. Während Führungsunterstützung und Nachrichtenwesen zumindest anteilig auch in Gao stattfinden dürften, wird ein Großteil dieser Fähigkeiten von Bamako im Süden aus bereitgestellt. Hier befindet sich nicht nur das Hauptquartier der MINUSMA, sondern auch das Transit Camp Midgard auf dem Flughafen der Hauptstadt. Dort sind Logistiker der Bundeswehr stationiert, weil hier die Transportflugzeuge landen, deren Fracht dann für den Weitertransport nach Gao auf der Straße oder wiederum per Flugzeug verladen wird. Bereits bis 13. April 2016 sollen dies „über 1.200 Tonnen Material, verteilt auf 16 Transportflugzeuge“, darunter „Einsatzfahrzeuge mit Waffenanlagen, Funkgeräten und Schutzausrüstung“ sowie 350 Soldaten gewesen sein.[3] Das Mandat umfasst jedoch auch den taktischen Lufttransport von Soldaten aus den Nachbarstaaten ins Einsatzgebiet sowie „bei Bedarf“ die Luftbetankung von französischen Kampfflugzeugen.

Auf diese Weise unterstützte die Bundeswehr schon zuvor die MINUSMA und die Vorgängermission AFISMA. Hierzu hatte sie parallel zur (angeblich spontanen) Intervention Frankreichs im Januar 2013 auf dem Flughafen Dakar in Senegal einen Luftwaffenstützpunkt aufgebaut und dort Maschinen vom Typ Transall und ab März 2013 auch einen Airbus 310 zur Luftbetankung stationiert. Bis zum 30. Juli 2014 haben die deutschen Transportflugzeuge „auf mehr als 470 Unterstützungsflügen etwa 4.500 Passagiere sowie rund 520 Tonnen Material von und nach Mali“ transportiert[4] und damit einen wesentlichen Beitrag dazu geleistet, AFISMA und die darauf folgende MINUSMA-Mission zu realisieren. Die größten Kontingente dieser 11.750 Kräfte umfassenden Mission stammen (neben Bangladesch mit 1.442) aus den Staaten Burkina Faso (1.720), Tschad (1.440), Togo (934), Niger (859), Guinea (850) und Senegal (666, Stand aller Zahlen: 30.4.2016). Dabei handelt es sich um Staaten, die eine tw. sehr enge militärische Kooperation mit Frankreich (und, nachgeordnet, Deutschland) pflegen und in denen das Militär eine starke innenpolitische Rolle spielt, die aber wenig bis gar keine eigenen Fähigkeiten für den strategischen Lufttransport haben.

Die Luftbetankung gestaltete sich in der Umsetzung jedoch bald völkerrechtlich kompliziert. Praktisch konnte sie nur französische Kampfflugzeuge betreffen. Während die ursprüngliche Intervention Frankreichs unter dem Operationsnamen „Serval“ nach Auffassung der Bundesregierung und der UN noch mit dem Mandat der AFISMA zu vereinbaren war, trat die offensive Bekämpfung des Terrorismus dabei immer klarer in den Vordergrund. Spätestens als die französische Mission unter dem neuen Namen „Barkhane“ auf Mauretanien, Burkina Faso, Niger und Tschad ausgedehnt wurde, wurde jedoch eine Einzelfallprüfung nötig, ob der jeweilige konkrete Auftrag des entsprechenden französischen Flugzeuges unter das UN-Mandat fällt oder nicht. Entsprechend wurde der Airbus zurückverlegt und mittlerweile unterstützt Deutschland Frankreich mit derselben Fähigkeit in Syrien. Die Transalls und damit der Stützpunkt in Senegal wurden zwischenzeitlich für den Einsatz zur Ebola-Bekämpfung in Westafrika umgewidmet. Nun sollen die Transportmaschinen für Flüge nach Gao im benachbarten Niger stationiert werden, von dessen Hauptstadt Niamey es nur halb so weit zum Camp Castor ist, wie von Bamako aus.

Beihilfe zum Bürgerkrieg

Alle bisher genannten deutschen Kontingente finden offiziell im Rahmen der MINUSMA statt. Zeitgleich mit dem Einsatz der Luftwaffe zur Unterstützung der Mission AFISMA wurde vom Bundestag im Februar 2013 jedoch die Beteiligung an einer weiteren Militärmission im Rahmen der EU beschlossen. Dabei handelt es sich um eine Ausbildungsmission für die malischen Streitkräfte. 2013 betrug das Bruttoinlandsprodukt Malis mit seinen etwa 16 Mio. Einwohner_innen knappe 17 Mrd. US$ (im Vergleich Deutschland: 3.726 Mrd.), wovon etwa 1,5 % in eine Armee mit etwa 10.000 Kräften floss. Die erst kurz zuvor wieder verstärkt im Norden Malis stationierten Einheiten waren in kurzer Zeit von der MNLA vernichtend geschlagen und – zumindest in der Wahrnehmung ihrer im Süden verbliebenen Kameraden – regelrecht massakriert worden. Aus Empörung hierüber und insgesamt unzufrieden mit dem Krisenmanagement des amtierenden Präsidenten Amadou Toumani Touré (dessen Amtszeit einen Monat später geendet hätte) hatten im März 2012 junge Offiziere in der Hauptstadt geputscht, was die Fähigkeiten von Regierung und Armee, politisch oder militärisch auf den Tuareg-Aufstand im Norden zu reagieren, weiter minimierte. International wurde der Putsch zwar verurteilt, aber recht schnell Bereitschaft signalisiert, der Forderung der Putschisten nach internationaler Unterstützung bei der Bekämpfung der MNLA nachzukommen. Das Erstarken der Islamisten im Norden und das Eingreifen Frankreichs, mit dem angeblich ein Vormarsch der Islamisten nach Bamako verhindert wurde, ließen diese Bereitschaft weiter wachsen und so beschloss die EU Anfang 2013, eine Ausbildungsmission nach dem Vorbild eines entsprechenden EUTM-Einsatzes im Bürgerkriegsland Somalia. Ziel war es, Soldaten auszubilden, die direkt danach in den Norden geschickt werden. Deutschland beteiligte sich hieran zunächst mit 180 Kräften, weitete dieses Mandat jedoch schrittweise auf mittlerweile 350 Soldatinnen und Soldaten aus. Gegenwärtig stellt Deutschland damit nicht nur das mit Abstand größte Kontingent der Mission, sondern hat im Sommer 2014 auch die Führung des Einsatzes übernommen.

Das Hauptquartier der EUTM liegt in einem ehemaligen Hotel in Bamako, die Ausbildung findet auf dem nahegelegenen Stützpunkt Koulikoro statt und umfasst inzwischen auch Artillerie-Übungen. Deutschland kann dabei auf lange Erfahrungen bei der Zusammenarbeit mit den malischen Streitkräften zurückblicken, die bereits in den 1970er Jahren begann. Im Rahmen der Ausbildungs- und Ausstattungshilfe wurden viele (über die Jahre wahrscheinlich hunderte) höherrangige malische Militärs in Deutschland aus- und fortgebildet. Der amtierende malische Kommandant des Feldlagers in Koulikoro konnte zum Beginn der EUTM-Mission die deutschen Soldaten in ihrer Muttersprache begrüßen und dem Deutschlandfunk Interviews auf Deutsch geben. Über viele Jahre, zuletzt seit 2005, waren zudem Beratergruppen der Bundeswehr vor Ort und organisierten die kostenlose Überlassung von militärischer Ausrüstung, nicht jedoch von Waffen und Munition. Einen Schwerpunkt bildete dabei schon traditionell das Pionierwesen und insbesondere der Brückenbau und andere Methoden zum spontanen Überwinden von Gewässern.

Betrachtet man die Geografie des Binnenlandes Mali, ist diese Priorisierung bemerkenswert. Schließlich strebt die Bevölkerung im Norden bereits seit Jahrzehnten eine möglichst hohe Autonomie an und wurden vergangene, meist von Tuareg dominierte Aufstände mehrfach durch Zusagen befriedet, die Stationierung vom Süden kontrollierter Sicherheitskräfte im Norden zu reduzieren. Während in Timbuktu das Denkmal „Flamme de la Paix“ an die symbolische Verbrennung hunderter Waffen nach einem solchen Friedensschluss im Jahr 1996

Informationsstelle Militarisierung (IMI) e.V. - Hechinger Str. 203 - 72072 Tübingen

Patrouille der MINUSMA-Polizeikräfte in Gao. Quelle: UN

erinnerte, lieferte Deutschland Ausrüstung und Know How, das es der malischen Armee ermöglichte, mit großen Kontingenten unerwartet den Niger zu überqueren und in den Norden vorzustoßen.

Die militärische Ausbildungs- und Ausstattungshilfe wurde nach dem Putsch 2012 kurzzeitig eingestellt, offenbar mittlerweile aber wieder aufgenommen. Im April 2016 nannte die Bundesregierung drei Projekte der Ausstattungshilfe im Umfang von insgesamt 3.15 Mio. Euro für den Zeitraum 2013-2016, darunter Instandsetzungsmaßnahmen an der Zentralwerkstatt der Pioniere in Bamako und die „Nachsorge am Ausbildungszentrum in Bapho (Wasserübungsplatz für Fähranlagen und Brückenbau; Pontoneinsatz)“.[5] Die Zahl der hierfür eingesetzten Berater wird von der Regierung mit zwei (vier ab Juli 2016) angegeben. Die Bundeswehr berichtete jedoch bereits im März 2015 unter dem Titel „Auf zu neuen Ufern“ von einer Ausbildungsmaßnahme mit „elf deutschen Soldaten und ihre[n] knapp 60 ‚Azubis‘“ in Segou, von Koulikoro etwa 100 km nordöstlich entlang des Niger gelegen: „Das Niger-Binnendelta ist eine Lebensader für die malische Bevölkerung. Für die Streitkräfte des westafrikanischen Landes hingegen ist er das größte Hindernis. Brücken gibt es in Mali kaum. Nur in der Hochwasserzeit zwischen Oktober und Januar kann der Fluss mit größeren Booten überquert werden. Mit der Hilfe deutscher Pioniere aus Minden lernen die malischen Soldaten den Fluss mit einfachen Mitteln zu überqueren“.[6]

Offenbar fand diese neunwöchige Ausbildung im Rahmen des EUTM-Einsatzes, jedoch außerhalb des Standortes statt. Für die Zukunft ist die Ausdehnung der EUTM auf mehrere Standorte entlang des Niger bis in den umkämpften Norden geplant. Damit wird der Einsatz zwangsläufig gefährlicher und „robuster“ und die Grenzen zum Kampfeinsatz verschwimmen weiter.

Gefährlich ist jedoch auch die EUTM-Mission bereits jetzt. Am 21. März meldete der Europäische Auswärtige Dienst (EAD) einen Angriff auf deren Hauptquartier in Bamako, bei dem ein Angreifer getötet worden sei. Wie viele Angreifer es gab und wer an dem Gefecht beteiligt war, wurde jedoch nicht veröffentlicht. Dass sich die Sicherheitslage weiter verschärft, unterstreicht auch das Erstarken der erst seit Anfang 2015 existierenden „Front de libération du Macina“ im Gebiet um Mopti, das wiederum nur gut 100 km nordöstlich von Segou liegt, wo die Ausbildungsmaßnahme zur Überwindung des Niger stattfand. Diese bewaffnete Gruppe rekrutiert aus der dort ansässigen Bevölkerungsgruppe der Fulbe, die beim Konflikt zwischen Norden und Süden zwischen die Fronten gerieten. Obwohl sie in Zentralmali und außerhalb des Azawad leben, wird ihnen oft pauschal von den Sicherheitskräften Sympathie für die Islamisten unterstellt. Bereits im Januar 2016 hatte Human Rights Watch einen Bericht veröffentlicht, wonach zahlreiche Fulbe von der malischen Armee misshandelt, willkürlich inhaftiert und in einigen Fällen auch exekutiert wurden.[7] Womöglich wird der Konflikt auch von einzelnen Fraktionen bewusst angeheizt und ethnisiert. Anfang Mai etwa berichteten internationale Presseagenturen übereinstimmend, dass nahe Mopti zunächst vier Vertreter der Fulbe in einem Restaurant von einer regierungstreuen Miliz erschossen und bei der anschließenden Beerdigung neun weitere Angehörige der Gemeinschaft getötet wurden.

Drohnenkrieg und Militarisierung – für seltene Erden?

Aktuell ist der Einsatz von 1.000 Soldaten der Bundeswehr in Mali mandatiert. Darüber hinaus sind weitere deutsche Soldaten ohne Mandat des Bundestages vor Ort, wie etwa die Beratergruppe und Personal an der „Ecole de Maintien de la Paix“

(EMP), wo afrikanische Polizisten für den Einsatz in „Friedensmissionen“ wie MINUSMA ausgebildet werden. Außerdem hat Deutschland auch die Führung der im Januar 2015 begonnenen zivil-militärischen Mission EUCAP Sahel Mali inne. Solche Missionen der EU zum Kapazitätsaufbau gelten ansonsten meist als „zivile“ Einsätze, da sie v. a. aus Berater_innen und Polizeikräften bestehen. Bei EUCAP Sahel Mali jedoch spielt die European Gendarmerie Force (EGF) eine zentrale Rolle und damit jene Einheiten der EU-Mitgliedsstaaten Spanien, Frankreich, Italien, Niederlande, Portugal, Rumänien und Polen, die sowohl unter zivilem Kommando, als auch militärisch mit Kombattantenstatus eingesetzt werden können. Im Rahmen der EUCAP-Mission in Mali werden zwar auch Lehrgänge für Verkehrspolizist_innen veranstaltet, zugleich steht jedoch auch jenes für die EGF typische Spektrum von Einsatzformen auf dem Programm, das vom Tränengas- und Schlagstockeinsatz gegenüber Demonstrationen über den Personenschutz inklusive Nahkampfausbildung bis hin zu geheimdienstlichen Ermittlungen reicht.

Zusammenfassend kann mit Fug und Recht davon gesprochen werden, dass Mali mit tatkräftiger Unterstützung Deutschlands umfassend militarisiert wird. Das von der UN für MINUSMA erteilte Mandat ist entsprechend ausgreifend und unbestimmt zugleich und damit völlig unrealistisch. In Bundeswehrkreisen wird deshalb auch von einem Einsatz ausgegangen, der Jahrzehnte dauern könnte. Sicherheitslage und regionales Umfeld sind in vielerlei Hinsicht mit Afghanistan vergleichbar. 2017 soll die zukünftig in Mali stationierte Drohne Heron I außerdem durch das Nachfolgemodell Heron TP ersetzt werden, die bewaffnungsfähig ist. Es braucht dann nur noch einen Vorfall mit einigen verwundeten oder verletzten Bundeswehrangehörigen, und die Forderung wird laut werden, dass nun auch Deutschland mit bewaffneten Drohnen auf die Jagd nach Terroristen gehen soll.

Diese Militarisierung findet statt, während unter den beteiligten europäischen Staaten keinerlei Einigkeit oder Konzept besteht, wie die zugrundeliegenden Konflikte gelöst und der malische Staat zukünftig organisiert werden soll. Zur Erinnerung: Die Bundeswehr bildet malische Soldaten aus, die nicht nur Minderheiten attackieren, sondern ihrerseits in einem schweren Konflikt mit der immer noch nach Unabhängigkeit strebenden MNLA steht. Diese kämpft in Koordination mit Frankreich jene Gebiete frei, die anschließend von MINUSMA und der Bundeswehr kontrolliert werden können, damit hier wiederum die malische Armee stationiert werden kann. Während im UN-Mandat das Ziel der territorialen Integrität verankert ist, unterstellen Viele Frankreich als wichtigstem militärischen Akteur jedoch ganz andere Ziele. Alexander Göbel etwa, „Afrika-Korrespondent“ des Deutschlandfunks, mutmaßte bereits im Juni 2015: „Fakt ist: Wie im Nachbarland Niger gibt es auch im Norden Malis Uran, außerdem Gold, Seltene Erden, Erdöl. Je näher die Tuareg-Rebellen ihrem Ziel kommen - einem unabhängigen Staat Azawad -, desto leichter dürfte es für Frankreich sein, später die Ressourcen zu kontrollieren. Ein Friedensvertrag, gar ein wirklich souveräner und stabiler malischer Staat, der würde dieser Strategie nur im Wege stehen.“[8] Vor allem stabile und demokratische Staatswesen – in Mali, Niger dem Tschad und allen anderen in diesen Konflikt gezogenen Ländern des Sahels – dürften diesen Zielen noch viel mehr im Wege stehen.

Anmerkungen

1 Bundesregierung verlegt Heron-Drohnen nach Mali, zeit.de vom 5.4.2016.
2 „‚Über Fußball kommt man immer ins Gespräch‘ – Eine Einsatzregion verstehen durch CIMIC“, Einsatz.Bundeswehr.de, 31.3.2016.
3 „MINUSMA: Wichtig für den Aufbau – Die Drehscheibe Bamako-Sénou“, Einsatz.Bundeswehr.de, 13.4.2016.
4 „Die Bundeswehr in Mali (MINUSMA)“, Einsatz.Bundeswehr.de, 5.4.2016.
5 Bundestags-Drucksache 18/8086.
6 „Auf zu neuen Ufern - deutsche und malische Pioniere überqueren gemeinsam den Niger“, Einsatz.Bundeswehr.de, 31.3.2015.
7 Human Rights Watch: Mali: Abuses Spread South - Islamist Armed Groups’ Atrocities, Army Responses Generate Fear, 19.02.2016.
8 Ein Friedensvertrag, gestützt auf lose Hoffnungen, deutschlandfunk.de, 20.6.2015.

Polizeitraining im Rahmen von MINUSMA. Quelle: UN

Informationsstelle Militarisierung (IMI) e.V. - Hechinger Str. 203 - 72072 Tübingen

Die ewige Konstruktion der russischen Gefahr

Rezension des Buches „Feindbild Russland“ von Hannes Hofbauer

von Mirko Petersen

Im Zuge der Ukraine-Krise ab Ende 2013 und des anschließenden Krieges im Osten des Landes wurden die Abstände zwischen den Schuldzuweisungen und Beschimpfungen Russlands vonseiten der europäischen und nordamerikanischen Politiker_innen, Wissenschaftler_innen und Presseorgane immer kürzer. Es schien außer Frage zu stehen, wer für die Gewalteskalation in der Ukraine verantwortlich war: Moskau, der Kreml, Putin… also die Namen, mit denen das größte Land der Welt in Verbindung gebracht wird.

Die Konstruktion des Feindbildes Russland war jedoch keineswegs ein neues Phänomen, das in Zeiten der Ukraine-Krise und des damit verbundenen geopolitischen Konfliktes zwischen Russland und dem Westen entstanden war. Dies zu zeigen, ist das Anliegen des Buches „Feindbild Russland. Geschichte einer Dämonisierung“ des Journalisten und Historikers Hannes Hofbauer, das vor kurzem im Wiener Promedia Verlag erschienen ist. Der Autor verfolgt das Phänomen europäischer Russophobie und strategischer Abwertung Russlands bis ins 15. Jahrhundert (als das Moskowiter Großreich entstand) zurück und zeigt Kontinuitäten und Brüche der westlich-russischen Beziehungen auf. Hofbauer stützt sich dabei v.a. auf eine große Bandbreite von Sekundärliteratur sowie auf diverse Interviews mit Expert_innen in Russland.

Vom 15. Jahrhundert bis zum Kalten Krieg

Im ersten Kapitel des Buches geht es um die Ursprünge des „im Westen des [europäischen] Kontinents verbreitete[n] Bild[es] vom ‚asiatischen, barbarischen Russland‘“ (S.13). Hofbauer siedelt die Ursprünge in den sechs Kriegen an, die das Moskauer Fürstentum und Polen-Litauen bzw. Livland zwischen 1492 und 1582 führten. Die in Kriegen übliche Feindbildkonstruktion entstand in diesem Fall in Polen und griff dann durch Ideentransfers in den deutschen Sprachraum über. Während hier viele Stimmen noch von der Verteidigung des „wahren“ Christentums gegenüber dem orthodoxen Christentum des Moskowiter Reiches sprachen, wandelte sich dies teilweise in den darauffolgenden Jahrhunderten. Verschiedene westeuropäische Strategen wogen die russische Gefahr gegen die osmanische Gefahr ab und kamen zu unterschiedlichen Ergebnissen. Eine interessante Parallele zum Ende des 20. Jahrhunderts wies das späte 17. und 18. Jahrhundert auf: Wenn ein westlich gesinnter Modernisierer wie Peter der Große die Macht in Russland übernahm (ähnlich wie später, auf verschiedene Art und Weise, Michail Gorbatschow und Boris Jelzin), so veränderte sich auch das Russlandbild in Westeuropa zum Positiven.

Im nächsten Kapitel liefert der Autor eine Analyse des Blicks aufs Russland im 19. Jahrhundert, speziell im Deutschen Bund bzw. Deutschen Reich, wo „die libertäre Öffentlichkeit […] anti-russisch [und] die dynastische Reaktion prorussisch gesinnt“ (S.32) war. Die Verschärfung der russischen Feindbildkonstruktion über politische Gesinnungen hinweg ereignete sich dann im Ersten Weltkrieg, was Hofbauer zu Beginn des darauffolgenden Kapitels behandelt, welches den Zeitraum der beiden Weltkriege umfasst. In diesem Kapitel finden zwei Aspekte Erwähnung, die für das Verständnis der heutigen Situation zentral sind. Zum einen ist dies die geopolitische Denkschule, die durch die viel beachteten Theorien des britischen Geografen Halford Mackinder einen Schub erfuhren. Mackinder sah die Kontrolle Russlands und der eurasischen Landmasse (das sog. Herzland) als Schlüssel zur globalen Vorherrschaft – ein Argumentationsmuster, das sich bis in die Gegenwart finden lässt, am prominentesten wohl in den Schriften des US-Strategen Zbigniew Brzezinski. Zum anderen hebt Hofbauer hervor, dass im Ersten Weltkrieg die Idee der Destabilisierung eines bestimmten Teils der russischen Peripherie zu einem wichtigen Muster der deutschen Kriegsführung gegen Russland wurde: „das Herauslösen der Ukraine aus dem Russischen Reich“ (S.45). Das Aufzeigen dieser Denkkontinuitäten bis in die Gegenwart kann als eine der Stärken dieses Buches bezeichnet werden.

Nach der Analyse der Zeit des Ersten Weltkriegs betrachtet Hofbauer einige der schlimmsten Vernichtungs- und Unterwerfungsfantasien des Nationalsozialismus in Bezug auf die Sowjetunion, in denen sich Imperialismus, Rassismus, Antisemitismus und Antikommunismus vermischten. Ihren Höhepunkt erreichte die Feindbildkonstruktion der Nazis nach dem Angriff auf die Sowjetunion im Juni 1941, also nach dem Ende des Hitler-Stalin-Paktes. Im darauffolgenden Kapitel, das die verschiedenen Phasen des Kalten Krieges behandelt, findet dann ein Bruch statt. Das Kapitel zum Kalten Krieg thematisiert fast nur noch die US-amerikanische Sichtweise auf die Sowjetunion und Washingtons Politik gegenüber der UdSSR, wobei die Politik der Regierung Ronald Reagans besonders viel Aufmerksamkeit erfährt. Dies begründet der Autor mit der dominanten Rolle der USA im Nachkriegseuropa. Trotzdem ist diese Vernachlässigung der europäischen Betrachtung der UdSSR in dieser Phase analytisch nicht ganz nachzuvollziehen, da sich hier z.B. sowohl ein Blick auf den deutschen Anti-Kommunismus unter Konrad Adenauer als auch auf die spätere Entspannungspolitik unter Willy Brandt gut an die vorherigen Kapitel hätte anfügen lassen können.

Von der Jelzin-Ära bis zum Krieg in der Ukraine

Im Anschluss an das Kapitel zum Kalten Krieg geht es um die Jelzin-Ära in Russland, die auf den Zusammenbruch der Sowjetunion folgte. Hier werden innenpolitische Entwicklungen in Russland, die ökonomische Schocktherapie im größten Land der Erde sowie die ersten Schritte zur NATO-Osterweiterung thematisiert. Hofbauer verdeutlicht, dass die westliche Vorstellung des Demokraten Boris Jelzin im Kontrast zum Autokraten Wladimir Putin nicht funktioniert. Die autokratische Politik in Russland wurde von den meisten westlichen Politiker_innen unter Jelzin noch für unproblematisch befunden. Erst als sich die Regierung unter Wladimir Putin der westlichen Politik entgegenstellte, wurde die Moskauer Autokratie problematisiert. Das Russland seit der Machtübernahme Putins wird anschließend genauer geschildert. Die Ana-

lyse dieser Phase ist ausgewogen gestaltet. Hofbauer erwähnt sowohl die Verbesserungen in Russland im Vergleich zu den Jelzin-Jahren, prangert aber auch Autokratie und Missstände an. Nur an wenigen Stellen kommt das russische Regime etwas zu verharmlost davon. Zu nennen ist hier die Beschreibung des Vorgehens Moskaus gegen ausländische NGOS, das per se als nachvollziehbar dargestellt wird (als Reaktion auf westliche Destabilisierung), ohne vollkommen fadenscheinig begründete (Generalverdacht: „ausländischer Agent“) politische Unterdrückungen zu erwähnen, wie z.B. die gegen die Organisation „Memorial“, die sich für die Aufarbeitung stalinistischer Verbrechen einsetzt.

Die aktuellen Entwicklungen, besonders mit Blick auf die Ukraine, rücken im weiteren Verlauf des Buches in den Vordergrund. Dies beginnt mit einer Analyse der vom Westen unterstützten „Farbrevolutionen“, u.a. der sog. Orangenen Revolution in der Ukraine im Jahr 2004 und setzt sich in den Kapiteln zum Ringen um die Ukraine und der westlichen Sanktionspolitik gegen Russland fort. All diese Themen werden detail- und kenntnisreich geschildert. In erster Linie behandelt Hofbauer das Engagement der Vereinigten Staaten und der Europäischen Union in Osteuropa, welches häufig zum Ziel hatte und hat, den politischen Einfluss Russlands in der Region zu minimieren. Hierzu ist jedes Mittel recht, bis hin zur Zusammenarbeit mit offen rechtsradikalen Gruppierungen. In Bezug auf die Ukraine hält der Autor aber ebenfalls fest: „Moskau wusste – und weiß – die wirtschaftliche Abhängigkeit der Ukraine für seine eigenen wirtschaftlichen und geopolitischen Interessen zu nutzen (S.178).“

Besonders das Kapitel zu den Sanktionen gegen Moskau wartet mit vielen wenig beachteten Fakten auf, z.B. dass sich die westlichen Sanktionen nicht nur gegen Politik- und Wirtschaftseliten, sondern auch gegen „eurasische“ Intellektuelle aus Russland richtet (also diejenigen, die sich gegen einen europafreundlichen Kurs der russischen Regierung aussprechen). Dazu Hofbauer: „Insbesondere die eurasische Idee gilt den Vertretern einer liberalen Demokratie aus dem Westen als großes Feindbild. Deshalb darf der führende Kopf der Eurasier, Aleksander Dugin, nicht nach EU-Europa und in die USA einreisen, und deshalb wird die Eurasische Jugendunion als Ganzes vom Austausch mit der westlichen Welt ferngehalten (S. 234).“

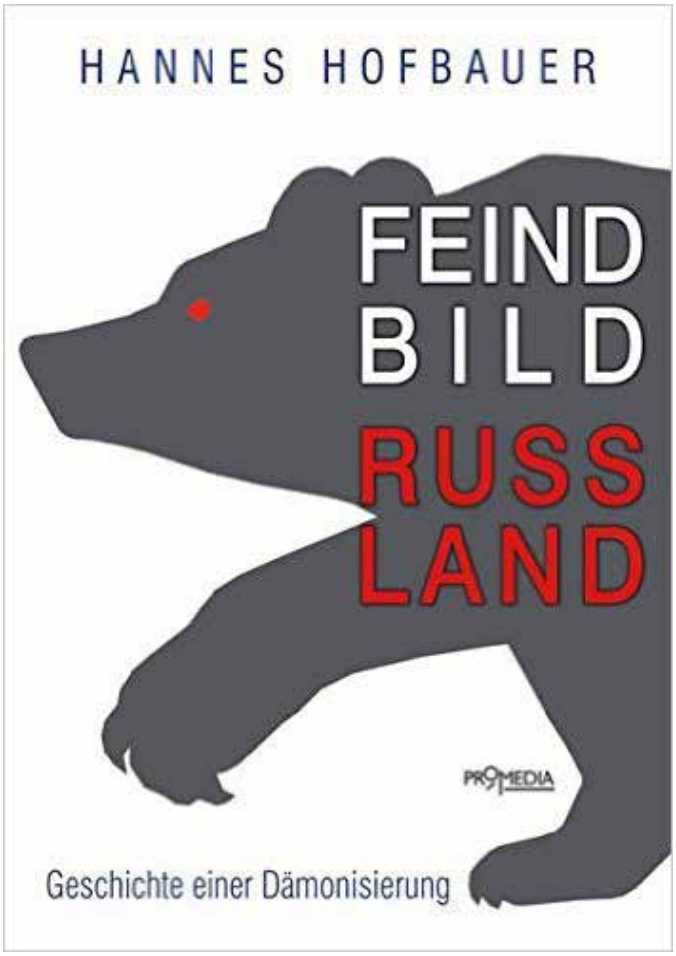
Im letzten Kapitel widmet sich Hofbauer dann expliziter der westlichen Feindbildkonstruktion und deren Konjunkturen seit 1999, also kurz vor dem Ende der Jelzin-Ära. Dabei stellt er fest: „Im Fünfjahresrhythmus verschlechterten sich die Beziehungen des Westens zu Russland. Den jeweiligen Zäsuren 1999 (NATO-Krieg gegen Jugoslawien), 2003 (Festnahme von Michail Chodorkowski), 2008 (Georgien-Krieg) und 2013/14 (Ukraine-Krise) folgte eine politische und medial aufgeladene Stimmung, die Schritt für Schritt in Hetze umschlug (S. 272).“ Genau dies ist es, was die Feindbildkonstruktion ausmacht. Deshalb ist es etwas verwunderlich, dass ein Buch, das das Wort „Feindbild“ im Titel trägt, sich relativ wenig der eigentlichen Konstruktion dieser Bilder widmet (am stärksten, wie erwähnt, im letzten Kapitel des Buches).

Kritik und Fazit

Die Nicht-Erfüllung dessen, was der Titel zumindest andeutet, stellt auch die größte Kritik an einem ansonsten gut recherchierten, informativen und angenehm lesbaren Buch dar. Auf den Begriff des Feindbildes geht der Autor nur ganz kurz im Vorwort ein und im folgenden Text kann sich der/die Leser_in häufiger fragen: Wer konstruiert jetzt eigentlich das Feindbild bzw. um wessen Feindbild handelt es sich genau? Wie wird es konstruiert? Worin besteht das Feindbild genau? Diese Fragen tauchen u.a. deshalb auf, weil die geografische Analyseeinheit (Deutschland, deutschsprachiger Raum, Westeuropa, EU, USA, der Westen) und die analysierten Akteure (Intellektuelle, Politiker_innen, Diplomat_innen, Propagandaapparate, Presse) häufig wechseln, ohne dass der Autor dies ausreichend reflektiert. Eine bessere Gestaltung dieser Erklärungen hätte das bereits gut gelungene Aufzeigen von Kontinuitäten und Brüchen in der Geschichte der Dämonisierung Russlands noch weiter verbessern können. Eine gelungene historische und zeitgeschichtliche Fundierung für bedeutende aktuelle Debatten hat Hannes Hofbauer mit seinem Buch aber allemal geliefert.

Als Fazit des Buches gibt uns der Autor für die Betrachtung der geopolitischen Konfrontation zwischen Russland und dem Westen das Folgende mit auf den Weg: „Wie auch immer unzulänglich und fehlerhaft Moskaus Integrationsversuche ausfallen sollten, ob sie auf nationaler, etatistischer oder eurasischer Grundlage stehen, im Westen werden sie mehrheitlich unter der Brille der Feindwahrnehmung betrachtet, abgelehnt, lächerlich gemacht oder als Gefahr für die eigenen Interessen dargestellt (S.295).“

Eckdaten zum Buch
Autor: Hannes Hofbauer
Titel: Feindbild Russland. Geschichte einer Dämonisierung
Umfang: 304 Seiten
Verlag und Erscheinungsjahr: Promedia Verlag (Wien), 2016.



Informationsstelle Militarisierung (IMI) e.V. - Hechinger Str. 203 - 72072 Tübingen

Alle Rüstungsexporte stoppen!

Die machtpolitische Funktion des Waffenhandels aufzeigen!

von Jürgen Wagner

Ende Januar 2016 trat Verteidigungsministerin Ursula von der Leyen vor die Presse und verkündete, bis 2030 würden nicht weniger als 130 Mrd. Euro in die Neuanschaffung von Rüstungsgütern gesteckt. Hierfür muss der Investitionshaushalt schnellstmöglich von 4,7 Mrd. Euro (2016) auf etwa 9 Mrd. Euro angehoben werden. Dies ist auch einer der Gründe dafür, dass der Haushalt nicht nicht mehr „nur“ wie ursprünglich geplant von 26,8 Mrd. Euro (2006) auf 35 Mrd. Euro (2019), sondern inzwischen auf satte 39,2 Mrd. (2020) steigen soll. [1]

Im Februar 2016 wurde dann bekannt, dass die deutschen Rüstungsexportgenehmigungen im Vorjahr mit fast 12,5 Mrd. Euro ein Allzeithoch erreicht haben.[2] Zu Recht wird argumentiert, dass diese Exporte zu Krieg und Chaos beitragen und mitbeteiligt sind, Menschen zur Flucht zu zwingen. Auch trifft zu, dass diese Zahlen im krassen Widerspruch zu den Aussagen von Wirtschaftsminister Sigmar Gabriel stehen, die Waffenausfuhren spürbar einschränken zu wollen.

Fakt ist: Weder Gabriel noch irgendein anderer führender deutscher Politiker hat die Absicht, die Rüstungsexporte spürbar einzuschränken – im Gegenteil. Die eigentliche Frage, der dieser Artikel nachgehen will, ist daher: Weshalb ist dies der Fall?

Kurz gesagt: Dies allein auf ein „effektives“ Lobbying zurückzuführen, ist analytisch nicht weit genug gedacht. Denn eine starke einheimische Rüstungsindustrie ist die Voraussetzung, um eine „wirkungsvolle“ Militär- und Machtpolitik betreiben zu können. Und zentrale Mittel, um dies zu erreichen, sind die Erhöhung der Rüstungsausgaben sowie die „Verbesserung“ der Wettbewerbs- und damit Exportfähigkeit der Branche. Oder noch kürzer auf den Punkt gebracht: Was gut ist für die deutsche Rüstungsindustrie, ist doppelt so gut für die machtpolitischen Ambitionen Deutschlands.

Gabriel als Totengräber der Rüstungsindustrie?

Wirtschaftsminister Sigmar Gabriel wird fälschlicherweise immer wieder vorgeworfen, aufgrund seiner restriktiven Haltung gegenüber dem Export von Rüstungsgütern betätige er sich als „Totengräber der wehrtechnischen Industrie Deutschlands“.[3] Wie er zu diesem, an sich ja honorigen Ruf kam, ist allerdings schleierhaft, denn bei der Erhöhung des Rüstungshaushaltes und dem Ausbau der Waffenexporte handelt es sich um Kernelemente der von der Bundesregierung im Oktober 2014 gestarteten „Agenda Rüstung“, der sich auch Gabriel verpflichtet fühlt.

Dies zeigte sich deutlich in seiner rüstungspolitischen Grundsatzrede vom 8. Oktober 2014, in der Gabriel nicht einmal Waffenlieferungen in Krisengebiete eine Absage erteilte, die Unterstützung der Peschmerga befürwortete er z.B. ausdrücklich: „Aber zugleich müssen wir – und das ebenfalls mit großer Klarheit – feststellen, dass es natürlich legitime sicherheits- und bündnispolitische Interessen gibt, welche die Lieferung von Rüstungsgütern und Kriegswaffen rechtfertigen können. […] Deutschland und seine Partner haben ein eigenes Interesse daran, Piraterie, Terrorismus und Proliferation von Waffen, wie sie im Nahen und Mittleren Osten auftreten, einzudämmen. […] Die Lieferungen an die Kurden im Norden des Irak, die der Abwehr einer fanatisch-grausamen Terrorbewegung wie dem so genannten ‚Islamischen Staat‘ dienen, sind weder ein Tabubruch und noch gar ein Widerspruch zu unseren Werten und Rechtsregeln.“[4]

Selbst wenn man es wohlwollend betrachtet, geht es also lediglich darum, Rüstungsexporte nur für Krisenregionen und hier auch nur in überschaubarem Ausmaße zu beschränken. Doch ein Großteil der deutschen Rüstungsexporte ist aus Gabriels Sicht ohnehin völlig unproblematisch, und hier gäbe es noch enormes Wachstumspotenzial – Rüstungslieferungen an zertifizierte Freunde: „Die Bundesregierung sollte die Industrie stärker als bisher in ihren Aktivitäten mit EU-, NATO- und NATO-gleichgestellten Ländern unterstützen. Die NATO hat 28 Mitgliedsstaaten. Sie geben zusammen 880 Milliarden Dollar für die Verteidigung aus. Hinzu kommen fünf EU-Länder, die nicht Mitglied der NATO sind – zusammen also 33 formale Bündnispartner. Auch Indien und Brasilien sind strategische Partner für Deutschland und Europa. In alle diese Demokratien mit ihren großen Volkswirtschaften und Verteidigungsetats kann die deutsche und die europäische wehrtechnische Industrie liefern.“[5]

Nachdem Gabriel in derselben Rede dann auch noch explizit eine „exportpolitische Flankierung für die Verteidigungsindustrie“ ankündigte[6], kann an seiner Absicht, künftig sogar verstärkt auf Waffenexporte zu setzen, genauso wenig Zweifel bestehen, wie an der des Großteils seiner Kollegen.

Ohne Exporte keine Rüstungsindustrie!

Ursächlich für die augenscheinliche Affinität zu Waffenexporten ist nicht zuletzt der Umstand, dass der heimische Markt trotz von der Leyens jüngster Rüstungsoffensive viel zu klein ist. Mit anderen Worten: Die deutsche Rüstungsindustrie wäre ohne Exporte schlicht nicht überlebensfähig. Solange es eine deutsche Rüstungsindustrie gibt, solange wird es also auch zwingend deutsche Rüstungsexporte geben. In den Worten von Claus Günther, der BDI-Vorsitzende des Ausschusses Sicherheit: „Wir brauchen Exporte, denn allein durch die dünne nationale Auftragsdecke wird die deutsche Rüstungsindustrie nicht überlebensfähig sein.“[7]

Weshalb die Rüstungsindustrie an Exporten interessiert ist, liegt auf der Hand; sie erhöhen die ohnehin schon ordentlichen Profite. Allerdings ist die Bundesregierung nur allzu bereit, hier unterstützend unter die Arme zu greifen, weil dies der angestrebten starken rüstungsindustriellen Basis zuträglich ist. So äußerte sich Gabriel in seiner rüstungspolitischen Grundsatzrede: „Die Erhaltung der Bündnisfähigkeit und der dazu notwendigen rüstungstechnologischen Kernkompetenzen sind ein zentrales außen- und sicherheitspolitisches Interesse der Bundesrepublik Deutschland.“[8] Aus diesem Grund kündigte er bei dieser Gelegenheit auch gleich noch eine „exportpolitische Flankierung für die Verteidigungsindustrie“ an, die dann im Oktober 2015 in das „Strategiepapier der Bundesregierung zur Stärkung der Verteidigungsindustrie in Deutschland“ einfließen sollte. In ihm wurde besagte Flankierung folgenderma-

ßen konkretisiert: „Auf dieser Basis wird die Bundesregierung daran festhalten, die Verteidigungsindustrie bei ihren Aktivitäten insbesondere in EU-, NATO- und der NATO gleichgestellten Ländern zu unterstützen. Diese Flankierung kann auch auf so genannte Drittstaaten ausgedehnt werden […]. Die Bundesregierung wird Exportaktivitäten nach Einzelfallprüfung mit dem außenwirtschaftlichen und sonstigen Instrumentarium flankieren und dabei auch speziell verteidigungsindustrielle Schlüsseltechnologien berücksichtigen.“[9]

Die Bundesregierung nennt dabei drei wesentliche Gründe, weshalb diese exportpolitische Flankierung zur Stärkung der rüstungsindustriellen Basis erforderlich sei: arbeitsmarktpolitische, wirtschaftliche und machtpolitische.

Wirtschaftlicher Nullfaktor – machtpolitisches Pfund

Was die Arbeitsplätze anbelangt, so sind in der Rüstungsindustrie nach Eigenangaben gerade einmal 98.000 Menschen beschäftigt, im Kernbereich sogar nur 17.000.[10] Selbst die höhere Zahl bedeutet über den Daumen gepeilt lediglich einen Anteil von 0,24 Prozent aller Erwerbstätigen in Deutschland. Studien belegen zudem, dass kein Sektor pro staatlich investierter Milliarde weniger Arbeitsplätze abwirft als der Rüstungsbereich. Auch volkswirtschaftlich ist die Relevanz der Rüstungsindustrie überschaubar. Sie steuert etwa 1 Prozent zum Bruttoinlandsprodukt (BIP) bei. Zum Vergleich: Allein die Autoindustrie kommt auf 7 Prozent.[11] Auch die viel beschworenen „Spin-Offs“, technologische Innovationen, die vom Rüstungssektor erfunden werden und danach massiv zur volkswirtschaftlichen Entwicklung beitragen, existieren lediglich in der Phantasie der Rüstungsbefürworter. In Wahrheit wird umgekehrt ein Schuh daraus: Innovationen gehen auf den zivilen Sektor zurück, derer sich die Rüstung dann bedient. So schrieb Martina Fischer bereits in einem Aufsatz aus dem Jahr 1994: „Das Argument, daß über Rüstung das technologische Niveau der Industrie insgesamt und dadurch die internationale Wettbewerbsfähigkeit zu steigern sei, wurde von verschiedenen rüstungs- und technologiepolitischen ExpertInnen bereits in den siebziger Jahren angezweifelt und vor allem im Verlaufe der achtziger Jahre anhand von Länderbeispielen sowohl bezogen auf die Industriestaaten wie auch für Dritte-Welt-Länder widerlegt.“[12]

Jahr	Einzelgenehmigungen gesamt (in Mio. €)	Sammelausfuhrgenehmigungen gesamt (in Mio. €)	Summe der Einzel- und Sammelgenehmigungen (in Mio. €)
2004	3806	2437	6243
2005	4215	2032	6258
2006	4189	3496	7685
2007	3668	5053	8721
2008	5788	2546	8334
2009	5043	1996	7039
2010	4754	737	5491
2011	5414	5381	10795
2012	4704	4172	8876
2013	5846	2494	8340
2014	3974	2545	6519
2015	7500	4960	12460

Quelle: Rüstungsexportberichte der Bundesregierung, Drucksache 18/7721 (26.02.2016)

Eine Konversion, also die Umstellung der Rüstungsproduktion auf die Herstellung ziviler Güter, wäre also möglich und gesellschaftlich wünschenswert, wie u.a. auch eine Resolution der Delegiertenkonferenz der IG Metall Stuttgart im September 2014 deutlich zum Ausdruck brachte: „Wir verurteilen Rüstungsproduktion und Rüstungsexporte […] Arbeitsplatzverluste in der Rüstungsindustrie sind durch Wandlung in Arbeitsplätze zur Herstellung ziviler, gesellschaftlich notwendiger Produkte zu kompensieren. Rüstungsarbeitsplätze erfordern Investitionen in teure Technologie. Für dieses Geld können in anderen Bereichen (Bildung, Gesundheit…) mehr und gesellschaftlich sinnvolle Arbeitsplätze geschaffen werden. Die Konversionsdebatte muss in den Rüstungsbetrieben nachhaltig geführt werden. Hier übernimmt die IG Metall eine aktive und steuernde Rolle.“[13]

Woran es hier fehlt, ist allein der politische Wille. Und das hat primär mit der dritten und entscheidenden Antwort zu tun, weshalb die Rüstungsindustrie und ihre Exporte gestärkt werden sollen: Eine eigenständige Rüstungsindustrie gilt als unerlässlicher Machtfaktor eines erstrangigen weltpolitischen Akteurs. Jedwede Abhängigkeit vom Kriegsgerät anderer Länder schränkt die machtpolitische Beinfreiheit ein. Gleichzeitig steigen durch Exporte die Stückzahlen und tragen somit durch Skaleneffekte – so zumindest die Theorie – zur Senkung der Stückpreise für den „Heimverbraucher Bundeswehr“ bei – es wird also über Exporte mehr militärische Schlagkraft pro investiertem Euro generiert.[14]

Spätestens seit den Auftritten von Bundespräsident Joachim Gauck, Verteidigungsministerin Ursula von der Leyen und von Außenminister Frank-Walter Steinmeier bei der Münchner Sicherheitskonferenz 2014 will Deutschland erklärtermaßen mehr militärische „Verantwortung“ übernehmen – also machtpolitisch in der allerersten Reihe mitspielen. Und das geht eben nur, wenn man auch über eine hierfür „notwendige“ industrielle Basis verfügt, wie der „Bundesverband der Sicherheits- und Verteidigungsindustrie“ der Politik hinter die Ohren schreibt: „Die Bundesrepublik Deutschland hat sich entschieden, Verantwortung für sicherheitspolitische Aufgaben zu übernehmen und sich mit ihren Partnern für die Durchsetzung gemeinsamer Werte und Ziele einzusetzen. […] Um die genannten Aufgaben entsprechend wahrnehmen zu können, kann es in einigen Fällen militärischer Maßnahmen bedürfen […]. Nur eine eigene deutsche Sicherheits- und Verteidigungsindustrie [kann] die politisch als wichtig eingeschätzte Versorgungssicherheit der deutschen Einsatzkräfte gewährleisten und so die Handlungsfähigkeit Deutschlands sichern.“[15]

Zu einem ähnlichen Ergebnis gelangt auch eine umfangreiche Untersuchung über die deutsche Rüstungsindustrie, in der es zum „Wert“ der Branche heißt: „[D]ie Rüstungspolitik [ist] ein integraler Bestandteil der deutschen Sicherheits- und Verteidigungspolitik sowie eine Kernkompetenz der Einsatzbereitschaft der Bundeswehr. […] Der Zugriff auf eine leistungsfähige und flexible rüstungsindustrielle Basis ist für die Bundesregierung somit eine Grundvoraussetzung ihrer militärischen und damit außen-, sicherheits- und verteidigungspolitischen Handlungsfähigkeit. Für den Handelsstaat Deutschland ist diese Komponente seiner staatlichen Handlungsfähigkeit eine grundlegende Voraussetzung für eine effektive und nachhaltige Interessensverfolgung in einer

multipolaren Weltordnung. […] Nicht seine ökonomische Dimension – sprich der Beitrag zur Wirtschaftsleistung und die Schaffung von Arbeitsplätzen – sondern die […] militärische und außenpolitische Dimension macht den Rüstungssektor zu einem unverzichtbaren Wirtschaftsbereich der deutschen Volkswirtschaft.“[16]

Die deutsche Großmachtpolitik in den Fokus der Kritik nehmen

Rüstungsexporte sind aus Sicht der Bundesregierung machtpolitisch geboten, wie auch die Aussagen des CDU-Rüstungsexperte Henning Otte weiter belegen: „Deutschland als souveräner Staat muss in der Lage sein, seine Soldaten in Kernbereichen mit Waffen aus eigener Produktion auszustatten, um nicht auf zweitklassiges Material vom Weltmarkt angewiesen zu sein. Damit diese Schlüsselindustrien lebensfähig sind, müssen sie auch exportieren können.“[17]

Die Gleichung ist also simpel: Ohne Rüstungsexporte keine deutsche Rüstungsindustrie. Ohne deutsche Rüstungsindustrie keine eigenständige deutsche Militärpolitik. Ohne eigenständige deutsche Militärpolitik keine deutsche Großmachtpolitik! Rüstungsexporte sind also das zwingende Ergebnis deutscher Großmachtambitionen.

Aus diesem Grund ist es zentral, neben der moralischen Verwerflichkeit von Rüstungsexporten auch diese strategisch-machtpolitische Funktion der Waffenausfuhren stärker in den Fokus der Kritik zu rücken!

Anmerkungen

1 Wagner, Jürgen: „Karten klar auf den Tisch“, IMI-Analyse 2016/02b.
2 Dämpfer für Gabriel – Rüstungsexporte auf Rekordniveau, Zeit Online, 19.2.2016.
3 Das Zitat stammt vom CSU-Sicherheitspolitiker und ehemaligen Beschäftigten des Panzerbauers KMW, Florian Hahn. Siehe Wie restriktiv geht Gabriel tatsächlich vor?, Süddeutsche Zeitung, 24.7.2015.
4 Rede von Bundesminister Gabriel zu den Grundsätzen deutscher Rüstungsexportpolitik, DGAP, Berlin, 8.10.2014.
5 Ebd.
6 Ebd.
7 Firmen und Politik beim Trialog, Cellsche Zeitung, 18.9.2014.
8 Rede von Bundesminister Gabriel zu den Grundsätzen deutscher Rüstungsexportpolitik, DGAP, Berlin, 8.10.2014.
9 Strategiepapier der Bundesregierung zur Stärkung der Verteidigungsindustrie in Deutschland, Berlin, 8.7.2015, S. 8f.
10 WifOR, Quantifizierung der volkswirtschaftlichen Bedeutung der Sicherheits- und Verteidigungsindustrie für den deutschen Wirtschaftsstandort, Berlin 2012, S. 44.
11 Henken, Lühr/Strutynski, Peter: Händler des Todes. Rüstungsexporte als Mittel deutscher Außenpolitik: Schädlich und unmoralisch, RLS-Standpunkt Nr. 5/2013; Linnenkamp, Hilmar/Mölling, Christian: Rüstung und Kernfähigkeiten. Alternativen deutscher Rüstungspolitik, SWP-Aktuell 45, Juni 2014, S. 2.
12 Fischer, Martina: Rüstungs- und Industriepolitik in Spanien, in: Karl, Wilfried (Hg.): Rüstungskooperation und Technologiepolitik als Problem der westeuropäischen Integration, Opladen 1994, S. 49-107, S. 64.
13 Resolution der Delegiertenkonferenz der IG Metall Stuttgart vom 20.9.2014.
14 Lösing, Sabine/Wagner, Jürgen: EU-Armee: Machtpolitische Imperative und Stolpersteine, in: AUSDRUCK (August 2015), S. 1-10.
15 Politische Bedeutung der Sicherheits- und Verteidigungsindustrie, BDSV, o.J.
16 Heidenkamp, Henrik: Deutsche Rüstungspolitik. Ein Politikfeld im Handlungsdruck, Opladen 2015, S. 73 und 18.
17 „Wir brauchen Waffen aus eigener Produktion“, Die Welt, 20.5.2015.

Bundeswehr-Großprojekte

Neben dem Bestreben, bis 2030 insgesamt 130 Mrd. Euro für die Neuanschaffung von Kriegsgerät ausgeben zu wollen, stellt die regelmäßige Evaluation der Bundeswehr-Großprojekte eine weitere Kernkomponente der „Agenda Rüstung“ von Verteidigungsministerin Ursula von der Leyen dar (siehe IMI-Analyse 2016/02). Sie wird auch dem Parlament zur Kenntnis gegeben, zuletzt im April 2016 im „3. Bericht des Bundesministeriums der Verteidigung zu Rüstungsangelegenheiten“.

Untersucht wurden dabei 20 Großprojekte mit einem Gesamtvolumen von über 60 Mrd. Euro. Dabei kam heraus, dass die vorgesehene Auslieferung um durchschnittlich 40 Monaten hinterherhinkt und die Projekte zusammen Mehrkosten von 12,7 Mrd. Euro aufweisen (siehe Tabelle). Den absoluten Vogel schießt dabei der Eurofighter ab: Bei einer zeitlichen Verzögerung von 136 Monaten belaufen sich seine Mehrkosten bislang auf satte 6,81 Mrd. Euro! Dahinter reiht sich gleich das Transportflugzeug Airbus A400M ein: 107 Monate Verspätung haben hier 1,47 Mrd. Euro zusätzliche Ausgaben verursacht!

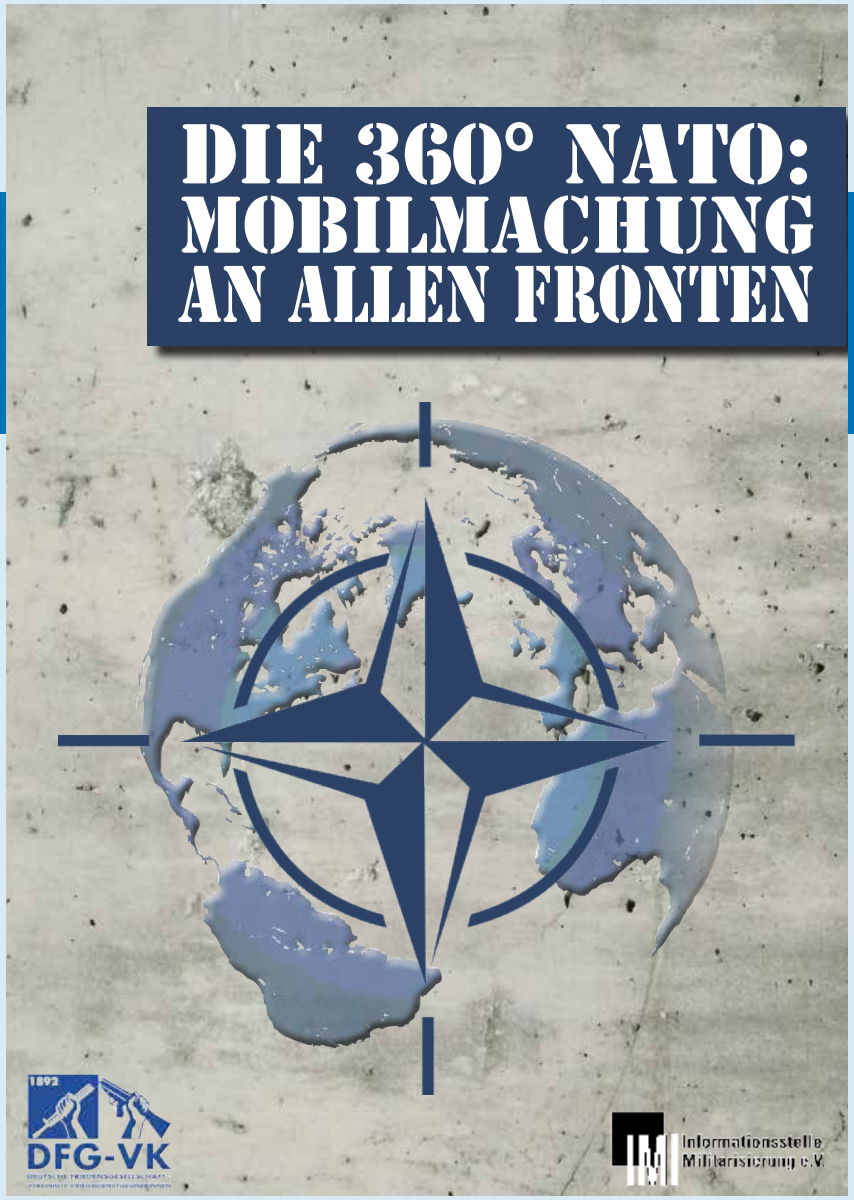
Apropos Airbus A400M: In diese Rechnung dürften die neuerlichen Triebwerksprobleme noch nicht einmal eingepreist worden sein, die Ende April 2016 öffentlich wurden. Sie scheinen so gravierend zu sein, dass innerhalb der Bundeswehr sogar darüber nachgedacht zu werden scheint, das Projekt komplett einzustampfen. So berichtete Spiegel Online am 9. Mai 2016: „Die Triebwerke sorgen nun intern für Alarmstimmung. Nach Informationen von SPIEGEL ONLINE wird in der Führung der Bundeswehr erstmals das Scheitern des gesamten Rüstungsprojekts als Szenario diskutiert. Für den Fall, dass sich die Triebwerksmängel nicht beheben lassen, heißt es, müsse man über einen Abschied aus dem A400M-Programm nachdenken und nach alternativen Transportfliegern suchen.“

Es bleibt abzuwarten, ob das Verteidigungsministerium mit diesen Überlegungen tatsächlich ernst machen wird. Denn ein solcher Schritt wäre sicher ein schwerer Schlag für die Finanzen und das Prestige des „Vorzeigerüstungskonzerns“ Airbus. Andererseits würde es aber der Ankündigung von Verteidigungsministerin Ursula von der Leyen entsprechen, die Rüstungsindustrie künftig etwas stärker darauf verpflichten zu wollen, auch auftragsgemäß zu liefern.

Jürgen Wagner

Quelle der Tabelle: 3. Bericht des BMVg zu Rüstungsangelegenheiten. Zeitüberschreitung in Monaten, Kosten in Mio. €

Typ	Ø	Boxer	Puma	Tiger	NH 90 TTH	NH 90 NTH	CH-53	A400 M	Euro-fighter	AESA-Radar	IRIS-T	Mete-or	Patriot KWA	F 125	K 130	P-3C Orion	SVF uA	SLW ÜA	Tand-em-X
Zeitüberschreitung	40	-7	54	80	152	0	33	107	136	9	9	0	3	30	54	0	45	12	0
Kosten	12691	345	1185	981	218	0	102	1470	6891	85	47	3	22	892	117	115	46	289	-116



In Kürze erscheint die gemeinsam von der IMI und der DfG-VK veröffentlichte Broschüre „Die 360° NATO - Mobilmachung an allen Fronten“. Sie kann in Print (76 S. für vorraussichtlich 4€) bestellt oder wie immer kostenlos von der Homepage heruntergeladen werden.

Informationsstelle
Militarisierung e.V.

Herausgeber des AUSDRUCKs ist die
Informationsstelle Militarisierung (IMI) e.V.
Die Beiträge spiegeln nicht notwendigerweise die Auffassung der Informationsstelle wieder.
Adresse: Hechinger Str. 203, 72072 Tübingen,
www.imi-online.de, e-mail: imi@imi-online.de,
Tel. 07071/49154